Guide de l'utilisateur Genetec ClearID™

Dernière mise à jour du document : 14 mai 2025

Mentions légales

©2025 Genetec Inc. Tous droits réservés.

Genetec Inc. distribue ce document avec un logiciel qui comprend un contrat de licence, qui est fourni sous licence et qui ne peut être utilisé qu'en conformité avec les conditions énumérées dans le contrat de licence. Le contenu de ce document est protégé par la loi sur la propriété intellectuelle.

Le contenu de ce manuel n'est fourni qu'à titre indicatif et peut être modifié sans avis préalable. Genetec Inc. décline toute responsabilité en relation avec d'éventuelles erreurs ou imprécisions pouvant figurer dans le contenu de ce manuel.

Il est interdit de copier, modifier ou reproduire cette publication sous toute forme et à toute fin que ce soit, ou de créer toute œuvre dérivée de celle-ci, sans autorisation écrite préalable de Genetec Inc.

Genetec Inc. se réserve le droit de modifier et d'améliorer ses produits comme bon lui semble. Ce document décrit l'état d'un produit au moment de la dernière révision du document et peut ne pas refléter le produit à tout moment à l'avenir.

Genetec Inc ne pourra en aucun cas être tenu pour responsable envers tout individu ou entité de toute perte ou de tout dommage fortuit ou consécutif résultant de l'utilisation des instructions fournies dans ce document ou dans les produits logiciels ou matériels décrits dans celui-ci.

Genetec[MC], AutoVu[MC], AutoVu MLC[MC], Citywise[MC], Cloud Link Roadrunner[MC], Community Connect[MC], Curb Sense[MC], Federation[MC], Flexreader[MC], Genetec Airport Sense[MC], Genetec Citigraf[MC], Genetec Clearance[MC], Genetec ClearID[MC], Genetec Cloudlink[MC], Genetec Mission Control[MC], Genetec Motoscan[MC], Genetec Patroller[MC], Genetec Retail Sense[MC], Genetec Traffic Sense[MC], KiwiVision[MC], KiwiSecurity[MC], Omnicast[MC], Privacy Protector[MC], Sipelia[MC], Stratocast[MC], Streamvault[MC], Streamvault Edge[MC], Synergis[MC], Valcri[MC], leurs logos respectifs ainsi que le logo Mobius Strip sont des marques commerciales de Genetec Inc. qui peuvent être déposées ou en instance de dépôt dans différents pays.

Les autres marques commerciales citées dans ce document appartiennent à leurs fabricants ou éditeurs respectifs.

Brevet en instance. Genetec[MC] Security Center, Omnicast[MC], AutoVu[MC], Stratocast[MC], Genetec Citigraf[MC], Genetec Clearance[MC] et les autres produits Genetec[MC] font l'objet de dépôts de brevets en attente et peuvent faire l'objet de brevets déposés, aux États-Unis et dans d'autres juridictions dans le monde.

Toutes les spécifications sont sujettes à modification sans avis préalable.

Informations sur le documents

Titre du document : Guide de l'utilisateur Genetec ClearID[MC]

Numéro du document d'origine : EN.709.002

Numéro de document : FR.709.002

Date de mise à jour du document : 14 mai 2025

Vous pouvez envoyer vos commentaires, corrections et suggestions concernant ce guide à l'adresse documentation@genetec.com.

À propos de ce guide

Ce guide est destiné aux utilisateurs de Genetec ClearID[MC]. Il décrit comment configurer et utiliser le système Genetec ClearID[MC].

Notes et avertissements

Les avis et avertissements suivants peuvent être utilisés dans ce guide :

- **Conseil :** Suggère une manière d'appliquer les informations d'un thème ou d'une étape.
- **Note :** Décrit un dossier particulier, ou développe un point important.
- **Important :** Souligne une information critique concernant un thème ou une étape.
- **Attention :** Indique qu'une action ou étape peut entraîner la perte de données, des problèmes de sécurité ou des problèmes de performances.
- **Avertissement :** Indique qu'une action ou une étape peut entraîner des dommages physiques, ou endommager le matériel.

IMPORTANT : Le contenu de ce guide peut faire référence à des informations publiées sur des sites Web de tiers qui étaient correctes au moment de leur publication. Toutefois, ces informations peuvent changer sans notification préalable de la part de Genetec Inc.

Table des matières

Preface

Mentions légales. ii
À propos de ce guide. iii

Chapitre 1 : À propos de ClearID

Présentation de ClearID. 2
À propos de l'architecture de ClearID. 5
Liste des sous-processeurs ClearID. 8
À propos de la sécurité des informations dans ClearID. 9
Qu'est-ce qui distingue ClearID des systèmes de contrôle d'accès traditionnels ?. 11
À propos des processus. 12
Fonctionnement de l'intégration. 13
Présentation de l'intégration. 15
Liste des fonctionnalités ClearID prises en charge. 26
Langues prises en charge. 30
Terminologie ClearID. 31
Vidéos ClearID. 32
À propos des rapports. 33
Se connecter à ClearID. 34
Se déconnecter de ClearID. 35
Activer l'aperçu de fonctionnalités. 36
Désactiver l'aperçu de fonctionnalités. 37
Personnalisation de la marque du portail. 38
Personnalisation des liens du menu d'aide. 40

Chapitre 2 : Nouveautés

Nouveautés de ClearID. 44
Fonctionnalités et améliorations précédentes. 46

Chapitre 3 : Préparation du déploiement

Options de licence. 71
Compatibilité. 74
Configuration système requise. 75
Ports de pare-feu. 76
Appareils pris en charge. 78
Meilleures pratiques. 81
Configurer ClearID pour un nouveau système Synergis. 81
Configurer ClearID avec un système Synergis existant. 82

Chapitre 4 : Module externe ClearID

À propos du module externe ClearID pour Security Center. 86
À propos des relations entre les titulaires de carte et les identités. 87
Télécharger et installer le module externe. 89
Créer le rôle module externe. 90
Connecter Security Center à ClearID. 91

Examiner les informations de titulaires de cartes et d'identifiants. 92
Ajouter un système. 94
Télécharger un fichier d’activation. 97
Configurer les réglages de connexion. 98
Accorder des privilèges utilisateur. 101
À propos des états du système ClearID. 102
À propos des champs personnalisés. 103
Modifier les champs personnalisés. 103
Relations de champs personnalisés. 107

Chapitre 5 : Gérer les identités et les utilisateurs

Créer des identités. 113
Champs d'identité. 115
Accorder des autorisations supplémentaires à des identités et des rôles. 117
Accorder des autorisations supplémentaires à des superviseurs. 121
Afficher les autorisations supplémentaires. 123
Modifier les autorisations supplémentaires. 124
Afficher les identités. 127
Modifier les identités. 130
Supprimer des identités. 132
Synchroniser les photos d'identité ClearID avec Security Center. 134
À propos des points d'ancrage. 135
Créer des points d'ancrage. 138
Modifier les points d'ancrage. 142
Consulter les journaux de points d'ancrage. 143
Accorder l’accès au portail Web. 146
Accorder un accès utilisateur au portail Web. 146
Accorder un accès administrateur au portail Web. 148
Consulter votre profil. 150
Configurer les préférences du thème du portail. 152
Consulter vos accès aux sites et aux secteurs. 154
À propos du processus de demande d'accès. 155
Demander un accès. 156
Ajouter des superviseurs manuellement. 164
Afficher les subordonnés. 166
Gérer les subordonnés. 169
Transférer les subordonnés. 175
À propos du rapport Subordonnés. 182
Réinitialiser les mots de passe utilisateur. 183
À propos des notifications par e-mail. 186
Personnaliser la bannière d’e-mail d'un site. 188
Configurer vos préférences de notification par e-mail. 190
À propos de la délégation. 192
Déléguer des tâches à un autre utilisateur. 195
À propos du rapport d'activité d'utilisateurs. 199
Afficher un rapport d'activité d'utilisateurs. 201
Niveaux utilisateur. 204
À propos du processus de demande d'identité. 210
Créer un modèle d'identité. 211

Modifier un modèle d'identité. 216
Demander des identités. 218
Demander une identité. 219
Demander des identités multiples à l'aide de l'importation CSV. 223
Annuler les demandes d'identité. 232
Approuver les demandes d'identité. 235
Modifier une demande d'identité. 238
À propos du rapport de demandes d'identités. 241
Vérifier l'état des demandes d'identité. 242

Chapitre 6 : Synchronisation d'identifiant

Configurer la duplication d'identifiants. 245
Consulter les journaux de synchronisation des identifiants. 247
Forcer la synchronisation des identifiants. 249

Chapitre 7 : Gérer les sites

À propos des sites. 251
Création de sites. 252
Ajouter des propriétaires de sites. 256
Activer la gestion des visiteurs pour un site. 257
Modifier les sites. 273
Définir la durée maximale d'accès à un site. 275
Configurer les documents de demande d'accès pour les sites. 276
Personnaliser les notifications par e-mail pour un site. 279
Personnaliser l'apparence des notifications par e-mail. 281
À propos des examens d'accès. 283
Configuration de l'expiration automatique pour les examens d'accès. 285
Configurer les examens d'accès à un secteur. 287
Programmer les examens d'accès. 287
Configurer les examens d'accès d'identité. 293
Programmer les examens d'accès d'identité. 293
Modifier les examens d'accès. 297
À propos du rapport d'examen d'accès. 298
Vérifier l'état des examens d'accès. 299
Terminer un examen d'accès à un secteur (propriétaire de site). 302
Terminer un examen d'accès (approbateur de secteur ou responsable de rôle). 311
Terminer un examen d'accès d'identité (superviseur). 320
Générer un résumé d'examen d'accès. 326
À propos du rapport de demandes d'accès. 328
Vérifier l'état des demandes d'accès. 329
À propos du rapport d'activité de site. 332
Afficher un rapport d'activité de site. 333
À propos du rapport Propriétaires de sites et de secteurs. 336
Afficher le rapport Propriétaires de sites et de secteurs. 337

Chapitre 8 : Gérer les secteurs

À propos des secteurs. 342
Créer des secteurs. 343
Ajouter des portes à un secteur. 346
Activer la gestion des visiteurs pour un secteur. 347

À propos des secteurs imbriqués. 349
Accorder automatiquement l'accès aux secteurs. 350
Ajouter des responsables de secteurs. 353
Ajouter des horaires à un secteur. 354
Configurer les documents de demande d'accès pour les secteurs. 356
Accorder l'accès à un secteur. 359
Examiner les accès à un secteur. 364
Approuver les demandes d’accès à un secteur. 366
Refuser les demandes d’accès à un secteur. 368

Chapitre 9 : Gestion des visiteurs

À propos du processus de demande de visite. 371
À propos du processus de liste de surveillance de demande de visite. 372
Inviter des visiteurs. 373
Inviter des visiteurs manuellement. 374
Inviter des visiteurs à l’aide de l’importation CSV. 379
Alertes SMS. 385
Examiner les événements de visite. 388
Copier un événement de visite. 390
Modifier les événements de visite. 391
Approuver les demandes de visite. 393
À propos des rapports de visiteurs. 395
Afficher un rapport de visiteurs. 396
Identifiants code QR pour les visiteurs. 398
Importer un format de carte personnalisé (identifiant code QR) dans Synergis. 398
Activer les identifiants code QR pour les visiteurs. 401
Configurer les appareils Qscan pour ClearID. 404
Configurer les appareils STid pour ClearID. 409
Automatiser l’accès et l’inscription des visiteurs à l'aide d'une macro. 433

Chapitre 10 : Gérez les listes de surveillance de visiteurs

À propos des listes de surveillance. 437
Ajouter des responsables de listes de surveillance. 439
Ajouter des listes de surveillance. 441
Ajouter une entrée à une liste de surveillance de personnes. 445
Ajouter une entrée à une liste de surveillance de sociétés. 448
Importer des entrées de liste de surveillance depuis un fichier. 449
Exporter les entrées de liste de surveillance dans un fichier. 451
Tester les entrées de liste de surveillance. 452
Supprimer les entrées de liste de surveillance. 454
Modifier les listes de surveillance. 456
Supprimer une liste de surveillance. 458
Contrôler les visiteurs manuellement. 460
Débloquer les visiteurs bloqués par une liste de surveillance. 464

Chapitre 11 : Contrôle d'accès basé sur les rôles

À propos du contrôle d'accès basé sur les rôles. 469
Ajouter des rôles. 472
Configurer les responsables de rôles. 474
Configurer les stratégies de contrôle d'accès basé sur les rôles. 476

Scénario 1 : Ajouter des employés à un rôle d'informaticien. 479
Scénario 2 : Ajouter des sous-traitants à un rôle d'ingénieur certifié. 479
Scénario 3 : Ajouter des employés à un rôle de personnel ADA. 480
Ajouter des attributs de provisionnement personnalisés à une identité. 482
Ajouter des membres aux rôles. 484
À propos du rapport d'activité de rôle. 486
Afficher un rapport d'activité de rôle. 487

Chapitre 12 : Connexion à d’autres systèmes

Authentifier votre connexion. 492
Configurer la synchronisation des données. 494
Synchroniser les identités à l'aide d'une API. 496
À propos de l’API ClearID. 496
Synchroniser les identités à l'aide de l’intégration SCIM. 498
À propos de la norme SCIM. 498
À propos des champs d'attributs Microsoft Entra ID. 498
Configurer l’intégration SCIM. 500
Réinitialiser les données d’identité d’une intégration SCIM. 515
Examiner l’état de la synchronisation de l’intégration SCIM. 516
Synchroniser les identités avec One Identity. 518
À propos de One Identity Synchronization Tool. 519
À propos des champs d'attributs One Identity Synchronization Tool. 522
À propos de l’application Web Azure. 524
Installer One Identity Synchronization Tool. 527
Configurer One Identity Synchronization Tool. 535
Consulter l'état de la synchronisation. 564
À propos des journaux One Identity Synchronization Tool. 566
Consulter les journaux One Identity Synchronization Tool. 566
Mettre à jour des identités existantes à partir de sources de données externes. 567
Synchroniser les identités par LDAP. 569
À propos de ClearID LDAP Synchronization Agent. 569
Correspondances d'attributs LDAP et d’attributs ClearID. 570
Configurer ClearID LDAP Synchronization Agent. 571

Chapitre 13 : Appareils de gestion des visiteurs

À propos de ClearID Self-Service Kiosk. 578
Inscription sur une borne en libre-service. 579
Auto inscription sur une borne en libre-service. 581
Configurer l’iPad de la borne en libre-service. 582
Personnaliser la configuration de la borne en libre-service. 585
Personnaliser le logo des badges de visiteurs de la borne en libre-service. 587
Ajouter des documents PDF à valider dans le kiosque en libre-service. 588
Activer la réimpression des badges. 591
Désactiver la photo du visiteur pendant l’inscription. 592
Enregistrement par opérateur mobile. 594
Configurer l'enregistrement par opérateur mobile. 597
Configurer l'imprimante d'étiquettes de la borne en libre-service (Brother QL-820NWBc, QL-820NWB ou QL-810W). 602
Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Bluetooth (Brother 820NWBc ou QL-820NWB). 603

Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Wi-Fi (Brother 820NWBc, QL-820NWB ou QL-810W). 606
Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Ethernet (Brother 820NWBc ou QL-820NWB). 609
Configurer l'imprimante d'étiquettes de la borne en libre-service (Brother TD-4550DNWB). . . 612
Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Bluetooth (Brother TD-4550DNWB). 613
Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Wi-Fi (Brother TD-4550DNWB). 616
Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Ethernet (Brother TD-4550DNWB). 619
Sélectionner une imprimante d'étiquettes de borne en libre-service. 622
Imprimer un badge de test sur la borne en libre-service. 629
Réinitialiser l’application mobile Self-Service Kiosk. 633
Options de la borne en libre-service. 635
Support de borne au sol. 637
Étagère pour imprimante pour le support de borne au sol. 641
Support de table pour borne. 643
Types de pièces d’identité. 646

Chapitre 14 : Dépannage

Module externe installé mais manquant dans Security Desk et Config Tool. 676
Le rôle module externe ne trouve pas de fichier avec certificat. 677
Les champs personnalisés ne sont pas affichés dans Security Desk. 678
Aucun compte actif trouvé pour l’utilisateur. 681
Notification de visite par e-mail non reçue par les visiteurs. 682
Les champs Hôtes de visiteurs sont vides dans Security Desk.. 683
Problèmes de connectivité (One Identity Synchronization Tool). 685
Problèmes de synchronisation des données (One Identity Synchronization Tool). 686
Problèmes de la borne en libre-service. 688
Problèmes d'impression d'étiquettes de la borne en libre-service. 691

Chapitre 15 : Ressources complémentaires

Assistance technique. 698
Glossaire 699

1

À propos de ClearID

Présentation de la solution de gestion des accès physiques en libre-service ClearID.

Cette section aborde les sujets suivants:

- "Présentation de ClearID", page 2
- "À propos de l’architecture de ClearID", page 5
- "À propos de la sécurité des informations dans ClearID", page 9
- "Qu’est-ce qui distingue ClearID des systèmes de contrôle d'accès traditionnels ?", page 11
- " À propos des processus ", page 12
- " Fonctionnement de l’intégration ", page 13
- " Présentation de l'intégration ", page 15
- "Liste des fonctionnalités ClearID prises en charge", page 26
- " Langues prises en charge ", page 30
- "Terminologie ClearID", page 31
- "Vidéos ClearID", page 32
- " À propos des rapports ", page 33
- "Se connecter à ClearID", page 34
- "Se déconnecter de ClearID", page 35
- " Activer l’aperçu de fonctionnalités ", page 36
- " Désactiver l’aperçu de fonctionnalités ", page 37
- " Personnalisation de la marque du portail ", page 38
- " Personnalisation des liens du menu d'aide ", page 40

Présentation de ClearID

Genetec ClearID[MC] est un moyen plus intelligent de gérer les accès physiques à l'aide d'une solution en libre-service pour Synergis[MC]. ClearID vous permet contrôler les accès et la conformité en exploitant une approche à base de règles via une interface web.

- Vous pouvez accéder au système depuis n'importe quel navigateur standard. Toutes les données et les fichiers qui sont importés dans le système sont automatiquement chiffrés.
- Le système ClearID est également intégré avec Active Directory. Cette intégration permet à l'entreprise d'utiliser son service Active Directory existant pour authentifier les utilisateurs et gérer l'accès au système.

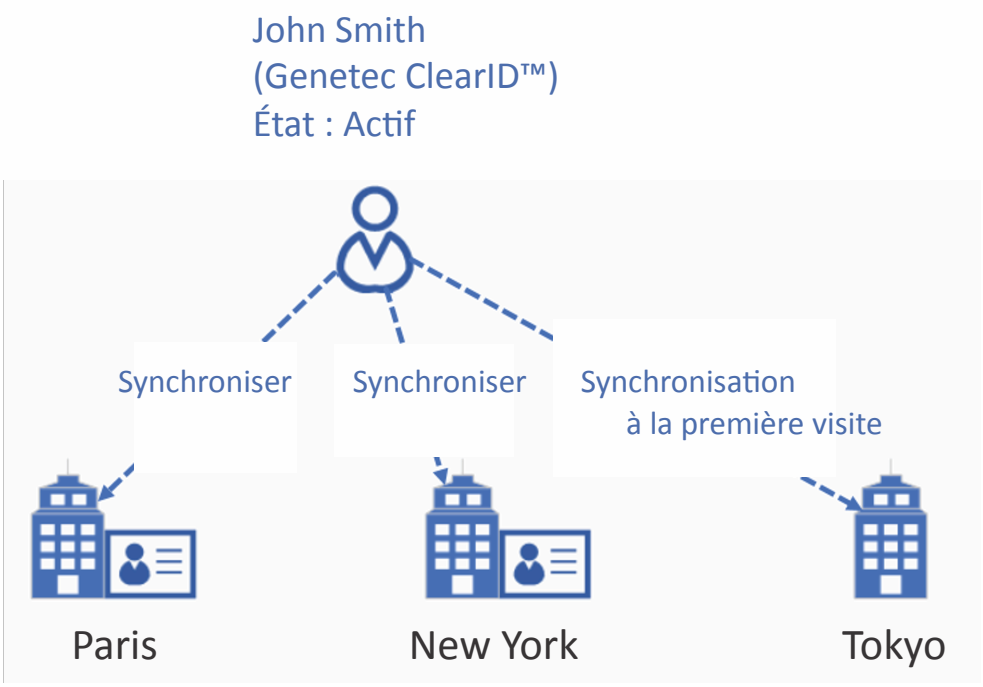
Pour une description complète du produit, consultez la page produit ClearID.

Avantages du système ClearID

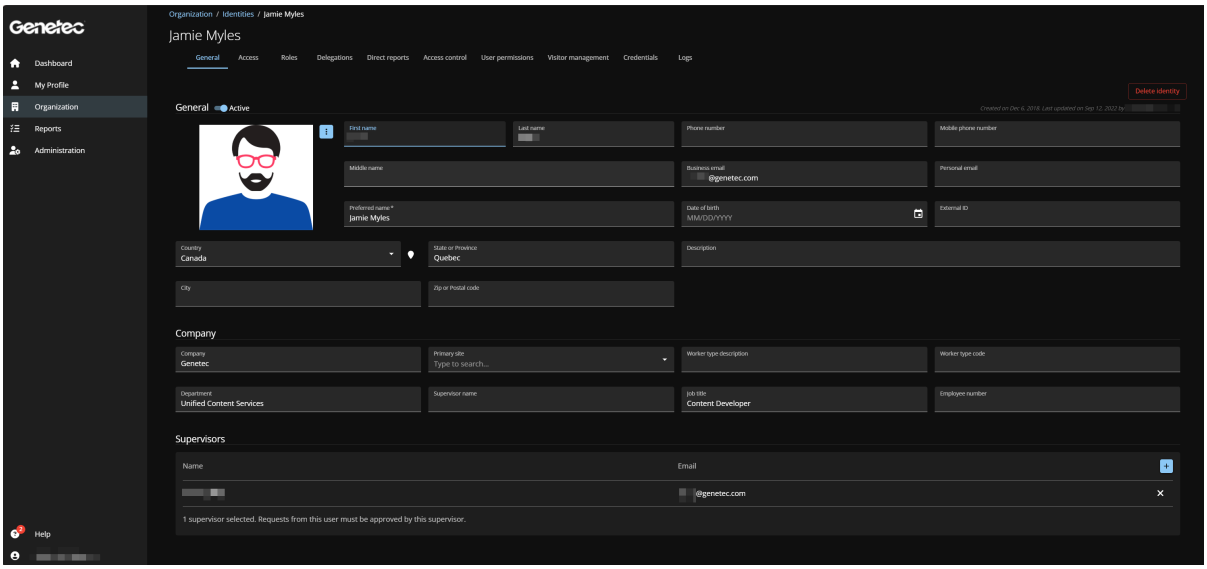
- Améliorez la circulation des personnes en utilisant la solution en libre-service pour gérer les accès physiques.
- Réduction des risques de failles de sécurité via une gestion des droits d'accès simplifiée.
- Standardisation et automatisation des politiques de sécurité pour l'intégration, la désactivation, les demandes d'accès et l'attribution d'identifiants pour plusieurs sites indépendants.
- Exploitation et amélioration de votre système de sécurité physique existant.
- Approche standard avec déploiement accéléré et nombre restreint d'intégrations pour réduire les besoins de maintenance.
- Besoins de maintenance d'infrastructure réduits via une approche distributée basée sur le nuage.
- Amélioration de l'efficacité et de la conformité aux réglementations internes et externes, telles que le RGPD et le contrôle des exportations.

Synchronisation

ClearID utilise une identité unique pour synchroniser les informations d'accès pour plusieurs sites indépendants gérés par différentes instances de Synergis.



Pour minimiser la duplication des informations personnelles dans chaque système de contrôle d'accès local, ClearID ne crée le titulaire de cartes automatiquement que lors de la première demande de visite d'un site.



Une fois l'accès accordé à un nouveau site, le système synchronise automatiquement toutes les informations d'identification permanentes liées à l'identité. Si l'entreprise utilise le même système de carte sur différents sites, le badge fonctionne sans intervention manuelle sur le nouveau site.

Lorsqu'une identité est désactivée dans ClearID, le titulaire de cartes est désactivé. L'identité est automatiquement synchronisée avec tous les titulaires de carte liés à tous les secteurs de tous les sites. Les identifiants restent actifs dans Security Center, mais l'accès est automatiquement refusé, car le titulaire de cartes est inactif.

Rubriques connexes

Vidéos ClearID, page 32
Brochure technique ClearID (8 pages)
ClearID - Page produit
ClearID - Page catalogue
Portail de conformité Genetec

À propos de l'architecture de ClearID

Genetec ClearID[MC] offre des options de localisation pour les centres de données aux États-Unis uniquement, en Europe uniquement, au Canada uniquement ou en Australie uniquement. Chaque option permet une synchronisation entre les sites locaux. Les modules de l'application Web effectuent des tâches ou échangent des données entre les sources de référence, ClearID et les terminaux.

IMPORTANT : Le transfert ou la copie d'un compte client d'une instance à une autre n'est pas pris en charge.

Architecture distribuée aux États-Unis

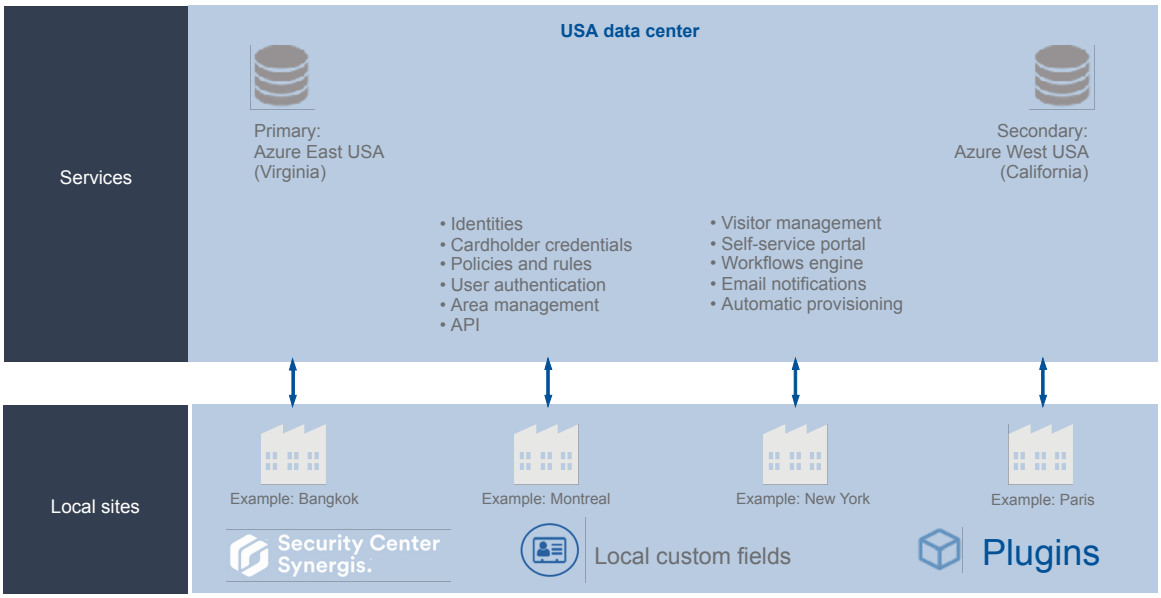
Le schéma suivant illustre la solution distribuée aux États-Unis. Le schéma indique quelles données sont stockées, l'emplacement de stockage et leur mode de cidculation entre les sites locaux et les services régionaux.

REMARQUE : Les données des services régionaux sont stockées dans le cloud.

ClearID exploite les éléments suivants :

- Plusieurs centres de données Azure pour minimiser le risque d'interruption de service.
- Données des employés chiffrées pour minimiser le risque de vol de données.
- Données géolocalisées pour minimiser les infrastructures et optimiser les performances de flux de données.

Genetec ClearID™ USA only architecture



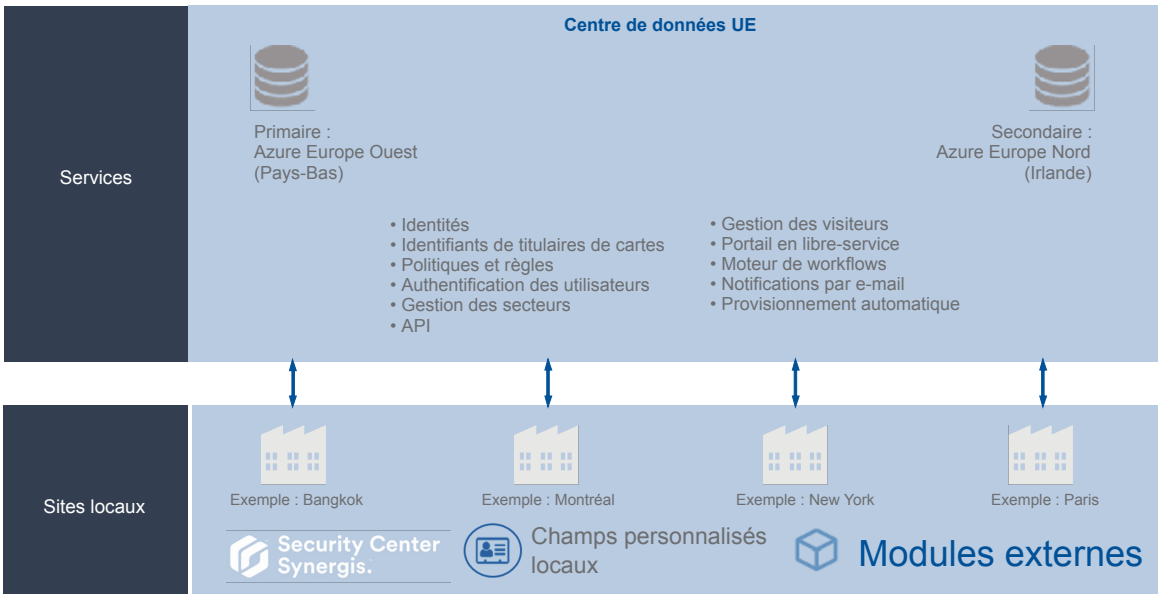
REMARQUE : [1]Pour en savoir plus sur les centres de données utilisés dans les déploiements régionaux, voir la rubrique *Microsoft Corporation* dans la section ClearID de la liste des sous-traitants Genetec.

Pour les visiteurs, les informations d'invité pertinentes sont stockées avec les informations liées à l'événement de visite. Ces informations sont ensuite transférées vers l'instance de Security Center qui gère le site visité.

Architecture Europe uniquement

Le diagramme suivant représente la solution Europe-uniquement, dans laquelle les données sont stockées dans des centres de données européens. Par exemple, lorsque les clients ou les politiques de l'entreprise exigent que les données soient stockées dans des centres de données européens.

Genetec ClearID™ Architecture Europe uniquement

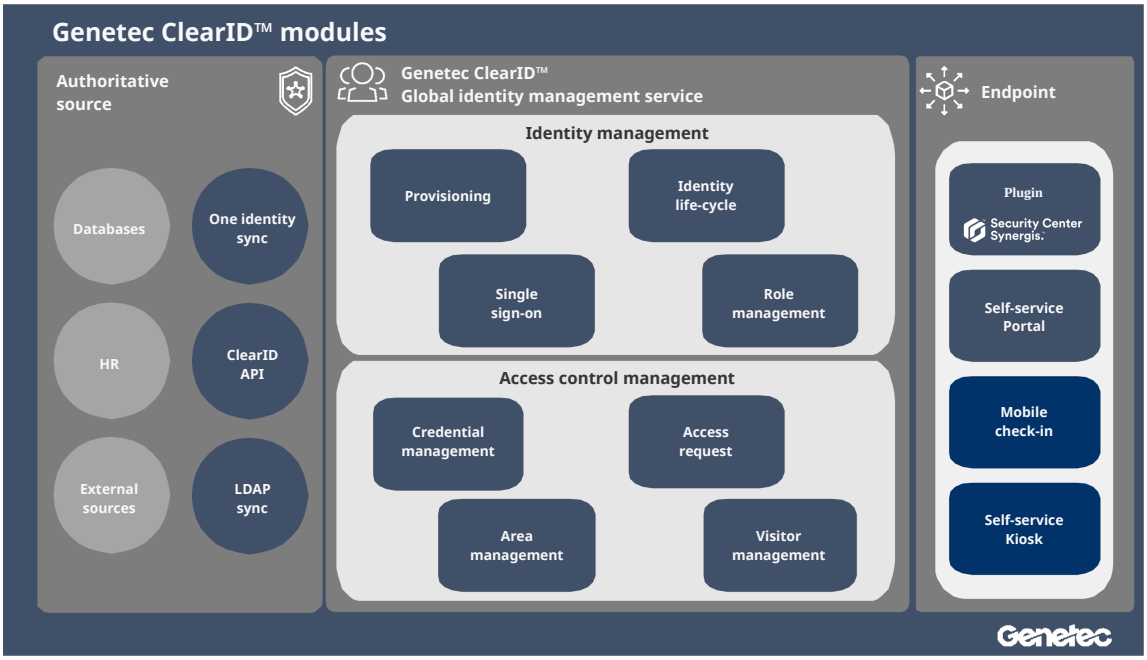


REMARQUE : Vous pouvez également choisir des solutions de stockage de données uniquement pour le Canada ou l'Australie.

- **Centres de données Canadiennes :**
  - Centre de données primaire : Azure Central Canada (Ontario)
  - Centre de données secondaire: Azure East Canada (Quebec)
- **Centres de données Australiennes :**
  - Centre de données primaire: Azure East Australia (New South Wales)
  - Centre de données secondaire: Azure Central Australia (Canberra)

Modules ClearID

Le schéma suivant illustre les modules de l'application Web ClearID accessibles par les clients :



- **Source faisant autorité :** Affiche les options de provisionnement d'identité disponibles pour les clients. Vous pouvez créer des identités dans ClearID à partir d'une des sources de données (bases de données, RH, sources externes) à l'aide d'un des outils (Genetec ClearID^{MC} One Identity Synchronization Tool, Genetec ClearID^{MC} API ou Genetec ClearID^{MC} LDAP Synchronization Agent).
- **Service mondial de gestion des identités :** Fournit une présentation générale des fonctionnalités et services de la plate-forme ClearID.
- **Extrémité :** Affiche les modules avec lesquels les clients interagissent directement. Ces modules permettent aux clients de saisir leurs données ou de configurer leurs systèmes.

Architecture dans le nuage

ClearID est déployé sur la plate-forme dans le cloud Microsoft Azure afin de tirer parti de sa sécurité réputée. Microsoft Azure a été audité par rapport aux normes SOC 1, SOC 2 et SOC 3. Les audits sont menés conformément aux normes ISO SSAE 16 et ISAE 3402. Les certifications sont régulièrement mises à jour et peuvent être fournies sur demande. Azure est également conforme à la norme ISO 27001.

L'architecture du service est conçue pour une haute disponibilité et une grande évolutivité. Les données stockées dans ClearID sont redondantes afin d'assurer la protection des données critiques et de réduire l'impact des pannes matérielles. Cette architecture, associée à la robustesse du cloud Microsoft Azure, signifie que nous pouvons nous engager contractuellement à assurer un taux de disponibilité de 99,9 %.

Contrôles de sécurité

Azure applique un ensemble rigoureux de contrôles de sécurité qui régissent les opérations et l'assistance. Microsoft déploie une combinaison de contrôles préventifs, défensifs et réactifs, dont les mécanismes suivants pour la protection contre les activités non autorisées des développeurs et/ou des administrateurs :

- Contrôles d'accès stricts aux données sensibles, dont l'authentification à deux facteurs par carte à puce pour effectuer des opérations sensibles.
- Combinaisons de contrôles qui améliorent la détection indépendante des activités malveillantes.
- Plusieurs niveaux de surveillance, de journalisation et de rapports.
- Des rapports de sécurité peuvent être utilisés pour surveiller les accès et pour identifier et désamorcer les menaces potentielles.

- Les opérations administratives de Microsoft, dont les accès au système, sont consignées à des fins d'audit en cas de modification non autorisée ou accidentelle.

Haute disponibilité

Les installations d'Azure sont conçues pour fonctionner 24h/24, 7j/7 et 365 j/an et exploiter diverses mesures afin de protéger les installations des pannes de courant, intrusions physiques et coupures réseau. Ces centres de données sont conformes aux normes sectorielles en matière de sécurité physique et de disponibilité. Le personnel d'exploitation de Microsoft gère, surveille et administre ces installations Azure.

Rubriques connexes

Politique de confidentialité

Fiche de confidentialité du produit - ClearID

Portail de conformité Genetec

Liste des sous-processeurs ClearID

Genetec ClearID[MC] utilise des fournisseurs tiers pour aider Genetec[MC] à fournir les services ClearID dans le cloud et qui peuvent, dans le cadre de leurs responsabilités, recueillir, consulter, stocker ou traiter des données de clients (y compris des données personnelles).

Pour les informations les plus récentes concernant les fournisseurs sous-traitants tiers, voir Liste des sous-traitants.

Rubriques connexes

À propos de la sécurité des informations dans ClearID, page 9

À propos de la sécurité des informations dans ClearID

L'ensemble des données et des fichiers importés dans Genetec ClearID[MC] sont chiffrés, et toutes les communications avec la plate-forme sont sécurisées. Ces mesures de chiffrement et de sécurité garantissent que les données sensibles, les fichiers et les communications ne sont visibles que par les utilisateurs qui disposant des accès adéquats.

Normes de chiffrement

- **Chiffrement des données :** Toutes les données personnelles gérées par ClearID sont chiffrées par AES-256 (Advanced Encryption Standard sur 256 bits) avec des clés symétriques générées automatiquement. Ce chiffrement automatique garantit que chaque blob de données, comme une identité, reçoit une clé AES unique.

  Pour une protection supplémentaire, la clé AES est également chiffrée avec une clé privée associée exclusivement à la clé privée du compte. Toutes les clés de chiffrement utilisées par ClearID sont gérées de manière sécurisée dans Azure Key Vault, qui prend en charge les HSM validés par la norme FIPS 140-2 de niveau 2.
- **Intégrité des données :** Une signature numérique (SHA-512 ave RSA) est générée pour détecter toute tentative de modification des données et garantir l'intégrité des informations et des actions au sein du système. L'analyse et l'identification unique de toutes les données à l'aide d'un algorithme complexe empêchent les attaquants de supprimer, modifier ou ajouter du contenu aux données stockées dans ClearID.
- **Chiffrement des communications :** Les communications au sein de la plate-forme sont sécurisées par le protocole HTTPS (Hypertext Transfer Protocol Secure) et par des certificats TLS (Transport Layer Security) pour garantir que seuls les tiers de confiance puissent accéder aux données gérées par ClearID. Ce chiffrement des communications garantit la confidentialité des informations et limite les risques d'attaques malveillantes visant à intercepter ou modifier les communications en transit.

Sécurité des réseaux et informations

En tant que fournisseur de solutions de sécurité de confiance pour des agences gouvernementales et des organisations publiques et privées de premier plan dans le monde, nous prenons très au sérieux le respect des lois locales. Cette conformité prend en compte les lois relatives à la sécurité des données et à la protection de la confidentialité des pays dans lesquels nous commercialisons nos produits et services.

Pour garantir le stockage et l'utilisation de manière appropriée et sécurisée de toutes les données des clients, ClearID est un système de gestion de la sécurité de l'information certifié ISO/IEC 27001:2013.

- **Développement et opérations sécurisés :** Nos équipes de développement et d'exploitation sont certifiées ISO 27001:2013. Notre équipe dédiée à la sécurité gère et examine les exigences d'architecture et de conception, en veillant au respect des normes et réglementations les plus strictes du secteur, y compris le Règlement général sur la protection des données (RGPD). Chaque modification apportée à ClearID est soumise à une série de tests automatisés très stricts et à des tests de pénétration répétés par des spécialistes du secteur de la sécurité informatique.
- **Architecture à confiance zéro :** Les données clients sont segmentées à travers une série de microservices. Chaque microservice a un rôle spécifique dans le système et le service a uniquement accès aux données minimales requises pour effectuer cette tâche. Il n'existe aucun référentiel central des données susceptible d'être attaqué. Les informations sont réparties entre des référentiels en silos indépendants. Le réseau du centre de données est considéré comme dangereux dans notre architecture de confiance zéro. Toutes les données transmises et reçues entre les microservices sont cryptées et signées numériquement.
- **Surveillance des services :** Nous sommes abonnés à divers fils et services de suivi des menaces, dont Check Point, Microsoft, Mandiant et Hyphen. En fonction de la nature des menaces en évolution, nous adaptons nos contrôles aussi souvent que nécessaire.

Les environnements de production sont constamment surveillés à l'aide des services de surveillance suivants :

- Exécution d'une série de transactions synthétiques toutes les 5 minutes pour émuler des utilisateurs dans le monde entier.
- Suivi en permanence de toute une série d'indicateurs sur les serveurs pour détecter toute anomalie, comme un nombre inhabituel d’échecs de requêtes web.
- Déclenchement automatique d'une alarme auprès de notre équipe de développement et d'exploitation, qui prend alors des mesures immédiates pour corriger le problème et limiter tout impact sur l'environnement de production.

L'objectif est de détecter les erreurs transitoires, les problèmes de centre de données, la dégradation des performances et les pannes des FAI avant que les utilisateurs ne s'aperçoivent du problème sur leur système.

Authentification des utilisateurs

Par défaut, ClearID utilise Azure Active Directory B2C et Azure AD B2B pour l’authentification des utilisateurs. Les entreprises peuvent également fédérer leurs identités utilisateur Active Directory (AD) existantes via Microsoft Azure Active Directory ou tout système prenant en charge la norme OpenID Connect pour fournir une fonction d'authentification unique (SSO) et s'assurer que le système est conforme aux exigences des politiques d'entreprise pour l'authentification des utilisateurs.

Le système d'authentification est basé sur le modèle d'authentification passive avec OAuth 2.0 et OpenID Connect, ce qui permet d'intégrer le serveur d'identité (AD ou autre) directement sur la page de connexion. Les administrateurs d'identité peuvent définir la façon dont les utilisateurs seront authentifiés. Il peut s’agir de mots de passe, jetons, biométrie, ou une combinaison de plusieurs de ces techniques.

L'utilisation d'Active Directory permet aux entreprises d'appliquer une grande variété de règles de validation des utilisateurs et des mots de passe, ainsi que des exigences d'expiration. Parmi ces exigences figurent notamment l'authentification multifacteur, la désactivation des identifiants utilisateur après plusieurs tentatives de connexion infructueuses et bien d'autres options de configuration.

Rubriques connexes

Politique de confidentialité

Fiche de confidentialité du produit - ClearID

Portail de conformité Genetec

Qu’est-ce qui distingue ClearID des systèmes de contrôle d'accès traditionnels ?

Utilisez les informations suivantes pour comprendre les différences entre Genetec ClearID[MC] et les systèmes de contrôle d'accès traditionnels.

Dans les systèmes de contrôle d'accès traditionnels, le personnel de sécurité est constamment impliqué dans les opérations de validation ou de refus d'accès aux emplacements physiques :

- Le personnel de sécurité doit contacter les propriétaires de salle avant d'accorder l'accès à un individu.
- Lorsque l'accès n'est plus requis, la personne ne recontacte jamais l'équipe de sécurité pour demander à être retirée de la salle.
- La plupart des sites ne suivent ou ne consignent pas les motifs d'accès.

Dans ClearID, le portail Web en libre-service diminue l’effort et augmente la souplesse en utilisant des *processus*, lorsque les employés, les responsables ou les propriétaires de différentes installations sécurisées demandent et accordent l’accès.

Les demandes sont traitées de la manière suivante :

1. Des demandes et des processus d'approbation distincts sont créés pour chaque demande.

   Chaque demande intègre l’identité du demandeur, l'heure de la demande et le motif de la demande, parmi d'autres informations d’historique.
2. Chaque demande génère des notifications par e-mail pour le demandeur et les approbateurs.
3. Une fois le récapitulatif de la demande confirmé, il est automatiquement affecté aux personnes pertinentes pour approbation.
4. Le responsable des employés, les propriétaires de secteurs et d'autres approbateurs reçoivent un e-mail leur demandant d'approuver, refuser ou modifier le demande envoyée.
5. Une fois le processus d'approbation terminé, le demandeur reçoit un e-mail lui indiquant si sa demande a été approuvée ou rejetée.

REMARQUE : Les demandes d'accès, d'identité ou de visite peuvent être restreintes à une période donnée, contrairement à la méthode traditionnelle.

Le portail en libre-service permet aux employés de demander l'accès à des secteurs spécifiques du même bâtiment ou d'un site différent. Même si le site est géré par une autre instance de Security Center.

Si une personne se rend pour la première fois dans des bureaux gérés par une instance différente de Synergis[MC], le système crée automatiquement un titulaire de cartes et synchronise tous les identifiants quelques heures en amont de l’arrivée de la personne sur le site. Le dernier jour du séjour, comme spécifié dans la demande d'accès, le système révoque automatiquement l'accès au secteur sécurisé.

Rubriques connexes

À propos des processus, page 12

À propos des processus

Genetec ClearID[MC] exploite des processus pour traiter, puis pour approuver ou refuser des demandes d'accès, de visite ou d'identité.

REMARQUE : Selon la façon dont vous configurez vos sites et vos secteurs, certains processus peuvent ne pas s'appliquer à votre environnement.

Les *processus* suivants sont fournis pour traiter les différents types de demandes :

Processus de demande d'accès

Un processus de demande d'accès est une série d'activités effectuées par le système ou par des personnes habilitées au cours du cycle de vie d'une demande d'accès. Les activités peuvent modifier l'état et les propriétés des demandes d'accès, affecter d'autres entités du système, ou attendre qu'une condition soit réunie.

Processus de demande de visite

Un processus de demande de visite est une série d'activités effectuées par le système ou par des personnes habilitées au cours du cycle de vie d'une demande de visite. Les activités peuvent modifier l'état et les propriétés des demandes de visite, affecter d'autres entités du système, ou attendre que certaines conditions soient réunies.

Processus de liste de surveillance de demande de visite

Un processus de liste de surveillance est une série d'activités effectuées par le système ou par des personnes habilitées au cours du cycle de vie d'une demande de visite si les listes de surveillance sont activées. Les activités peuvent modifier l'état et les propriétés des listes de surveillance, affecter d'autres entités du système, ou attendre que certaines conditions soient réunies.

Processus de demande d'identité

Un processus de demande d'identité est une série d'activités effectuées par le système ou par des personnes habilitées au cours du cycle de vie d'une demande d'identité. Ces activités peuvent créer une identité individuelle ou plusieurs identités en important un fichier CSV, et ajouter chaque nouvelle identité à un rôle afin d'hériter des accès pertinents sur une période donnée.

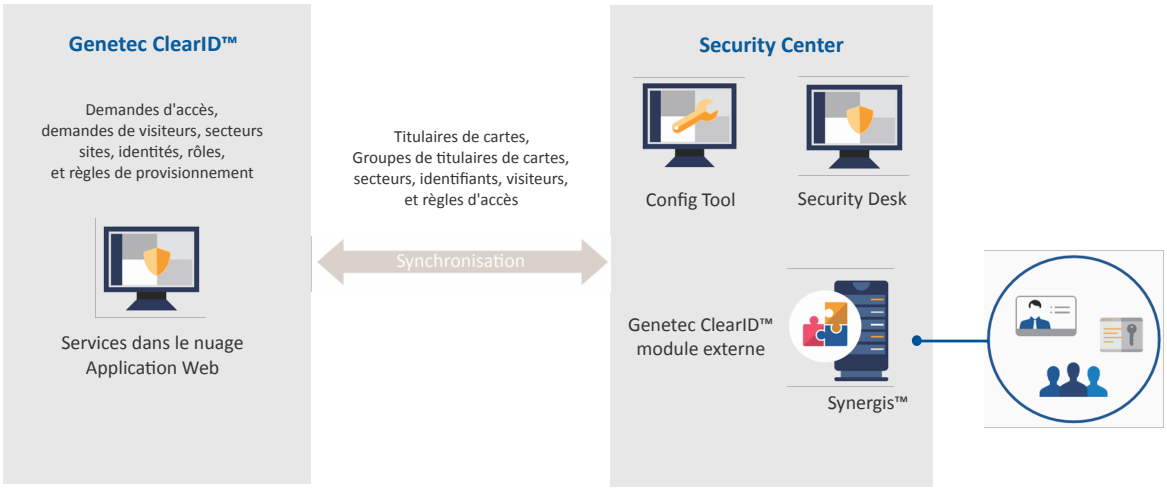
Rubriques connexes

À propos du processus de demande d'accès, page 155
À propos du processus de demande de visite, page 371
À propos du processus de liste de surveillance de demande de visite, page 372
À propos du processus de demande d'identité, page 210

Fonctionnement de l’intégration

Le module externe Genetec ClearID[MC] est nécessaire pour synchroniser les données entre l'application web Genetec ClearID[MC] et Security Center.

Composants de l’intégration du module externe ClearID



- **ClearID :** Genetec ClearID[MC] est un moyen plus intelligent de gérer les accès physiques à l’aide d'une solution en libre-service pour Synergis[MC].
- **Module externe ClearID :** Le module externe ClearID est installé sur un serveur Security Center et est exécuté en tant que rôle module externe. Le module externe Genetec ClearID[MC] intègre Genetec ClearID[MC] avec Security Center, et connecte Synergis[MC] et les services ClearID dans le cloud. Toutes les actions effectuées dans Genetec ClearID sont synchronisées automatiquement avec Synergis.
- **Security Center :** Security Center est une plate-forme réellement unifiée qui marie vidéosurveillance, contrôle d’accès, reconnaissance automatique de plaques d'immatriculation, détection d'intrusion et communications au sein d'une même solution intuitive et modulaire. En tirant parti d'une approche unifiée de la sécurité, votre organisation devient plus efficace, prend de meilleures décisions et réagit aux situations et aux menaces avec une plus grande confiance.

  Le module externe ClearID est installé sur un serveur Security Center. Le module externe peut être installé sur le Répertoire ou un serveur d'extension.
- **Config Tool :** Le module externe ClearID est également installé sur un poste de travail Config Tool. L'administrateur Security Center utilise Config Tool pour créer et configurer le rôle module externe, les réglages de base de données et les réglages de connexion à ClearID. Vous pouvez également configurer une connexion proxy si nécessaire. Par exemple, lorsque les serveurs n'ont pas accès à Internet.
- **Security Desk :** Les opérateurs Security Desk peuvent créer des identifiants, inscrire des visiteurs ou affecter et imprimer des badges.
- **Synergis :** Security Center Synergis[MC] est le système de contrôle d'accès (SCA) sur IP qui renforce la sécurité physique de votre organisation ainsi que votre capacité à réagir aux menaces. Synergis[MC] prend en charge un éventail croissant de matériel de contrôle de portes et de verrous électroniques. Avec Synergis[MC], vous pouvez exploiter vos équipements de réseau et de sécurité existants.

Les informations suivantes sont extraites de Synergis et exploitées par ClearID :

- Règles d'accès
- Secteurs
- Titulaires de cartes
- Groupes de titulaires de cartes
- Identifiants
- Horaires
- Visiteurs

REMARQUE : Dans Config Tool et Security Desk, les icônes des entités gérées par ClearID ont un point bleu dans l'angle inférieur droit :

- Règles d'accès ( )
- Secteurs ( )
- Titulaires de cartes ( )
- Groupes de titulaires de cartes ( )
- Identifiants ( )
- Partitions ClearID ( )
- Visiteurs ( )

Rubriques connexes

Télécharger et installer le module externe, page 89

Présentation de l'intégration

Vous pouvez intégrer l'application Web Genetec ClearID[MC] avec Security Center en installant et configurant le module externe ClearID et en suivant une série d'étapes.

Le tableau suivant répertorie les tâches requises pour l'intégration dans Security Center, et décrit comment vérifier que l'intégration a réussi.

Étape	Tâche	Informations complémentaires
	Comprendre les prérequis et les problèmes clés avant le déploiement	
1	Découvrez ce que vous pouvez faire avec ClearID.	• Présentation de ClearID, page 2. • Qu'est-ce qui distingue ClearID des systèmes de contrôle d'accès traditionnels ?, page 11. • À propos des processus , page 12. • Liste des fonctionnalités ClearID prises en charge, page 26. • Langues prises en charge , page 30.
2	Avant l'installation du module externe, veuillez lire les notes de version pour découvrir les nouvelles fonctionnalités.	• Nouveautés de ClearID, page 44.
3	Familiarisez-vous avec les termes courants et leurs équivalents dans Security Center.	• Terminologie ClearID, page 31.
4	Prenez connaissance des différents composants et de leur mode d'interaction.	• Fonctionnement de l'intégration , page 13. • À propos de l'architecture de ClearID, page 5. • Liste des sous-processeurs ClearID, page 8. • À propos de la sécurité des informations dans ClearID, page 9.
5	En savoir plus sur les fonctionnalités clés et comprendre le produit.	• Vidéos ClearID, page 32.
	Préparation du déploiement	
1	Vérifiez que le module externe est installé sur un serveur répondant à la configuration système recommandée et exécutant une version compatible de Security Center.	• Compatibilité , page 74. • Configuration système requise , page 75. • Ports de pare-feu , page 76.
2	En savoir plus sur les appareils pris en charge pour l'utilisation de ClearID.	• Appareils pris en charge , page 78.

3	Familiarisez-vous avec les meilleures pratiques de déploiement.	• Meilleures pratiques , page 81.
		  • Configurer ClearID pour un nouveau système Synergis , page 81.
		  • Configurer ClearID avec un système Synergis existant , page 82.

	Préparer Security Center	

Étape	Tâche	Informations complémentaires
1	Vérifiez que votre licence Security Center a un certificat valable pour le module externe. Allez sur la page d'accueil de Config Tool, cliquez sur **À propos** > **Certificats**, et vérifiez que le module externe ClearID est présent dans la liste.	• Vos informations de licence sont incluses dans l'e-mail de mise à jour de licence que nous vous avons envoyé. Cet e-mail contient des liens vers le pack de téléchargement et d'autres informations de licence. • Pour acquérir une licence, voir Options de licence.
2	Pour gérer les visiteurs dans ClearID, vérifiez que le module de gestion des visiteurs de Synergis[MC] est activé. Allez sur la page d'accueil de Config Tool, cliquez sur **À propos** > **Synergis[MC]**, et vérifiez que Visiteurs est présent dans la liste.	• Vos informations de licence sont incluses dans l'e-mail de mise à jour de licence que nous vous avons envoyé. Cet e-mail contient des liens vers le pack de téléchargement et d'autres informations de licence. • Pour acquérir une licence, voir Options de licence.
	Déployer le module externe	
1	Sur un serveur Security Center, téléchargez et installez le module externe.	• Télécharger et installer le module externe , page 89.
2	Créer le rôle de module externe. **IMPORTANT :** Chaque rôle module externe ne peut communiquer ou se connecter qu'à un seul nom de système ClearID à la fois. Pour les environnements avec plusieurs systèmes, vous devez créer un rôle de module externe pour chaque système.	• Créer le rôle module externe , page 90.

3	Connectez Security Center à ClearID.
	REMARQUE : Pour les environnements avec plusieurs systèmes, répétez ces tâches pour chaque système.
		• Connecter Security Center à ClearID , page 91.
		  • Examiner les informations de titulaires de cartes et d'identifiants , page 92.
		  • Ajouter un système , page 94.
		  • Télécharger un fichier d'activation , page 97.
		  • Configurer les réglages de connexion , page 98.

4	Accordez aux utilisateurs les privilèges nécessaires pour exploiter le module externe. **REMARQUE :** Les opérateurs Security Desk n'ont pas besoin de privilèges particuliers pour utiliser ce module externe.	• Accorder des privilèges utilisateur , page 101. • Reportez-vous à la rubrique « Affecter des privilèges aux utilisateurs » du *Guide de l'administrateur Security Center*. • Pour obtenir la liste de tous les privilèges disponibles, consultez la feuille de calcul Privilèges Security Center relative à votre version.
5	En savoir plus sur les états du système.	• À propos des états du système ClearID, page 102.

Étape	Tâche	Informations complémentaires
6	En savoir plus sur les champs d'identité.	• Champs d'identité, page 115.

7	En savoir plus sur les champs personnalisés.	• À propos des champs personnalisés , page 103.
		  • Modifier les champs personnalisés , page 103.
		  • Relations de champs personnalisés, page 107.

	Gérer les identités et les utilisateurs	

1	Créez, affichez ou modifiez vos identités.	• Créer des identités , page 113.
		• Afficher les identités , page 127.
		• Modifier les identités , page 130.
		  • Accorder des autorisations supplémentaires à des identités et des rôles , page 117.
		  • Accorder des autorisations supplémentaires à des superviseurs , page 121.
		  • Afficher les autorisations supplémentaires , page 123.
		  • Modifier les autorisations supplémentaires , page 124.
		• Supprimer des identités, page 132

2	Accordez l'accès au portail Web aux utilisateurs ou aux administrateurs.	• Accorder un accès utilisateur au portail Web , page 146. • Accorder un accès administrateur au portail Web , page 148.
3	Consultez votre profil.	• Consulter votre profil , page 150.
4	Consultez vos accès aux secteurs et au site.	• Consulter vos accès aux sites et aux secteurs , page 154.
5	En savoir plus sur l'envoi de demandes d'accès.	• À propos du processus de demande d'accès , page 155. • Demander un accès , page 156.
6	Ajoutez vos superviseurs.	• Ajouter des superviseurs manuellement , page 164.
7	Affichez et gérez les subordonnés.	• Afficher les subordonnés , page 166. • Gérer les subordonnés , page 169. • Transférer les subordonnés , page 175.

Étape	Tâche	Informations complémentaires
14	Découvrez comment réinitialiser les mots de passe des utilisateurs.	• Réinitialiser les mots de passe utilisateur , page 183.
9	En savoir plus sur les notifications par e-mail envoyées par ClearID.	• À propos des notifications par e-mail , page 186. • Personnaliser la bannière d’e-mail d'un site , page 188.
10	En savoir plus sur la délégation.	• À propos de la délégation , page 192. • Déléguer des tâches à un autre utilisateur , page 195.
11	Comprendre les différents niveaux d'utilisateurs et ce qu'ils permettent de faire.	• Niveaux utilisateur , page 204.

12	En savoir plus sur l’envoi de demandes d'identité.	• À propos du processus de demande d'identité , page 210.
		• Créer un modèle d'identité , page 211.
		• Demander des identités , page 218.
		  • Demander une identité , page 219.
		  • Demander des identités multiples à l’aide de l’importation CSV , page 223.
		• Annuler les demandes d'identité, page 232
		• Approuver les demandes d'identité, page 235
		• À propos du rapport de demandes d'identités, page 241
		• Vérifier l’état des demandes d'identité, page 242

	Duplication des identifiants	
1	Configurez la duplication des identifiants.	• Configurer la duplication d’identifiants, page 245
2	Examiner les journaux d’identifiants	• Consulter les journaux de synchronisation des identifiants, page 247
3	Forcer la synchronisation des identifiants	• Forcer la synchronisation des identifiants, page 249
	Gérer les sites	
1	Apprenez-en davantage sur les sites.	• À propos des sites , page 251.
2	Créez vos sites dans ClearID.	• Création de sites , page 252.

Étape	Tâche	Informations complémentaires
3	Activez la gestion des visiteurs pour les sites.	• Activer la gestion des visiteurs pour un site , page 257. • Afficher les sites où un utilisateur peut inviter des visiteurs, page 272.
4	Accordez les autorisations d'accès à ClearID à vos utilisateurs.	• Accorder l’accès au portail Web , page 146.
5	Apprenez-en davantage sur les analyses d'accès.	• À propos des examens d'accès , page 283.

6	Configurez des analyses d'accès.	• Configurer les examens d'accès à un secteur , page 287.
		  • Programmer les examens d'accès , page 287.
		• Configurer les examens d'accès d'identité , page 293.
		  • Programmer les examens d'accès d'identité , page 293.

7	Apprenez-en davantage sur le rapport d'analyses d'accès.	• À propos du rapport d’examen d'accès , page 298.
14	Vérifiez l'état des analyses d'accès.	• Vérifier l’état des examens d'accès , page 299.
9	Réalisez une analyse d'accès.	• Terminer un examen d'accès à un secteur (propriétaire de site) , page 302. • Terminer un examen d'accès (approbateur de secteur ou responsable de rôle) , page 311. • Terminer un examen d’accès d’identité (superviseur) , page 320.
10	Générez un rapport d’examen d'accès.	• Générer un résumé d’examen d'accès , page 326.
11	Découvrez-en plus sur le rapport de demandes d'accès.	• À propos du rapport de demandes d'accès , page 328.
12	Vérifiez l'état de vos demandes d'accès.	• Vérifier l’état des demandes d'accès , page 329.
13	Découvrez-en plus sur le rapport d'activité du site.	• À propos du rapport d'activité de site , page 332.

Étape	Tâche	Informations complémentaires

14	Découvrez et gérez les intégrations de point d’ancrage.	• À propos des points d'ancrage , page 135.
		  • Créer des points d'ancrage , page 138.
		  • Modifier les points d'ancrage , page 142.
		  • Consulter les journaux de points d'ancrage , page 143.

	Gérez vos espaces	
1	En savoir plus sur les secteurs.	• À propos des secteurs , page 342.
2	Créez vos secteurs dans ClearID.	• Créer des secteurs , page 343.
3	Ajoutez des portes aux secteurs.	• Ajouter des portes à un secteur , page 346.
4	Activez la gestion des visiteurs pour vos secteurs.	• Activer la gestion des visiteurs pour un secteur , page 347.
5	En savoir plus sur les secteurs imbriqués et les règles d'accès	• À propos des secteurs imbriqués, page 349 • Accorder automatiquement l'accès aux secteurs, page 350
6	Ajoutez vos responsables de secteurs.	• Ajouter des responsables de secteurs , page 353.
7	Ajoutez vos horaires de secteur.	• Ajouter des horaires à un secteur , page 354.
14	Autorisez les utilisateurs à accéder à un secteur.	• Accorder l'accès à un secteur , page 359.
9	Vérifiez qui a accès à votre secteur.	• Examiner les accès à un secteur , page 364.
10	Approuvez les demandes d'accès à votre secteur.	• Approuver les demandes d’accès à un secteur , page 366.
11	Rejetez les demandes d'accès à votre secteur.	• Refuser les demandes d’accès à un secteur , page 368.
	Gérer les visiteurs	
1	En savoir plus sur les processus de demande de visite.	• À propos du processus de demande de visite , page 371. • À propos du processus de liste de surveillance de demande de visite , page 372.

Étape	Tâche	Informations complémentaires

2	Invitez des visiteurs.	• Inviter des visiteurs , page 373.
		  • Inviter des visiteurs manuellement , page 374.
		  • Inviter des visiteurs à l'aide de l'importation CSV , page 379.

3	Vérifiez les événements de visite.	• Examiner les événements de visite , page 388.
4	Copiez un événement de visite.	• Copier un événement de visite , page 390.
5	Modifier un événement de visite	• Modifier les événements de visite , page 391.
6	Découvrez-en plus sur le rapport de visiteurs.	• À propos des rapports de visiteurs , page 395.
7	Affichez un rapport de visiteurs.	• Afficher un rapport de visiteurs , page 396.
14	En savoir plus sur l'utilisation des codes QR en tant qu'identifiants pour les visiteurs.	• Identifiants code QR pour les visiteurs , page 398.
9	Importez le format de carte personnalisé (identifiant code QR).	• Importer un format de carte personnalisé (identifiant code QR) dans Synergis, page 398.
10	Activez les identifiants code QR pour les visiteurs.	• Activer les identifiants code QR pour les visiteurs , page 401.

11	Configurez les lecteurs de codes à barres Qscan pour ClearID.	• Configurer les appareils Qscan pour ClearID, page 404.
		  • Connecter un lecteur de codes à barres Qscan à un contrôleur Mercury , page 404.
		  • Configurer un lecteur Qscan pour la prise en charge de codes QR hexadécimaux 40 bits , page 407.

12	Configurez les appareils STid pour ClearID.	• Configurer les appareils STid pour ClearID, page 409.
		  • À propos des lecteurs de codes QR STid , page 410.
		  • Créer une configuration de lecteur de codes QR STid , page 413.
		  • Transférer votre configuration de lecteur vers votre lecteur de codes QR STid , page 428.

Étape	Tâche	Informations complémentaires
13	Configurez les macros pour l'enregistrement et l'accès automatique à un parking ou une installation sécurisée.	• Automatiser l'accès et l'inscription des visiteurs à l'aide d'une macro , page 433.
	Gérez les listes de surveillance de visiteurs	
1	En savoir plus sur les listes de surveillance.	• À propos des listes de surveillance , page 437.
2	Ajoutez des responsables de listes de surveillance.	• Ajouter des responsables de listes de surveillance , page 439.

3	Ajoutez vos listes de surveillance.	• Ajouter des listes de surveillance , page 441.
		  • Ajouter une entrée à une liste de surveillance de personnes , page 445.
		  • Ajouter une entrée à une liste de surveillance de sociétés , page 448.
		  • Importer des entrées de liste de surveillance depuis un fichier , page 449.
		  • Exporter les entrées de liste de surveillance dans un fichier , page 451.
		  • Tester les entrées de liste de surveillance , page 452.

4	Contrôlez vos visiteurs manuellement	• Contrôler les visiteurs manuellement , page 460.
5	Débloquez les visiteurs bloqués par une liste de surveillance.	• Débloquer les visiteurs bloqués par une liste de surveillance , page 464.
	Gérer le contrôle d'accès basé sur les rôles	
1	Découvrez le contrôle d'accès basé sur les rôles.	• À propos du contrôle d'accès basé sur les rôles , page 469.
2	Ajoutez vos rôles.	• Ajouter des rôles , page 472.
3	Ajoutez des responsables de rôles.	• Configurer les responsables de rôles , page 474.
4	Configurez vos stratégies de contrôle d'accès basées sur les rôles.	• Configurer les stratégies de contrôle d'accès basé sur les rôles , page 476.
5	Ajoutez des attributs de provisionnement personnalisés à une identité.	• Ajouter des attributs de provisionnement personnalisés à une identité , page 482.
6	Ajoutez les membres au rôle.	• Ajouter des membres aux rôles , page 484.
	Connecter d'autres systèmes	

Étape	Tâche	Informations complémentaires
1	Apprenez à authentifier les connexions système de non-utilisateurs.	• Authentifier votre connexion , page 492.

2	Synchronisez les attributs d'identité par LDAP.	• Synchroniser les identités par LDAP , page 569.
		  • À propos de ClearID LDAP Synchronization Agent, page 569.
		  • Correspondances d'attributs LDAP et d'attributs ClearID, page 570.
		  • Configurer ClearID LDAP Synchronization Agent, page 571.

3	Synchronisez les attributs d'identité avec une API.	• Synchroniser les identités à l'aide d'une API, page 496. • À propos de l'API ClearID, page 496.

4	Synchronisation des attributs d'identité via One Identity.	• Synchroniser les identités avec One Identity , page 518.
		  • À propos de One Identity Synchronization Tool , page 519.
		  • À propos des champs d'attributs One Identity Synchronization Tool , page 522.
		  • Installer One Identity Synchronization Tool , page 527.
		  • Configurer One Identity Synchronization Tool , page 535.
		• Consulter l'état de la synchronisation , page 564.
		• À propos des journaux One Identity Synchronization Tool, page 566.
		• Consulter les journaux One Identity Synchronization Tool , page 566.
		• Mettre à jour des identités existantes à partir de sources de données externes, page 567.

Inscription des visiteurs en libre-service		

1	En savoir plus sur Genetec ClearID^{MC} Self-Service Kiosk.	• À propos de ClearID Self-Service Kiosk , page 578.
		  • Inscription sur une borne en libre-service , page 579.
		  • Auto inscription sur une borne en libre-service , page 581.

Étape	Tâche	Informations complémentaires

2	En savoir plus sur les options disponibles dans ClearID Self-Service Kiosk.	• Options de la borne en libre-service , page 635.
		  • Support de borne au sol , page 637.
		  • Étagère pour imprimante pour le support de borne au sol , page 641.
		  • Support de table pour borne , page 643.

3	En savoir plus sur les types de pièces d'identité (ID) pris en charge par la fonction de numérisation de ClearID Self-Service Kiosk.	• Types de pièces d'identité, page 646.

4	Configurez votre borne ClearID Self-Service Kiosk.	• Configurer l'iPad de la borne en libre-service , page 582.
		  • Personnaliser la configuration de la borne en libre-service , page 585.
		  • Personnaliser le logo des badges de visiteurs de la borne en libre-service , page 587.
		• Configurer l'imprimante d'étiquettes de la borne en libre-service (Brother QL-820NWBc, QL-820NWB ou QL-810W) , page 602.
		• Configurer l'imprimante d'étiquettes de la borne en libre-service (Brother TD-4550DNWB) , page 612.
		• Sélectionner une imprimante d'étiquettes de borne en libre-service , page 622.
		REMARQUE : L'imprimante Brother TD-4550DNWB **n'est plus disponible** à l'achat via Genetec. Nous prenons en charge et vendons désormais l'imprimante Brother QL820NWBc (CD-KIOSK-PRINTER-NA-KIT).

5	Testez l'impression des badges de vos visiteurs.	• Imprimer un badge de test sur la borne en libre-service , page 629.
6	Réinitialisez l'application mobile de la borne ClearID Self-Service Kiosk (si nécessaire).	• Réinitialiser l'application mobile Self-Service Kiosk , page 633.
	Dépannage	
1	Découvrez comment résoudre les problèmes susceptibles de survenir.	• Module externe installé mais manquant dans Security Desk et Config Tool, page 676. • Le rôle module externe ne trouve pas de fichier avec certificat, page 677. • Les champs personnalisés ne sont pas affichés dans Security Desk, page 678. • Aucun compte actif trouvé pour l'utilisateur, page 681. • Notification de visite par e-mail non reçue par les visiteurs, page 682.

Étape	Tâche	Informations complémentaires
		• Les champs Hôtes de visiteurs sont vides dans Security Desk., page 683. • Problèmes de connectivité (One Identity Synchronization Tool) , page 685. • Problèmes de synchronisation des données (One Identity Synchronization Tool) , page 686. • Problèmes de la borne en libre-service , page 688. • Problèmes d'impression d'étiquettes de la borne en libre-service , page 691. • Consulter les journaux de points d'ancrage , page 143.

Rubriques connexes

Options de licence, page 71

Liste des fonctionnalités ClearID prises en charge

Découvrez les fonctionnalités prises en charge par Genetec ClearID[MC].

Le tableau suivant répertorie les fonctionnalités disponibles dans ClearID.

Fonctionnalité
Gestion des identités
Gestion des subordonnés par le superviseur.
Transfert de subordonnés
Configuration permettant aux superviseurs d'avoir une autorisation de gestion élevée sur leurs subordonnés. • Mettre à jour les champs d'information du profil. • Mettre à jour les paramètres de contrôle d'accès.
Processus de demande d'identité et approbation pour l'embarquement : • Une identité à la fois. • Plusieurs identités à la fois (importation CSV).
Permissions pour les identités ou les rôles de visualiser et de modifier les identités.
Gestion de secteurs
Déléguer la gestion des secteurs contrôlés à un ou plusieurs propriétaires de secteurs.
Le propriétaire ou l'approbateur de secteur peut afficher, ajouter et supprimer des personnes dans des **secteurs**.
Le propriétaire ou l'approbateur de secteur peut afficher, ajouter et supprimer des rôles dans des **secteurs**.
Le propriétaire ou l'approbateur de secteur peut accorder un accès temporaire à un rôle.
Un titulaire de cartes permanent peut demander un accès temporaire à un secteur (processus intégré).
Les actions des processus sont capturées et disponibles dans l'historique des processus.
Les approbateurs de secteur peuvent approuver ou refuser les demandes d'accès.
Les approbateurs de secteur peuvent effectuer des examens d'accès aux secteurs.
Le superviseur des employés peut devoir approuver les demandes d'accès des employés.
Notifications par e-mail lorsqu'une demande d'accès est soumise.
Notifications par e-mail lorsqu'une demande d'accès est approuvée ou refusée.
Gestion des rôles
Déléguer les rôles de gestion ou le groupe de titulaires de carte à un ou plusieurs propriétaires de rôle.
Les responsables de rôles peuvent ajouter ou supprimer des personnes de leurs groupes.

Fonctionnalité
Provisionnement et synchronisation automatiques des groupes de titulaires de carte pour plusieurs sites
Les propriétaires de rôles peuvent demander l'accès à un secteur pour l'ensemble de leur groupe.
Les responsables de rôles peuvent effectuer des examens d'accès aux rôles.
Gestion multisite
Gestion globale des titulaires de cartes pour plusieurs systèmes Synergis[MC]
Prise en charge (intégrée) des fuseaux horaires
Synchronisation automatique des identifiants permanents lorsqu'une personne change de site.
La synchronisation des titulaires de cartes ne survient que lorsque les titulaires sont modifiés, et s'ils ont accès au système Synergis concerné. Cette approche limite le nombre de titulaires de cartes qui sont synchronisés avec chaque système Synergis.
La synchronisation des groupes de titulaires de cartes ne survient que lorsque les groupes sont modifiés, et s'ils ont accès au système Synergis concerné. Cette approche limite le nombre de groupes de titulaires de cartes qui sont synchronisés avec chaque système Synergis.
Les propriétaires de sites peuvent configurer des horaires d'analyse d'accès ou déclencher des analyses d'accès manuelles.
Les propriétaires de sites peuvent générer un rapport d'analyses d'accès.
Gestion des visiteurs
Pré-enregistrer les visiteurs sur un portail web
Le processus d'approbation des visiteurs peut être personnalisé en fonction du secteur sélectionné.
Provisionnement automatique des visiteurs avec attribution automatique des secteurs requis
Inscription des visiteurs via `Security Desk`

Badges papier et identifiants temporaires
• Les badges papier sont généralement utilisés pour d'importants volumes de visiteurs nécessitant un accès temporaire, par exemple :
  • Organisation d'une conférence ou d'un salon professionnel pour des partenaires commerciaux.
  • Pour identifier les personnes visitant un secteur, des badges de visiteurs temporaires peuvent également être portés par les visiteurs.
• Des identifiants temporaires sont délivrés aux visiteurs par l'équipe de sécurité ou la réception après leur enregistrement. Ces identifiants temporaires sont remis à l'équipe de sécurité ou à la réception lorsque le visiteur quitte le *site* ou *le secteur*.

Escorte de visiteurs avec plusieurs hôtes de visiteurs
Notification par e-mail lorsqu'un visiteur est approuvé.

Fonctionnalité
Enregistrer et signaler le motif de la visite. Le personnel de sécurité peut utiliser les informations liées au motif de visite pour déterminer qui entre ou sort d'un bâtiment et pour quel motif.
Notification par e-mail envoyée au visiteur avec invitation à une réunion, détails sur le site et pièces jointes facultatives
Envoyer une notification par SMS à l'hôte lorsqu'un visiteur s'inscrit. Ces notifications par SMS peuvent être envoyées à n'importe quel numéro de téléphone valide.
Envoyer une notification par e-mail au responsable de liste de surveillance lorsque les informations sur un visiteur correspondent à une personne ou une société d'intérêt dans une liste de blocage ou de notification de personnes ou de sociétés.
L'entrée du visiteur est bloquée lorsque ses informations correspondent à une personne ou une société d'intérêt dans une liste de blocage ou de notification de personnes ou de sociétés.
Options configurables de Genetec ClearID[MC] Self-Service Kiosk. Par exemple, la personnalisation du code QR de l'écran d'accueil, de l'identifiant, des combinaisons d'options d'enregistrement, de sortie et d'auto-enregistrement qui sont affichées.
Options pour récupérer des informations complémentaires sur les visiteurs durant le processus de création d'un événement de visite. Par exemple, le numéro de livraison, le véhicule, le nom du passager, le numéro d'identification ou la plaque d'immatriculation.
Contrôle automatique configurable des visiteurs (délai de grâce).
Rapports
Rapports incluant des téléchargements CSV (le cas échéant). Rapports de demande de flux de travail : • Rapport Demandes d'accès • Rapport d'examen d'accès • Rapport de visiteurs Rapports d'historique : • Rapport d'activité de rôle • Rapport d'activité du site • Rapport Propriétaires de sites et de secteurs. • Rapport d'activité d'utilisateurs
Plateforme
Logo d'entreprise pour les notifications du portail et par e-mail
Plateforme dans le nuage ClearID est un service dans le cloud. Un serveur dédié n'est pas nécessaire. Toutefois, une connexion aux serveurs Synergis est nécessaire. Cette connexion est fournie par le module externe ClearID.
Interface Web HTML5 avec prise en charge mobile Les utilisateurs peuvent utiliser leurs appareils mobiles pour parcourir le portail ClearID.

Fonctionnalité
Une API REST est disponible pour automatiser les fonctions du portail Web. • Créer ou éditer une identité dans le système. • Désactiver l'accès pour une personne. • Ajouter une personne à un rôle. • Supprimer une personne d'un rôle. • Créer un événement pour les visiteurs. • Accuser réception d'une demande d'accès.
Synchroniser l'identité à l'aide de Microsoft SQL Server.
Synchroniser l'identité à partir d'une source personnalisée à l'aide de l'API Identity REST.
Sécurité et authentification
Prise en charge des authentifications multifacteur pour les utilisateurs utilisant OpenID Connect
Authentification unique à l'aide de Microsoft Office 365
Authentification unique à l'aide de Microsoft Azure Active Directory (AD)
Certification ISO 27001 Pour plus d'informations, voir Ressources de cybersécurité.
Chiffrement AES -256 avec RSA Les données personnelles traitées par ClearID sont toujours chiffrées.

Rubriques connexes

Portail de conformité Genetec

Langues prises en charge

Genetec ClearID[MC] est disponible dans les langues suivantes :

Portail Web ClearID

- Anglais
- Français
- Espagnol
- Néerlandais
- Allemand
- Italien
- Portugais
- Japonais

REMARQUE : La langue qui s'affiche dans l'interface utilisateur du portail Web est déterminée par les paramètres de langue de votre navigateur Web.

Module externe ClearID

- Anglais

Genetec ClearID[MC] One Identity Synchronization Tool

- Anglais

Genetec ClearID[MC] LDAP Synchronization Agent

- Anglais

Application mobile Genetec ClearID[MC] Self-Service Kiosk

- Anglais
- Français
- Espagnol
- Néerlandais
- Allemand
- Italien
- Portugais
- Japonais

Documentation

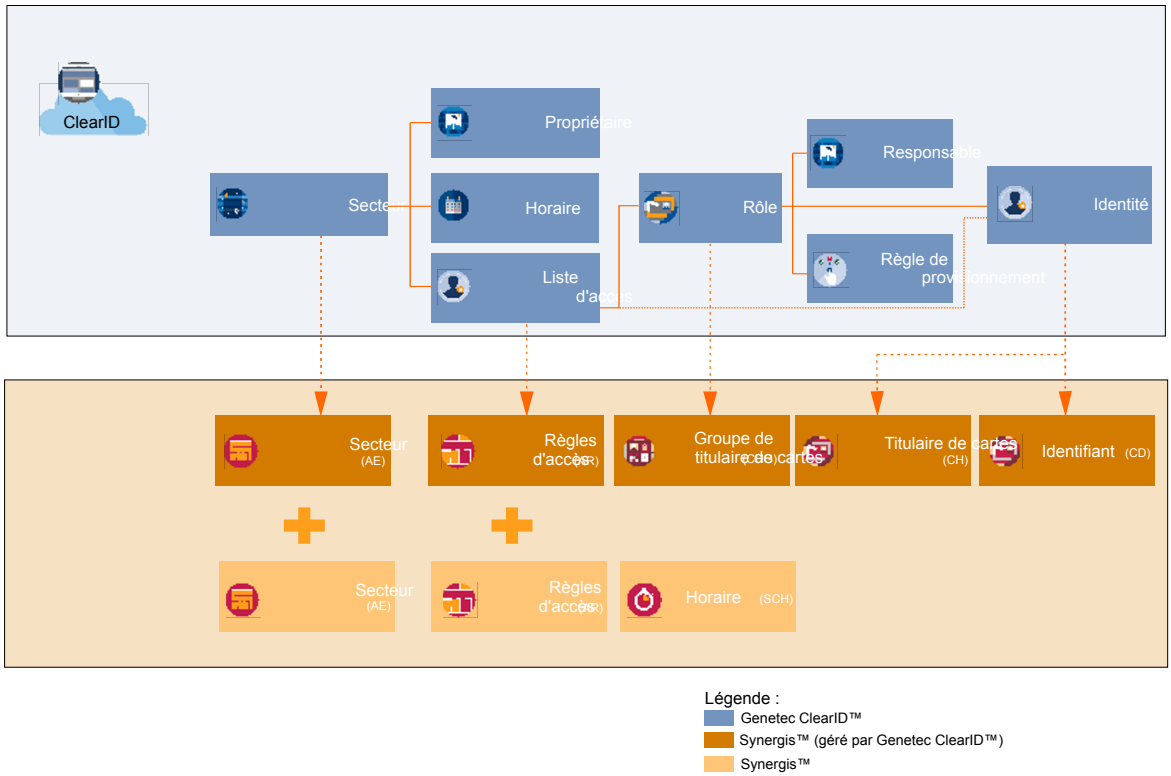
- *Guide de l'utilisateur Genetec ClearID[MC]* (Anglais)
- *Guide de l'utilisateur Genetec ClearID[MC]* (Français)
- *Guide de l'utilisateur Genetec ClearID[MC]* (Espagnol)

IMPORTANT : La traduction de la documentation est en cours. Il se peut que la documentation dans les langues autres que l'anglais soit indisponible lors de la publication. Pour la dernière version de la documentation, voir le Genetec TechDoc Hub.

Terminologie ClearID

Genetec ClearID[MC] utilise des termes particuliers. Voici la définition de termes courants, ainsi que leurs équivalents dans Security Center.

Le schéma suivant présente les termes ClearID et leurs équivalents dans Security Center :

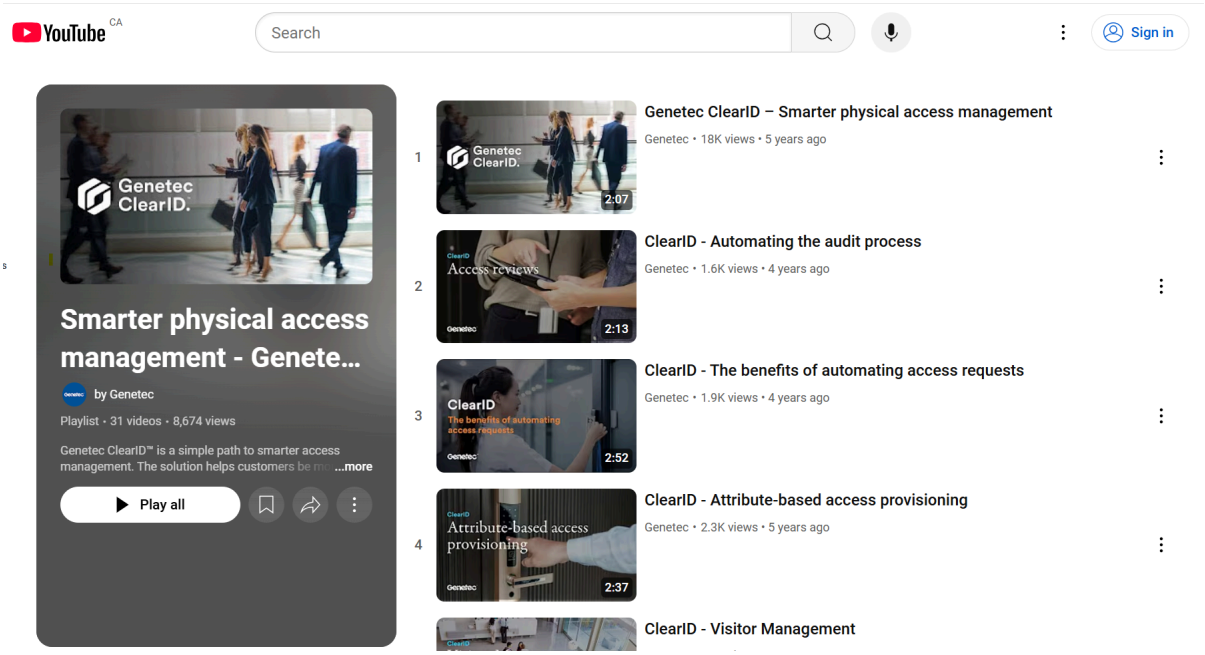


Le tableau suivant présente les termes ClearID et leurs équivalents dans Security Center :

ClearID	Security Center
Identité	Titulaire de cartes
Secteur	Secteur
Rôle	Groupe de titulaires de cartes
Horaire (défini dans Security Center) et liste d'accès (définie dans ClearID)	Règles d'accès

Vidéos ClearID

Utilisez les vidéos de formation Genetec ClearID[MC] pour découvrir et comprendre les principales fonctionnalités du produit. Vous pouvez accéder à toutes les vidéos dans un même endroit, la liste de lecture des vidéos ClearID.



Cliquez sur l'image pour accéder à la liste de lecture Vidéos ClearID.

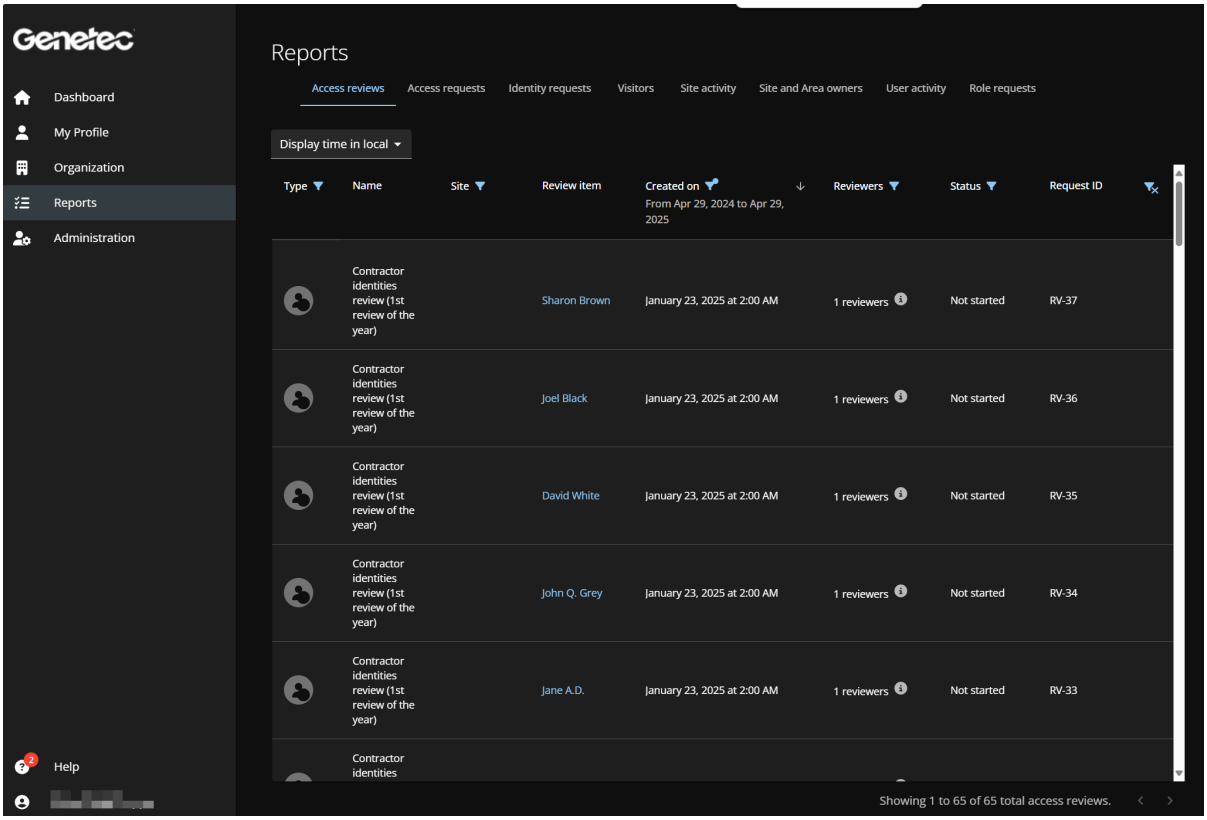
Vous pouvez également lancer les vidéos individuellement depuis les rubriques pertinentes ou la page d'accueil de la documentation.

Rubriques connexes

Présentation de ClearID, page 2

À propos des rapports

Genetec ClearID[MC] fournit plusieurs rapports pour vous aider à gérer votre site et diverses activités. Les rapports peuvent vous aider à comprendre l'état des demandes d'accès, des examens d'accès et des événements de visite en cours ou à venir. Les rapports peuvent également servir à examiner des informations d'historique sur les rôles, les sites, les propriétaires de sites et de secteurs et les utilisateurs.



Vous pouvez utiliser les rapports suivants pour consulter l'état des éléments suivants :

- Rapport d'examen d'accès
- Rapport Demandes d'accès
- Rapport de demandes d'identité
- Rapport Subordonnés
- Rapport Propriétaires de sites et de secteurs
- Rapport sur les visiteurs

Vous pouvez utiliser les rapports suivants pour consulter des informations d'historique concernant les éléments suivants :

- Rapport d'activité de rôle
- Rapport d'activité du site
- Rapport d'activité d'utilisateurs

Se connecter à ClearID

Connectez-vous à votre compte Genetec ClearID[MC] pour envoyer des demandes de visite ou d'accès.

Avant de commencer

- Les cookies et JavaScript doivent être activés dans votre navigateur Web
- Si vous n'utilisez pas un système Active Directory d'entreprise, activez votre compte ClearID en cliquant sur le lien d'activation dans votre e-mail.

Procédure

1 Dans votre navigateur web, tapez ou sélectionnez l'hôte spécifié dans l'e-mail d'activation de votre compte.

Exemple :

- États-Unis : https://portal.clearid.io/
- Australie : https://portal.au.clearid.io/
- Canada : https://portal.ca.clearid.io/
- Europe : https://portal.eu.clearid.io/

REMARQUE : Si une connexion d'entreprise (authentification unique à l'aide de Microsoft Office 365 ou similaire) est utilisée, le compte est automatiquement activé et aucun e-mail d'activation n'est reçu.

2 Sur la page de *connexion*, entrez votre *nom d'utilisateur* et cliquez sur **Connexion**.

Vous êtes redirigé vers la page de connexion à votre compte utilisateur.

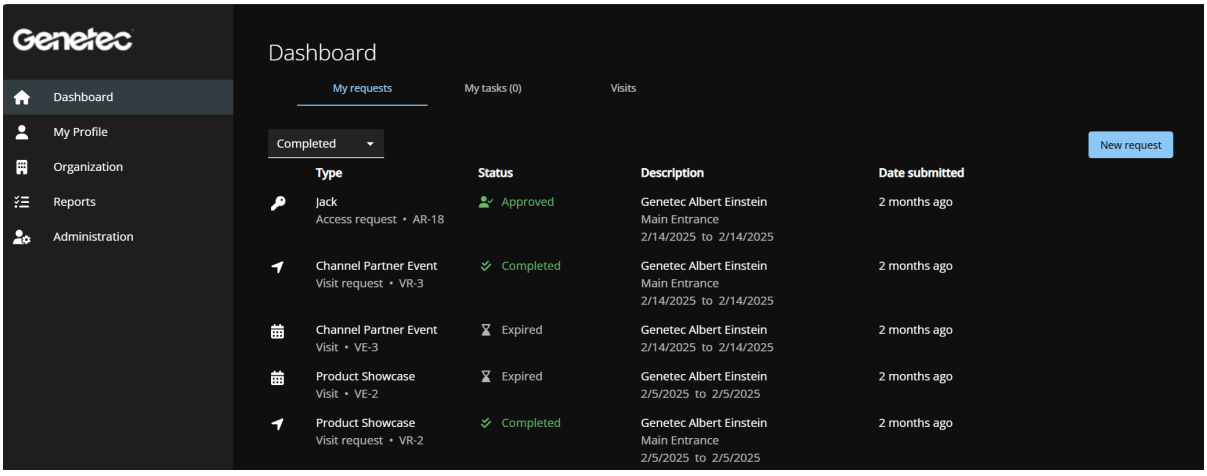
3 (Facultatif) Sélectionner un compte.

- L'ID de compte est affiché dans l'URL en haut de chaque page.

  Par exemple, *https://nomdhôte/iddecompte/pageactuelle*.
- L'ID de compte peut varier en fonction du compte auquel l'utilisateur est connecté.

CONSEIL : Si vous disposez de plusieurs comptes, vous pouvez passer d'un compte à l'autre à tout moment en cliquant sur **Changer de compte** dans les options de compte situées sous l'ID utilisateur.

La page *Mes demandes* est affichée et vous pouvez commencer à utiliser ClearID.



Rubriques connexes

Créer des identités, page 113
Authentifier votre connexion, page 492

Se déconnecter de ClearID

Pour quitter Genetec ClearID[MC], vous pouvez vous déconnecter de votre compte utilisateur.

À savoir

Vous êtes automatiquement déconnecté du système après une période d'inactivité définie. La période d'inactivité varie en fonction de la configuration de votre environnement. La valeur par défaut est de 30 minutes.

Procédure

- En haut de la page, cliquez sur votre nom, puis cliquez sur **Déconnexion**.

  CONSEIL : Une fois que vous êtes déconnecté de votre compte, fermez toutes les fenêtres de navigateur que vous utilisiez avec ClearID.

Activer l’aperçu de fonctionnalités

Si disponibles, les utilisateurs peuvent activer une ou plusieurs fonctionnalités en avant-première dans Genetec ClearID[MC] afin de les évaluer avant leur sortie officielle.

Avant de commencer

L’option **Aperçu de fonctionnalités** doit être activée pour votre organisation.

À savoir

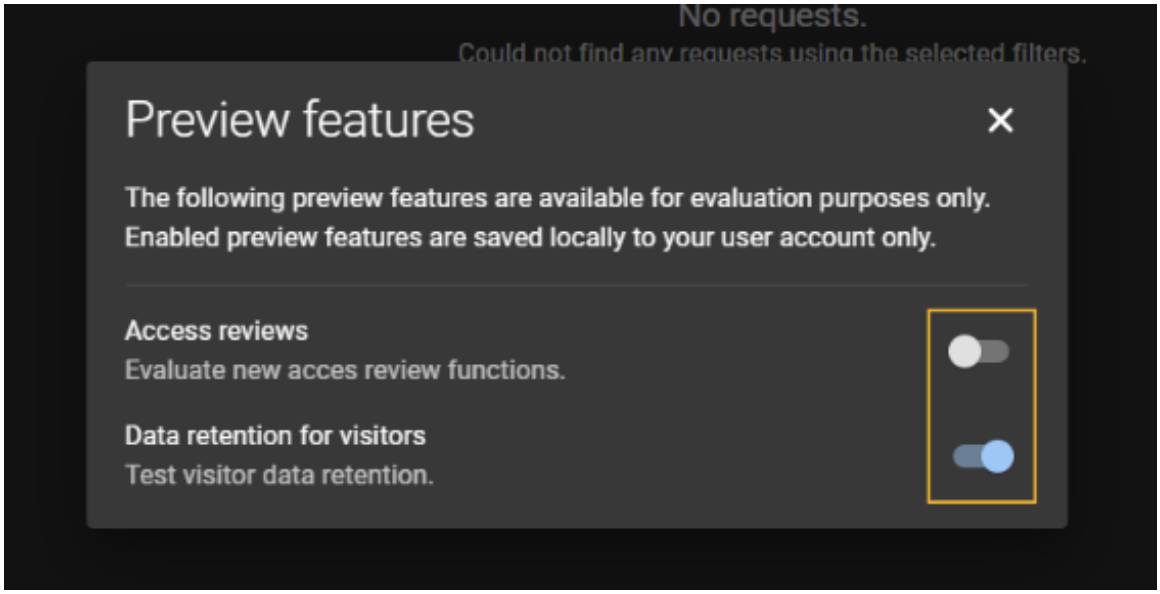
- L’aperçu des fonctionnalités est réservé à des fins d'évaluation.
- Les fonctionnalités activées sont enregistrées localement que pour votre compte utilisateur.

Procédure

1 Sur le portail web ClearID, cliquez sur votre nom d'utilisateur.

2 Cliquez sur **Aperçu de fonctionnalités**.

3 Dans la boîte de dialogue *Aperçu de fonctionnalités*, activez les fonctionnalités que vous souhaitez tester.



4 Cliquez sur pour fermer la boîte de dialogue.

Désactiver l’aperçu de fonctionnalités

Les utilisateurs peuvent désactiver les aperçus de fonctionnalités dans Genetec ClearID[MC] s'ils ne souhaitent plus les tester ou les voir.

Avant de commencer

L’option **Aperçu de fonctionnalités** doit être activée pour votre organisation.

À savoir

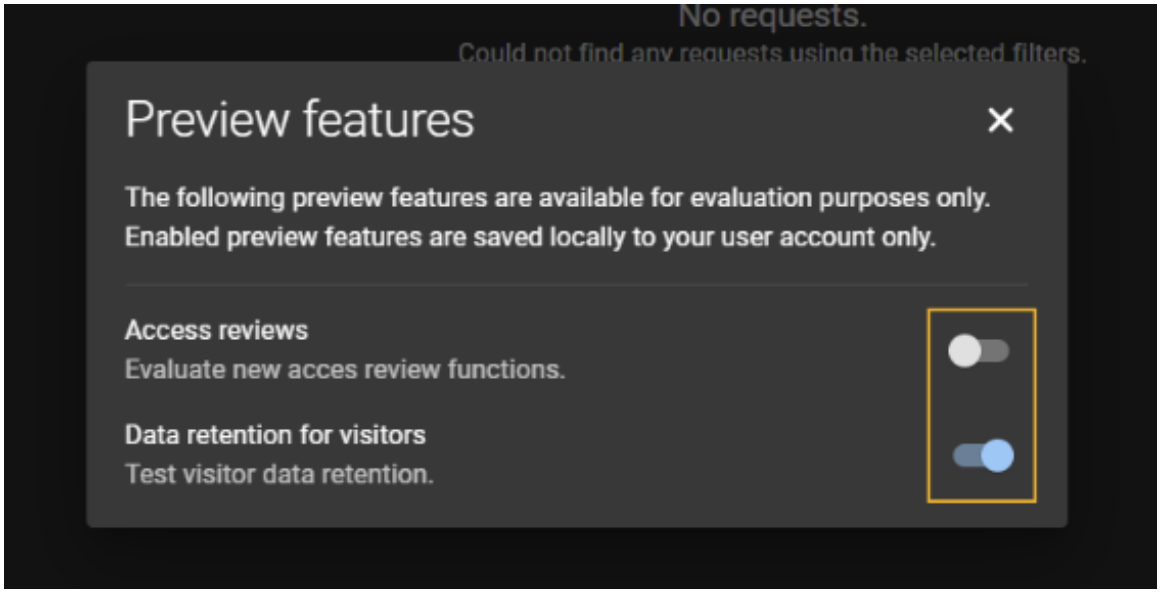
- L’aperçu des fonctionnalités est réservé à des fins d'évaluation.
- Les fonctionnalités activées sont enregistrées localement que pour votre compte utilisateur.

Procédure

1 Sur le portail web ClearID, cliquez sur votre nom d'utilisateur.

2 Cliquez sur **Aperçu de fonctionnalités**.

3 Dans la boîte de dialogue *Aperçu de fonctionnalités*, désactivez les fonctionnalités qui ne vous intéressent plus.



4 Cliquez sur ✕ pour fermer la boîte de dialogue.

Personnalisation de la marque du portail

En tant qu'administrateur de compte , vous pouvez personnaliser le logo et la couleur d'accentuation du portail Genetec ClearID[MC] pour l'aligner sur l'image de marque de votre entreprise.

Avant de commencer

Vous devez être un *administrateur de comptes* pour personnaliser la marque du portail ClearID .

À savoir

- Vous pouvez définir différentes options de personnalisation pour les thèmes clairs et sombres dans ClearID.

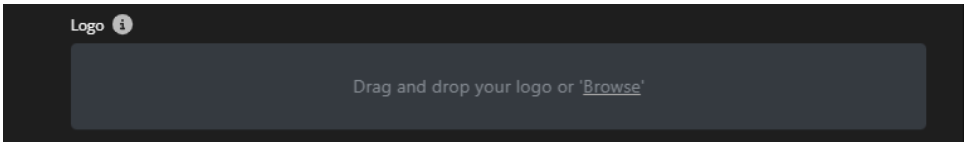
Procédure

1 Sur le portail web ClearID, cliquez sur **Administration** > **Configuration du compte**.

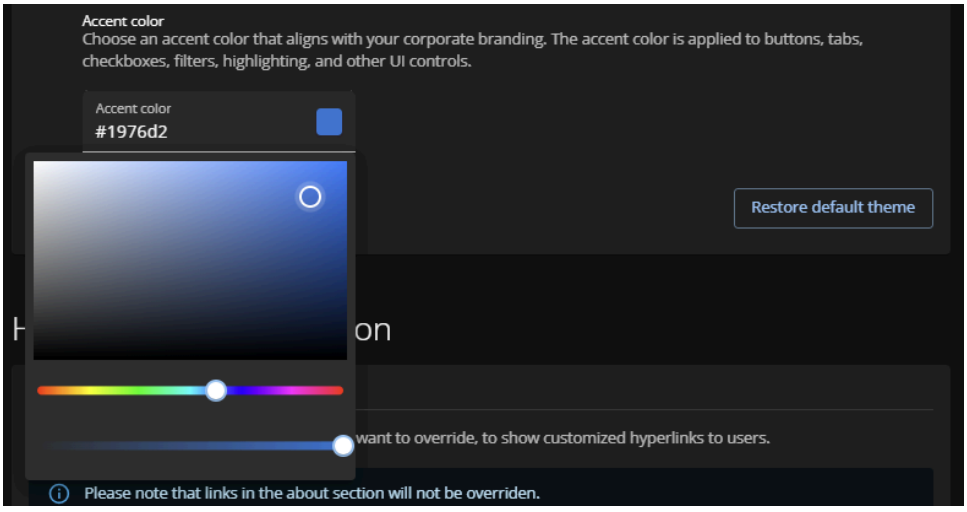
2 Dans la section *Marque*, choisissez un thème clair ou un thème sombre.

a) Sélectionnez le logo et la couleur d'accentuation.

- **Logo :** Cliquez sur **Parcourir** ou glisser-déposer une image depuis votre navigateur de fichier pour télécharger votre logo. L'image doit avoir une résolution comprise entre 20x20 et 2000x500 pixels.



- **Couleur d'accentuation :** Utilisez le sélecteur de couleur pour choisir une couleur et régler l'opacité, ou tapez le code hexadécimal de la couleur dans le champ **Couleur d'accentuation**.

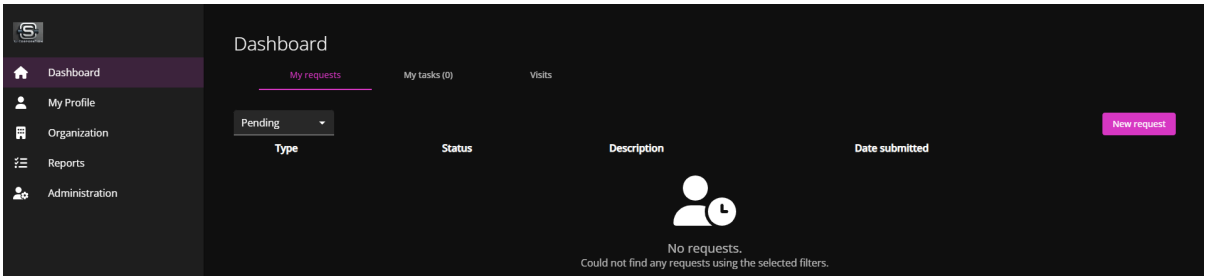


- **(Facultatif) :** Cliquez sur **Restaurer le thème par défaut** pour restaurer la marque du portail par défaut.

3 Cliquez sur **Enregistrer**.

4 (Facultatif) Répétez les étapes 2 à 3 pour d'autres thèmes si nécessaire.

Une image de marque personnalisée est appliquée au logo du portail, aux boutons et à la couleur de mise en avant.


Dashboard
Dashboard
My Profile
Organization
Reports
Administration
My requests
My tasks (0)
Visits
Pending
New request
Type
Status
Description
Date submitted
No requests.
Could not find any requests using the selected filters.

Personnalisation des liens du menu d'aide

En tant *qu'administrateur de compte*, vous pouvez personnaliser les liens du menu **Aide** de Genetec ClearID^{MC} , en dirigeant les utilisateurs du portail vers les ressources et pages assistance de votre entreprise.

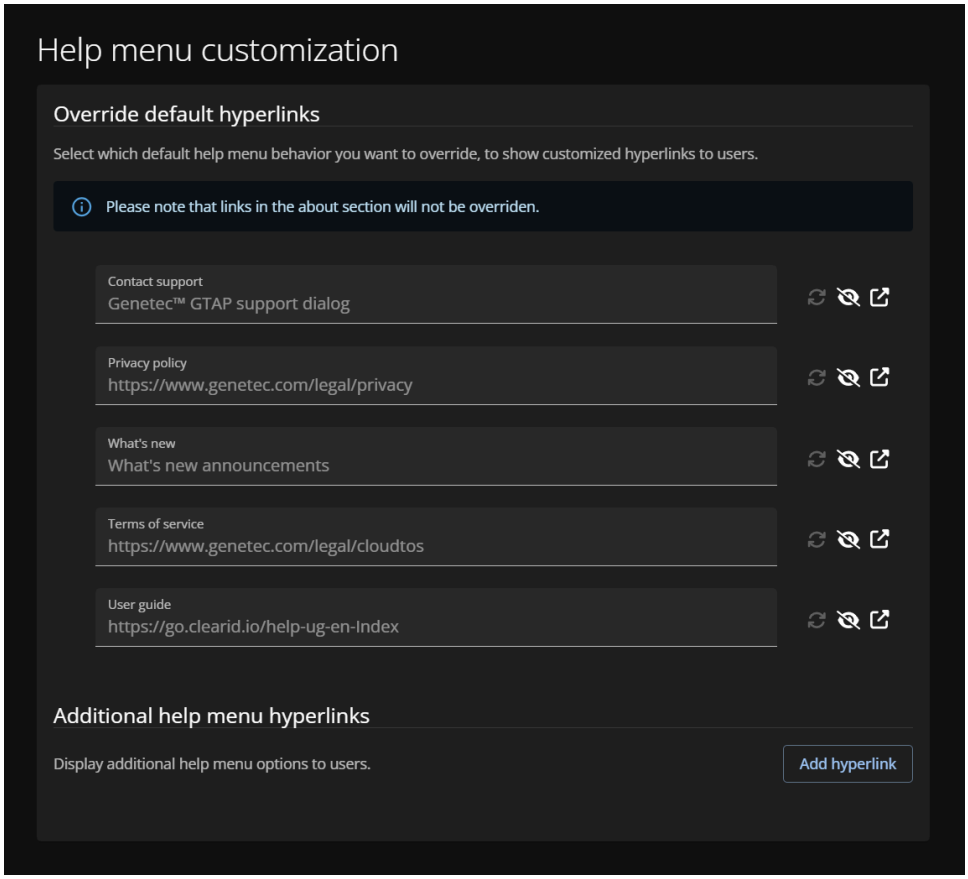
Avant de commencer

Vous devez être *administrateur de comptes* pour personnaliser les liens dans le menu **Aide** ClearID .

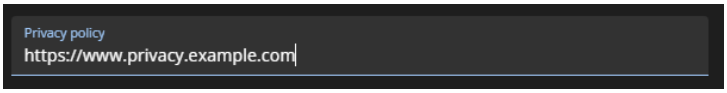
Procédure

1 Dans le portail Web ClearID , cliquez sur **Configuration du compte d’administration** > **..**

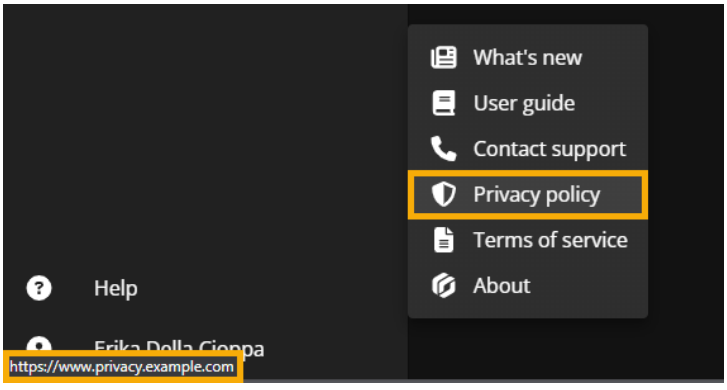
2 Dans la section *Remplacer les hyperliens par défaut*, modifier les liens par défaut du menu **Aide**.
REMARQUE : Vous ne pouvez pas remplacer le lien **À propos**.



a) Sélectionnez l'élément de menu **Aide** que vous souhaitez modifier.
b) Tapez l'URL vers laquelle vous souhaitez que l'utilisateur soit dirigé sous l'en-tête sélectionné.



c) Cliquez sur **Enregistrer**.

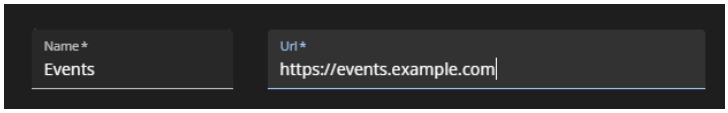


3 (Facultatif) Dans la sous-section *Liens hypertexte du menu Aide supplémentaire*, ajoutez d'autres liens au menu.

a) Cliquez sur **Ajouter un lien hypertexte** pour ajouter un nouvel élément de menu.

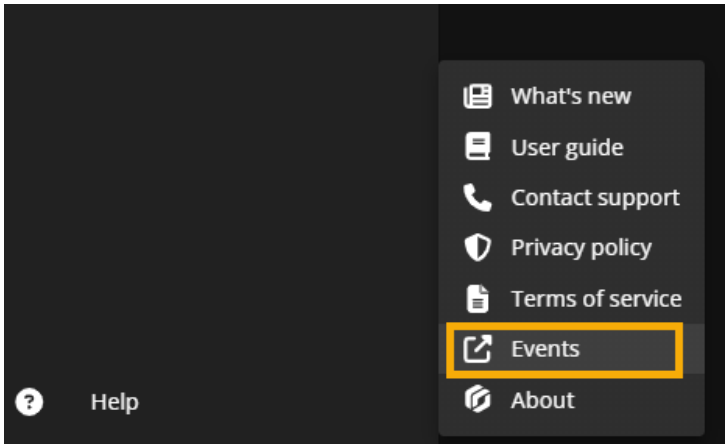
b) Dans le champ **Nom**, saisissez un nom pour votre nouvel élément de menu.

c) Dans le champ **URL**, saisissez l'URL du nouvel élément de menu.



d) Cliquez sur **Enregistrer**.

Le nouveau lien est ajouté au menu sous les liens du portail par défaut.



4 (Facultatif) Utilisez les icônes à côté de chaque lien pour réinitialiser, masquer ou afficher les éléments de menu.

- Cliquez sur **Revenir à la valeur par défaut** ( ) pour rétablir le lien personnalisé à la valeur par défaut du portail.
- Cliquez sur **Masquer** ( ) pour masquer le lien du menu.
- Cliquez sur **Afficher**( ) pour afficher un lien précédemment masqué.
- Cliquez sur **Aller à l'URL** ( ) pour accéder à la page liée.
- Cliquez sur **Supprimer** ( ) pour supprimer le lien personnalisé.

2

Nouveautés

Découvrez les nouveautés de la dernière mise à jour de ClearID.

Cette section aborde les sujets suivants:

- "Nouveautés de ClearID", page 44
- " Fonctionnalités et améliorations précédentes ", page 46

Nouveautés de ClearID

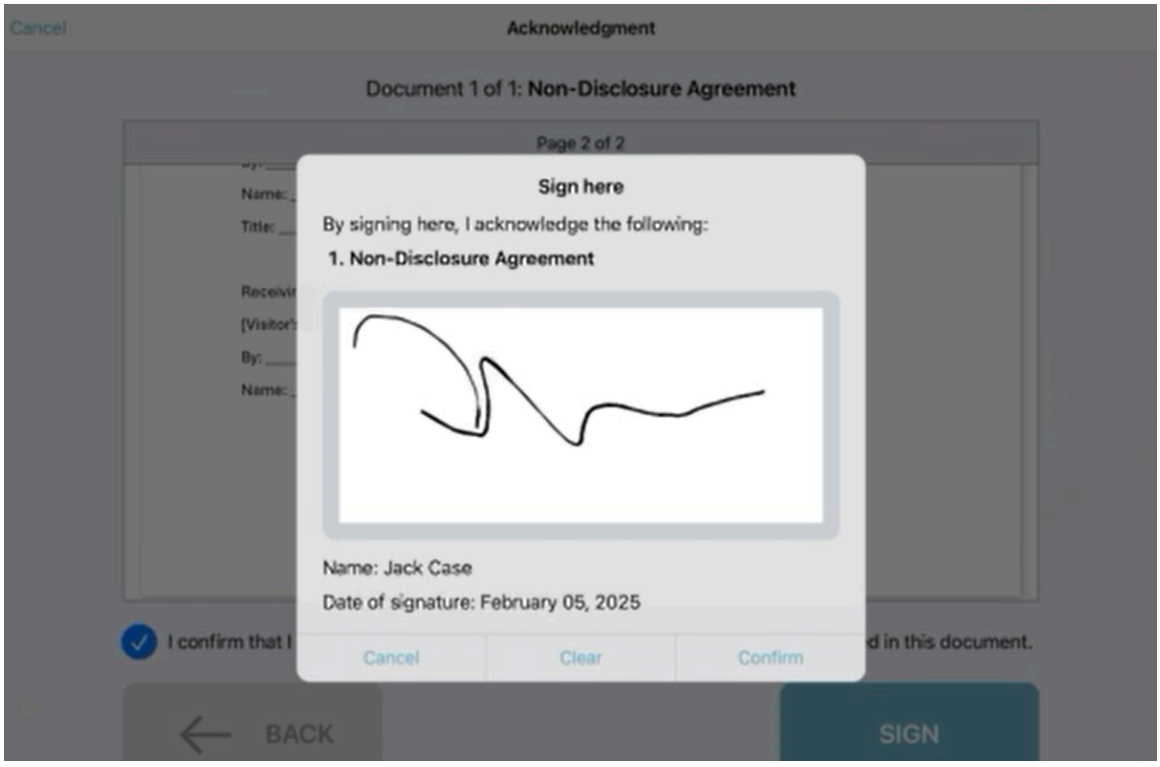
Découvrez les nouveautés de la dernière mise à jour de Genetec ClearID[MC].

Nouveautés : Janvier 2025

- **Enregistrer les visiteurs à l'aide de l'enregistrement par opérateur mobile ClearID :** Auparavant, les visiteurs ne pouvaient s'enregistrer aux événements qu'à l'aide de l'iPad de la borne en libre-service. Désormais, les réceptionnistes, les agents de sécurité et les agents des événements hébergés peuvent rapidement enregistrer les visiteurs à l'aide de l'application ClearID Self Service Kiosk sur un iPhone. L'enregistrement par opérateur mobile utilise l'iPhone pour scanner des codes QR et rechercher les informations de visite.

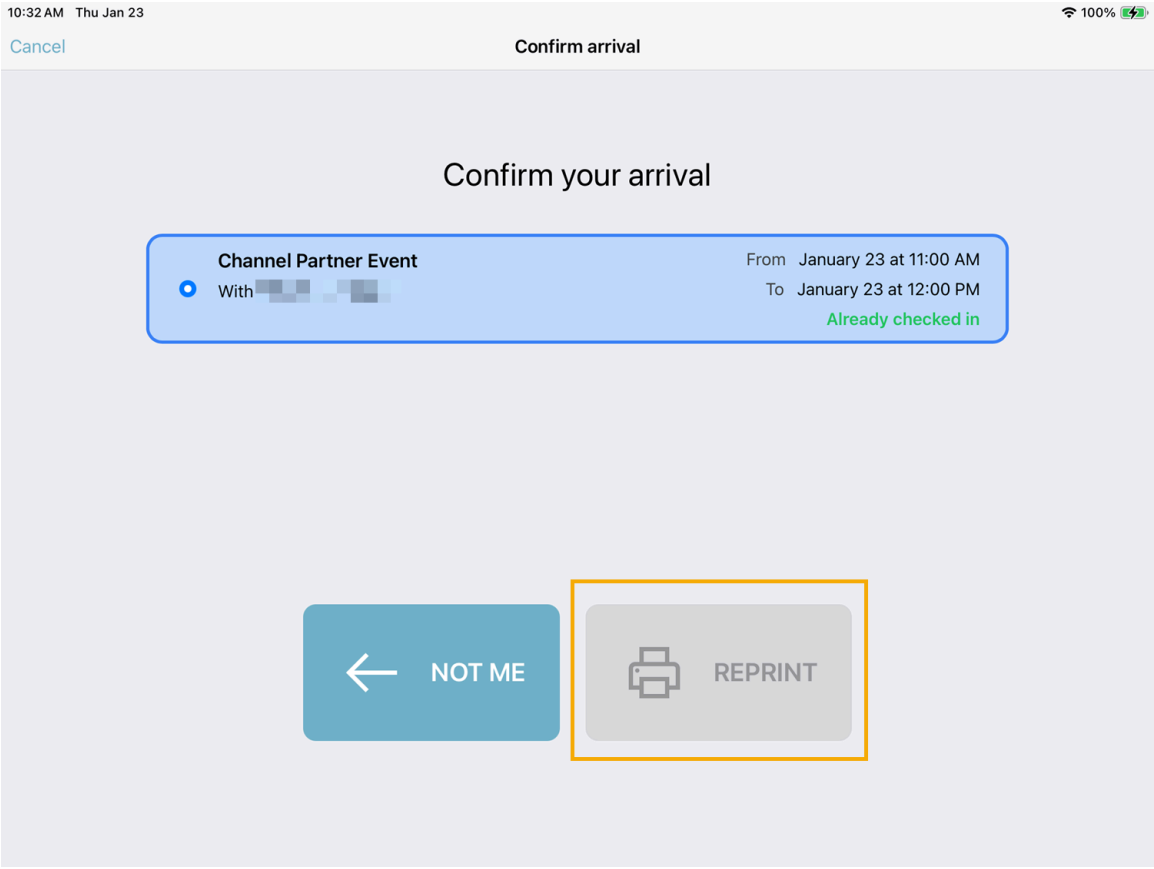
  Pour en savoir plus, voir Enregistrement par opérateur mobile , page 594 et Configurer l'enregistrement par opérateur mobile , page 597.
- **Prenez des décisions en connaissance de cause lorsque vous accordez l'accès aux employés. :** Vous pouvez désormais indiquer que les employés doivent charger des justificatifs lorsqu'ils envoient des demandes d'accès à des secteurs sécurisés pour lesquels des certifications spécialisées sont requises. Les *propriétaires de sites* et les *approbateurs de secteurs* peuvent examiner les documents soumis pour s'assurer que les employés qui ont besoin d'un accès respectent les réglementations du secteur et les politiques de l'entreprise avant de leur accorder l'accès.

  Pour en savoir plus, voir Configurer les documents de demande d'accès pour les sites , page 276 et Configurer les documents de demande d'accès pour les secteurs , page 356.
- **Obliger les visiteurs à respecter les exigences du site :** Vous pouvez dorénavant obliger les visiteurs à lire et à signer des documents de conformité lors du processus d'inscription sur Self-Service Kiosk. Les *administrateurs de comptes* peuvent ajouter jusqu'à cinq documents sur la borne, comme des accords de non-divulgation ou de non-responsabilité, des consignes à suivre sur le site, etc.



  Pour en savoir plus, voir Ajouter des documents PDF à valider dans Self-Service Kiosk.
- **Les visiteurs peuvent réimprimer les badges :** Les visiteurs peuvent désormais réimprimer les badges perdus ou endommagés directement depuis Self-Service Kiosk. En tant que *propriétaire de site*, vous

pouvez activer l'option **Réimprimer le badge** afin que les visiteurs puissent revenir sur la borne pour réimprimer leur badge temporaire.



Pour en savoir plus, voir Activer la réimpression des badges.

- **Protéger la confidentialité des visiteurs :** Les *propriétaires de sites* peuvent désormais désactiver la capture photo lors de l'inscription des visiteurs sur la borne Self-Service Kiosk.

  Pour en savoir plus, voir Désactiver la photo du visiteur pendant l'inscription.

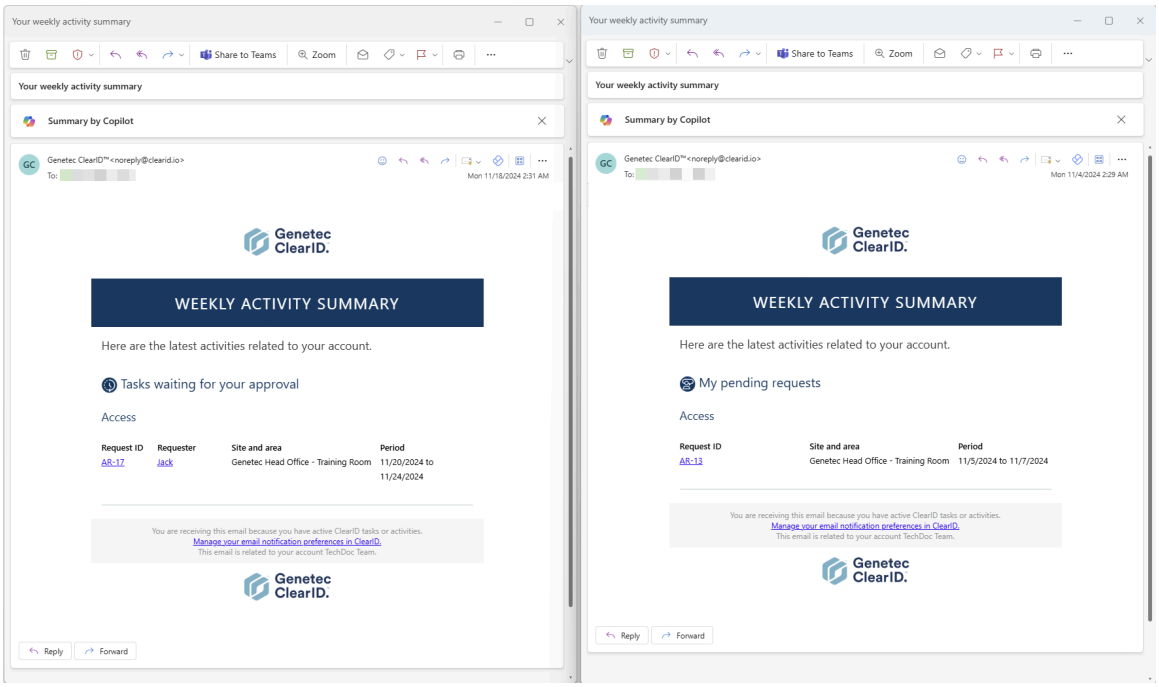
Pour une liste complète de toutes les annonces précédentes, voir Fonctionnalités et améliorations précédentes.

Fonctionnalités et améliorations précédentes

La solution Genetec ClearID[MC] intègre les fonctionnalités et améliorations suivantes.

Nouveautés : Décembre 2024

- **Suivre vos tâches en attente :** Vous pouvez désormais recevoir un Résumé d'activité hebdomadaire par e-mail tous les lundis qui détaille les tâches et requêtes en attente qui nécessitent une approbation. L'e-mail n'est pas envoyé en l'absence de tâches ou de requêtes en attente. Pour gérer vos préférences d'e-mail, allez dans **Mon profil** > **Préférences** > **Notifications**.



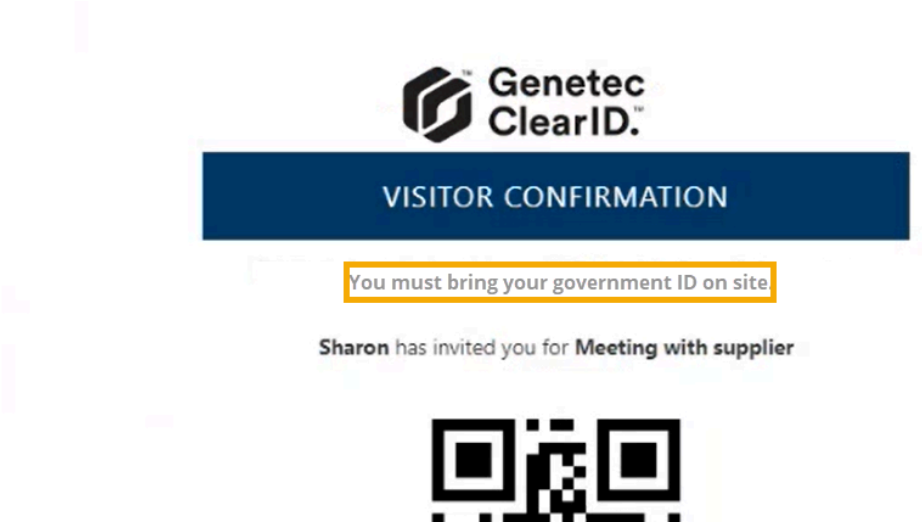
Pour en savoir plus, voir À propos des notifications par e-mail et Configurer vos préférences de notification par e-mail.

Nouveautés : Octobre 2024

- **Synchroniser les photos d'identité ClearID avec Security Center :** Les *administrateurs de comptes* peuvent désormais choisir ClearID en tant que source officielle pour toutes les photos de titulaires de cartes dans Security Center. Vous pouvez activer la synchronisation des photos d'identité afin de remplacer automatiquement les photos des titulaires de cartes dans Security Center par celles de ClearID.

  REMARQUE : La taille des photos d'identité dans ClearID est limitée à 5 mégaoctets.

  Pour en savoir plus, voir Synchroniser les photos d'identité avec Security Center.
- **Personnaliser le texte d'en-tête et de pied de page des e-mails de notification :** Les *administrateurs de comptes* et les *propriétaires de sites* peuvent désormais personnaliser le texte qui figure dans l'en-tête et le pied de page des e-mails de notification. Utilisez les champs texte personnalisés pour fournir des informations aux visiteurs, comme le matériel ou la documentation nécessaire lors de leur visite, ou les étapes à suivre avant de venir.



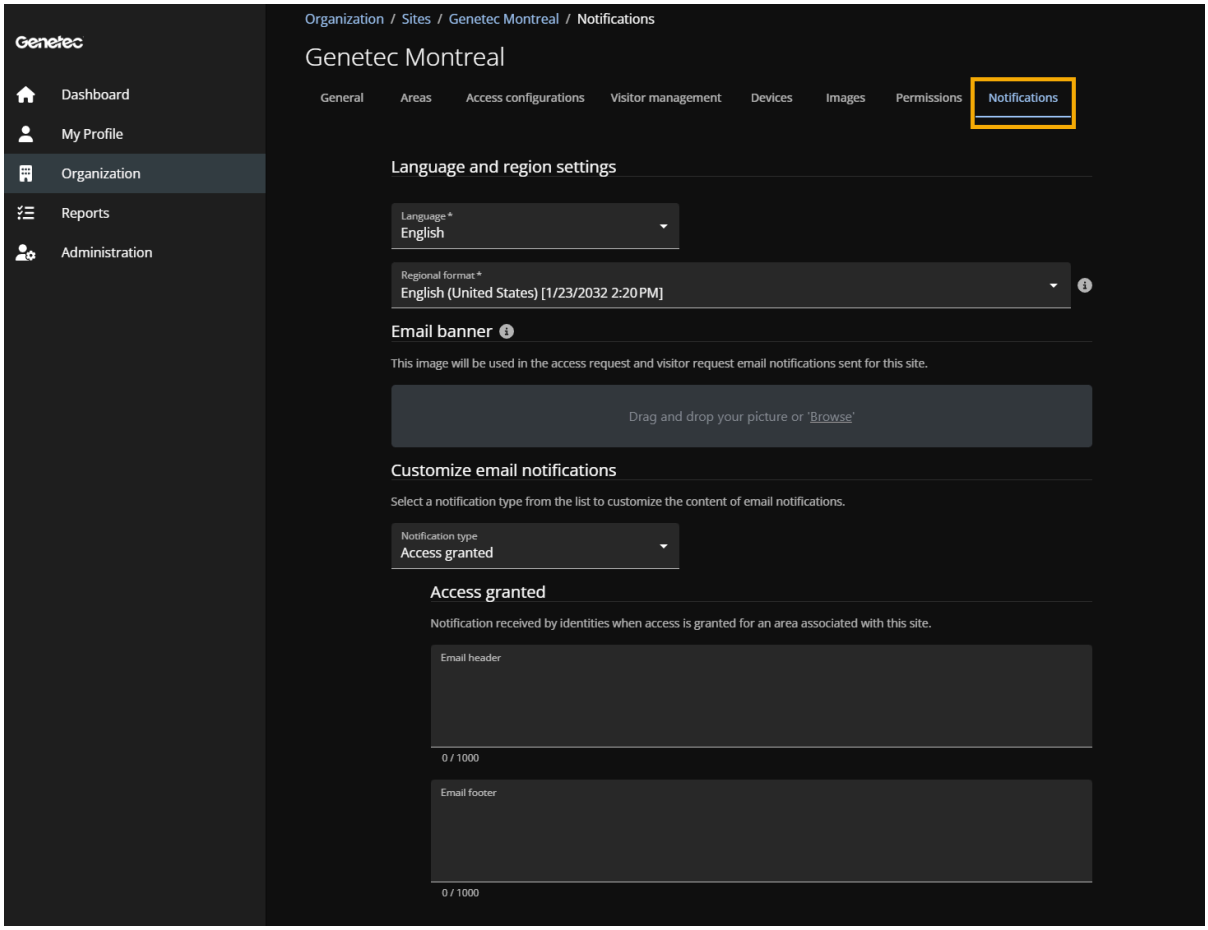
Pour en savoir plus, voir Personnaliser les notifications par e-mail pour un site , page 279.

- **L'application mobile ClearID Self-Service Kiosk version 2.2 est désormais disponible. :** La dernière mise à jour apporte des correctifs ainsi que des diagnostics améliorés pour les événements de visite. Les fonctionnalités principales de la borne restent les mêmes.

  Pour télécharger l'application mobile ClearID Self-Service Kiosk, rendez-vous sur l'App Store.

IMPORTANT : Modifications de l'interface utilisateur

- **Les réglages de langue, de région et de notification ont déménagé :** Auparavant, les réglages de langue et de région et les réglages de notification étaient configurés par un *Administrateur de compte* ou un *Propriétaire de site* en cliquant sur **Organisation** > **Sites** > **Général**. Désormais, ces réglages sont disponibles dans l'onglet **Notifications** en cliquant sur **Organisation** > **Sites** > **Notifications**.



Pour en savoir plus, voir Création de sites , page 252 et Modifier les sites , page 273.

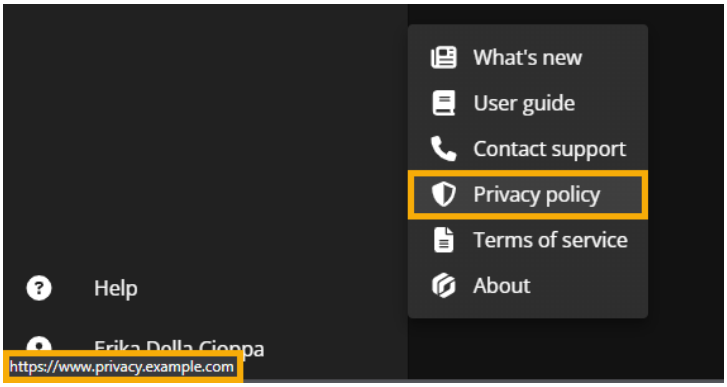
Nouveautés : Septembre 2024

- **Synchronisation des identifiants de titulaires de cartes :** Les comptes ClearID qui se connectent à plusieurs systèmes Security Center disposent d'un nouveau réglage de configuration. L'administrateur peut désormais désigner le système Security Center qui doit servir de source pour la synchronisation des identifiants avec d'autres systèmes. Cette option rend la synchronisation des identifiants automatique et prévisible et permet aux employés d'accéder à plusieurs sites à l'aide d'un seul badge.

  Pour en savoir plus, voir Configurer la duplication d'identifiants , page 245.
- **Gestion des identités simplifiée :** Vous pouvez désormais utiliser l'intégration SCIM (System for Cross-domain Identity Management) pour synchroniser les attributs système provenant d'une source de données externe avec ClearID. Ces attributs d'identité peuvent ensuite être utilisés dans ClearID pour affecter des personnes à des rôles et pour automatiser le contrôle d'accès basé sur les rôles.

  Pour en savoir plus, voir Synchroniser les identités à l'aide de l'intégration SCIM.
- **La version 2.1.2 de l'application ClearID Self-Service Kiosk est désormais disponible :** La dernière mise à jour inclut des améliorations de performances et d'évolutivité , des corrections de bugs et quelques modifications mineures de l'interface utilisateur. Les fonctionnalités principales de la borne restent les mêmes.

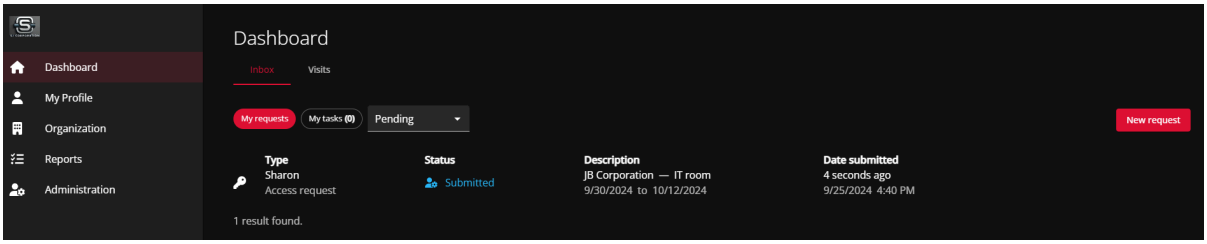
  Pour télécharger l'application mobile ClearID Self-Service Kiosk, rendez-vous sur l'App Store.
- **Personnalisation des liens du menu d'aide :** Les administrateurs de comptes peuvent désormais personnaliser les liens dans le menu Aide de ClearID, afin de rediriger les utilisateurs du portail vers les pages d'assistance et les ressources de votre entreprise.



Pour plus d'informations, voir Personnalisation des liens du menu d'aide.

Nouveautés : Juin 2024

- **Personnalisation de la marque du portail :** Les administrateurs de comptes peuvent désormais personnaliser le logo et la couleur d'accentuation sur le portail ClearID pour respecter la charte graphique de votre entreprise. Les utilisateurs du portail peuvent afficher le portail en mode clair ou en mode sombre.



Pour en savoir plus, voir Personnalisation de la marque du portail , page 38.

- **Centres de données géo-spécifiques :** Vous pouvez désormais stocker vos données dans une région qui correspond à l'emplacement|lieu géographique de votre système ou à l'endroit où vous souhaitez que les données soient stockées. Vous pouvez choisir entre des options de centre de données plus régionales pour répondre aux exigences réglementaires ou à d'autres besoins de stockage de données géo-spécifiques.
  - **Centres de données Canadiennes :** Toutes les données sont stockées dans des centres de données situés au Canada.
    - Centre de données primaire : Azure Central Canada (Ontario)
    - Centre de données secondaire: Azure East Canada (Quebec)
  - **Centres de données Australiennes :** Toutes les données sont stockées dans des centres de données situés en Australie.
    - Centre de données primaire: Azure East Australia (New South Wales)
    - Centre de données secondaire: Azure Central Australia (Canberra)

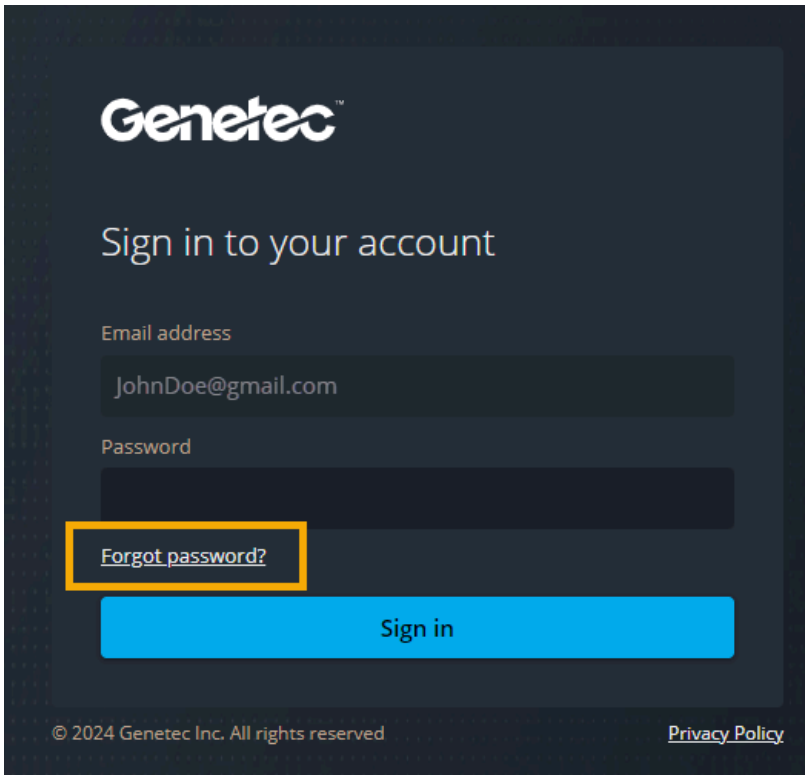
  Pour en savoir plus, voir À propos de l'architecture de ClearID, page 5.
- **Rapport d'activité d'utilisateurs :** Les administrateurs de compte peuvent désormais consulter l'activité liée aux identités et aux superviseurs dans le *rapport d'activité* de l'utilisateur. Il est désormais possible de filtrer les résultats dans la colonne **Type d'activité** pour afficher les activités pour ces types action :
  - Superviseur ajouté ou supprimé
  - Identité créé, mise à jour, ou supprimé

  Pour plus d'informations, voir À propos du rapport d'activité utilisateur et Affichage d'un rapport d'activité utilisateur.

Nouveautés : Avril 2024

- **Mise à jour du système de connexion à ClearID :** Nous avons apporté une mise à jour au système de connexion à ClearID susceptible d'affecter votre organisation. Les utilisateurs qui n'utilisent pas l'authentification unique (SSO) pourront être obligés de réinitialiser leur mot de passe lors de leur première connexion à ClearID. Dans le cadre de cette transition :
  - L'authentification à plusieurs facteurs (MFA) devient obligatoire pour tous les utilisateurs qui se connectent aux applications Genetec[MC].
  - Un code, qui est envoyé à l'adresse e-mail associée au compte de l'utilisateur, sert de deuxième facteur d'authentification.

  REMARQUE : Ce changement n'affecte pas les utilisateurs des organisations qui intègrent leur système de gestion des identités d'entreprise avec ClearID. Ces utilisateurs peuvent continuer à utiliser l'authentification unique SSO fournie par leur organisation.



  Pour en savoir plus, voir Réinitialiser le mot de passe d'un utilisateur.

Nouveautés : Février 2024

- **Suivi des entités gérées par ClearID dans Synergis[MC] :** Vous pouvez désormais suivre les entités gérées par ClearID dans Config Tool et Security Desk. Ces entités sont mises en évidence par un point bleu dans le coin inférieur droit de l'icône de entité . Exemple :

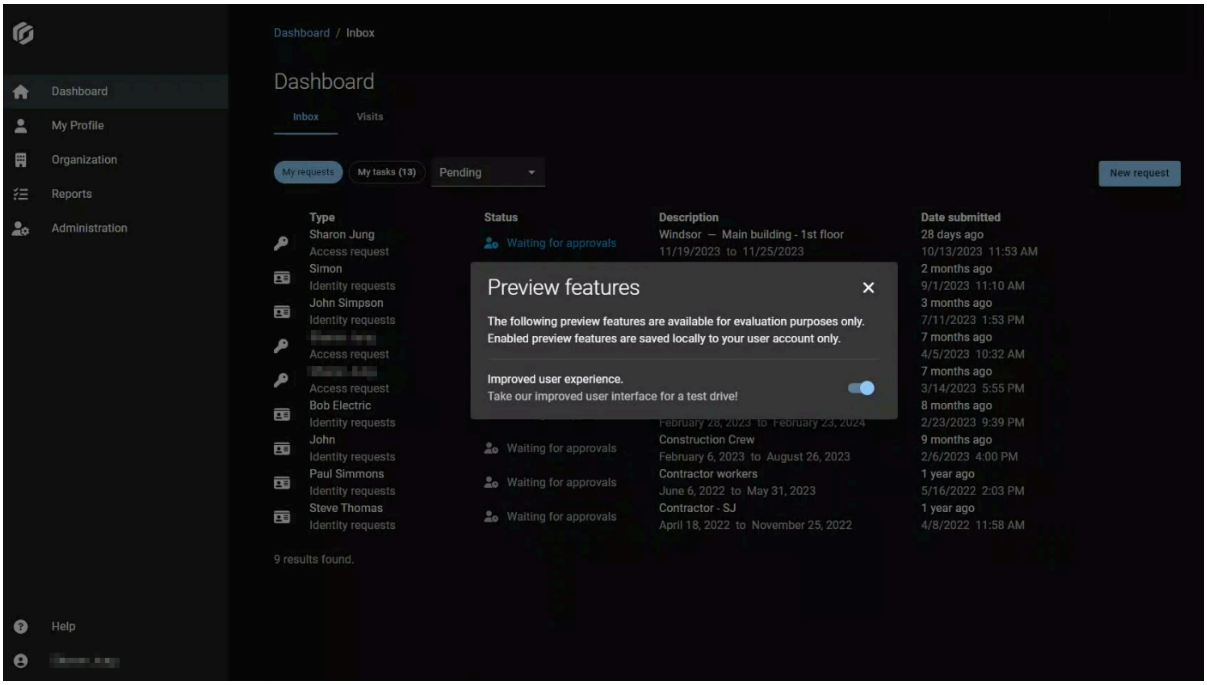
  Règles d'accès ( )

  Pour en savoir plus, voir Fonctionnement de l'intégration , page 13.
- **assistance du scanner de codes QR Zebra DS 9300 :** ClearID prend désormais en charge le scanner de code QR Zebra DS 9300.

Pour en savoir plus, voir Appareils pris en charge , page 78, Activer la gestion des visiteurs pour un site , page 257, ou reportez-vous à la documentation du fabricant.

Nouveautés : Décembre 2023

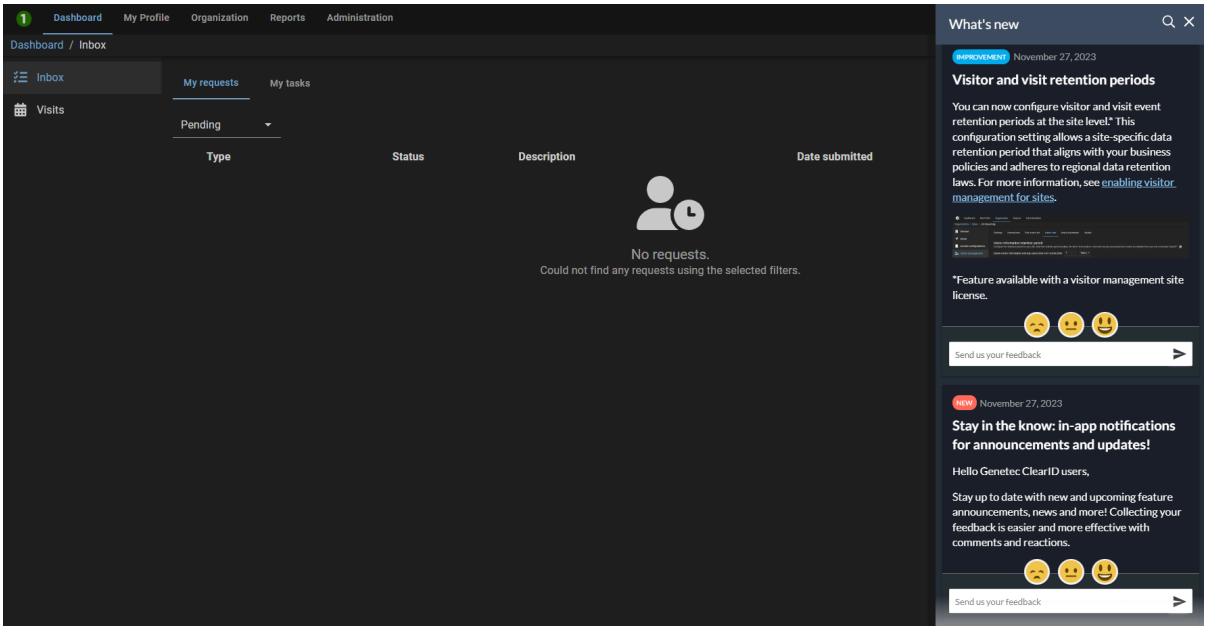
- **Fonctions d'aperçu :** ClearID intègre désormais un aperçu de nouvelles fonctionnalités. Les utilisateurs peuvent activer une ou plusieurs fonctionnalités (si disponibles) afin d'y accéder en avant-première.



REMARQUE : L'aperçu de fonctionnalités est réservé à des fins d'évaluation. Les fonctionnalités activées sont enregistrées localement que pour votre compte utilisateur.

Pour en savoir plus, voir Activer l'aperçu de fonctionnalités , page 36 et Désactiver l'aperçu de fonctionnalités , page 37.

- **Notifications dans l'application :** ClearID intègre désormais des notifications dans l'application pour les annonces de nouvelles fonctionnalités et d'améliorations, des sondages et d'autres mises à jour du produit sur le portail web.



Restez au courant des fonctionnalités nouvelles et à venir, des annonces, des actualités, etc. Recueillir vos commentaires est encore plus simple. Vous pouvez directement envoyer des réactions par émoji ou vos commentaires concernant chaque annonce ou notification à notre équipe produit.

- **Mise à jour de l'architecture de ClearID :** Le traitement des données d'identité a évolué.

  Pour en savoir plus sur les centres de données qui sont utilisés pour le déploiement mondial, voir la rubrique *Microsoft Corporation* dans la section ClearID de la liste des sous-traitants Genetec.
- **Genetec ClearID^{MC} Self-Service Kiosk 1.13.9 :** L'application mobile ClearID Self-Service Kiosk version 1.13.9 est désormais disponible.

  Cette version de maintenance contient les éléments suivants :

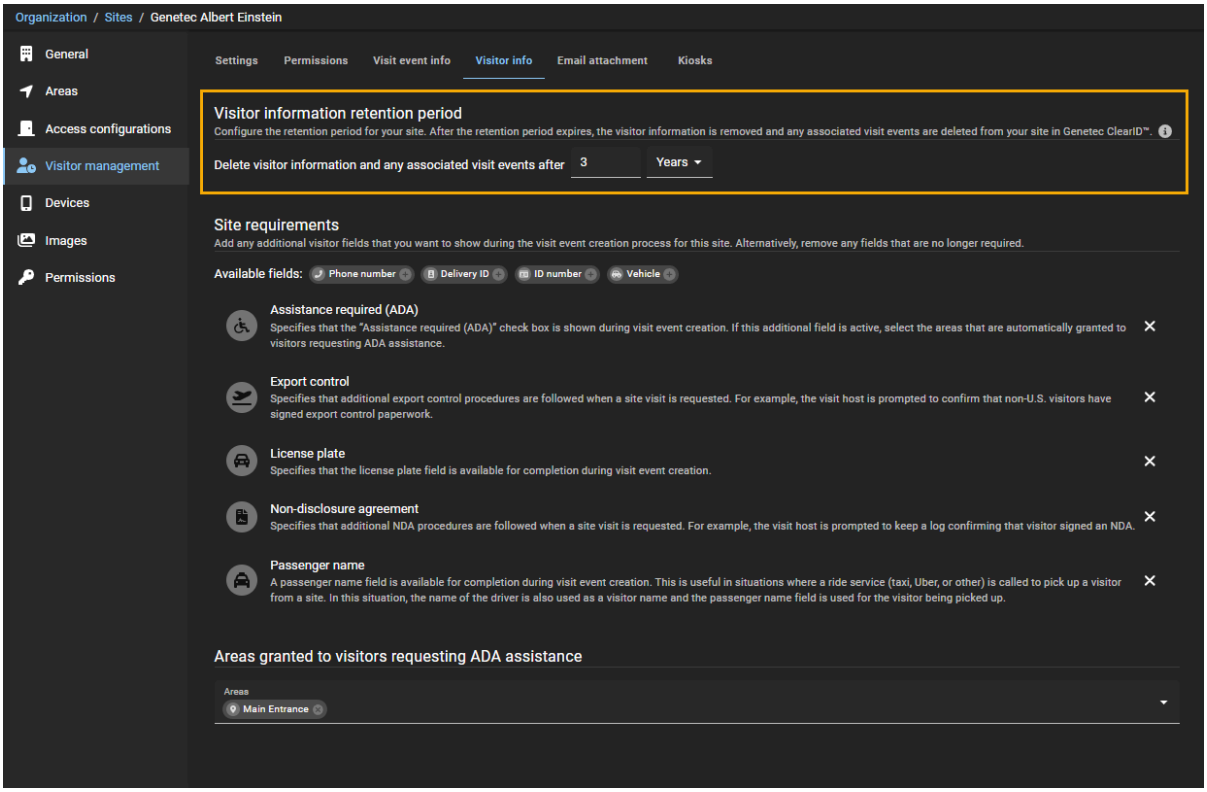
  - Amélioration des performances
  - Mises à jour pour la compatibilité avec iOS 17.1.1

  Pour télécharger l'application mobile ClearID Self-Service Kiosk, rendez-vous sur l'App Store.

Nouveautés : Novembre 2023

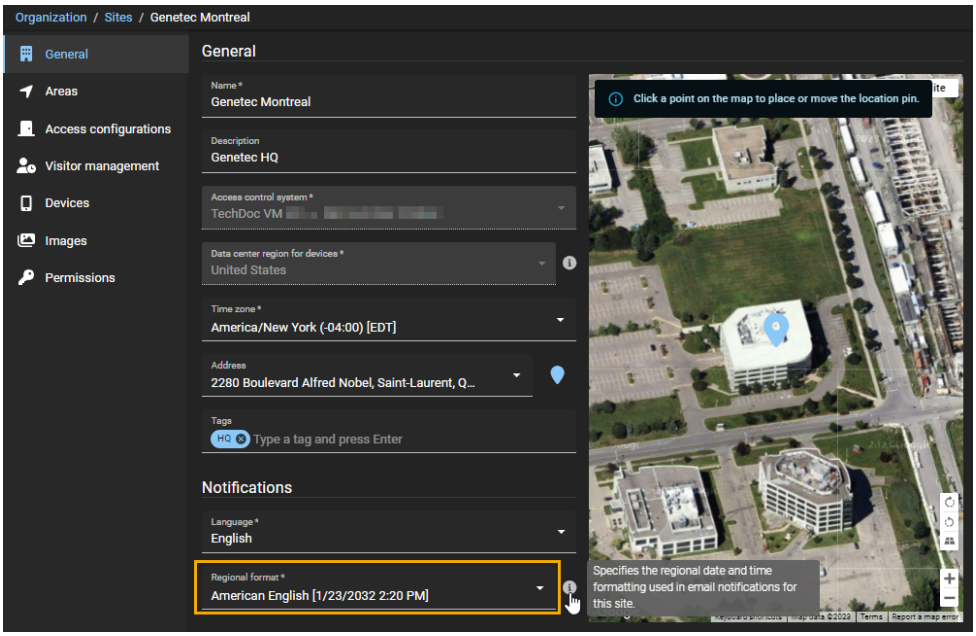
- **Rétention des données de visiteurs :** Vous pouvez désormais configurer une période de rétention des informations sur les visiteurs. À l'issue de la période de rétention, les données de visiteurs et les événements de visite associés sont supprimés de votre site dans ClearID.

  REMARQUE : La période de rétention est configurable par site afin d'assurer la conformité avec les réglementations régissant les données de votre région.



Pour en savoir plus, voir Activer la gestion des visiteurs pour un site , page 257.

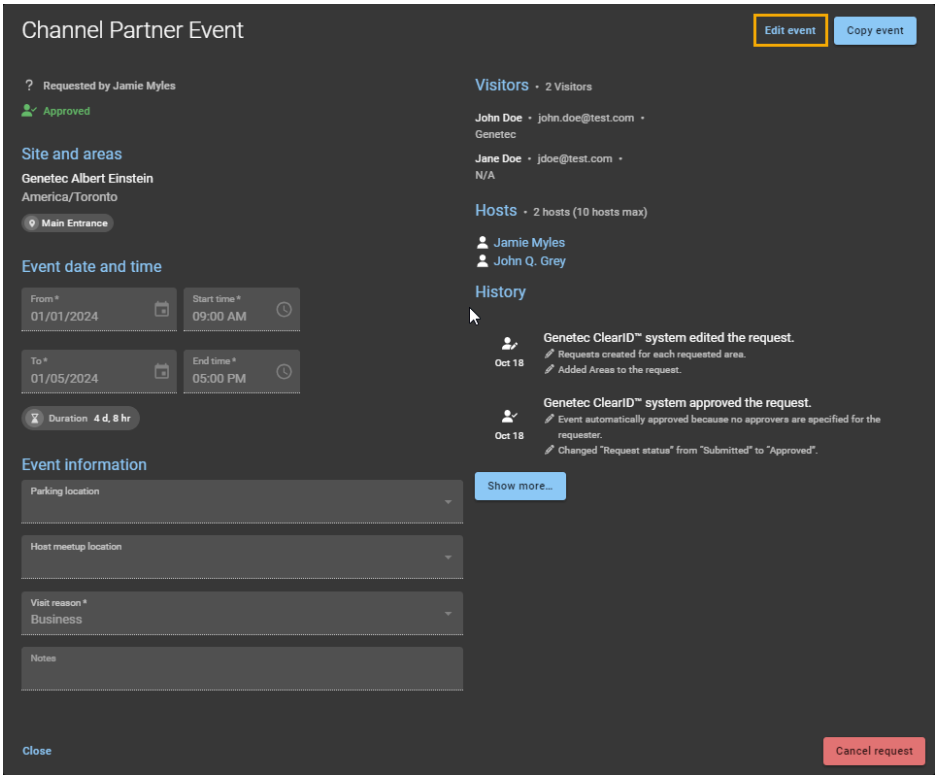
- **Notifications par e-mail :** Vous pouvez désormais configurer vos e-mails de notification pour spécifier un **Format régional** adapté à vos sites. Les e-mails de notification utilisent le format de date et d'heure standard à l'emplacement du site en fonction du format régional sélectionné.



Pour en savoir plus, voir Création de sites , page 252 et Modifier les sites , page 273.

- **Mettre à jour les événements de visite planifiés :** Vous pouvez désormais modifier les événements de visite, pour changer les informations ou ajouter ou supprimer des visiteurs et des hôtes. La mise à jour des informations sur l'événement de visite permet d'informer les visiteurs en cas de changements affectant l'événement prévu.

REMARQUE : Les événements peuvent être modifiés avant le début de l'événement de visite.

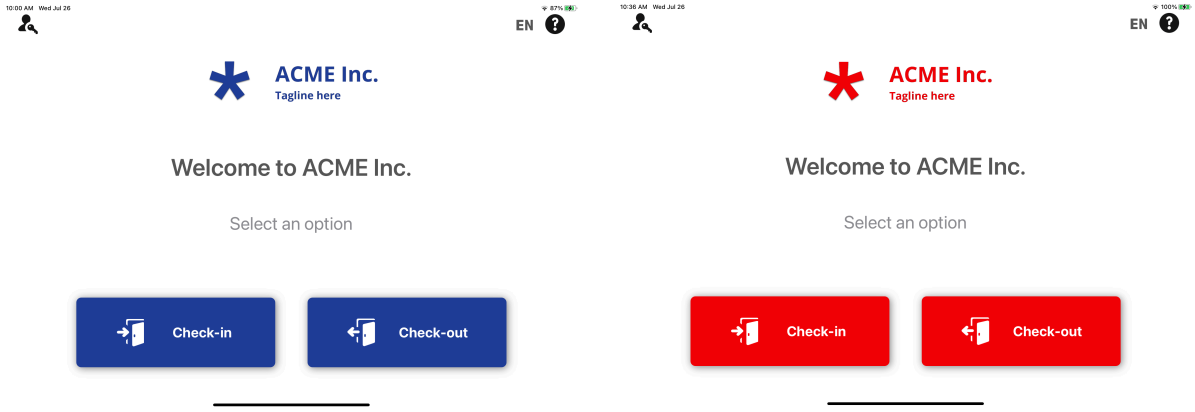


Pour en savoir plus, voir Modifier les événements de visite , page 391.

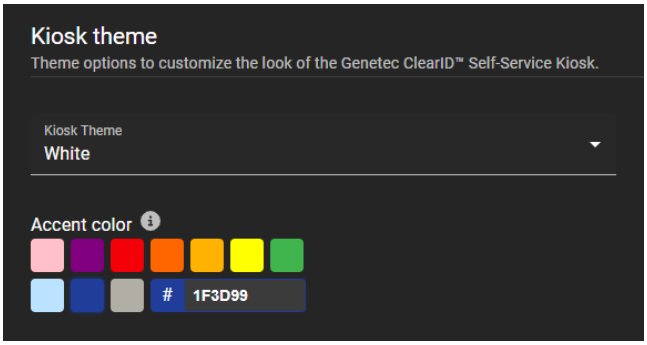
Nouveautés : Octobre 2023

- **Personnalisation de la borne :** L'application Genetec ClearID[MC] Self-Service Kiosk a été enrichie pour permettre la personnalisation de l'habillage de la borne.

  Les exemples suivants montrent le thème blanc avec une couleur d'accentuation.



Vous pouvez choisir le thème blanc pour la borne. Lorsque vous choisissez le thème blanc, vous avez le choix entre dix couleurs d'accentuation. Vous pouvez aussi entrer un code HEX qui correspond à votre charte graphique.



Pour en savoir plus, voir Personnaliser la configuration de la borne en libre-service , page 585 ou Activer la gestion des visiteurs pour un site , page 257.

- **Genetec ClearID Self-Service Kiosk 1.13.8 :** L'application mobile ClearID Self-Service Kiosk version 1.13.8 est désormais disponible.

  L'application mobile de la borne est désormais compatible avec les éléments suivants :

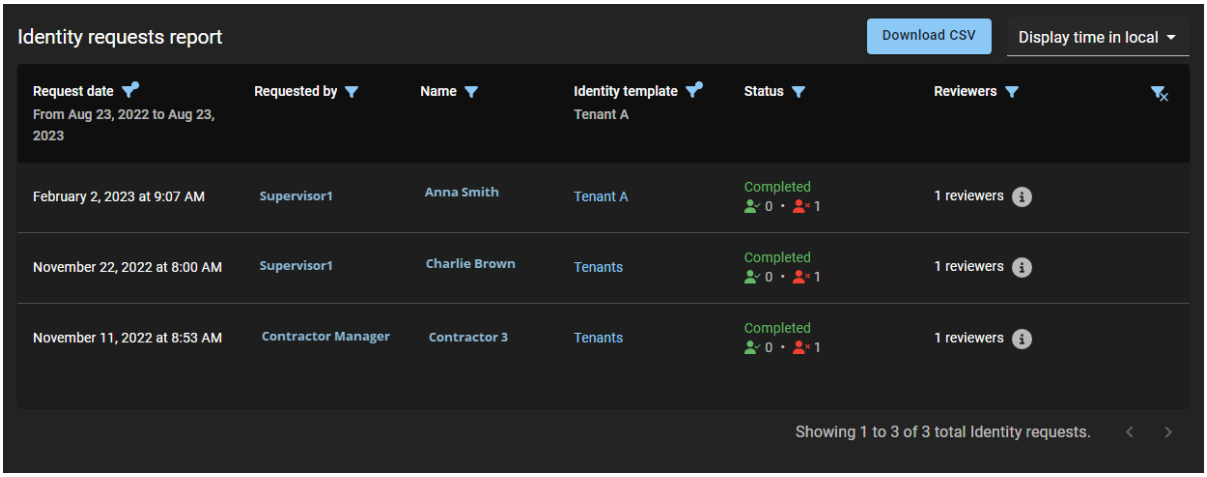
  - Personnalisation du thème de la borne
  - Mises à jour de la traduction pour l'inscription et la radiation et des messages de bienvenue et d'assistance.

  Pour en savoir plus, voir Personnaliser la configuration de la borne en libre-service , page 585 ou Activer la gestion des visiteurs pour un site , page 257.

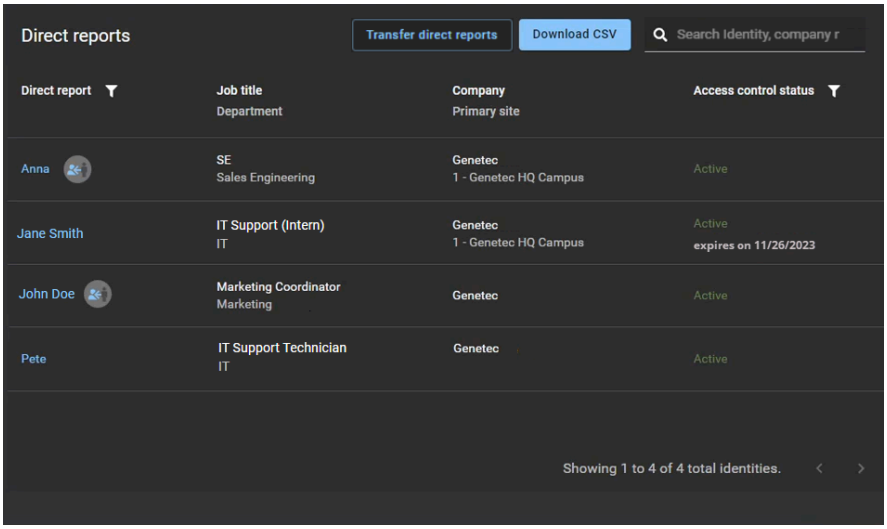
  Pour télécharger l'application mobile Genetec ClearID[MC] Self-Service Kiosk, rendez-vous sur l'App Store.

Nouveautés : Août 2023

- **Rapports :** ClearID intègre désormais deux rapports supplémentaires à des fins d'audit et de suivi :
  - **Rapport de demandes d'identité :** Les administrateurs de comptes peuvent désormais utiliser le rapport **Demandes d'identité** pour consulter toutes les activités associées.



  Pour en savoir plus, voir À propos des rapports , page 33, À propos du rapport de demandes d'identités , page 241 et Vérifier l'état des demandes d'identité , page 242.
  - **Rapport Subordonnés :** Les superviseurs ou les administrateurs de comptes peuvent désormais utiliser le rapport **Subordonnés** pour consulter l'état du contrôle d'accès et d'autres informations sur les subordonnés.



Pour en savoir plus, voir À propos des rapports , page 33, À propos du rapport Subordonnés , page 182 et Afficher les subordonnés , page 166.

- **Mise à jour du kit de borne :** Les kits ClearID Self-Service Kiosk intègrent et prennent désormais en charge l'iPad 10.9 pouces de 10e génération d'Apple.

  Pour en savoir plus, voir Options de la borne en libre-service , page 635 et Appareils pris en charge , page 78.

Nouveautés : Juillet 2023

- **Outil de synchronisation One Identity :** Genetec ClearID[MC] One Identity Synchronization Tool a été mis à jour pour simplifier la synchronisation et prendre en compte la fin de vie (End of Life ou EOL) de Microsoft® Azure AD Graph.

  IMPORTANT : La bibliothèque Microsoft Graph remplace la bibliothèque Azure Active Directory Graph (EOL depuis le **30 juin 2023** - Fin de vie de l'API Azure AD Graph). La nouvelle bibliothèque prend en charge toutes les correspondances précédentes.
  Qui est concerné ? Les clients ClearID qui utilisent **Azure AD** en tant que source de données pour synchroniser les identités dans ClearID avec One Identity Synchronization Tool.

  Pour en savoir plus, consultez la documentation officielle de Microsoft : Migrer vos applications d'Azure AD Graph vers Microsoft Graph.

  Étapes suivantes Contactez votre chargé de déploiement de l'équipe ClearID pour la mise à niveau de

  One Identity Synchronization Tool.

  REMARQUE : Si vous n'utilisez pas Azure AD en tant que source de données, vous n'êtes pas concerné par ce changement, et la mise à niveau est inutile.
  Pour en savoir plus sur l'outil de synchronisation, voir Synchroniser les identités avec One Identity , page 518.

  Pour en savoir plus sur les autorisations d'API Azure AD, voir À propos de l'application Web Azure , page 524.

Nouveautés : Juin 2023

- **Genetec ClearID Self-Service Kiosk 1.13.7 :** L'application mobile ClearID Self-Service Kiosk version 1.13.7 est désormais disponible.

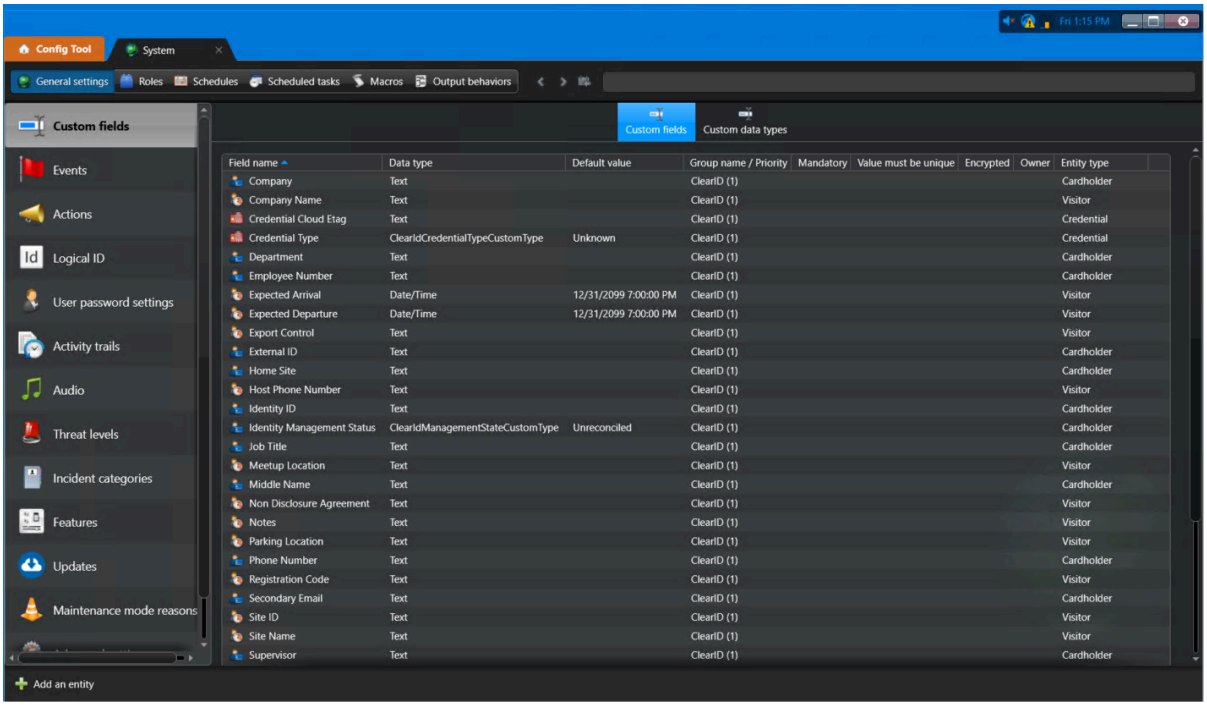
L'application mobile de la borne est désormais compatible avec les éléments suivants :

- Imprimante d'étiquettes Brother QL-820NWBc
- iOS 16
- 135 types de pièces d'identité nouveaux ou mis à jour

Pour en savoir plus, voir Appareils pris en charge , page 78, Options de la borne en libre-service , page 635, Configurer l'imprimante d'étiquettes de la borne en libre-service (Brother QL-820NWBc, QL-820NWB ou QL-810W) , page 602 et Types de pièces d'identité, page 646.
Pour télécharger l'application mobile Genetec ClearID[MC] Self-Service Kiosk, rendez-vous sur l'App Store.

Nouveautés : Mai 2023

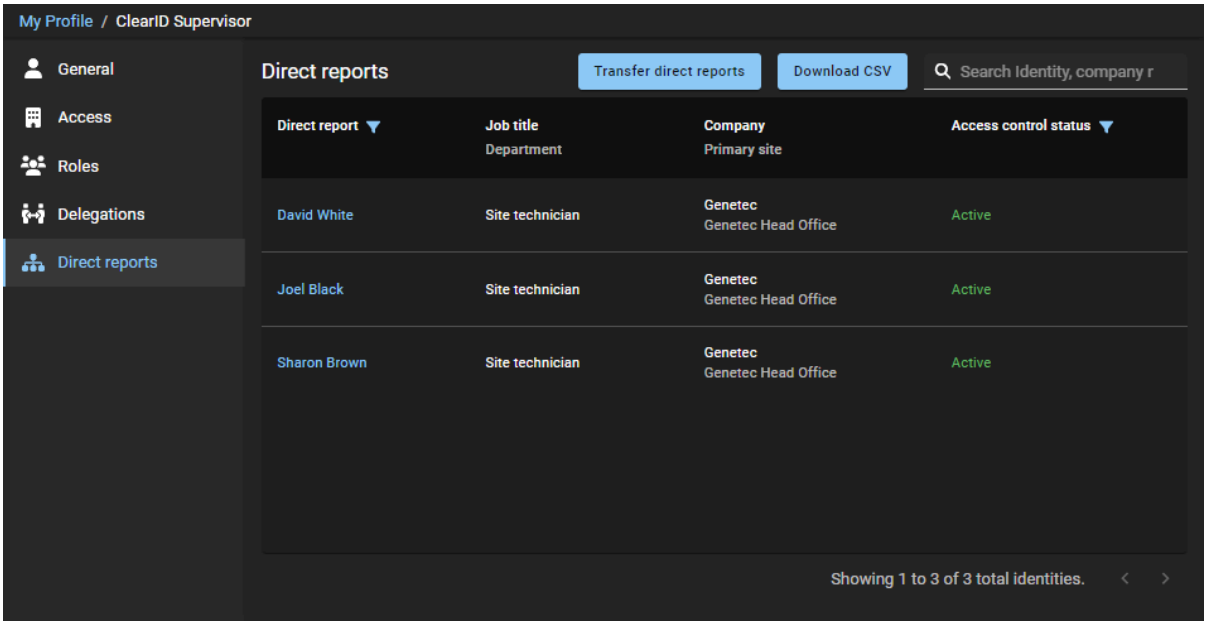
- **Mises à jour des champs personnalisés :** Les informations sur les champs personnalisés ClearID ont été mises à jour pour vous aider à mieux comprendre la relation entre les noms de champs d'identité ClearID et les champs de types d'entités Security Center.



Pour en savoir plus, voir À propos des champs personnalisés , page 103, Modifier les champs personnalisés , page 103 et Relations de champs personnalisés, page 107.

Nouveautés : Mars 2023

- **Transférer les subordonnés :** Les superviseurs, administrateurs de comptes ou identités ayant des droits en écriture pour les identités peuvent désormais transférer les subordonnés vers d'autres identités.



IMPORTANT : Cette fonctionnalité est conçue pour les identités qui sont gérées en local dans ClearID.

Si les identités sont gérées à l'aide d'une source de données externe, le transfert de subordonnés sera remplacé.

Pour en savoir plus, voir Transférer les subordonnés.

- **Modifications de la licence Synergis^{MC} :** Les modalités de la licence Synergis ont évolué. Pour Security Center 5.11 ou ultérieur (Synergis Base Enterprise ou Synergis Base Professional), le module de gestion des visiteurs Synergis est désormais inclus par défaut.

  REMARQUE : Le module de gestion des visiteurs Synergis est nécessaire si le client ClearID a la licence ClearID CD-SITE-VM-1Y.

  Pour en savoir plus, voir Options de licence , page 71.

Nouveautés : Février 2023

- **Genetec ClearID Self-Service Kiosk 1.13.6 :** L'application mobile Genetec ClearID Self-Service Kiosk version 1.13.6 est désormais disponible.

  L'application mobile Genetec ClearID Self-Service Kiosk version 1.13.6 prend désormais en charge les éléments suivants :

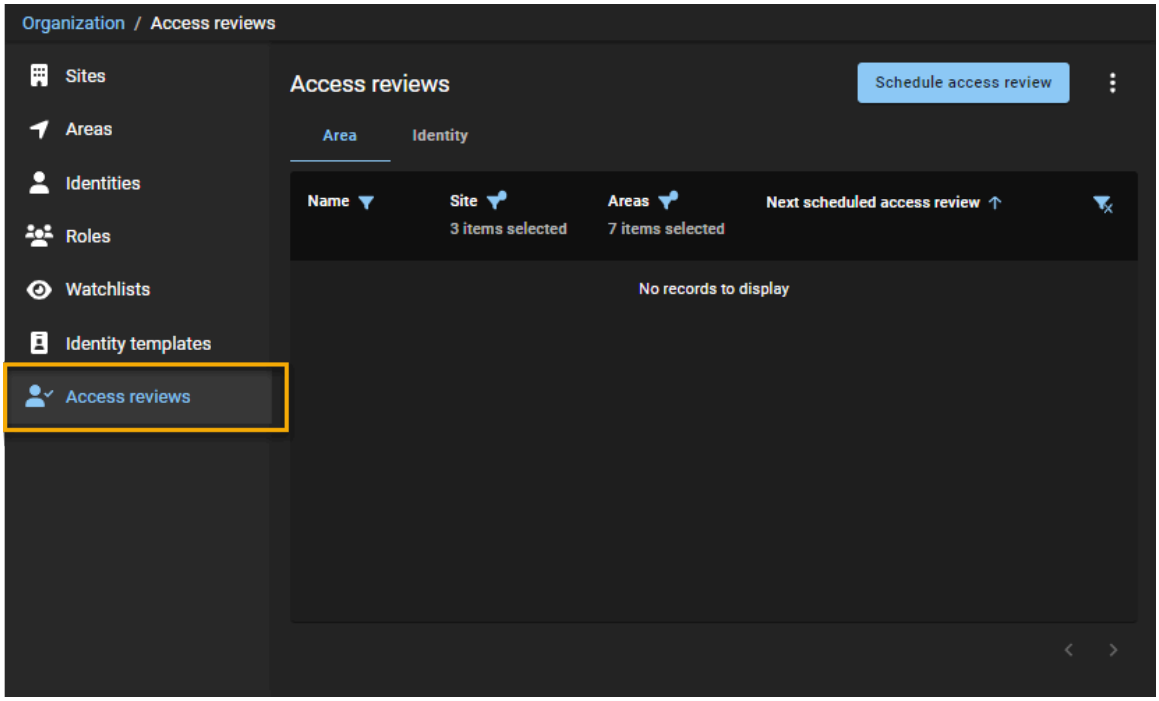
  - Imprimante thermique Brother TD-4550DNWB (avec étiquettes prédécoupées).

  Pour en savoir plus, voir Appareils pris en charge , page 78, Options de la borne en libre-service , page 635 et Configurer l'imprimante d'étiquettes de la borne en libre-service (Brother TD-4550DNWB) , page 612.

  Pour télécharger l'application mobile Genetec ClearID^{MC} Self-Service Kiosk, rendez-vous sur l'App Store.

IMPORTANT : Modifications de l'interface utilisateur

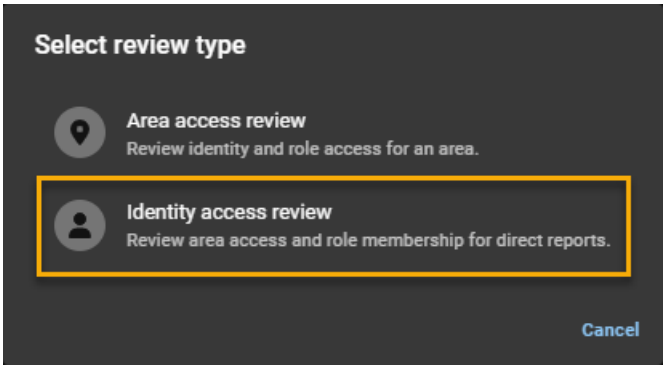
- **Les examens d'accès ont été déplacés :** Les examens d'accès précédents étaient créés et planifiés au niveau d'un site en cliquant sur **Organisation** > **Sites** > **Examens d'accès**. Les paramètres d'examens d'accès sont désormais configurés au niveau global en cliquant sur **Organisation** > **Examens d'accès**.



Améliorations apportées aux examens d'accès

- **Analyses d'accès :** Les examens d'accès incluent désormais une nouvelle option *d'examen d'accès d'identité*.

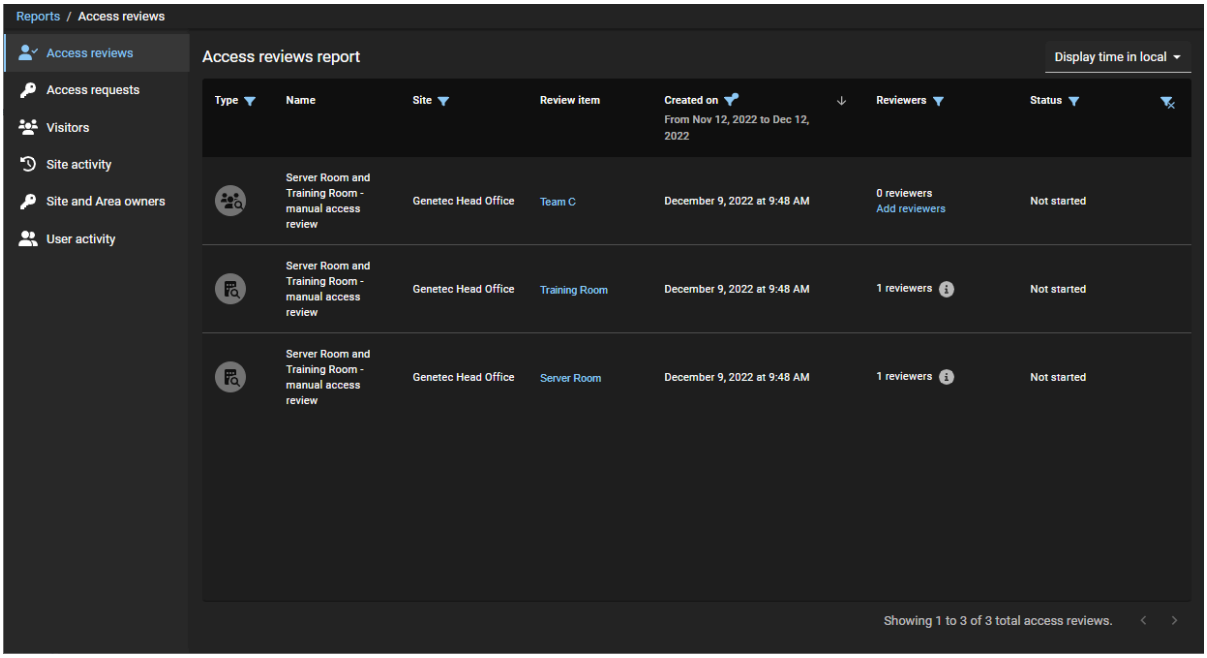
  Un examen d'accès d'identité est le processus par lequel un superviseur examine l'accès de ses subordonnés directs. Cet examen inclut la confirmation ou la mise à jour de l'accès au secteur, de la plage de dates du contrôle d'accès ou de l'appartenance à un rôle pour leurs subordonnés directs afin de garantir la conformité en matière de sécurité et la préparation à l'audit.



  Les examens d'accès incluent également des mises à jour de la boîte de dialogue **Planification de l'examen d'accès de site**.

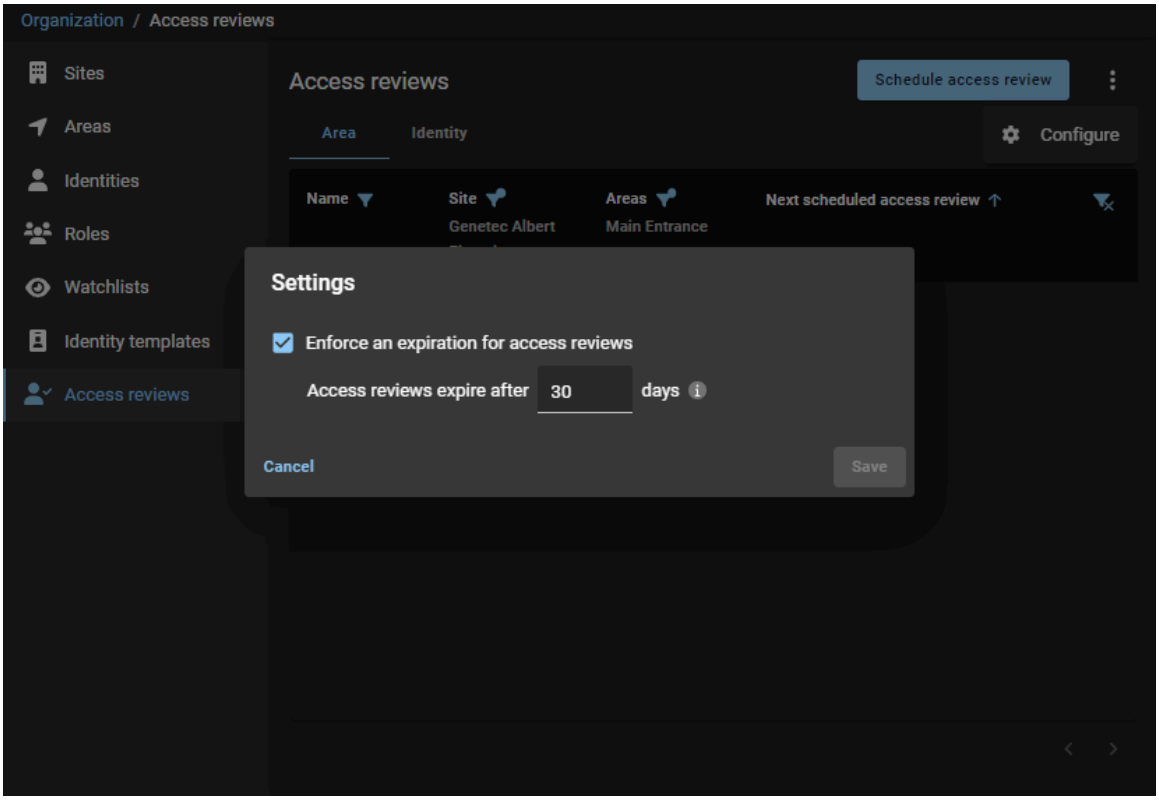
  Pour en savoir plus, voir Configurer les examens d'accès à un secteur , page 287 et Configurer les examens d'accès d'identité , page 293.

- **Mises à jour du rapport d'examen d'accès :** Le rapport d'examen d'accès inclut désormais des mises à jour des données de rapport et un filtrage.



Pour en savoir plus, voir À propos du rapport d’examen d'accès , page 298 et Vérifier l’état des examens d'accès , page 299.

- **Expiration automatique pour les examens d’accès :** Les administrateurs de compte peuvent désormais définir une période d’expiration automatique pour tous les examens d’accès.

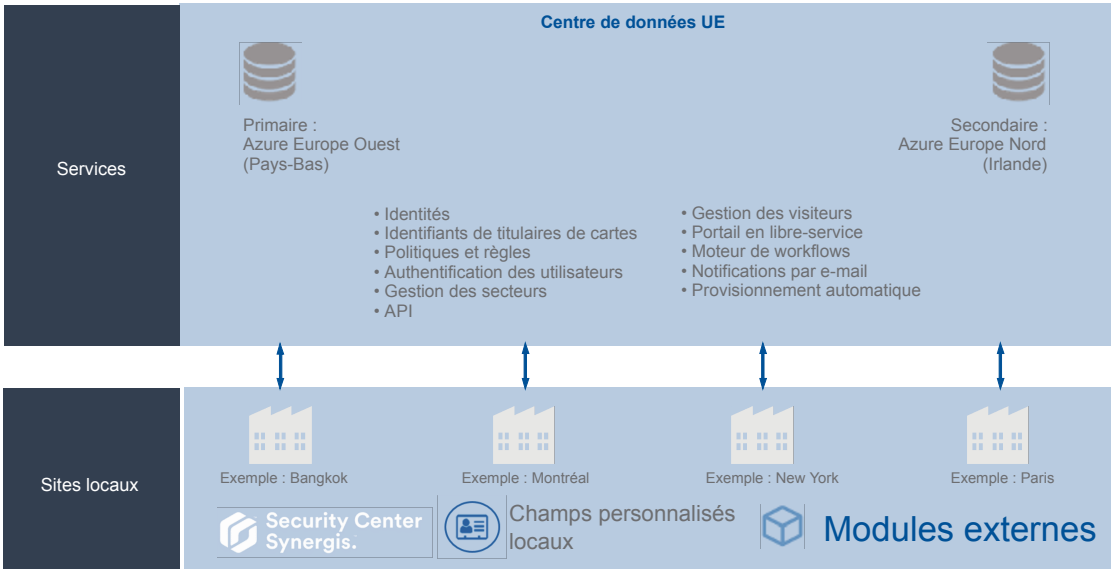


Pour en savoir plus, voir Configuration de l’expiration automatique pour les examens d’accès, page 285.

Nouveautés : Janvier 2023

- **Architecture uniquement pour l'Europe (DÉSORMAIS DISPONIBLE) :** ClearID propose désormais une solution exclusivement européenne pour les clients dont toutes les données doivent être stockées en Europe.

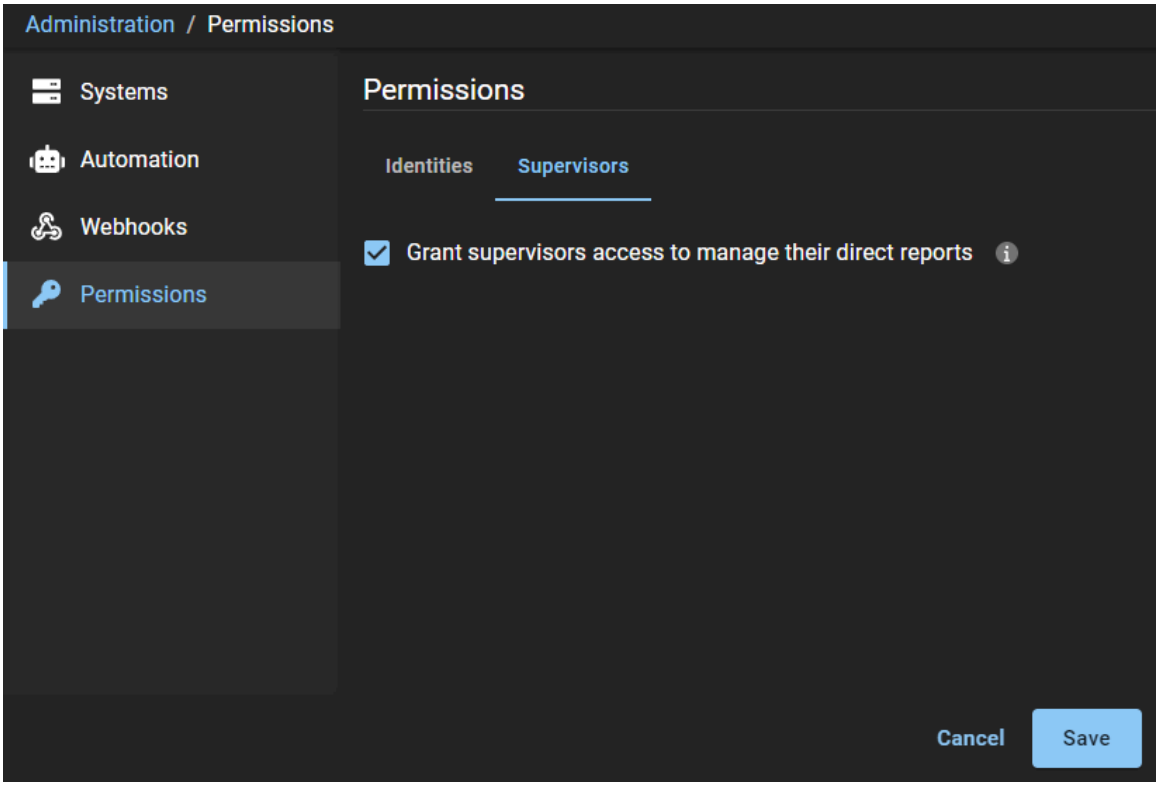
Genetec ClearID™ Architecture Europe uniquement



Pour en savoir plus, voir À propos de l'architecture de ClearID, page 5.

Nouveautés : Novembre 2022

- **Amélioration des autorisations du superviseur :** Les administrateurs peuvent maintenant accorder aux superviseurs plus de contrôle pour gérer leurs subordonnés. Les superviseurs peuvent désormais modifier les champs d'informations d'identité **Généraux** et les paramètres de **Contrôle d'accès**.



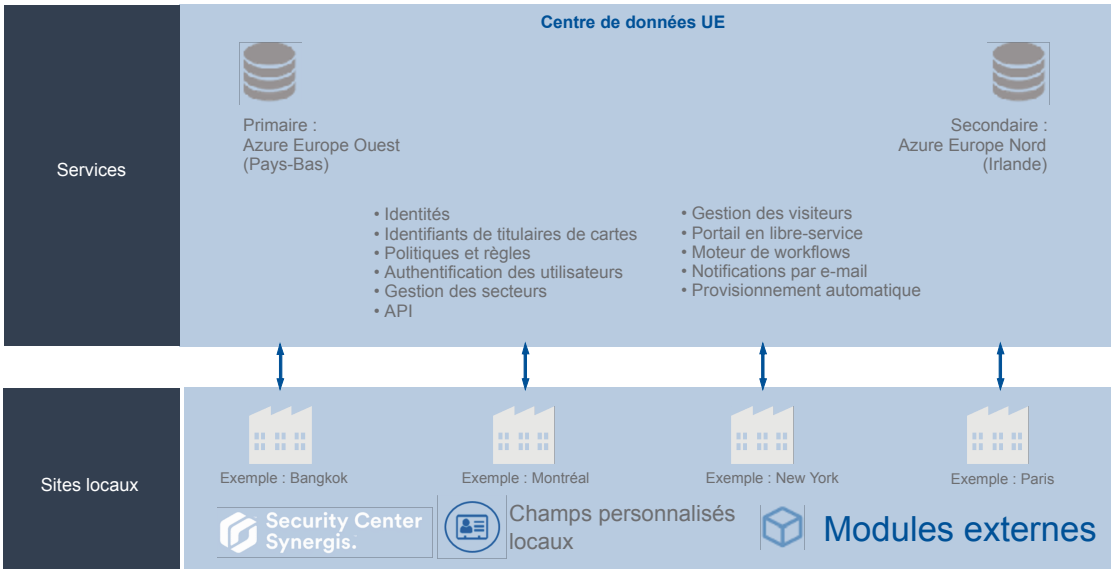
Cette option est utile pour toute organisation qui souhaite décentraliser certaines fonctions administratives en permettant aux superviseurs de gérer leurs subordonnés.

Pour en savoir plus, voir Gérer les subordonnés , page 169.

Nouveautés : Bientôt disponible

- **Architecture Europe uniquement (prochainement) :** ClearID propose désormais une solution exclusivement européenne pour les clients dont toutes les données doivent être stockées en Europe.

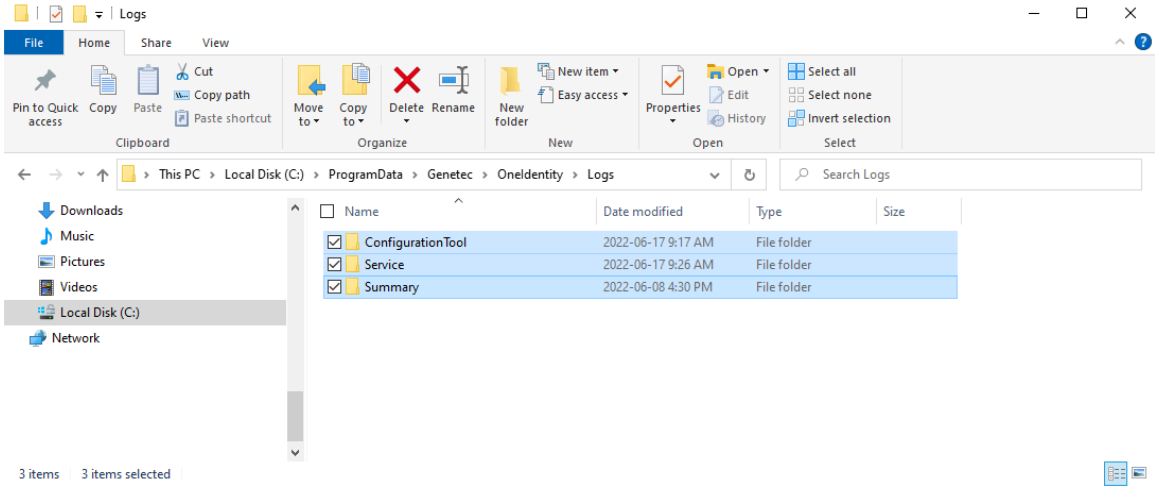
Genetec ClearID™ Architecture Europe uniquement



Pour en savoir plus, voir À propos de l'architecture de ClearID, page 5.

Nouveautés : Septembre 2022

- **Genetec ClearID One Identity Synchronization Tool :** Genetec ClearID One Identity Synchronization Tool a été mis à jour et prend désormais les fonctionnalités suivantes :
  - **Journalisation améliorée :** Des journaux récapitulatifs identifient les problèmes qui sont potentiellement survenus pendant la synchronisation. Consultez le fichier *Recap.txt* dans le dossier des journaux *Summary* pour un aperçu de la synchronisation.



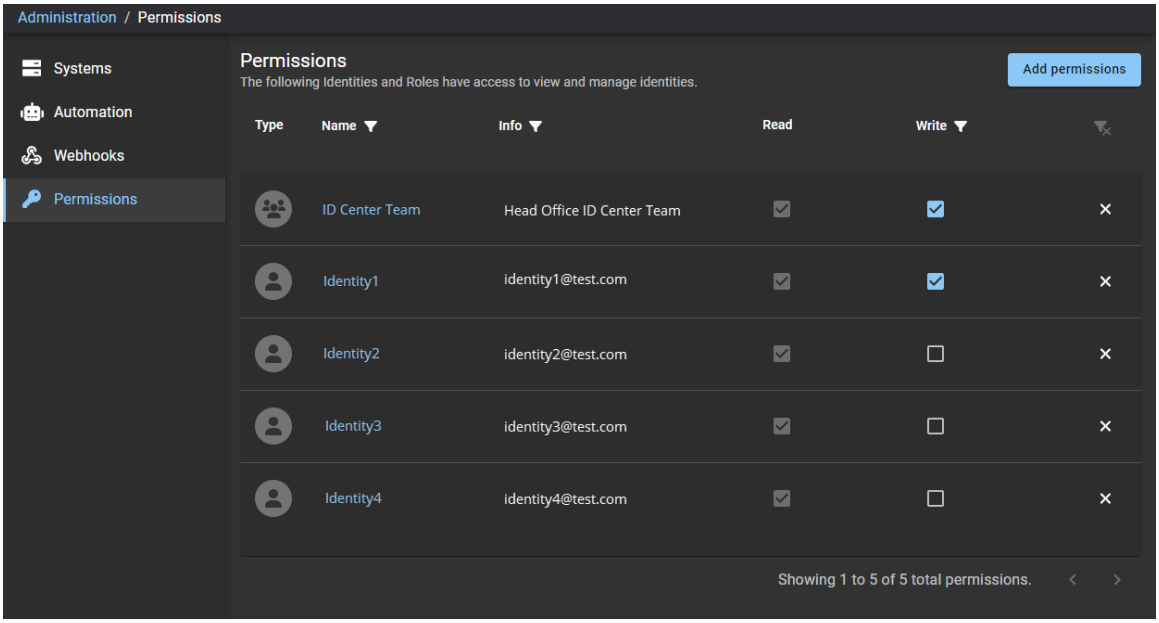
Pour en savoir plus, voir Consulter les journaux One Identity Synchronization Tool , page 566.

  - **La bibliothèque Microsoft Graph remplace la bibliothèque Azure Active Directory Graph. :** La bibliothèque Microsoft Graph remplace la bibliothèque Azure Active Directory Graph, désormais obsolète. La nouvelle bibliothèque prend en charge toutes les correspondances précédentes. Pour en savoir plus, voir À propos de l'application Web Azure , page 524.

Pour en savoir plus sur l'outil de synchronisation, voir Synchroniser les identités avec One Identity , page 518.

Nouveautés : Août 2022

- **Autorisations d'identité :** Les administrateurs de compte peuvent désormais ajouter des autorisations supplémentaires aux identités ou aux rôles afin que les utilisateurs puissent afficher ou gérer les identités.



Pour plus d'informations, voir Attribution de permissions supplémentaires.

Nouveautés : Juillet 2022

- **Genetec ClearID Self-Service Kiosk 1.13.3 :** L'application mobile Genetec ClearID Self-Service Kiosk version 1.13.3 est désormais disponible.

  L'application mobile Genetec ClearID Self-Service Kiosk version 1.13.3 prend désormais en charge les types de pièces d'identité (ID) suivants :

  - EAU - Permis de conduire
  - EAU - Carte d'identité
  - EAU - ID de résident

  Pour en savoir plus, voir Types de pièces d'identité, page 646.

  Pour télécharger l'application mobile Genetec ClearID[MC] Self-Service Kiosk, rendez-vous sur l'App Store.

Nouveautés : Mai 2022

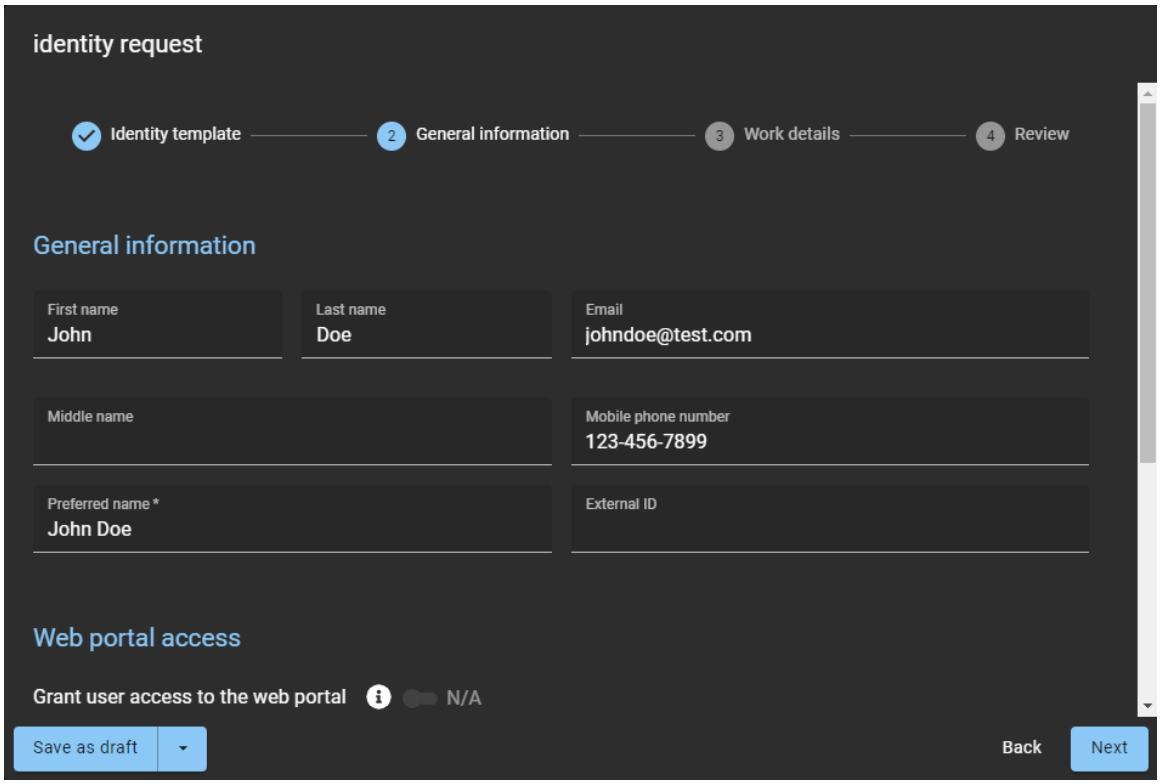
- **Meilleures pratiques ClearID :** Le manuel d'utilisation ClearID présente désormais les meilleures pratiques pour les situations suivantes :

  - Configurer ClearID pour un nouveau système Synergis.
  - Configurer ClearID pour un système Synergis existant.

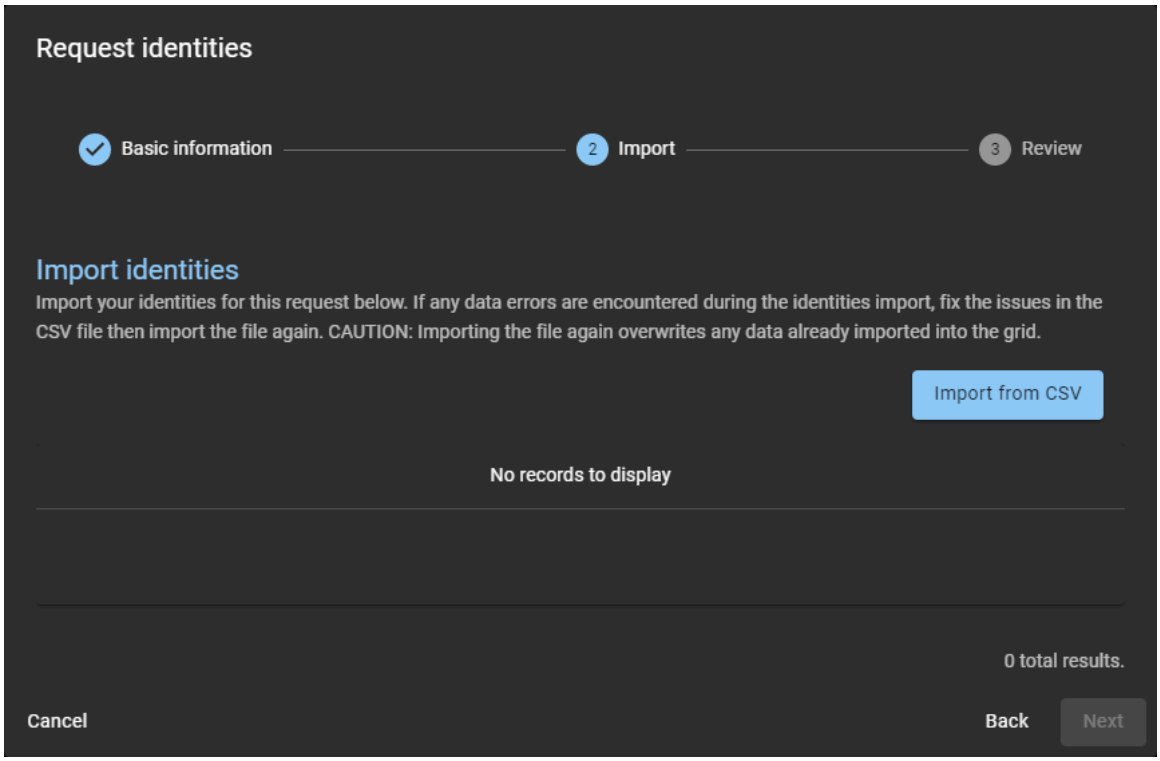
  Ces meilleures pratiques vous aideront à planifier le déploiement de votre système ClearID.

  Pour en savoir plus, voir Meilleures pratiques , page 81.
- **Demander des identités :** Un assistant Demande d'identité est désormais disponible pour envoyer une demande d'identité individuelle ou plusieurs demandes à la fois (par importation CSV) pour différents types d'employés ou de fournisseurs. Les demandes d'identité individuelles ou multiples peuvent être répétées à l'aide d'un modèle pour des employés particuliers qui doivent bénéficier d'un même accès à un site, un secteur ou un bâtiment particulier.

L’exemple suivant montre une demande d’identité individuelle :

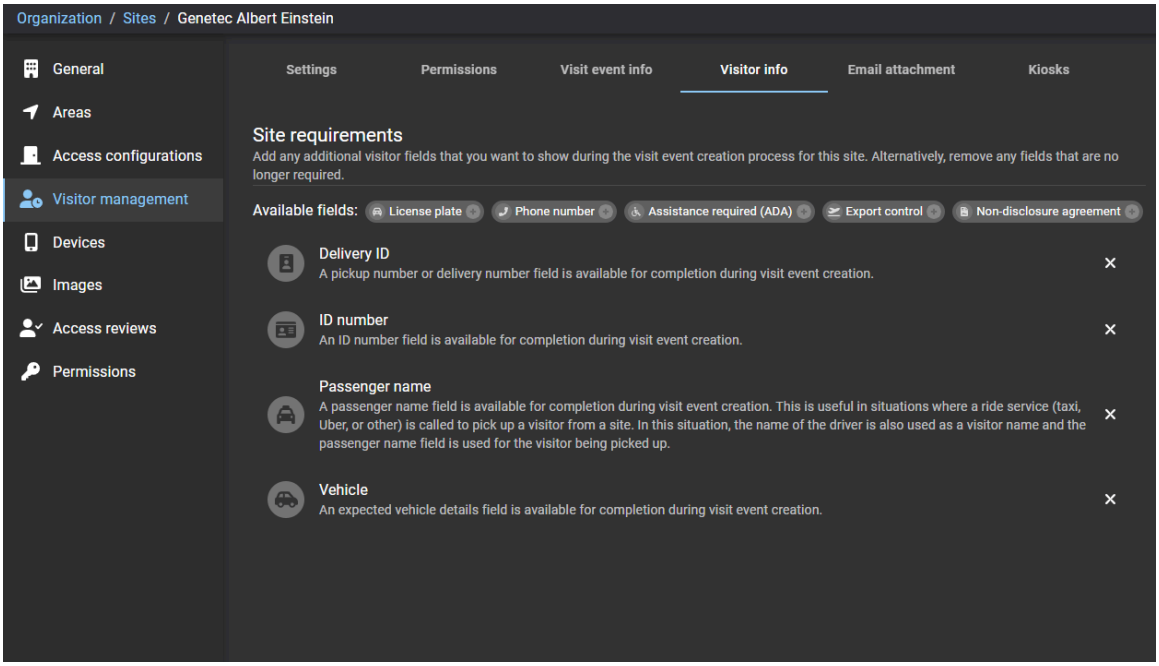


L’exemple suivant montre une demande d’identités (importation CSV) :



Pour en savoir plus, voir À propos des processus , page 12, Créer un modèle d'identité , page 211, Demander une identité , page 219 et Demander des identités multiples à l’aide de l’importation CSV , page 223.

- **Amélioration de la gestion des visiteurs :** La gestion des visiteurs pour les sites propose désormais en option des champs d’information supplémentaires sur les visiteurs :
  - ID de dépôt
  - Numéro d'ID
  - Nom du passager
  - Véhicule



Pour en savoir plus, voir l'onglet **Infos sur le visiteur** dans Activer la gestion des visiteurs pour un site , page 257.

Nouveautés : Mars 2022

- **Genetec ClearID Self-Service Kiosk 1.13.1 :** L'application mobile Genetec ClearID Self-Service Kiosk version 1.13.1 est désormais disponible.

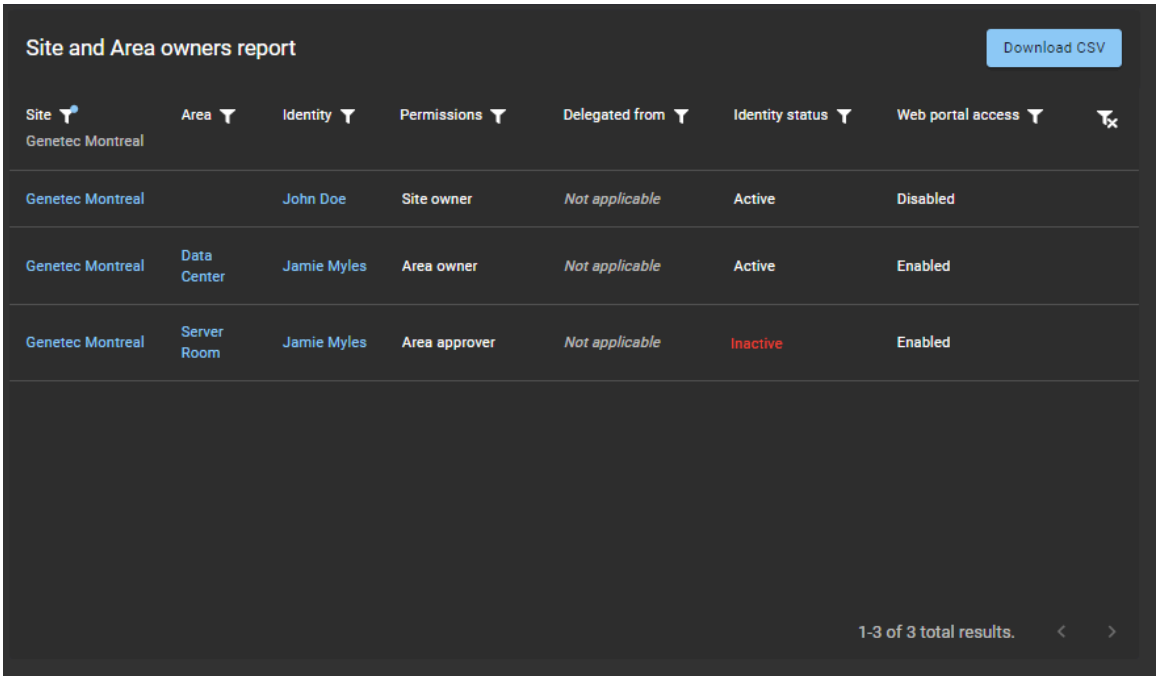
  L'application mobile ClearID Self-Service Kiosk version 1.13.1 prend désormais en charge 78 types de pièces d'identité (ID) supplémentaires ainsi que de nouveaux pays.

  Pour en savoir plus, voir Types de pièces d'identité, page 646.

  Pour télécharger l'application mobile Genetec ClearID[MC] Self-Service Kiosk, rendez-vous sur l'App Store.

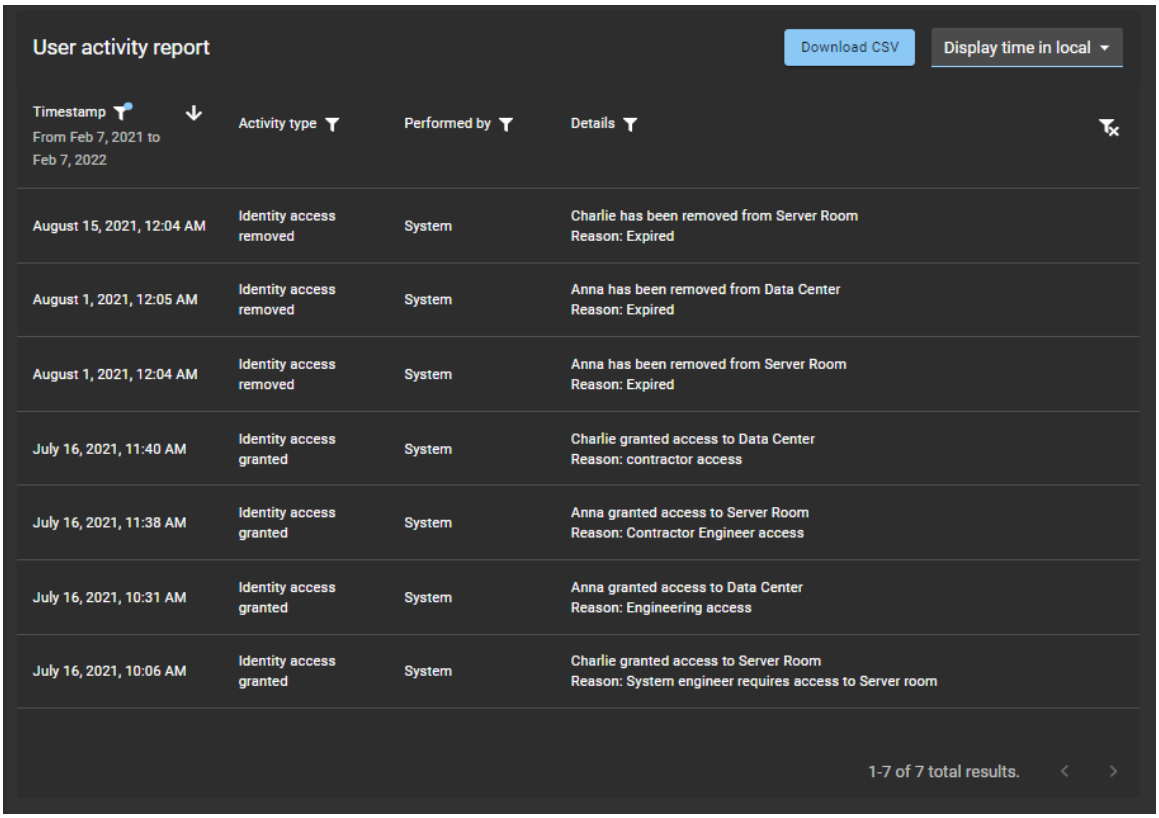
Nouveautés : Janvier 2022

- **Rapports :** ClearID propose désormais trois rapports supplémentaires à des fins d'audit et de suivi :
  - **Rapport Propriétaires de sites et de secteurs. :** Les administrateurs de comptes peuvent désormais utiliser le rapport **Propriétaires de sites et de secteurs** pour obtenir une vue d'ensemble des identités et de leurs autorisations. Lorsque le rapport est utilisé par un propriétaire de site, seules les informations sur ses propres sites sont affichées.



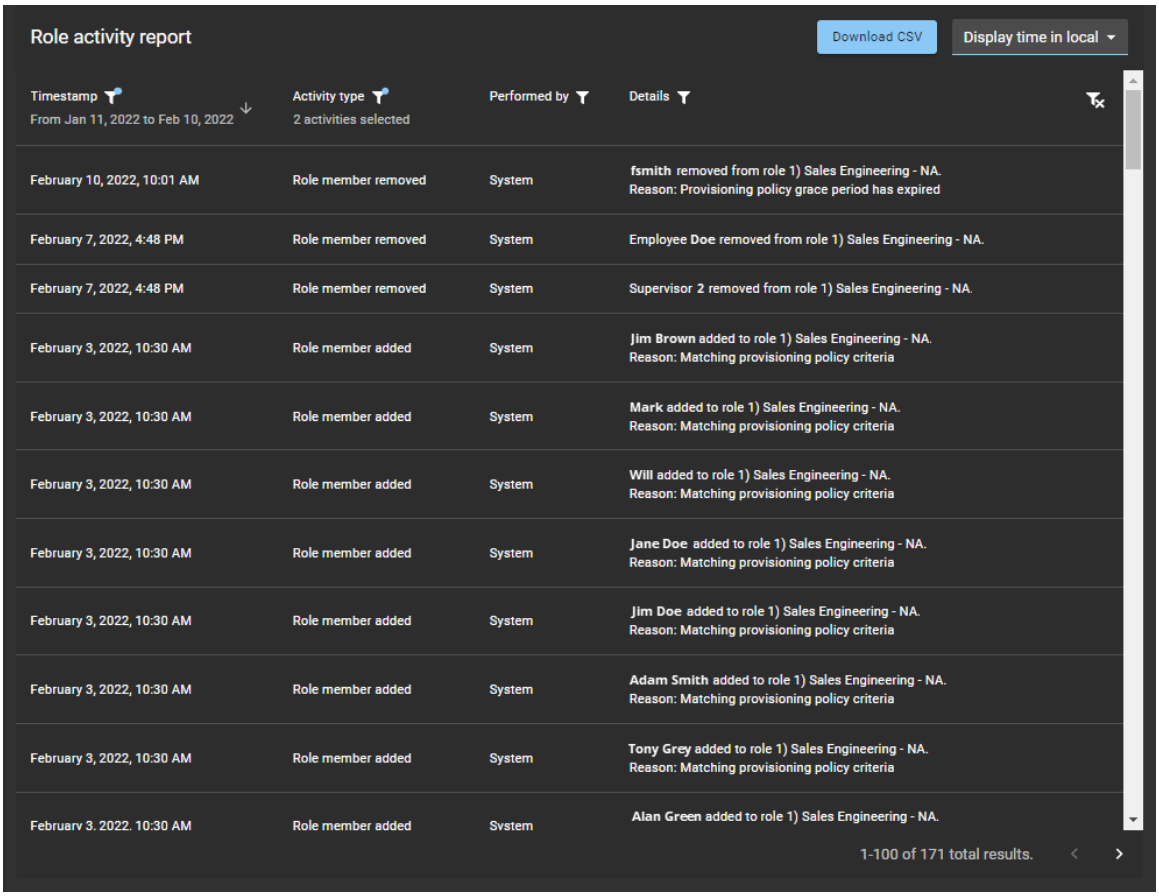
Pour en savoir plus, voir À propos des rapports , page 33 et Afficher le rapport Propriétaires de sites et de secteurs , page 337.

- **Rapport d'activité d'utilisateurs :** Les administrateurs de comptes peuvent désormais utiliser le rapport **Activité d'utilisateurs** pour consulter toutes les activités associées aux utilisateurs.



Pour en savoir plus, voir À propos des rapports , page 33 et Afficher un rapport d'activité d'utilisateurs , page 201.

- **Rapport d'activité de rôle :** Les administrateurs de comptes peuvent désormais utiliser le rapport **Activité de rôle** pour consulter toutes les activités associées aux rôles. Lorsque le rapport est consulté par un gestionnaire ou un propriétaire de rôle, seule l'activité associée à leurs rôles est affichée.



Pour en savoir plus, voir À propos des rapports , page 33 et Afficher un rapport d'activité de rôle , page 487.

Module externe ClearID

Le module externe ClearID est une nouvelle intégration pour Security Center 5.7 SR6 ou ultérieur.

3

Préparation du déploiement

Vérifiez les exigences de compatibilité et de déploiement.

Cette section aborde les sujets suivants:

- " Options de licence ", page 71
- " Compatibilité ", page 74
- " Configuration système requise ", page 75
- " Ports de pare-feu ", page 76
- " Appareils pris en charge ", page 78
- " Meilleures pratiques ", page 81

Options de licence

Utilisez les informations suivantes pour comprendre les licences disponibles pour Genetec ClearID[MC] ou la borne Genetec[MC] ClearID[MC] Self-Service Kiosk. Pour mettre à jour votre licence, contactez-nous en indiquant les références mentionnées dans cette rubrique.

Options de licence ClearID

Référence	Description	Conditions
CD-STANDARD-1Y	Abonnement d'un an pour un site pour une identité ClearID ; moins de 1000 entités.	Cette référence est obligatoire pour utiliser ClearID.
CD-SITE-1Y	Abonnement d'un an pour un site ClearID. L'abonnement inclut le provisionnement automatique, le portail en libre-service et l'affectation de propriétaires de groupes et de secteurs.	Vous devez souscrire au moins un abonnement à un site pour utiliser ClearID.
CD-SITE-VM-1Y	Abonnement d'un an pour un site ClearID. Cet abonnement inclut le provisionnement automatique, le portail en libre-service, l'affectation de propriétaires de groupes et de secteurs, la gestion des visiteurs et les listes de surveillance (contrôle des visiteurs internes uniquement). **REMARQUE :** Cette référence ne concerne que les options du module de gestion des visiteurs.	Vous devez souscrire au moins un abonnement à un site pour utiliser ClearID.
CD-SITE-VM-XTRA-VISITS-1Y (Facultatif)	La licence pour les visites supplémentaires ajoute 50 000 visites à la licence sur site de gestion des visiteurs CD-SITE-VM-1Y pendant un an.	
CD-IDSYNC-SERVICE-1Y (Facultatif)	Service d'abonnement qui synchronise les identités depuis une source de données externe : Active Directory (AD), fichier (CSV), base de données (Microsoft SQL Server, Oracle Database ou ODBC), Azure AD ou API personnalisée durant un an.	**IMPORTANT :** Utilisez CD-IDSYNC-SERVICE-1Y si vous devez synchroniser une source de données externe.
CD-KIOSK-LIC-1Y	Licence d'abonnement annuel pour une borne (Remises disponibles à partir de dix bornes)	Cette licence est utilisée en combinaison avec différentes options matérielles pour la borne en libre-service.

REMARQUE : Références également disponibles pour des abonnements de trois et cinq ans. Des remises sont également disponibles pour les achats en volume.

Options de licence Synergis

Pour synchroniser les données entre ClearID et Synergis[MC], l'une des références suivantes est requise :

REMARQUE : Les options de licence Synergis suivantes intègrent toutes la référence CD-SC-PLUGIN par défaut. Ce pack fournit une licence pour une connexion aux services ClearID dans le cloud. Il vous faut une licence par Répertoire.

Référence	Description	Conditions
GSC-BASE-E **5.11 ou ultérieur**	Le pack Synergis Enterprise de base. **REMARQUE :** Le pack de base intègre par défaut le module de gestion des visiteurs Synergis.	
GSC-BASE-P **5.11 ou ultérieur**	Le pack Synergis Enterprise de base. **REMARQUE :** Le pack de base intègre par défaut le module de gestion des visiteurs Synergis.	
GSC-Sy-E **Versions antérieures à la 5.11**	Le pack Synergis Enterprise contient une licence pour les éléments suivants : • Prise en charge du Gestionnaire d'accès • Security Desk distant • Concepteur de badges	Pour en savoir plus, voir la section suivante sur la gestion des visiteurs.
GSC-Sy-P **Versions antérieures à la 5.11**	Le pack Synergis Professional contient une licence pour les éléments suivants : • Deux gestionnaires d'accès • 256 lecteurs maximum • Dix clients maximum • Security Desk distant • Concepteur de badges	Pour en savoir plus, voir la section suivante sur la gestion des visiteurs.
SCS-Base	Security Center SaaS Edition (Classic) - Pack de base **REMARQUE :** Le pack de base intègre par défaut le module de gestion des visiteurs Synergis.	

Options de licence pour la gestion des visiteurs

IMPORTANT : Si vous utilisez GSC-Sy-E ou GSC-Sy-P, l'une des références Synergis suivantes est requise pour la gestion des visiteurs :

Référence	Description	Conditions
GSC-Sy-E-Vis **Versions antérieures à la 5.11**	Ce pack contient une licence pour le module *gestion des visiteurs*.	Synergis Enterprise est obligatoire si vous activez le module de gestion des visiteurs.
GSC-Sy-P-Vis **Versions antérieures à la 5.11**	Ce pack contient une licence pour le module gestion des visiteurs.	Synergis Professional est obligatoire si vous activez le module de gestion des visiteurs.

REMARQUE : Pour les sites avec gestion des visiteurs, la licence peut inclure du matériel de borne et une licence de borne.
Pour les derniers tarifs, voir Genetec Parts Manager ou contactez le service commercial.

Votre licence Security Center contient-elle toutes les options dont vous avez besoin ?

En plus du certificat pour le module externe, vérifiez que votre licence Security Center inclut toutes les options que vous comptez utiliser dans Security Center. Par exemple, si vous avez intégré un système qui gère les visiteurs, vous aurez besoin de l'option Gestion des visiteurs dans Security Center. Si une option est manquante, un message d'erreur est affiché lorsque le serveur tente de créer ou modifier l'entité associée à l'option concernée.

Pour la liste des options de licence disponibles, voir « Options de licence » dans le *Guide de l'administrateur Security Center*.

Rubriques connexes

Présentation de l'intégration, page 15

Compatibilité

Le portail web Genetec ClearID[MC] et le module externe ClearID sont compatibles avec Security Center 5.11 ou ultérieur.

Le portail Web et le module externe prennent en charge les versions de Security Center pour une durée maximale de 3 ans à compter de la date de sortie de la première version GA.

Versions de Security Center prises en charge

Reportez-vous aux informations suivantes pour comprendre quand chaque version de Security Center cessera d'être prise en charge pour une utilisation avec ClearID :

Version de Security Center	Date de sortie de la première version GA de Security Center	Fin de prise en charge de Security Center dans ClearID
5.11	Septembre 2022	Septembre 2025
5.12	Décembre 2023	Décembre 2026
5.13	Décembre 2024	Décembre 2027

IMPORTANT : Vous devez avoir Synergis[MC] Professional ou Enterprise pour utiliser ClearID. Pour en savoir plus, voir Options de licence , page 71.

Configuration système requise

Pour un fonctionnement efficace du système Genetec ClearID[MC] dans votre navigateur Web, l'ordinateur ou l'appareil mobile que vous utilisez doit répondre à certaines exigences logicielles et matérielles.

Voici la configuration requise pour l’application Web ClearID :

Configuration requise pour les ordinateurs

- Les cookies et JavaScript sont activés dans votre navigateur Web.

L'application Web ClearID est compatible avec les navigateurs suivants :

- Google Chrome (dernière version)
- Microsoft® Edge (dernière version)

Configuration requise pour le module externe ClearID

La configuration système suivante est requise pour exécuter le module externe ClearID :

Synergis Professional ou Omnicast Professional est requis pour la prise en charge des modules externes dans Security Center.

Matériel

Le module externe ClearID doit être installé sur un serveur qui répond aux spécifications serveur recommandées décrites dans la configuration système requise pour Security Center.

Réseau

Le serveur sur lequel le module externe est installé doit avoir un accès à Internet pour permettre la connexion entre Synergis[MC] et les services ClearID dans le cloud. Toutes les communications utilisent le port TCP 443.

IMPORTANT : Toutes les données transférées vers l’application Web ClearID sont chiffrées en transit et au repos.

Ports de pare-feu

La configuration suivante des ports, des URL et du réseau est nécessaire pour assurer le bon fonctionnement de Genetec ClearID[MC].

Portail Web ClearID

La configuration réseau suivante est requise pour le portail Web :

- Port TCP 443 sortant
- **.clearid.io* - Autoriser tout le trafic sortant pour ce domaine
- **.core.windows.net* - Autoriser tout le trafic sortant pour ce domaine
- **.launchdarkly.com* - Autoriser tout le trafic sortant pour ce domaine

Module externe ClearID

La configuration réseau suivante est requise pour le module externe :

- Port TCP 443 sortant
- **.clearid.io* - Autoriser tout le trafic sortant pour ce domaine
- **.servicebus.windows.net* - Autoriser tout le trafic sortant pour ce domaine
- **.core.windows.net* - Autoriser tout le trafic sortant pour ce domaine

REMARQUE : Le serveur sur lequel le module externe est installé doit avoir un accès à Internet pour permettre la connexion entre Synergis[MC] et les services ClearID dans le cloud.

Genetec ClearID[MC] One Identity Synchronization Tool

La configuration réseau suivante est requise pour l'outil de synchronisation One Identity :

- Port TCP 443 sortant
- **.clearid.io* - Autoriser tout le trafic sortant pour ce domaine

Genetec ClearID[MC] LDAP Synchronization Agent

La configuration réseau suivante est requise pour l'agent de synchronisation LDAP :

- Port TCP 443 sortant
- **.clearid.io* - Autoriser tout le trafic sortant pour ce domaine

Genetec ClearID[MC] Self-Service Kiosk

Les fonctionnalités ou configurations réseau suivantes sont requises pour la borne en libre-service :

- Port TCP 443 sortant
- **.clearid.io* - Autoriser tout le trafic sortant pour ce domaine
- Imprimante d'étiquettes **(mode Wi-Fi seulement)** Bonjour - utilisé pour la découverte d'appareils
- Imprimante d'étiquettes **(mode Wi-Fi seulement)** SNMP - utilisé pour obtenir des informations sur l'état de l'imprimante
- Imprimante d'étiquettes **(mode Wi-Fi seulement)** Port UDP ou TCP 9100 - pour envoyer les données d'impression

Autres exigences

Les ressources suivantes sont utilisées par ClearID pour enrichir l’expérience utilisateur, mais elles sont facultatives.

Google Maps :

- https://www.google.com/
- https://maps.googleapis.com
- https://fonts.googleapis.com/
- https://maps.gstatic.com/

Microsoft Application Insights :

- https://dc.services.visualstudio.com/
- https://dc.applicationinsights.azure.com/
- https://dc.applicationinsights.microsoft.com/

REMARQUE : Ces ressources ne sont pas obligatoires pour utiliser le portail ClearID, mais certains éléments de l'interface utilisateur risquent de ne pas être formatés correctement en leur absence.

Appareils pris en charge

Pour savoir quels appareils sont pris en charge pour utiliser Genetec ClearID[MC] ou Genetec ClearID[MC] Self-Service Kiosk, reportez-vous à la liste des appareils pris en charge.

Pour chaque appareil, le micrologiciel et le niveau de certification sont indiqués.

- **Certifié :** Genetec Inc. a testé et validé l'appareil.
- **Conception compatible :** Cet appareil a les mêmes caractéristiques qu'un appareil certifié, mais n'a pas été testé ou validé par Genetec Inc.

Appareils pour les bornes

Les appareils iPad suivants sont pris en charge avec ClearID Self-Service Kiosk.

Fabricant	Modèle	Type d'appareil	Version
Apple	Non applicable	• iPad 10,9 pouces[1] • iPad 10,2 pouces[2]	**Certifié :** iOS 16.1 ou ultérieur

REMARQUE :

- [1] D'autres modèles d'iPad peuvent également être pris en charge (sans le support de borne) s'ils exécutent la version minimale d'iOS requise pour l'application mobile Kiosk. Vous pouvez par exemple utiliser un iPad Pro. Toutefois, en raison de ses dimensions, l'iPad Pro n'est pas compatible avec le support de borne. Pour en savoir plus sur les exigences relatives à l'adaptateur secteur pour iPad, voir Options de la borne en libre-service , page 635.
- [2] Nous ne commercialisons plus l'iPad de 10,2 pouces ni le support pour borne associé.

Imprimante d'étiquettes pour les bornes

Les imprimantes d'étiquettes suivantes sont prises en charge avec ClearID Self-Service Kiosk.

Fabricant	Modèle	Type d'appareil	Version
Brother	QL-820NWBc (réseau, Wi-Fi, Bluetooth) **REMARQUE :** Seules les étiquettes DK-2205 ou DK2251 (62mm en noir ou en rouge et noir) sont prises en charge avec cette imprimante.	Imprimante d'étiquettes thermique	**Conception compatible**
Brother	QL-820NWB (réseau, Wi-Fi, Bluetooth)	Imprimante d'étiquettes thermique	**Conception compatible (OBSOLÈTE)** **REMARQUE :** Le modèle QL-820NWBc remplace l'imprimante QL-820NWB qui n'est plus commercialisée.
Brother	QL-810W	Imprimante d'étiquettes thermique	**Conception compatible**

Fabricant	Modèle	Type d'appareil	Version
	(Wi-Fi seulement)		
Brother	TD-4550DNWB (réseau, Wi-Fi, Bluetooth) **REMARQUE :** Seules les étiquettes RD001U1S (57mm en noir) sont prises en charge avec cette imprimante.	Imprimante d'étiquettes thermique	**Conception compatible**

Appareils de codes QR (lecteur de codes à barres 2D)

Les appareils suivants sont pris en charge pour utiliser les codes QR avec ClearID en tant qu'identifiants pour les visiteurs.

Fabricant	Gamme	Modèle	Type d'appareil	Version
IBC	Qscan	Qscan (pour aires de stationnement)	Scanneur de codes à barres	**Prise en charge native :** Micrologiciel qswie26m.bin
IBC	Qscan	QscanT (pour les tourniquets)	Scanneur de codes à barres	**Conception compatible**
IBC	Qscan	QscanI (version d'intérieur)	Scanneur de codes à barres	**Conception compatible**
Zebra	DS9300	DS9308	Scanneur de codes à barres	**Conception compatible**

Appareils OSDP STid

Les appareils OSDP STid suivants sont pris en charge avec ClearID pour utiliser les codes QR en tant qu'identifiants pour les visiteurs.

Fabricant	Gamme	Modèle	Référence	Type d'appareil	Version
STid	Architect®	ARC-AQ	SY-ARC-W33-AQPH5-7OS1	Lecteur de codes QR • Classic Reader • QR Code Module	**Conception compatible** Tous les lecteurs STid avec la version 10 ou ultérieure du micrologiciel[1]
STid	Architect®	ARC-BQ	SY-ARC-W33-BQPH5-7OS1	Lecteur de codes QR • Keypad Reader • Module QR	**Conception compatible** Tous les lecteurs STid avec la version 10 ou

Fabricant	Gamme	Modèle	Référence	Type d'appareil	Version
					ultérieure du micrologiciel[1]
STid	Architect® Blue	ARCS-AQ/BT	SY-ARCS-W33-AQBT1-7OS1	Lecteur de codes QR • Lecteur classique • Crypto processor • Module code QR • Bluetooth	**Conception compatible** Tous les lecteurs STid avec la version 10 ou ultérieure du micrologiciel[1]
STid	Architect® Blue	ARCS-BQ/BT	SY-ARCS-W33-BQBT1-7OS1	Lecteur de codes QR • Keypad Reader • Crypto processor • Module code QR • Bluetooth	**Conception compatible** Tous les lecteurs STid avec la version 10 ou ultérieure du micrologiciel[1]
STid	SECard[2] - High security programming kit (logiciel de configuration de lecteur de codes QR)	Non applicable	KIT-SECARD-BT-V3.X	• Codeur USB STid ARC-G • Clé USB contenant le logiciel SECard	**Conception compatible** Version 3.5 ou ultérieure du logiciel

Clé des codes de modèle STid :

- ARCS = processeur de chiffrement
- AQ = lecteur + code QR
- BQ = pavé numérique + code QR
- BT = Bluetooth

[1] Si vous réutilisez des lecteurs existants, reportez-vous à la *documentation STid* pour savoir comment les mettre à niveau avec la version 10 ou ultérieure du micrologiciel.

IMPORTANT : [2] Genetec Inc. n'assure pas une assistance sur la solution SECard de STid. Les clients doivent utiliser la version autonome du logiciel SECard de STid pour configurer le fonctionnement des lecteurs OSDP STid avec le tableau de SCA ClearID.

Rubriques connexes

Options de la borne en libre-service, page 635

Configuration système requise, page 75

Meilleures pratiques

Suivez ces meilleures pratiques pour vous aider à planifier, concevoir et configurer avec succès le déploiement de vos systèmes Genetec ClearID[MC].

Ces informations sont destinées aux utilisateurs finaux, aux intégrateurs ou aux personnes chargées de la planification, de la conception et de la configuration d'un système ClearID.

Consultez les meilleures pratiques suivantes avant de planifier vos déploiements :

- Configurer ClearID pour un nouveau système Synergis, page 81
- Configurer ClearID avec un système Synergis existant, page 82

Configurer ClearID pour un nouveau système Synergis

Tenez compte des meilleures pratiques suivantes lorsque vous concevez un nouveau système Synergis[MC] compatible avec Genetec ClearID[MC] pour une mise en œuvre éventuelle de ClearID.

Ces informations sont destinées aux utilisateurs finaux, aux intégrateurs ou aux personnes chargées de la planification, de la conception et de la configuration d'un système ClearID.

IMPORTANT : Chaque système a des exigences particulières, et ces meilleures pratiques ne peuvent pas suffire pour déployer un système. Les étapes de déploiement varient en fonction de l'architecture et de la configuration existante de votre organisation.

- Utilisez ces informations comme point de départ à des fins de planification de base.
- Si vous avez besoin d'une assistance lors de votre déploiement, adressez-vous à votre contact de déploiement.

BONNE PRATIQUE : Veillez à toujours tester la mise en œuvre d'un nouveau déploiement en environnement de démo avant de passer le système en production.

Tâches en amont du déploiement de ClearID

1. Planifiez vos **Sites** et vos **Secteurs** en fonction de vos exigences en matière d'accès.

   CONSEIL : Pensez à des noms parlants qui évoquent les **sites** ou les **secteurs** qui seront demandés par les utilisateurs.

   a. Identifiez les *Sites* et les *Secteurs* pour lesquels vous souhaitez contrôler les accès.

      - Exemples de sites : Bâtiment principal, bureau satellite 1, bureau satellite 2, etc.
      - Exemples de secteurs : 1er étage, 2e étage, salle des serveurs, auditorium, etc.

      REMARQUE : Un site correspond généralement à un bâtiment physique ou à un groupe de bâtiments connexes. La configuration du site s'applique à l'intégralité du site, et doit donc être contrôlée par les mêmes ensembles de règles (configurations des accès et configurations de la gestion des visiteurs).

   b. Identifiez les *Rôles* dont vous aurez besoin pour regrouper les accès et les identités.

      - Exemples de rôles : Ventes, Marketing, Direction, Faculté, Étudiants, Équipe d'exploitation, Fournisseurs, Employés permanents, Employés à temps partiel, etc.

   c. (Facultatif) Envisagez le provisionnement basé sur les attributs afin d'automatiser l'affectation aux rôles.

   REMARQUE : Notez ces sites, secteurs et rôles, dont vous aurez besoin au cours des tâches de déploiement (étapes 3, page 82 et 4, page 82) détaillées plus loin.

2. (Facultatif) Testez votre configuration dans un environnement ClearID de démonstration.
   a. Reliez votre compte ClearID de démo à un système Synergis de démo.
   b. Contactez votre chargé de compte Genetec Inc. pour demander un compte ClearID DEMO ainsi qu'un système Synergis de démo.
      IMPORTANT : La configuration effectuée en environnement de démo ne peut pas être transférée vers un système en production.

Tâches de déploiement

1. Reliez votre nouveau système Synergis en production à votre compte ClearID en production.
   a. Installez le module externe ClearID.
   b. Connectez Security Center à ClearID.
2. Synchronisez les identités avec votre source de données.

   Selon vos besoins particuliers, procédez de l'une des manières suivantes :

   - Synchronisez vos identités avec Genetec ClearID[MC] One Identity Synchronization Tool.
   - Synchronisez vos identités en passant par l'API.
3. Sur le portail Web ClearID, créez les **sites** et les **secteurs** que vous avez recensés plus tôt.
   a. Créez vos sites.
   b. Créez vos secteurs.
4. Sur le portail Web ClearID, créez les **rôles** et les **règles de provisionnement basées sur les attributs** que vous avez définies plus tôt.
   a. Créez vos rôles.
   b. (Facultatif) Créez des règles de provisionnement basées sur les attributs afin d'automatiser l'affectation aux rôles.

Rubriques connexes

À propos des relations entre les titulaires de carte et les identités, page 87
À propos des champs personnalisés, page 103
À propos des champs d'attributs One Identity Synchronization Tool, page 522

Configurer ClearID avec un système Synergis existant

Tenez compte des meilleures pratiques suivantes lorsque vous configurez Genetec ClearID[MC] avec un système Synergis[MC] existant.

Ces informations sont destinées aux utilisateurs finaux, aux intégrateurs ou aux personnes chargées de la planification, de la conception et de la configuration d'un système ClearID.

IMPORTANT : Chaque système a des exigences particulières, et ces meilleures pratiques ne peuvent pas suffire pour déployer un système. Les étapes de déploiement varient en fonction de l'architecture et de la configuration existante de votre organisation.

- Utilisez ces informations comme point de départ à des fins de planification de base.
- Si vous avez besoin d'une assistance lors de votre déploiement, adressez-vous à votre contact de déploiement.

BONNE PRATIQUE : Veillez à toujours tester la mise en œuvre d'un nouveau déploiement en environnement de démo avant de passer le système en production.

Tâches en amont du déploiement de ClearID

1. Préparez vos informations sur les titulaires de cartes.
   a. Dans Security Center, vérifiez que les titulaires de cartes existants sont dotés des informations nécessaires pour les associer aux identités ClearID.
      IMPORTANT : Le champ **E-mail** ou le champ personnalisé **ID externe** doit être renseigné.
      - Cette vérification permet de garantir que les identités existantes et à venir seront associées à des titulaires de cartes préexistants.
      - Les futurs titulaires de cartes créés par ClearID seront déjà associés correctement.
2. Planifiez vos **Sites** et vos **Secteurs** en fonction de vos exigences en matière d'accès.
   CONSEIL : Partez de votre système Synergis existant lorsque vous évaluez vos besoins. Pensez à des noms parlants qui évoquent les **sites** ou les **secteurs** qui seront demandés par les utilisateurs.
   a. Identifiez les *Sites* et les *Secteurs* pour lesquels vous souhaitez contrôler les accès.
      - Exemples de sites : Bâtiment principal, bureau satellite 1, bureau satellite 2, etc.
      - Exemples de secteurs : 1er étage, 2e étage, salle des serveurs, auditorium, etc.

      REMARQUE : Un site correspond généralement à un bâtiment physique ou à un groupe de bâtiments connexes. La configuration du site s'applique à l'intégralité du site, et doit donc être contrôlée par les mêmes ensembles de règles (configurations des accès et configurations de la gestion des visiteurs).
   b. Identifiez les *Rôles* dont vous aurez besoin pour regrouper les accès et les identités.
   c. (Facultatif) Envisagez le provisionnement basé sur les attributs afin d'automatiser l'affectation aux rôles.

   REMARQUE : Notez ces sites, secteurs et rôles, dont vous aurez besoin au cours des tâches de déploiement (étapes 3, page 83 et 4, page 83) détaillées plus loin.
3. (Facultatif) Testez votre configuration dans un environnement ClearID de démonstration.
   a. Reliez votre compte ClearID de démo à un système Synergis de démo.
   b. Contactez votre chargé de compte Genetec Inc. pour demander un compte ClearID DEMO ainsi qu'un système Synergis de démo.
      IMPORTANT : La configuration effectuée en environnement de démo ne peut pas être transférée vers un système en production.

Tâches de déploiement

1. Reliez votre système Synergis en production à votre compte ClearID en production.
   a. Installez le module externe ClearID.
   b. Connectez Security Center à ClearID.
2. Synchronisez les identités avec votre source de données.

   Selon vos besoins particuliers, procédez de l'une des manières suivantes :
   - Synchronisez vos identités en passant par l'API.
   - Synchronisez vos identités avec Genetec ClearID[MC] One Identity Synchronization Tool.
3. Sur le portail Web ClearID, créez les **sites** et les **secteurs** que vous avez recensés plus tôt.
   a. Créez vos sites.
   b. Créez vos secteurs.
4. Sur le portail Web ClearID, créez les **rôles** et les **règles de provisionnement basées sur les attributs** que vous avez définies plus tôt.
   a. Créez vos rôles.
   b. (Facultatif) Créez des règles de provisionnement basées sur les attributs afin d'automatiser l'affectation aux rôles.

Rubriques connexes

À propos des relations entre les titulaires de carte et les identités, page 87
À propos des champs personnalisés, page 103
À propos des champs d'attributs One Identity Synchronization Tool, page 522

4

Module externe ClearID

Découvrez comment télécharger et installer le module externe.

Cette section aborde les sujets suivants:

- "À propos du module externe ClearID pour Security Center", page 86
- "À propos des relations entre les titulaires de carte et les identités", page 87
- " Télécharger et installer le module externe ", page 89
- " Créer le rôle module externe ", page 90
- " Connecter Security Center à ClearID ", page 91
- " Accorder des privilèges utilisateur ", page 101
- "À propos des états du système ClearID", page 102
- " À propos des champs personnalisés ", page 103

À propos du module externe ClearID pour Security Center

Le module externe Genetec ClearID[MC] intègre Genetec ClearID[MC] avec Security Center, et connecte Synergis[MC] et les services ClearID dans le cloud. Toutes les actions effectuées dans Genetec ClearID sont synchronisées automatiquement avec Synergis.

REMARQUE : Genetec ClearID[MC] a été conçu en privilégiant l'API. Cet accent placé sur l'API signifie que l'administrateur de compte peut créer une intégration API et utiliser ses propres outils ou services pour communiquer avec notre API.

Vous pouvez télécharger le module externe ClearID pour Security Center ici.

Rubriques connexes

API ClearID

À propos des relations entre les titulaires de carte et les identités

Selon les types de systèmes que vous souhaitez intégrer dans Genetec ClearID[MC], vous pouvez choisir de gérer vos titulaires de cartes et vos identifiants manuellement, ou de les gérer automatiquement avec ClearID.

ClearID ne sait pas à quelle *identité* correspond un *titulaire de cartes* qui n'a pas été créé par ClearID. Dans cette situation, ClearID analyse différents champs de titulaire de cartes, identifie des relations et les associe aux identités correspondantes au sein du système ClearID.

ClearID compare les informations suivantes avant de créer une relation entre un titulaire de cartes et une identité :

- **GUID (Global unique identifier) :** Lorsque notre système crée un titulaire de carte, nous utilisons le même GUID que l'identité pour le créer.

  CONSEIL : Vous trouverez le GUID dans l'URL de l'enregistrement d'identité d'un utilisateur ClearID.

  ```
  https://demo.clearid.io/techdoc/organization/identities/139e92cd-44b9-427e-8727-
  ```

  ```
  bf7681ef0a8d
  ```

  Où **139e92cd-44b9-427e-8727-bf7681ef0a8d** correspond au GUID.
- **Adresse e-mail :** Si l'e-mail professionnel est le même que l'e-mail du titulaire de la carte.
- **ID externe :** Ce champ est un identifiant externe pour la création des identités dans ClearID à l'aide de l'API du service d'identité. Le module externe ClearID crée ce champ dans Security Center sous forme de champ personnalisé pour les titulaires de cartes.

BONNE PRATIQUE : Dans Config Tool, vérifiez que tous vos titulaires de cartes ont une adresse e-mail professionnelle ou un ID externe valable avant d'ajouter vos systèmes dans ClearID. Cette étape vérifie que les titulaires de cartes sont correctement associés aux identifiants correspondants.Pour en savoir plus, voir Configurer ClearID avec un système Synergis existant , page 82.

Scénario 1 : gérer automatiquement les titulaires de carte et les identifiants

Cochez le bouton radio **Genetec ClearID : Les modifications des titulaires de cartes et identifiants sont synchronisées avec Security Center** si vous avez un système Security Center et que vous souhaitez que ClearID crée et gère vos titulaires de cartes et vos identifiants.

Par exemple, un client a déployé un nouveau système Security Center, mais aucun titulaire de cartes ni identifiant n'a encore été défini. En installant le module externe ClearID et en ajoutant l'accès aux identités, les titulaires de cartes et identifiants correspondants sont renseignés au sein du système Security Center et sont synchronisés automatiquement.

CONSEIL : Utilisez la configuration des identifiants sur le portail ClearID pour synchroniser vos identifiants.

Pour en savoir plus sur la synchronisation des identifiants, voir Configurer la duplication d'identifiants , page 245.

Scenario 2 : gérer manuellement les titulaires de carte et les identifiants

Cochez le bouton radio **Security Center : Les identifiants dans ClearID sont en lecture seule** si vous souhaitez que ClearID utilise les titulaires de cartes et les identifiants existants sans gérer leur état. Dans ce cas, ClearID a accès aux titulaires de cartes et identifiants Security Center en lecture seule, car ClearID doit connaître vos titulaires de cartes et identifiants mais ne doit en aucun cas pouvoir les modifier.

Par exemple, un client a configuré Security Center avec 1000 titulaires de cartes et il utilise le module externe ClearID pour connecter le système à ClearID :

- Si le bouton radio **Genetec ClearID : Les modifications des titulaires de cartes et identifiants sont synchronisées avec Security Center** n'est pas sélectionné lors de l'ajout des systèmes, aucune information de titulaires de cartes ou d'identifiants n'est modifiée ou synchronisée. Les titulaires de carte et les identifiants doivent être créés et synchronisés à l'aide d'autres solutions. Par exemple, le protocole LDAP (Lightweight Directory Access Protocol), le rôle Synchroniseur de titulaires de cartes globaux, les modules externes d'importation, etc.
- Si le système Security Center est déjà synchronisé par LDAP, ClearID doit être synchronisé avec la même source LDAP.

CONSEIL : Utilisez LDAP ou le rôle *Synchroniseur de titulaires de cartes globaux* de Security Center pour créer et synchroniser les titulaires de cartes et les identifiants.

Pour en savoir plus sur la synchronisation des titulaires de cartes globaux, voir Gestion des titulaires de cartes globaux.

Rubriques connexes

Examiner les informations de titulaires de cartes et d'identifiants, page 92

Ajouter un système, page 94

Synchroniser les photos d'identité ClearID avec Security Center, page 134

Télécharger et installer le module externe

Pour intégrer l'application Web Genetec ClearID[MC] dans Security Center, vous devez installer le module externe ClearID sur un serveur Security Center.

Avant de commencer

Vérifiez les points suivants :

- Votre serveur répond aux exigences système recommandées.
- Une version compatible de Security Center est installée.

À savoir

BONNE PRATIQUE : Bien qu'il soit possible d'héberger le rôle ClearID sur n'importe quel serveur, hébergez ce rôle sur un serveur d'extension dédié afin d'optimiser les performances système.

- Pour installer ou configurer le module externe dans Security Center, vous devez être un administrateur de site. Par exemple, un administrateur de sécurité local, un intégrateur système ou un administrateur Security Center.
- Synergis Professional ou Omnicast Professional est requis pour la prise en charge des modules externes dans Security Center.
- Le basculement et l'option Federation[MC] ne sont pas pris en charge.

Procédure

1 Ouvrez la page Téléchargements de produits.

2 Dans la liste **Download Finder**, sélectionnez votre version de Security Center.

3 Recherchez votre pack en saisissant son nom et téléchargez-le.

4 Téléchargez le fichier *.exe* du module externe ici.

5 Suivez les invites de votre navigateur pour télécharger le fichier *.exe*.

6 Arrêtez le serveur Genetec puis fermez Security Desk et Config Tool.

7 Ouvrez le dossier décompressé, faites un clic droit sur le fichier *setup.exe*, et sélectionnez **Exécuter en tant qu'administrateur**.

8 Accédez à l'emplacement du fichier téléchargé, effectuez un clic-droit sur le fichier *setup.exe*, puis cliquez sur **Exécuter en tant qu'administrateur**.

9 Suivez les instructions d'installation.

Le module externe est installé sous *C:\Program Files (x86)\Genetec Inc\Genetec Security Center Plugins - ClearID* par défaut.

10 Sur la dernière page de l'*Assistant d'installation*, cliquez sur **Terminer**.

Lorsque vous avez terminé

Revenez dans Config Tool, et connectez le module externe ClearID au compte de service ClearID dans le cloud.

BONNE PRATIQUE : Utilisez Genetec[MC] Update Service (GUS) pour maintenir le module externe ClearID à jour. Pour en savoir plus, voir À propos du Genetec Update Service.

Rubriques connexes

Fonctionnement de l'intégration, page 13

Créer le rôle module externe

Avant de pouvoir configurer et utiliser le module externe Genetec ClearID[MC], vous devez créer le rôle module externe dans Config Tool.

Avant de commencer

Téléchargez et installez le module externe.

À savoir

- Pour installer ou configurer le module externe dans Security Center, vous devez être un administrateur de site. Par exemple, un administrateur de sécurité local, un intégrateur système ou un administrateur Security Center.
- Chaque rôle module externe ne peut communiquer ou se connecter qu'à un seul nom de système ClearID à la fois. Pour les environnements avec plusieurs systèmes, vous devez créer un rôle de module externe pour chaque système.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Modules externes*.

2 Dans la tâche *Modules externes*, cliquez sur **Ajouter une entité** ( ) et sélectionnez **Module externe**.

L'assistant création de module externe apparaît.

3 Sur la page *Informations spécifiques*, sélectionnez le serveur qui héberge le rôle de module externe, le type de module externe et la base de données du rôle de module externe, puis cliquez sur **Suivant**.

Si votre système n'utilise pas de serveurs d'extension, l'option **Serveur** n'est pas affichée.

IMPORTANT : L'entrée du champ **Serveur de base de données** peut être défini par défaut sur le paramètre *(local)\SQLEXPRESS*. S'il ne s'agit pas du serveur approprié, choisissez le serveur pertinent dans la liste **Serveur de base de données**.

4 Sur la page *Informations de base*, spécifiez les informations sur le rôle :

a) Entrez le **Nom de l'entité**.

b) Entrez la **Description de l'entité**.

c) Sélectionnez la **Partition** pour le rôle de module externe.

Si votre système n'utilise pas de serveur d'extension, l'option **Partition** n'est pas affichée. Les partitions sont de groupes logiques qui servent à contrôler la visibilité des entités. Seuls les utilisateurs qui sont membres de la partition peuvent afficher ou modifier le rôle.

d) Cliquez sur Suivant.

5 Sur la page *Résumé de l'opération*, vérifiez les informations, puis cliquez sur **Créer** ou sur **Précédent** pour apporter des modifications.

Une fois que le rôle a été créé, le message suivant est affiché : L'opération s'est déroulée avec succès.

6 Cliquez sur **Fermer**.

7 Si votre environnement nécessite plusieurs systèmes ClearID, répétez cette procédure pour chaque rôle supplémentaire.

Le rôle module externe apparaît dans le navigateur d'entités.

Lorsque vous avez terminé

Vous pouvez à présent connecter Security Center à ClearID.

Connecter Security Center à ClearID

Avant de connecter le rôle module externe Genetec ClearID[MC] à votre compte ClearID, vous devez ajouter votre système ClearID et télécharger un fichier d'activation. Ce fichier d'activation sert ensuite à connecter votre système Security Center à l'application Web ClearID.

Avant de commencer

Créez le rôle de module externe.

À savoir

- Pour créer des systèmes dans ClearID, vous devez être un administrateur global.
- Pour installer ou configurer le module externe dans Security Center, vous devez être un administrateur de site. Par exemple, un administrateur de sécurité local, un intégrateur système ou un administrateur Security Center.
- Ce fichier d'activation est utilisé pour authentifier les communications entre votre système Security Center et l'application Web ClearID.

Procédure

1 (Facultatif) Si vous avez des titulaires de cartes Synergis[MC] préexistants, examinez vos informations de titulaires de cartes et d'identités.

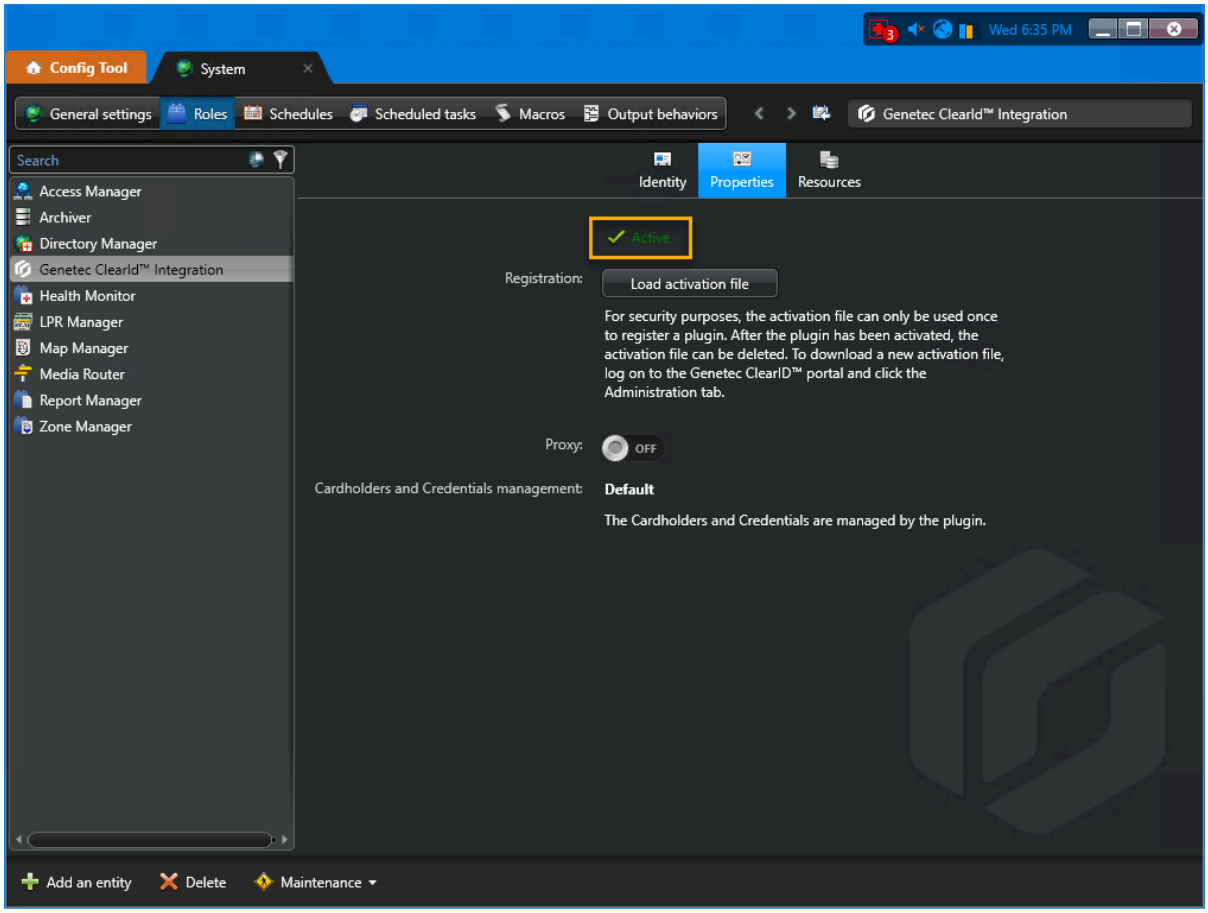
2 Ajoutez un système à ClearID.

3 Téléchargez le fichier d'activation du système que vous venez de créer.

4 Configurez les paramètres de connexion à l'aide du fichier d'activation que vous venez de télécharger.

5 Si votre environnement nécessite plusieurs systèmes ClearID, répétez ces étapes pour chaque nom de système.

Le module externe ClearID est maintenant connecté à Security Center.



Rubriques connexes

Synchroniser les photos d'identité ClearID avec Security Center, page 134

Examiner les informations de titulaires de cartes et d'identifiants

Pour que les titulaires de cartes soient associés correctement à leurs identités correspondantes dans Genetec ClearID[MC] lorsque des systèmes sont ajoutés, vérifiez que tous les titulaires de cartes ont bien une adresse e-mail professionnelle valable.

Avant de commencer

En savoir plus sur les relations entre les titulaires de carte et les identités.

À savoir

Cette procédure ne concerne que la configuration de ClearID avec un système Synergis[MC] existant qui contient des titulaires de cartes.

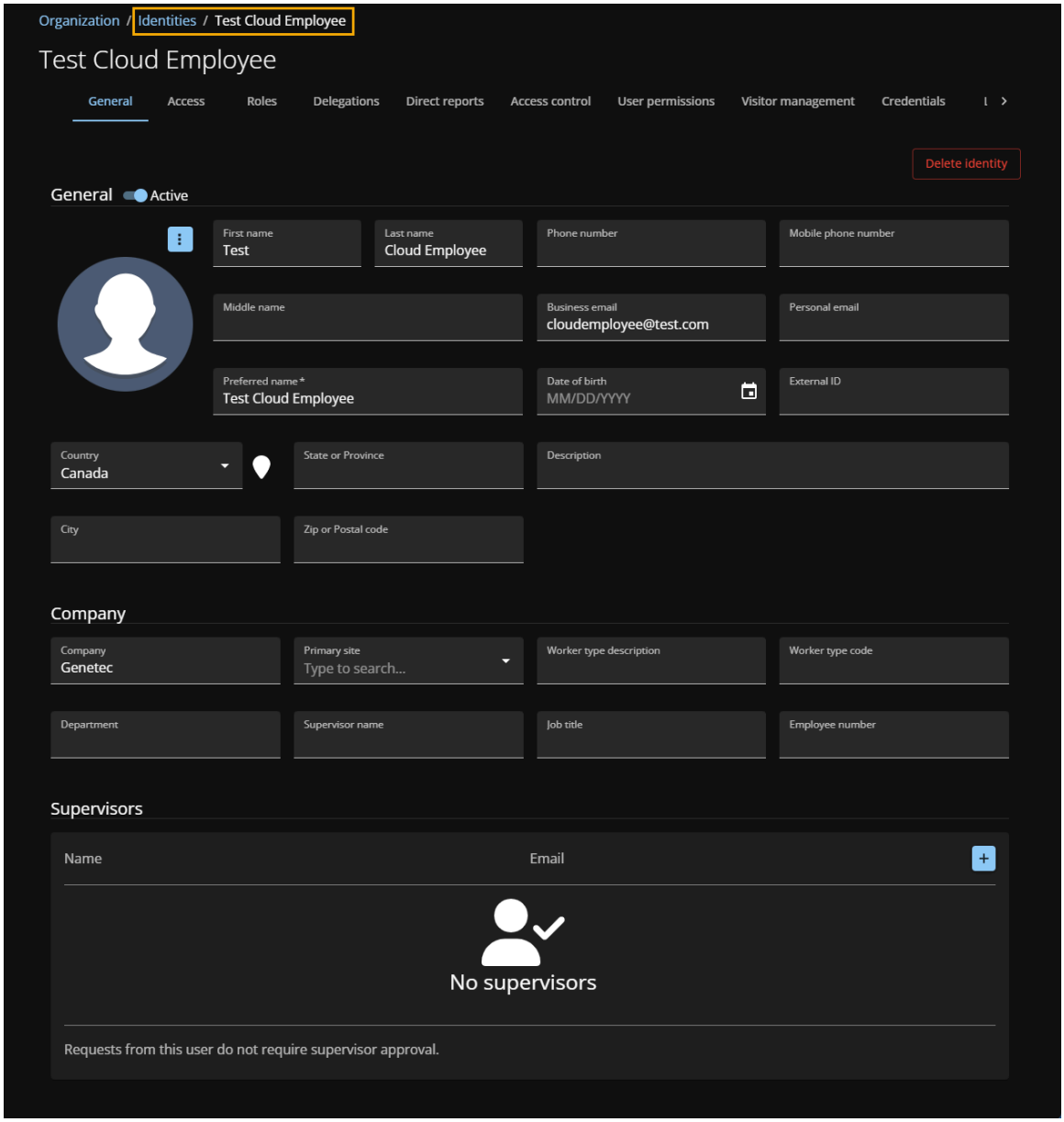
- Tous les titulaires de cartes existants dans Security Center doivent avoir une adresse e-mail professionnelle valable pour pouvoir être associés à leurs identités correspondantes dans ClearID.
- Si tous les titulaires de cartes sont créés par ClearID, le GUID est utilisé pour associer automatiquement les titulaires de cartes aux identités correspondantes.

Procédure

Pour examiner les identités dans ClearID :

1 Sur la page *d'accueil*, cliquez sur **Organisation** > **Identités**.

2 Cliquez sur une identité dans la liste pour afficher ses détails.
L'exemple suivant montre une identité ClearID :



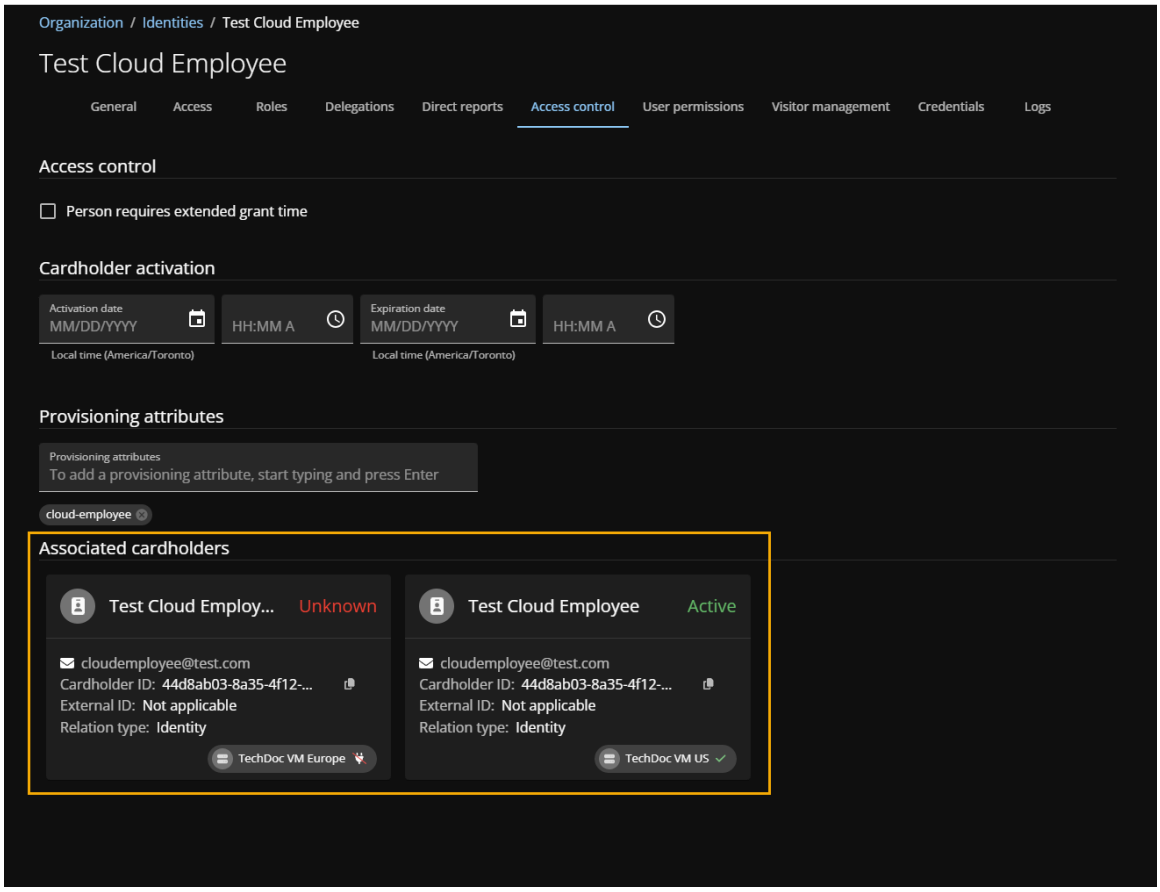
Pour examiner les titulaires de cartes associés à une identité ClearID :

1 Sur la page *d'accueil*, cliquez sur **Organisation** > **Identités**.

2 Cliquez sur une identité dans la liste pour afficher ses détails.

3 Cliquez sur **Contrôle d'accès**.

Une liste de titulaires de cartes Security Center associés à des identités ClearID est affichée dans la section *Titulaires de cartes associés*.



Lorsque vous avez terminé

Ajoutez vos systèmes.

Rubriques connexes

À propos des relations entre les titulaires de carte et les identités, page 87
Synchroniser les photos d'identité ClearID avec Security Center, page 134

Ajouter un système

Avant de connecter le rôle module externe Genetec ClearID^{MC} à votre compte ClearID, vous devez ajouter vos systèmes Security Center dans ClearID.

Avant de commencer

- Créez le rôle de module externe.

- (Facultatif) Si vous avez des titulaires de cartes Synergis[MC] préexistants, suivez les meilleures pratiques dans Configurer Genetec ClearID[MC] avec un système Synergis[MC] existant.
  - Dans Config Tool, vérifiez que tous vos titulaires de cartes ont une adresse e-mail professionnelle ou un ID externe valable avant d'ajouter vos systèmes dans ClearID. Cette étape vérifie que les titulaires de cartes sont correctement associés aux identifiants correspondants.
- Connectez Security Center à ClearID.

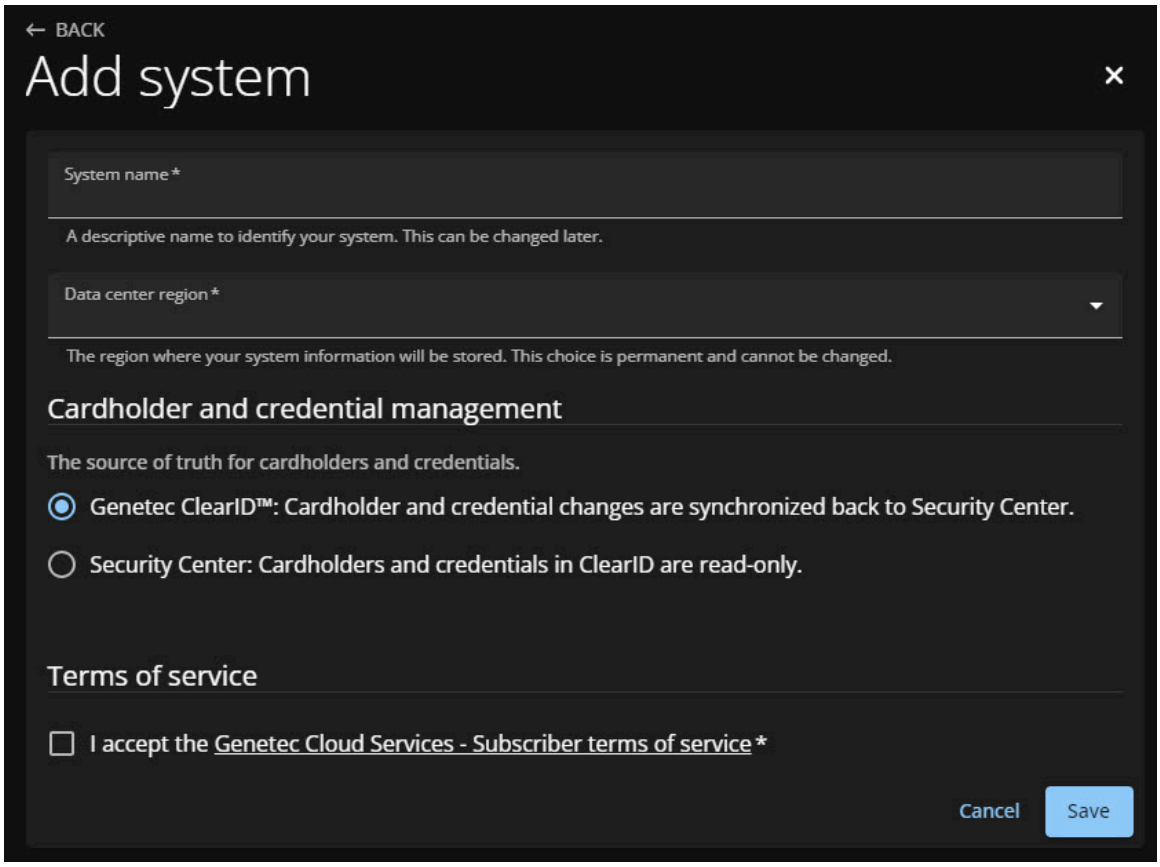
À savoir

- Pour créer des systèmes dans ClearID, vous devez être un administrateur global.

Procédure

1 Connectez-vous à votre compte ClearID.

2 Sur la page d' *Accueil*, cliquez sur **Administration** > **Ajouter un système**.



REMARQUE : L'option **Région du centre de données** n'est pas disponible pour les comptes déployés dans des architectures régionales, comme les centres de données limités à l'Europe, au Canada ou à l'Australie.

3 Dans la boîte de dialogue *Ajouter un système*, remplissez tous les champs :

a) Saisissez un nom de système.

CONSEIL : Utilisez un nom de système qui représente le nom du compte et la région du centre de données associé. Par exemple, `GenetecEuropeSC`.

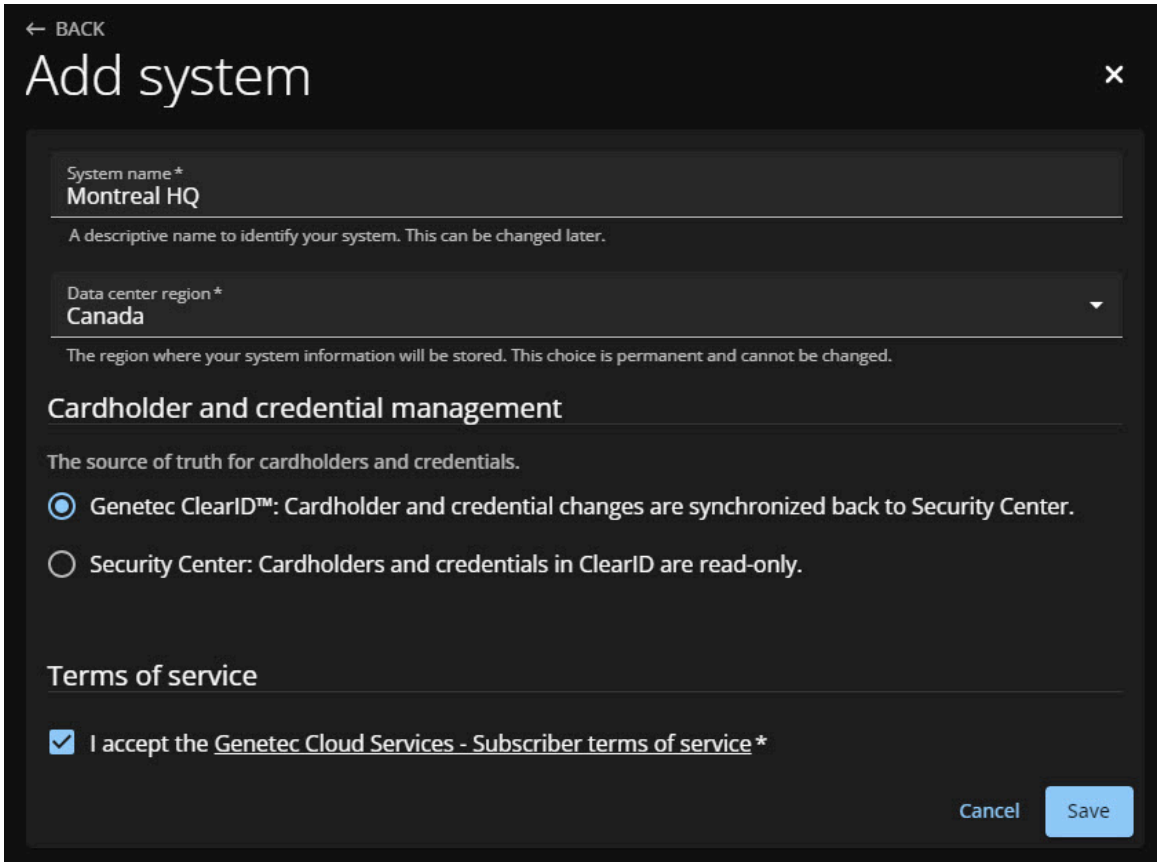
b) Dans la liste **Région du centre de données**, sélectionnez une région correspondant à l'emplacement géographique de votre système ou à l'endroit où vous souhaitez stocker les données.

c) Si vous souhaitez que ClearID remplisse automatiquement les champs des titulaires de cartes et des identifiants, sélectionnez **Genetec ClearID^{MC} : Les modifications des titulaires de cartes et des identifiants sont synchronisées avec Security Center**.

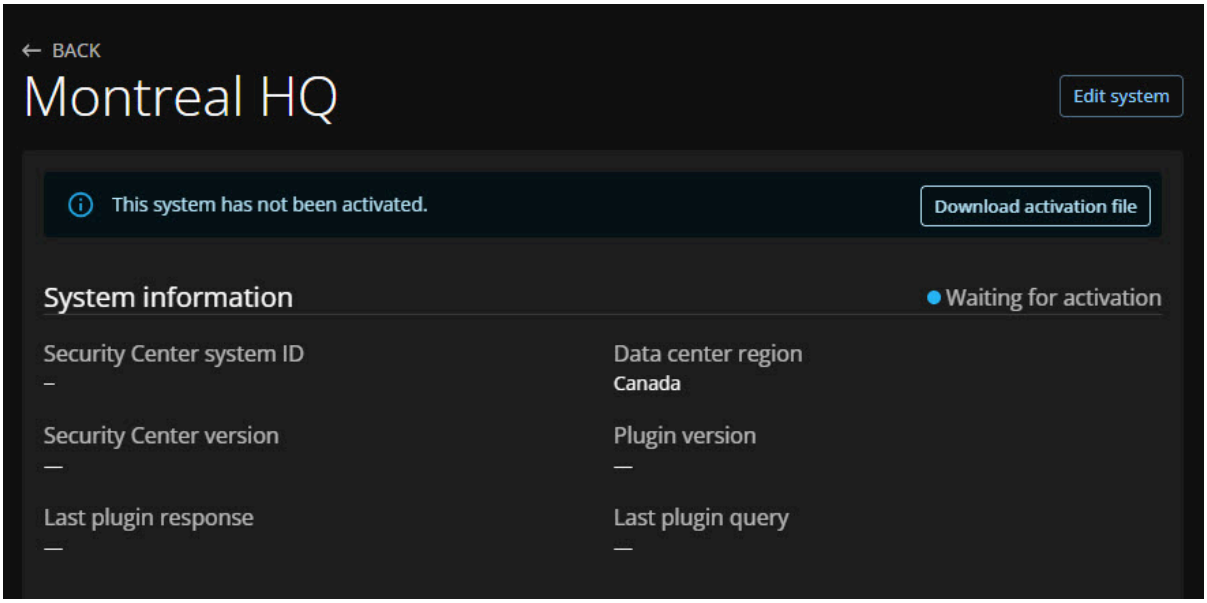
Il s'agit de l'option par défaut.

d) Si vous souhaitez gérer les champs de titulaires de cartes et d'identifiants manuellement, sélectionnez **Security Center : Les titulaires de cartes et les identifiants dans ClearID sont en lecture seule**.

e) Cochez la case pour accepter les conditions générales et cliquez sur **Enregistrer**.



Votre nouveau système est créé. Le système reste inactif tant que vous n'avez pas téléchargé un fichier d'activation et inscrit le module externe ClearID.



Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles.

Lorsque vous avez terminé

Téléchargez le fichier d'activation.

Rubriques connexes

À propos des états du système ClearID, page 102
À propos des relations entre les titulaires de carte et les identités, page 87

Télécharger un fichier d'activation

Avant de connecter le rôle module externe Genetec ClearID[MC] à votre compte ClearID, vous devez télécharger un fichier d'activation. Ce fichier d'activation sert ensuite à connecter votre système Security Center à l'application Web ClearID.

Avant de commencer

Ajouter un système

À savoir

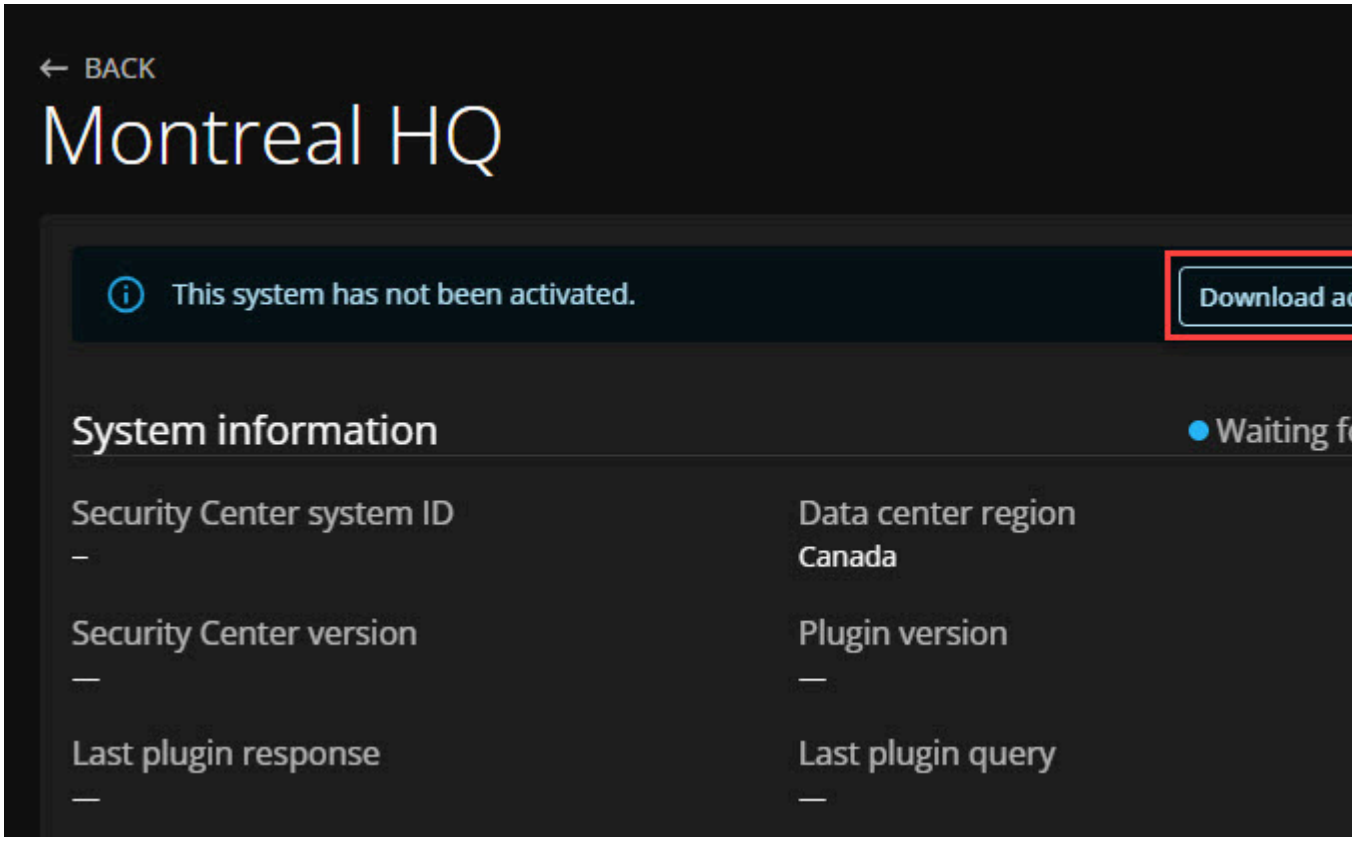
- Pour installer ou configurer le module externe dans Security Center, vous devez être un administrateur de site. Par exemple, un administrateur de sécurité local, un intégrateur système ou un administrateur Security Center.

Procédure

1 Depuis le *Tableau de bord*, cliquez sur le bouton **Administration** onglet.

2 Sur le **Systèmes** page, sélectionnez un système.

3 Cliquer **Télécharger le fichier d'activation** pour enregistrer le fichier dans *json* format.



CONSEIL : Notez l'emplacement du fichier d'activation pour une utilisation ultérieure. Par défaut, les fichiers d'activation sont nommés *systemname-systemID-activation-file.json*.

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles.

Lorsque vous avez terminé

Configurez les paramètres de connexion.

Configurer les réglages de connexion

Pour configurer les paramètres de connexion, vous devez charger un fichier d'activation précédemment téléchargé. Ce fichier d'activation sert ensuite à connecter votre système Security Center à l'application Web Genetec ClearID[MC].

Avant de commencer

Téléchargez un fichier d'activation .

À savoir

- Pour installer ou configurer le module externe dans Security Center, vous devez être un administrateur de site. Par exemple, un administrateur de sécurité local, un intégrateur système ou un administrateur Security Center.

- Ce fichier d'activation est utilisé pour authentifier les communications entre votre système Security Center et l'application Web ClearID.
- Pour des raisons de sécurité, le fichier d'activation ne peut être utilisé qu'une seule fois pour enregistrer un module externe. Une fois le module externe activé, le fichier d'activation peut être supprimé.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Modules externes*.

2 Sélectionnez Intégration ClearID dans le navigateur d'entités, puis cliquez sur l'onglet **Propriétés**.

3 Cliquez sur **Charger le fichier d'activation** et sélectionnez le fichier d'activation que vous avez précédemment téléchargé.

4 (Facultatif) Configurer les paramètres du serveur proxy :

Un serveur proxy est un serveur qui vérifie et transfère les demandes client entrantes à d'autres serveurs pour une communication ultérieure. Par exemple, lorsqu'un client n'est pas en mesure de répondre aux exigences d'authentification de sécurité du serveur mais doit avoir accès à certains services.

- **ACTIVÉ :** Spécifie qu'un serveur proxy est requis pour accéder à Internet. Cette option est généralement utilisée par les clients situés derrière un pare-feu ou lorsque l'accès réseau à Internet est restreint.
- **DÉSACTIVÉ :** Spécifie qu'aucun serveur proxy n'est requis. Il s'agit de la valeur par défaut.
- **URL proxy :** Si le proxy est activé, entrez l'URL du proxy fournie par votre organisation. Par exemple, *https://proxy:8080/outgoing*. Ces informations sont généralement fournies par l'équipe d'administration réseau.

5 (Facultatif) Configurer les paramètres d'authentification proxy :

L'authentification proxy est le processus de validation des identifiants utilisateur permettant d'accéder à un serveur proxy. Cette authentification inclut généralement un nom d'utilisateur et peut également comprendre un mot de passe.

- **ACTIVÉ :** Spécifie que l'authentification proxy est requise.
- **DÉSACTIVÉ :** Spécifie qu'aucune authentification proxy n'est requise.
- **Nom d'utilisateur proxy :** Si l'authentification proxy est **ACTIVÉE**, entrez le nom d'utilisateur proxy fourni par votre organisation.

6 Si l'authentification proxy est définie sur **ACTIVÉE**, définissez un mot de passe d'authentification proxy :

a) Cliquez sur **Définir le mot de passe**.

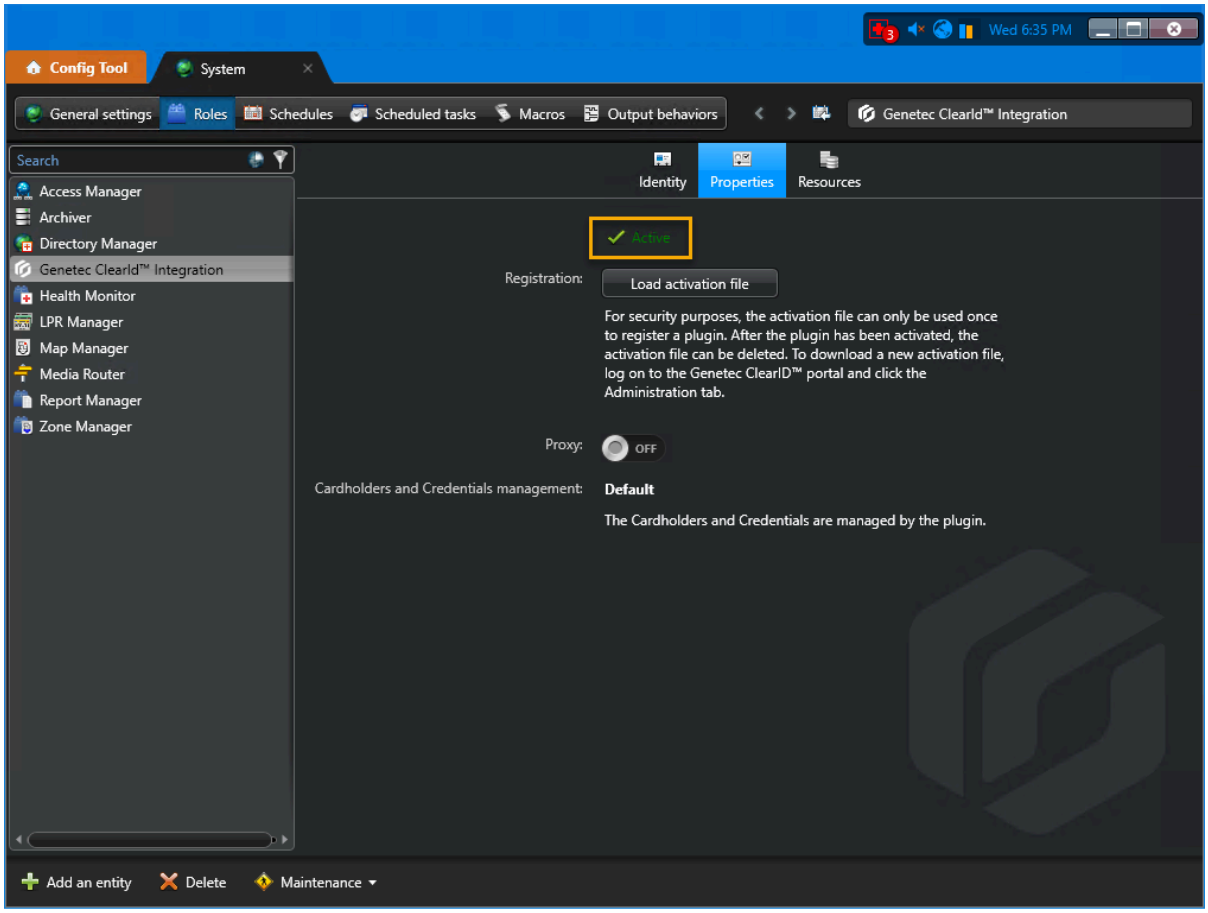
b) Saisissez un **Nouveau mot de passe**, puis confirmez le mot de passe.

REMARQUE : Utilisez les bonnes pratiques du secteur pour créer des mots de passe fiables.

c) Cliquez sur **Appliquer** pour enregistrer le mot de passe.

7 Cliquez sur **Appliquer** pour enregistrer toutes les modifications.

Le module externe ClearID est maintenant connecté à Security Center.


Wed 6:35 PM
Config Tool
System
General settings
Roles
Schedules
Scheduled tasks
Macros
Output behaviors
Genetec Clearid™ Integration
Search
Access Manager
Archiver
Directory Manager
Genetec Clearid™ Integration
Health Monitor
LPR Manager
Map Manager
Media Router
Report Manager
Zone Manager
Identity
Properties
Resources
Active
Registration:
Load activation file
For security purposes, the activation file can only be used once to register a plugin. After the plugin has been activated, the activation file can be deleted. To download a new activation file, log on to the Genetec ClearID™ portal and click the Administration tab.
Proxy:
OFF
Cardholders and Credentials management:
Default
The Cardholders and Credentials are managed by the plugin.
Add an entity
Delete
Maintenance

Accorder des privilèges utilisateur

Pour permettre aux utilisateurs d'accéder aux fonctionnalités et aux tâches du module externe Genetec ClearID^{MC}, vous devez leur accorder les bons privilèges utilisateur dans Security Center.

À savoir

Pour que les administrateurs puissent installer et configurer le module externe dans Config Tool, et que les opérateurs puissent utiliser les fonctions dans Security Desk, les privilèges utilisateur pertinents doivent être accordés à leurs comptes utilisateur.

Cette rubrique indique les privilèges utilisateur minimum requis.

REMARQUE : Vous aurez parfois besoin de privilèges supplémentaires, en fonction des tâches que vous souhaitez effectuer dans Config Tool et dans Security Desk. Pour en savoir plus, voir la feuille de calcul des Privilèges Security Center correspondant à votre version.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Gestion des utilisateurs*.

2 Sélectionnez l'utilisateur pertinent, puis cliquez sur l'onglet **Privilèges**.

3 Définissez les privilèges suivants sur **Autoriser** :

- **Privilèges d'application** > **Security Desk**
- **Privilèges d'application** > **Config Tool**
- **Privilèges administratifs** > **Gestion du système** > **Afficher les propriétés de rôle**
- **Privilèges administratifs** > **Gestion du système** > **Afficher les propriétés de serveur**
- **Privilèges des tâches** > **Administration** > **Modules externes**

4 (Facultatif) Définissez les privilèges de champ personnalisé dont vous avez besoin sur **Autoriser**.

- **Privilèges administratifs** > **Gestion du contrôle d'accès** > **Afficher les propriétés du groupe de titulaires de carte** > **Modifier les propriétés du groupe de titulaires de carte** > **Modifier les champs personnalisés**
- **Privilèges administratifs** > **Gestion du contrôle d'accès** > **Afficher les propriétés du titulaire de carte** > **Modifier les propriétés du titulaire de carte** > **Modifier les champs personnalisés**
- **Privilèges administratifs** > **Gestion du contrôle d'accès** > **Afficher les propriétés des identifiants** > **Modifier les propriétés des identifiants** > **Modifier les champs personnalisés**
- **Privilèges administratifs** > **Gestion du contrôle d'accès** > **Afficher les propriétés des visiteurs** > **Modifier les propriétés des visiteurs** > **Modifier les champs personnalisés**
- **Privilèges administratifs** > **Gestion du système** > **Afficher les paramètres généraux** > **Modifier les définitions de champs personnalisés**

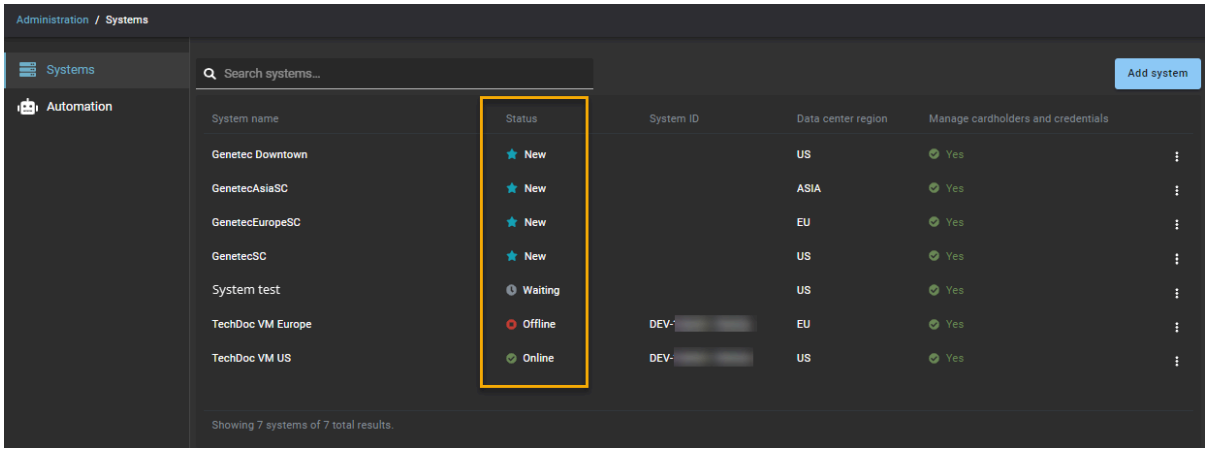
5

Rubriques connexes

À propos des champs personnalisés, page 103

À propos des états du système ClearID

Lorsque vous créez ou configurez un système Genetec ClearID[MC], le système passe par plusieurs états successifs avant de basculer en état en ligne ou actif. Vous pouvez consulter l'état d'un système ClearID en temps réel sur la page *Systèmes*.



Les états suivants concernent uniquement les systèmes ClearID :

- **Création :** Indique qu'un nouveau *nom de système* est en cours de création.
- **Nouveau :** Indique que le *nom du système* a été créé avec succès. Le fichier d'activation peut maintenant être téléchargé pour enregistrer le système.
- **Non disponible :** Indique que l'API n'est pas disponible ou ne peut pas répondre.
- **Hors ligne :** Indique que le système est hors ligne. Cet état est affiché si le module externe n'a pas envoyé de *pulsation* a ClearID depuis 10 à 15 minutes.
- **En ligne :** Indique que le système est inscrit, en ligne et connecté au module externe ClearID.
- **Inconnu :** Indique que l'état du système ne peut pas être obtenu.
- **En attente :** Indique que le fichier d'activation a été téléchargé et que le système est en attente d'activation.
- **Avertissement :** Indique que les services ClearID dans le cloud ou que le module externe ClearID n'a pas traité une demande de message pendant 10 minutes.

CONSEIL : Survolez un état du système avec la souris dans la colonne **État** pour afficher une description de l'état dans l'interface utilisateur.

Rubriques connexes

Ajouter un système, page 94

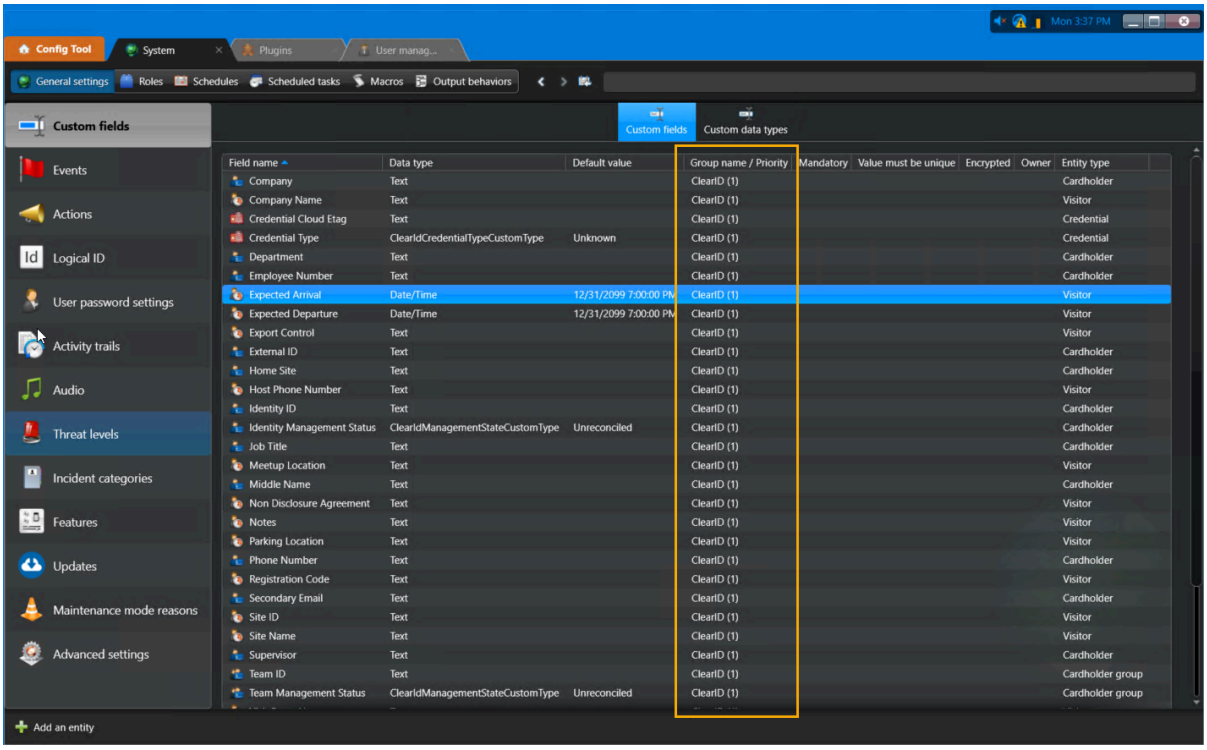
À propos des champs personnalisés

Un champ personnalisé est une propriété définie par l'utilisateur et associée à un type d'entité. Les champs personnalisés sont pratiques pour stocker des informations complémentaires.

Dans Security Center, Genetec ClearID[MC] utilise des champs personnalisés pour des fonctions liées aux visiteurs, identifiants et titulaires de cartes. Le nom de groupe **ClearID** sert à identifier les champs personnalisés associés à ClearID. Il est disponible dans la colonne **Nom du groupe/priorité**.

IMPORTANT : Les champs personnalisés ClearID doivent être utilisés en lecture seule. Les valeurs de ces champs personnalisés sont renseignées et gérées par ClearID. Si vous avez des champs personnalisés existants dont le nom et le type d'entité correspondent aux champs personnalisés ClearID, les champs existants sont utilisés.

La liste complète pour votre organisation est disponible dans Config Tool. Dans la tâche *Système*, cliquez sur **Paramètres généraux** > **Champs personnalisés**.



REMARQUE : Seuls les utilisateurs dotés du privilège *Modifier les définitions de champs personnalisés* peuvent voir les champs personnalisés.

Rubriques connexes

Accorder des privilèges utilisateur, page 101

Modifier les champs personnalisés

Vous pouvez modifier les champs personnalisés Genetec ClearID[MC] dans Config Tool afin qu'ils soient visibles par des groupes ou des utilisateurs particuliers. Par exemple, vous pouvez afficher la raison de la visite, le code d'enregistrement, l'arrivée prévue et le départ prévu pour un groupe comprenant votre équipe de sécurité ou l'équipe d'accueil du bâtiment.

Avant de commencer

Vérifiez que le bouton radio **Genetec ClearID: Les modifications des titulaires de cartes et identifiants sont synchronisées avec Security Center** est sélectionné pour le système ClearID, sans quoi aucun champ personnalisé n'est affiché.

À savoir

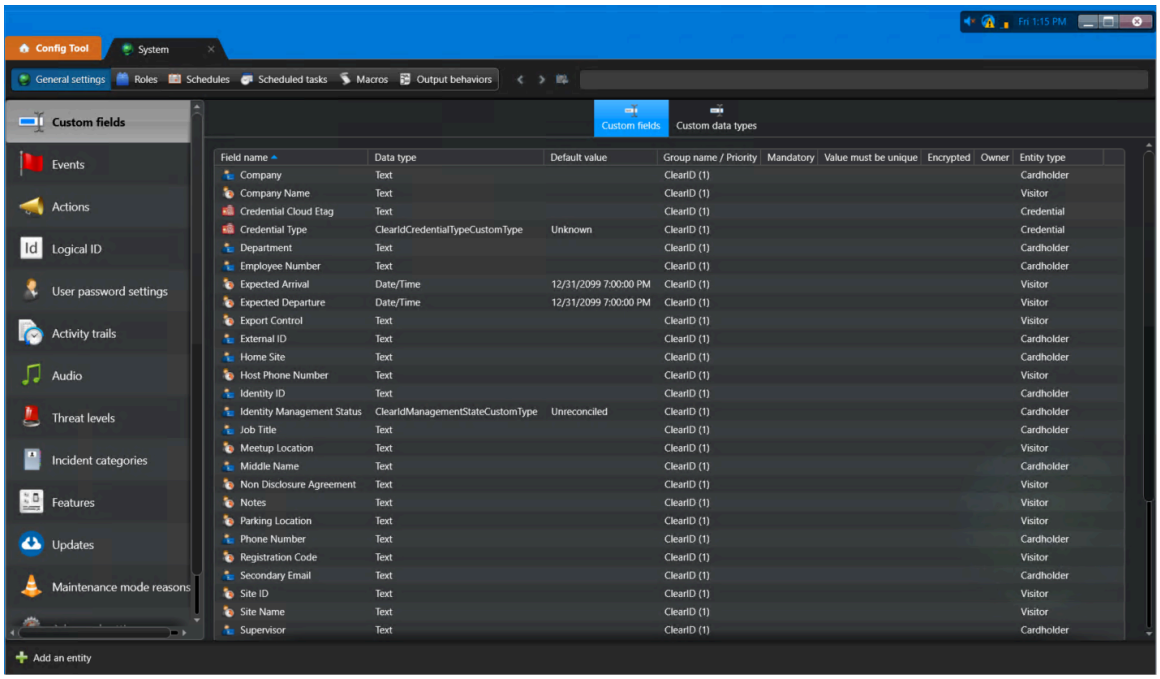
Seuls les utilisateurs dotés du privilège *Modifier les définitions de champs personnalisés* peuvent voir les champs personnalisés.

- Au moins une identité doit être synchronisée pour que les champs personnalisés soient affichés.

Procédure

1 Dans Config Tool, ouvrez la tâche *Système*.

2 Cliquez sur **Champs personnalisés**.

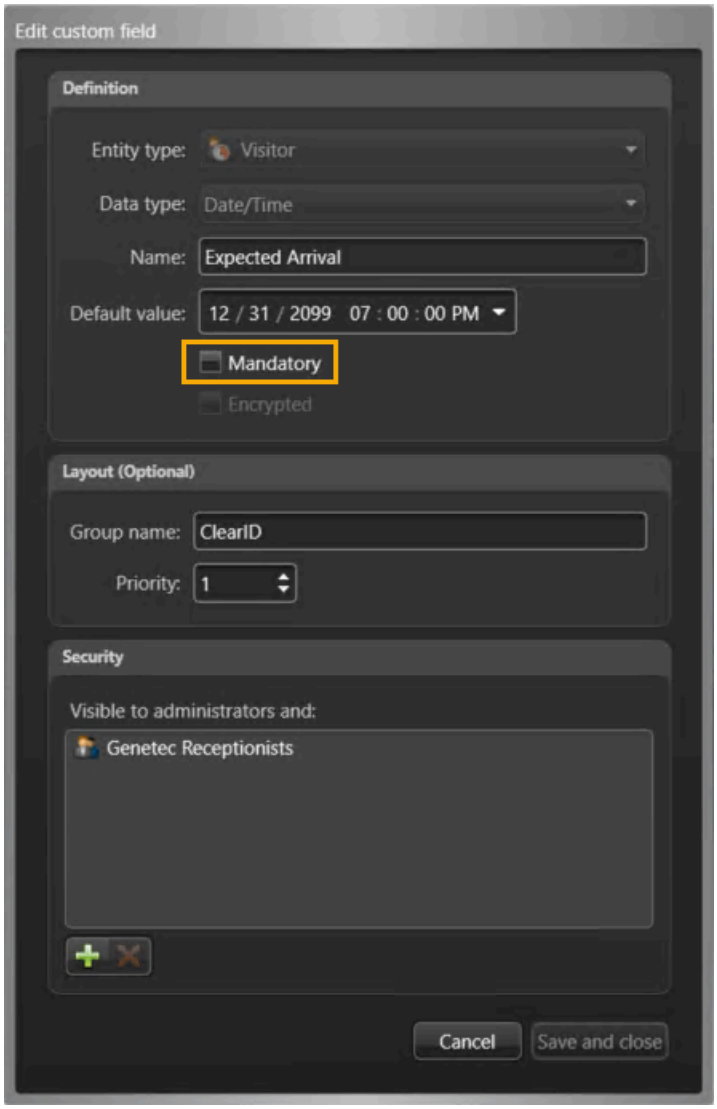


3 Dans l'onglet **Champs personnalisés**, cliquez deux fois sur un **Nom de champ** pour sélectionner le champ personnalisé que vous souhaitez modifier.

4 Dans la boîte de dialogue *Modifier le champ personnalisé*, apportez les modifications nécessaires.

a) Dans la section *Définition*, apportez les modifications nécessaires.

IMPORTANT : Ne cochez pas la case **Obligatoire** pour les champs personnalisés. Dans ClearID, les champs personnalisés ne doivent pas être obligatoires ou uniques, sans quoi vous rencontrerez des problèmes de synchronisation.



b) Dans la section *Disposition*, apportez les modifications nécessaires.

Vous pouvez par exemple ajouter un nom de groupe pour classer vos champs personnalisés, ou vous pouvez supprimer un champ d'un groupe auquel il ne doit plus appartenir.

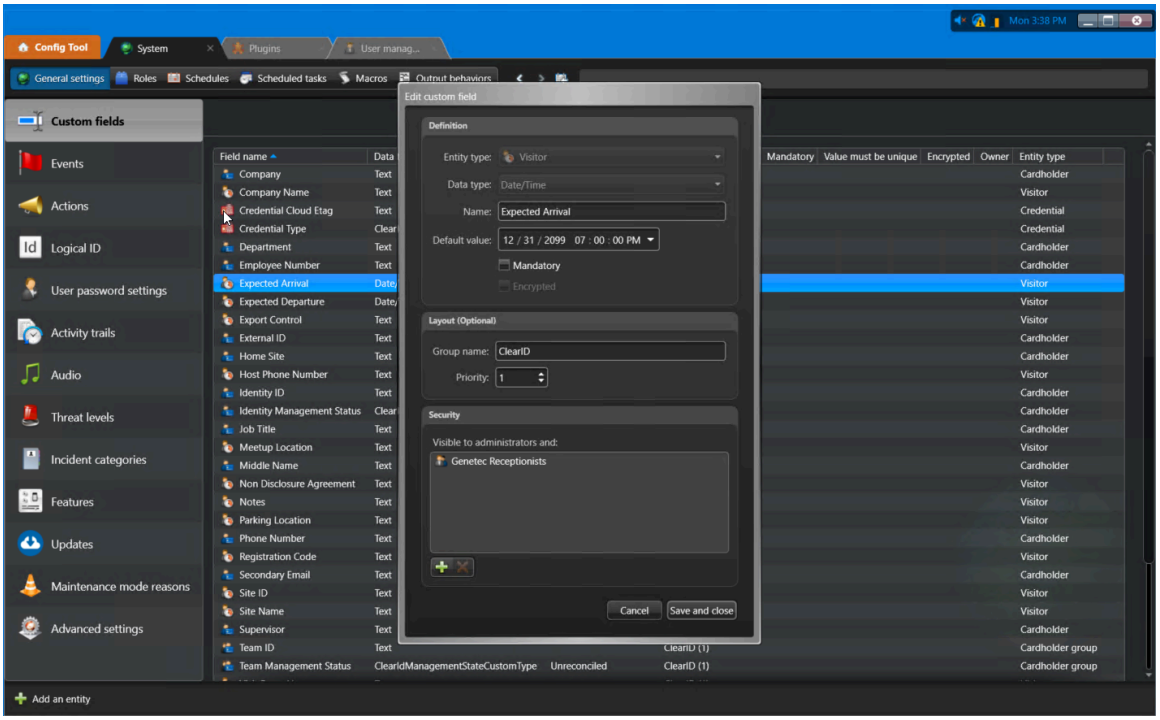
c) Dans la section *Sécurité*, apportez les modifications nécessaires.

Vous pouvez par exemple ajouter des utilisateurs ou des groupes d'utilisateurs dans la section *Sécurité* afin qu'ils puissent voir le champ personnalisé.

Pour en savoir plus sur les *groupes d'utilisateurs* et les *champs personnalisés*, voir « Créer des groupes d'utilisateurs » et « À propos des champs personnalisés » dans le *Guide de l'administrateur Security Center*.

d) Cliquez sur **Enregistrer et fermer**.

L'exemple suivant illustre le champ personnalisé *Arrivée prévue*. À l'aide de la section *Sécurité* de la boîte de dialogue *Modifier le champ personnalisé*, le groupe d'utilisateurs **Réceptionnistes Genetec** a été ajouté afin que le champ personnalisé *Arrivée prévue* puisse être consulté par les membres du groupe.

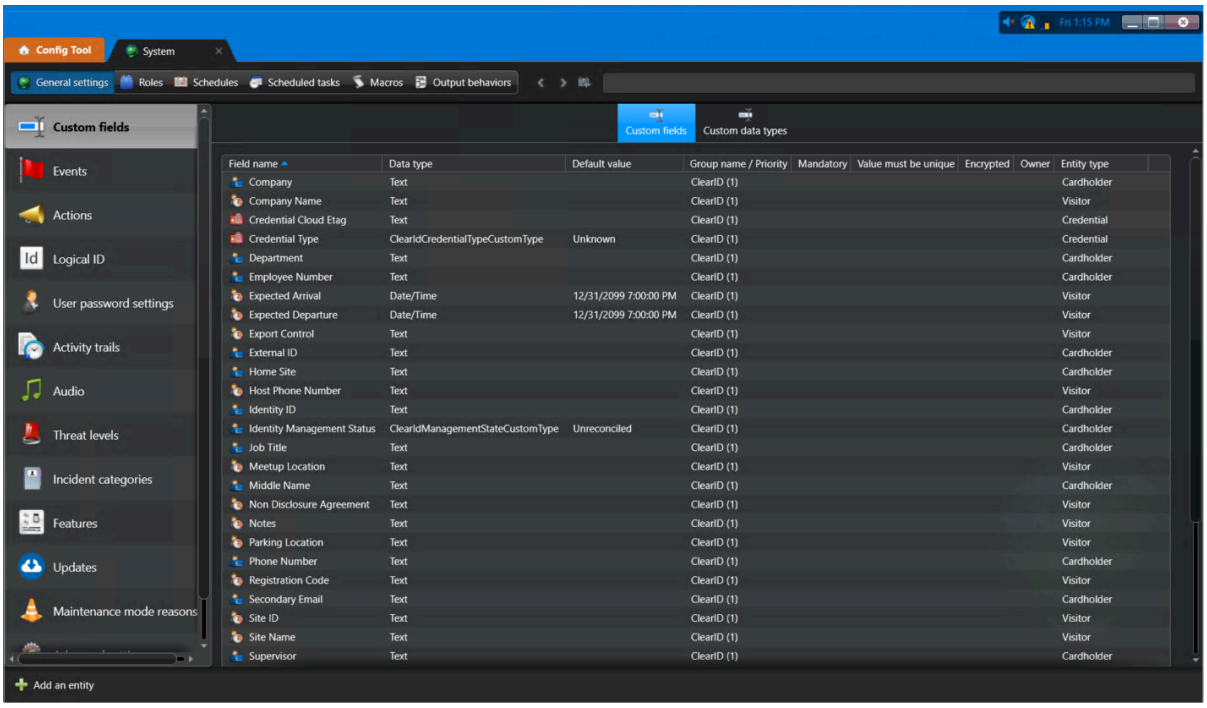


Rubriques connexes

Les champs personnalisés ne sont pas affichés dans Security Desk, page 678
Accorder des privilèges utilisateur, page 101

Relations de champs personnalisés

Utilisez les informations suivantes sur les champs personnalisés pour comprendre la relation entre les noms de champs d'identité Genetec ClearID[MC] et les champs de types d'entités Security Center.



Champs de titulaires de cartes

Les champs de titulaires de cartes servent à synchroniser les informations d'un titulaire de cartes avec une identité dans ClearID.

Nom du champ	Type de donnée	Valeur par défaut	Nom du groupe (et priorité)
Société	Texte		ClearID (1)
Département	Texte		ClearID (1)
Numéro d'employé	Texte		ClearID (1)
ID externe	Texte		ClearID (1)
Site d'origine	Texte		ClearID (1)
ID d'identité	Texte		ClearID (1)
État de la gestion d'identité	ClearIdManagementStateCustomType	Non rapproché	ClearID (1)
Intitulé du poste	Texte		ClearID (1)
Deuxième prénom	Texte		ClearID (1)

Nom du champ	Type de donnée	Valeur par défaut	Nom du groupe (et priorité)
Numéro de téléphone	Texte		ClearID (1)
E-mail de secours	Texte		ClearID (1)
Superviseur	Texte		ClearID (1)
Code de type de travailleur	Texte		ClearID (1)
Description de type de travailleur	Texte		ClearID (1)

Champs de groupes de titulaires de cartes

Les champs de groupes de titulaires de cartes servent à synchroniser les informations d'un groupe de titulaire de cartes avec un rôle dans ClearID.

- L'**ID d'équipe** représente l'ID de rôle dans ClearID.
- L'**État de la gestion d'équipe** indique si ClearID gère les titulaires de cartes et les identifiants ou non (gérés par ClearID, pas gérés par ClearID, supprimés par ClearID ou non rapprochés).

Nom du champ	Type de donnée	Valeur par défaut	Nom du groupe (et priorité)
ID d'équipe	Texte		ClearID (1)
État de la gestion de groupe	ClearIdManagementStateCustomType	Non rapproché	ClearID (1)

Champs d'identifiants

Les champs d'identifiants sont utilisés par ClearID pour maintenir les identifiants à jour.

Nom du champ	Type de donnée	Valeur par défaut	Nom du groupe (et priorité)
Cloud Etag de l'identifiant	Texte		ClearID (1)
Type d'identifiant	ClearIdCredentialTypeCustomType	Inconnu	ClearID (1)

Champs de visiteurs

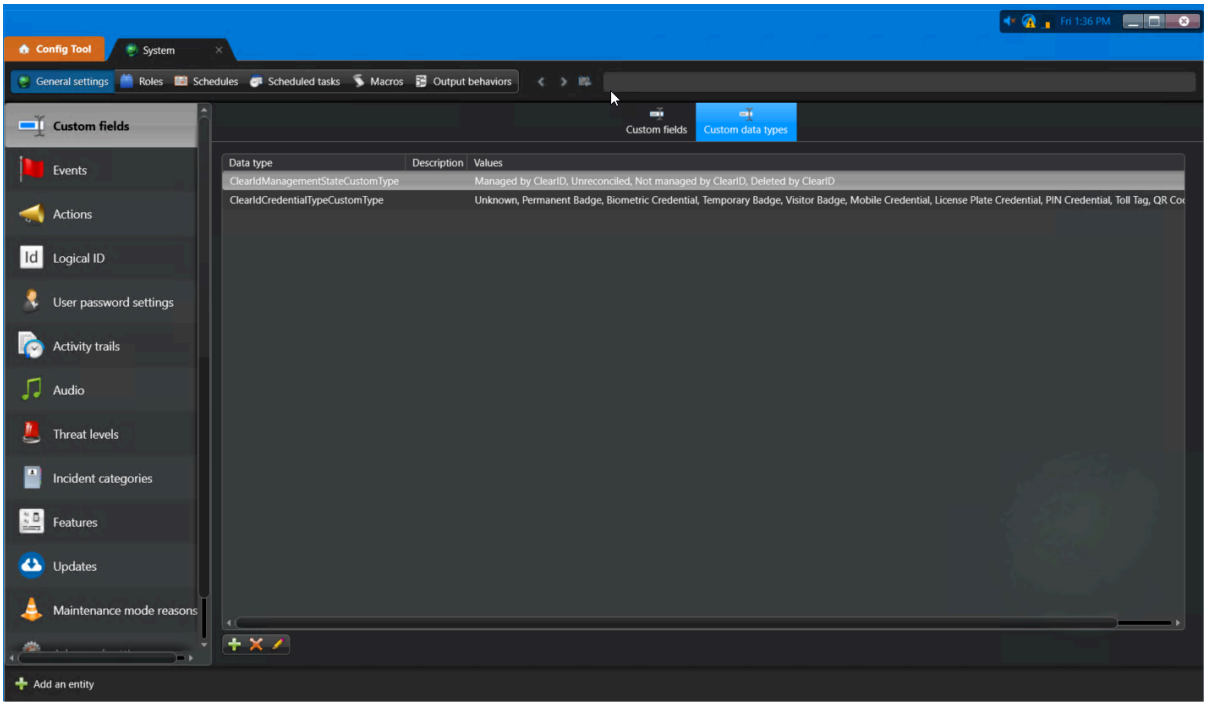
Ces champs de visiteurs servent à synchroniser les informations sur les visiteurs.

Nom du champ	Type de donnée	Valeur par défaut	Nom du groupe (et priorité)
Nom de la société	Texte		ClearID (1)

Nom du champ	Type de donnée	Valeur par défaut	Nom du groupe (et priorité)
Arrivée prévue	Date et heure	12/31/2099 19:00:00	ClearID (1)
Départ prévu	Date et heure	12/31/2099 19:00:00	ClearID (1)
Contrôle des exportations	Texte		ClearID (1)
Numéro de téléphone de l'hôte	Texte		
Lieu de rendez-vous	Texte		ClearID (1)
Accord de non-divulgation	Texte		ClearID (1)
Remarques	Texte		ClearID (1)
Emplacement de stationnement	Texte		ClearID (1)
Code d'inscription	Texte		ClearID (1)
ID de site	Texte		ClearID (1)
Nom du site	Texte		ClearID (1)
Nom de l'événement de visite	Texte		ClearID (1)
Motif de la visite	Texte		ClearID (1)
ID de visiteur	Texte		ClearID (1)
État de la liste de surveillance	Texte		ClearID (1)

Types de données personnalisés

Les types de données personnalisés servent à spécifier les valeurs acceptées associées aux types de données pour certains champs personnalisés.



REMARQUE : Tous les champs personnalisés sont des étiquettes servant à définir une propriété associée à un type d'entité Security Center potentiellement utile. Les champs inclus dans cette description ne sont que descriptifs. Les types de données personnalisés ne sont pas forcément pertinents ni utilisés par ClearID.

Type de donnée	Valeurs
ClearIdManagementStateCustomType	Géré par ClearID, Non rapproché, Non géré par ClearID, Supprimé par ClearID
ClearIdCredentialTypeCustomType	Inconnu, Badge permanent, Identifiant biométrique, Badge temporaire, Badge de visiteur, Identifiant mobile, Identifiant plaque d'immatriculation, Identifiant Code PIN, Carte de péage, Code QR

5

Gérer les identités et les utilisateurs

Découvrez comment gérer les identités et les utilisateurs.

Cette section aborde les sujets suivants:

- " Créer des identités ", page 113
- "Champs d'identité", page 115
- " Accorder des autorisations supplémentaires à des identités et des rôles ", page 117
- " Accorder des autorisations supplémentaires à des superviseurs ", page 121
- " Afficher les autorisations supplémentaires ", page 123
- " Afficher les identités ", page 127
- " Modifier les identités ", page 130
- " Supprimer des identités ", page 132
- " Synchroniser les photos d'identité ClearID avec Security Center ", page 134
- " À propos des points d'ancrage ", page 135
- " Créer des points d'ancrage ", page 138
- " Consulter les journaux de points d'ancrage ", page 143
- " Accorder l’accès au portail Web ", page 146
- " Consulter votre profil ", page 150
- " Consulter vos accès aux sites et aux secteurs ", page 154
- " À propos du processus de demande d'accès ", page 155
- " Demander un accès ", page 156
- " Ajouter des superviseurs manuellement ", page 164
- " Afficher les subordonnés ", page 166
- " Gérer les subordonnés ", page 169
- " Transférer les subordonnés ", page 175
- " À propos du rapport Subordonnés ", page 182
- " Réinitialiser les mots de passe utilisateur ", page 183
- " À propos des notifications par e-mail ", page 186
- " À propos de la délégation ", page 192
- " Déléguer des tâches à un autre utilisateur ", page 195
- " À propos du rapport d'activité d'utilisateurs ", page 199
- " Afficher un rapport d'activité d'utilisateurs ", page 201
- " Niveaux utilisateur ", page 204
- " À propos du processus de demande d'identité ", page 210
- " Créer un modèle d'identité ", page 211
- " Demander des identités ", page 218

- " Annuler les demandes d'identité ", page 232
- " Approuver les demandes d'identité ", page 235
- " À propos du rapport de demandes d'identités ", page 241
- " Vérifier l’état des demandes d'identité ", page 242

Créer des identités

Vous aurez parfois besoin de créer une identité manuellement dans Genetec ClearID[MC]. Par exemple, pour une identité qui ne fait pas partie du processus d'importation ou de synchronisation de masse des identités par LDAP ou One Identity ou avec une API.

À savoir

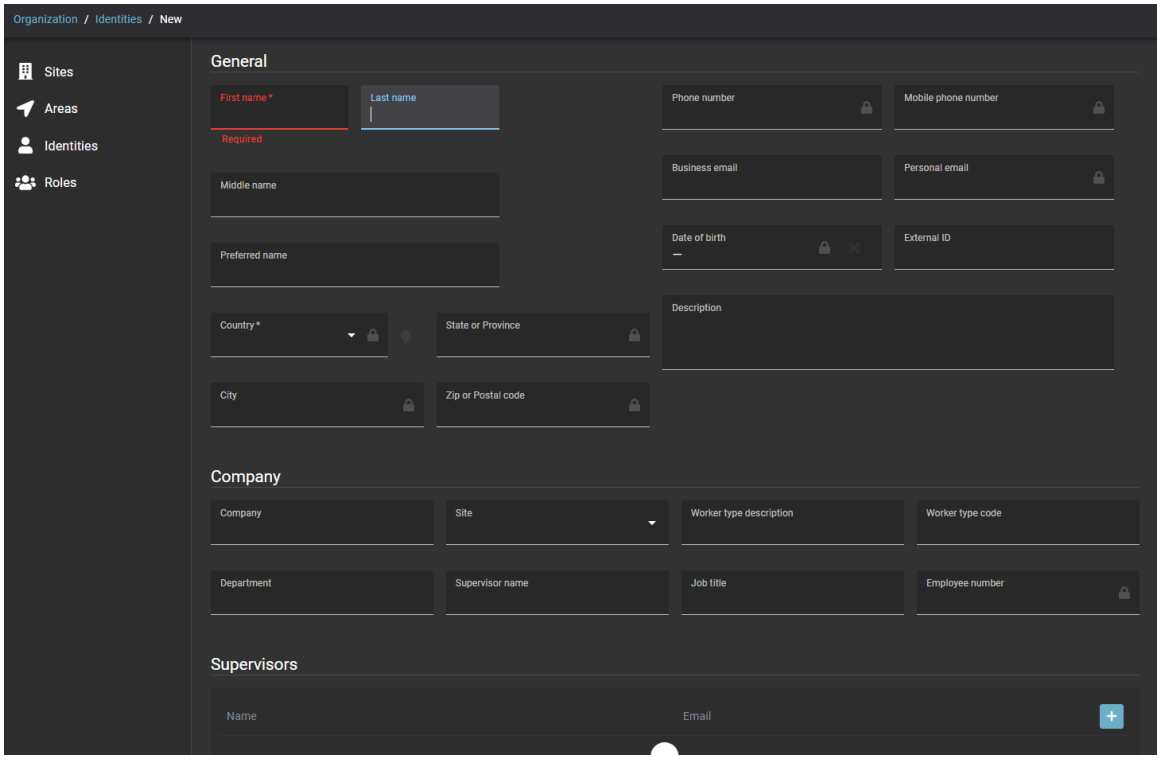
Seul un administrateur de compte peut créer des identités.

Cette tâche décrit comment un administrateur de compte peut créer une identité manuellement sur le portail web lorsqu'elle ne fait pas partie d'une importation ou synchronisation de masse par LDAP ou One Identity ou avec une API. Par exemple, vous pouvez ajouter une identité manuellement pour un *fournisseur* ou encore un *intégrateur système*.

Procédure

1 Cliquez sur **Organisation** > **Identités**.

2 Cliquez sur **Ajouter une identité** .



3 Renseignez les champs obligatoires :

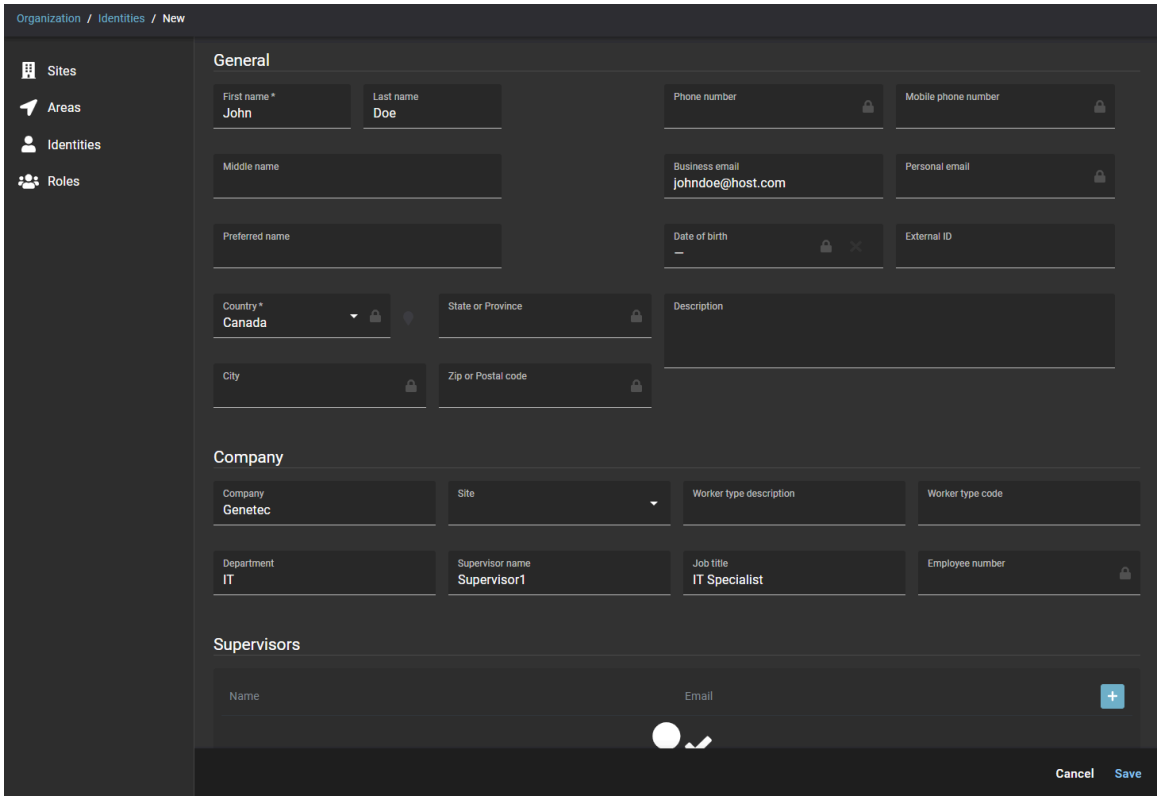
a) Entrez un `Prénom`.

b) Entrez un `Nom`.

c) Sélectionnez un pays dans la liste.

CONSEIL : Entrez la première lettre du pays pour faire défiler la liste des pays.

4 (Facultatif) Renseignez les autres champs, selon vos besoins. Par exemple :
   a) Entrez une `Adresse e-mail`.
   b) Entrez un `Nom de société`.
   c) Entez un `Département`.
   d) Entrez un `Nom de superviseur`.
   e) Entrez une `Fonction`.
   f) Renseignez les autres champs selon vos besoins.



5 Cliquez sur **Enregistrer** pour créer l'identité dans Genetec ClearID[MC].

Lorsque vous avez terminé

Accordez l'accès au portail web à l'identité.

Rubriques connexes

Se connecter à ClearID, page 34
Afficher les subordonnés, page 166

Champs d'identité

Utilisez les informations suivantes pour comprendre les champs d'identité utilisés par Genetec ClearID[MC]. Le tableau suivant indique les champs obligatoires, les champs utilisés par Security Center et les champs qui peuvent être exploités pour les règles de provisionnement.

Champs d'identité ClearID	Type ou format	Obligatoire dans ClearID	Transmis à Security Center	Nom du champ Security Center	Disponible dans les règles de provisionnement
Date d'activation	Date		✓	Activation	
e-mail professionnel	E-mail		✓	Adresse e-mail	
Urbain	Texte				
Société	Texte		✓	Société	✓
Pays	Caractère ISO 3	✓			✓
Date de naissance	Date				
Département	Texte		✓	Département	✓
Description	Texte		✓	Description	✓
Nom d’affichage	Texte		✓	Nom de l'entité	
Numéro d'employé	Texte		✓	Numéro d'employé	
Date d'expiration	Date		✓	Expiration	
Délai d'accès prolongé requis	Vrai ou faux		✓	Utiliser le délai d’accès prolongé	✓
ID externe	Texte		✓	ID externe	✓
Prénom	Texte	✓	✓	Prénom	
Site principal	ID unique		✓	Site principal	✓
ID d'identité	ID unique		✓	Identité	
Intitulé du poste	Texte		✓	Intitulé du poste	✓
Nom	Texte		✓	Nom	
Deuxième prénom	Texte		✓	Deuxième prénom	

Champs d'identité ClearID	Type ou format	Obligatoire dans ClearID	Transmis à Security Center	Nom du champ Security Center	Disponible dans les règles de provisionnement
Numéro de téléphone mobile	Numéro de téléphone				
e-mail personnel	E-mail		✓	Email secondaire	
Numéro de téléphone	Numéro de téléphone		✓	Numéro de téléphone	
Attributs de provisionnement	Liste				✓
État/province	Texte				
État	Actif ou Inactif	✓	✓	État	✓
Nom du superviseur	Texte		✓	Superviseur	✓
Superviseur(s)	Liste des identités				✓
Code type d'employé	Texte			Code type d'employé	✓
Description du type de travailleur	Texte		✓	Description du type de travailleur	✓
Code postal	Texte		✓		

Rubriques connexes

Configurer les stratégies de contrôle d'accès basé sur les rôles, page 476

Accorder des autorisations supplémentaires à des identités et des rôles

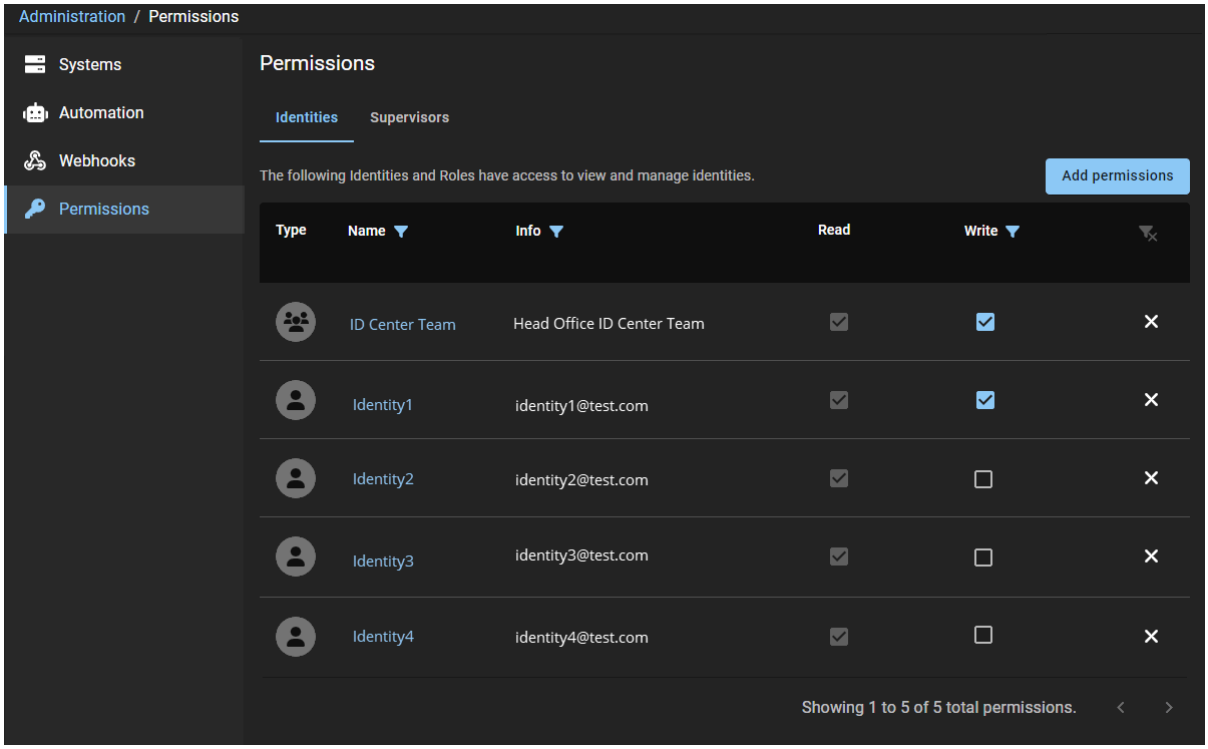
Certaines organisations voudront accorder des autorisations d'accès au-delà des autorisations par défaut accordées aux utilisateurs Genetec ClearID[MC]. Vous pouvez accorder des autorisations supplémentaires aux identités et aux rôles afin qu'ils puissent afficher ou gérer toutes les identités du système.

À savoir

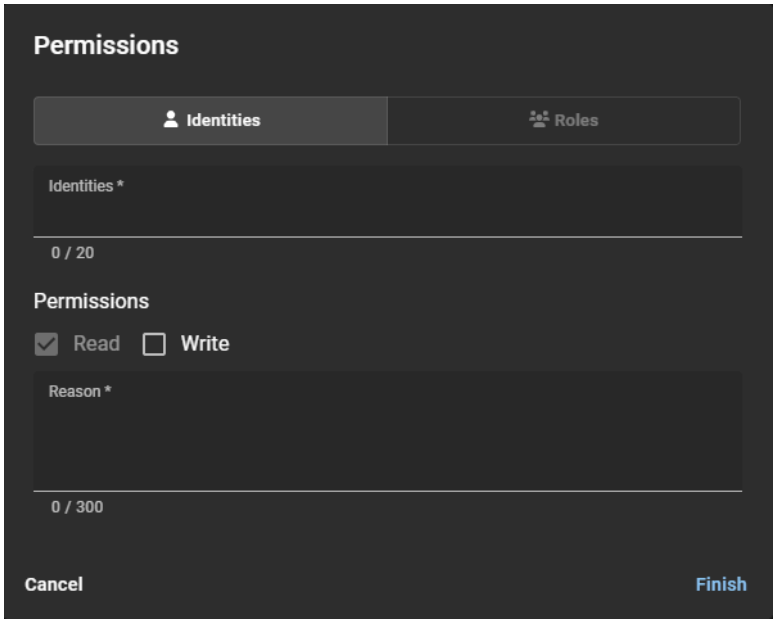
Seul un administrateur de compte peut ajouter des autorisations d'identité et de rôle.

Procédure

1 Sur la page *Accueil*, cliquez sur **Administration** > **Autorisations**.



2 Cliquez sur **Ajouter des permissions**.



3 Dans la boîte de dialogue *Autorisations*, sélectionnez **Identités** ou **Rôles** pour ajouter les autorisations dont vous avez besoin.

4 Si vous avez sélectionné **Identités**, remplissez ce qui suit :

a) Dans le champ **Identités**, saisissez une ou plusieurs identités auxquelles vous souhaitez accorder un accès supplémentaire.

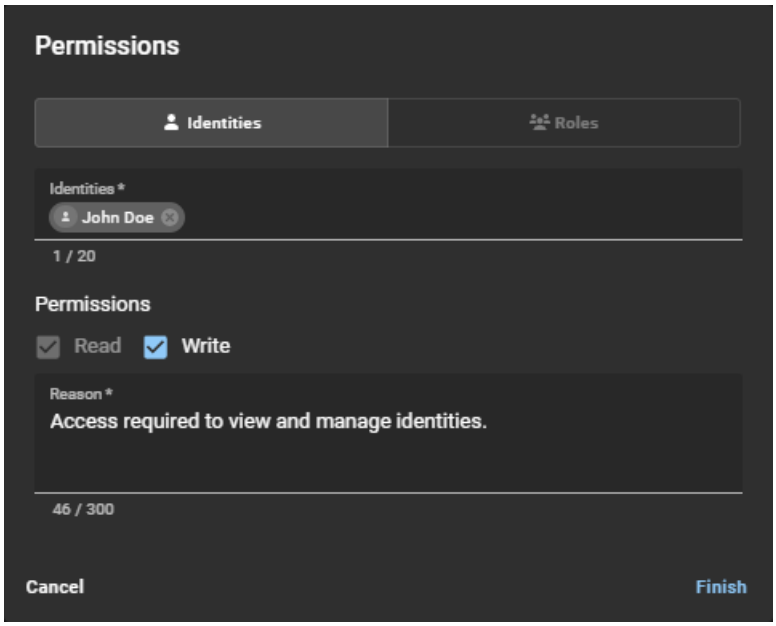
20 identités maximum peuvent être prises en charge par requête.

b) Dans la section *Autorisations*, sélectionnez les autorisations que vous souhaitez ajouter aux identités sélectionnées précédemment.

- **Lecture :** L'accès en lecture permettant d'afficher les identités est accordé par défaut.
- **Écrire :** Cochez la case **Écrire** pour ajouter des autorisations de modification des identités.

REMARQUE : Si vous effectuez des mises à jour d'identités synchronisées avec une source de données externe, la synchronisation peut écraser votre autorisation d'écriture. Les autorisations en écriture sont utiles pour les identités qui sont saisies manuellement dans ClearID.

c) Dans le champ **Raison**, saisissez la raison pour laquelle l'accès a été ajouté.



5 Si vous avez sélectionné **Rôles**, remplissez ce qui suit :

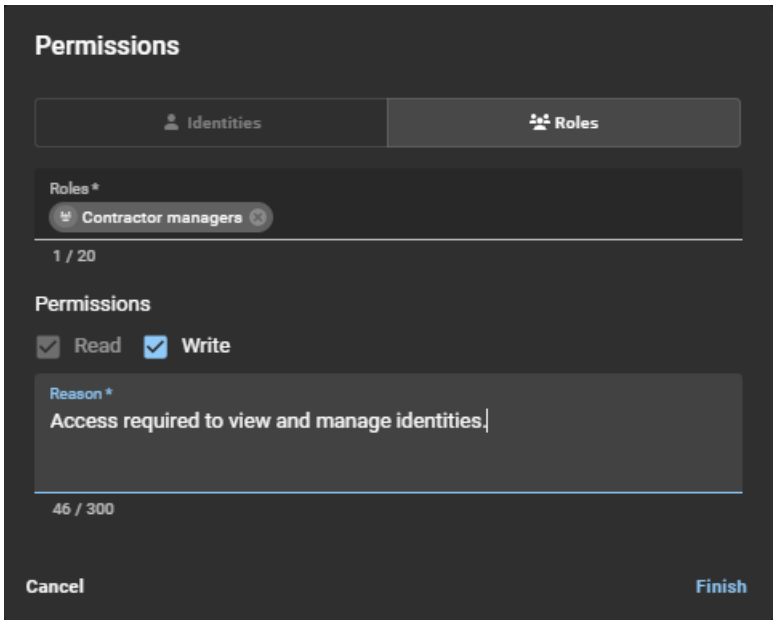
a) Dans le champ **Rôles**, saisissez un ou plusieurs rôles auxquels vous souhaitez accorder un accès supplémentaire.

20 rôles maximum peuvent être pris en charge.

b) Dans la section *Autorisations*, sélectionnez les autorisations que vous souhaitez ajouter aux rôles sélectionnés précédemment.

- **Lecture :** L'accès en lecture permettant d'afficher les identités est accordé par défaut.
- **Écrire :** Cochez la case **Écrire** pour ajouter des autorisations de modification des identités.

c) Dans le champ **Raison**, saisissez la raison pour laquelle l'accès a été ajouté.



6 Cliquez sur **Terminer** pour soumettre vos modifications.

Les identités ou les rôles spécifiés disposent désormais des autorisations requises pour afficher et gérer les identités.

Lorsque vous avez terminé

Afficher les identités ou Modifier les identités.

Rubriques connexes

Transférer les subordonnés, page 175

Accorder des autorisations supplémentaires à des superviseurs

Certaines organisations voudront accorder des autorisations d'accès au-delà des autorisations par défaut accordées aux superviseurs Genetec ClearID[MC]. Vous pouvez accorder aux superviseurs des autorisations supplémentaires afin qu'ils puissent gérer leurs subordonnés.

À savoir

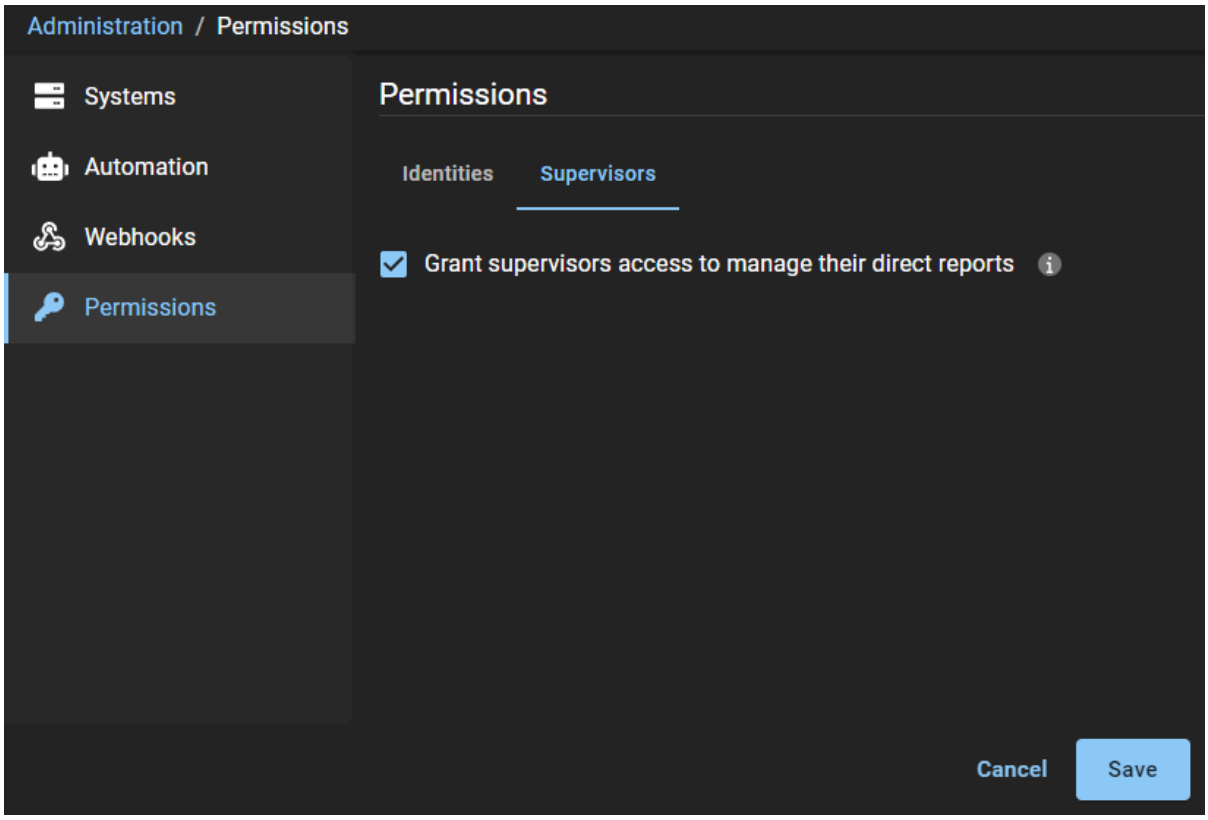
Seul un administrateur de compte peut accorder l'accès aux superviseurs pour gérer leurs subordonnés.

Procédure

1 Sur la page *Accueil*, cliquez sur **Administration** > **Autorisations**.

2 Cliquez sur l'onglet **Superviseurs**.

3 Cochez la case **Autoriser les superviseurs à gérer leurs subordonnés directs** pour accorder aux superviseurs les autorisations requises pour mettre à jour les informations du profil d'identité **Général** et les paramètres de contrôle d'accès .



4 Cliquez sur **Enregistrer** pour confirmer les modifications.

Les superviseurs ont maintenant plus de contrôle pour gérer leurs subordonnés. Ils peuvent maintenant modifier les champs d'informations d'identité **General** et les paramètres de **Contrôle d'accès**.

Lorsque vous avez terminé

Modifier les informations de vos subordonnés.

Rubriques connexes

Transférer les subordonnés, page 175

Afficher les autorisations supplémentaires

Vous pouvez utiliser la page *Autorisations* pour vérifier quelle identité ou quel rôle dispose d'un accès supplémentaire pour afficher et gérer les identités. Vous pouvez également utiliser la page *Permissions* pour vérifier l'accès des superviseurs à la gestion de leurs subordonnés.

Avant de commencer

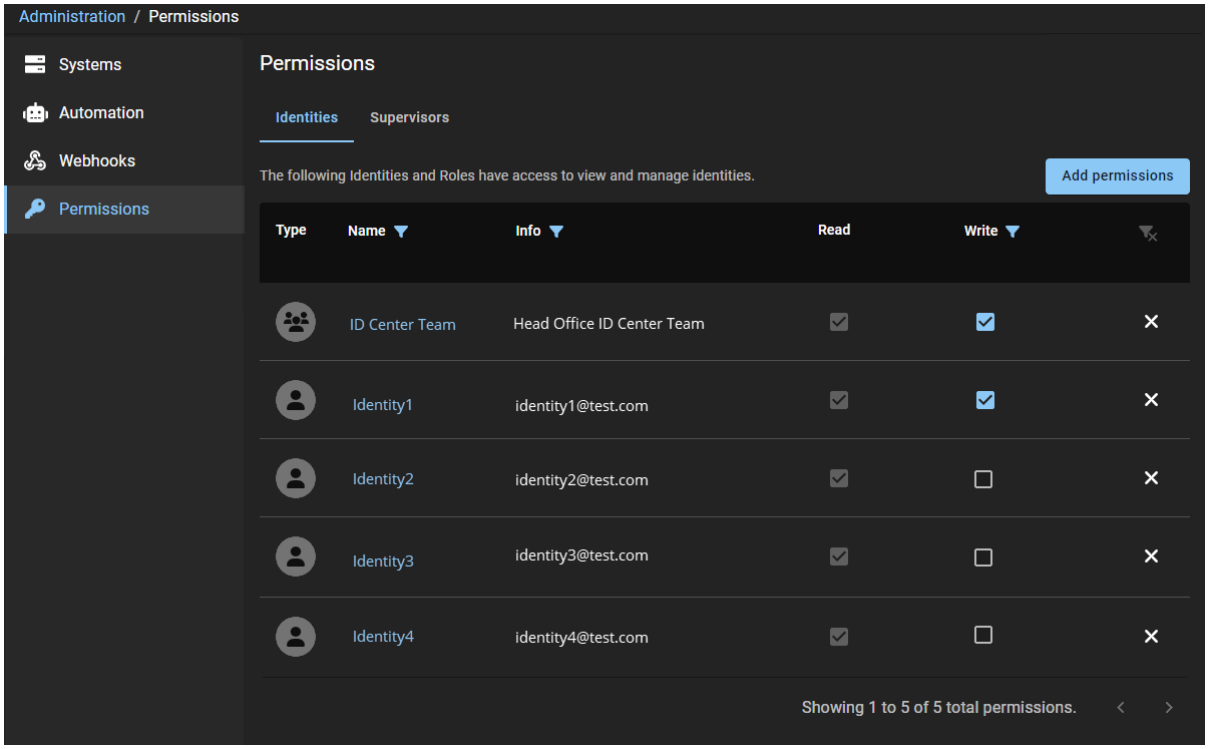
- Accorder des permissions supplémentaires pour les identités et les rôles.
- Accorder des autorisations supplémentaires aux superviseurs.

À savoir

Seul un administrateur de compte peut afficher les autorisations d'identité et de rôle ou les autorisations de superviseur.

Procédure

1 Sur la page *Accueil*, cliquez sur **Administration** > **Autorisations**.



Dans la colonne **Type**, chaque ligne possède un identificateur visuel qui indique si l'entrée est un rôle ou une identité.

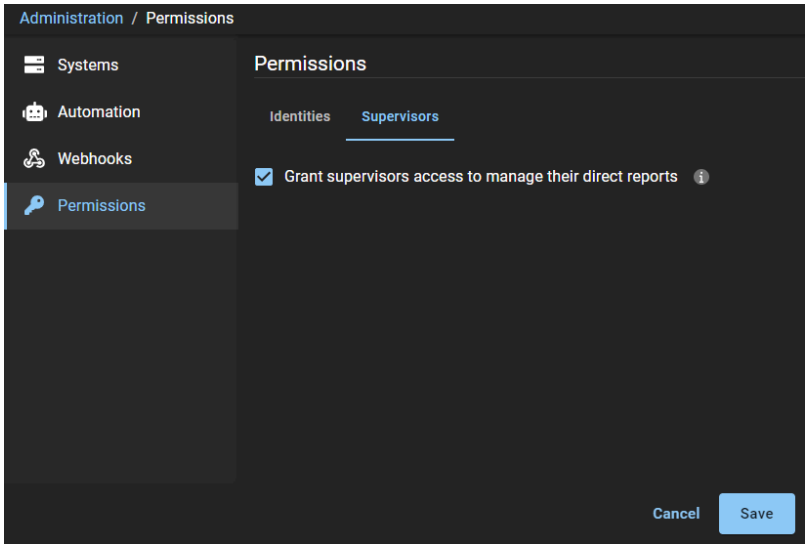
2 Dans la colonne **Nom**, cliquez sur pour filtrer les résultats par nom d'identité ou de rôle.

3 Dans la colonne **Info**, cliquez sur pour filtrer les résultats par adresse e-mail ou saisissez les mots à rechercher dans les informations d'autorisation.

4 Dans la colonne **Écrire**, cliquez sur pour filtrer les résultats par autorisation. Par exemple, pour voir quelles identités ont des autorisations de **Lecture et d'Écriture**.

5 (Facultatif) Cliquez sur **Effacer les filtres** () pour réinitialiser les filtres et restaurer la vue de page par défaut.

6 (Facultatif) Cliquez sur l'onglet **Superviseurs** pour vérifier si les superviseurs ont accès à la gestion de leurs subordonnés.



Lorsque vous avez terminé

Modifier les autorisations supplémentaires.

Modifier les autorisations supplémentaires

Vous pouvez utiliser la page *Autorisations* pour modifier quelle identité ou quel rôle dispose d'un accès supplémentaire pour afficher et gérer les identités. Vous pouvez également utiliser la page *Permissions* pour modifier l'accès des superviseurs à la gestion de leurs subordonnés.

Avant de commencer

Afficher les autorisations supplémentaires.

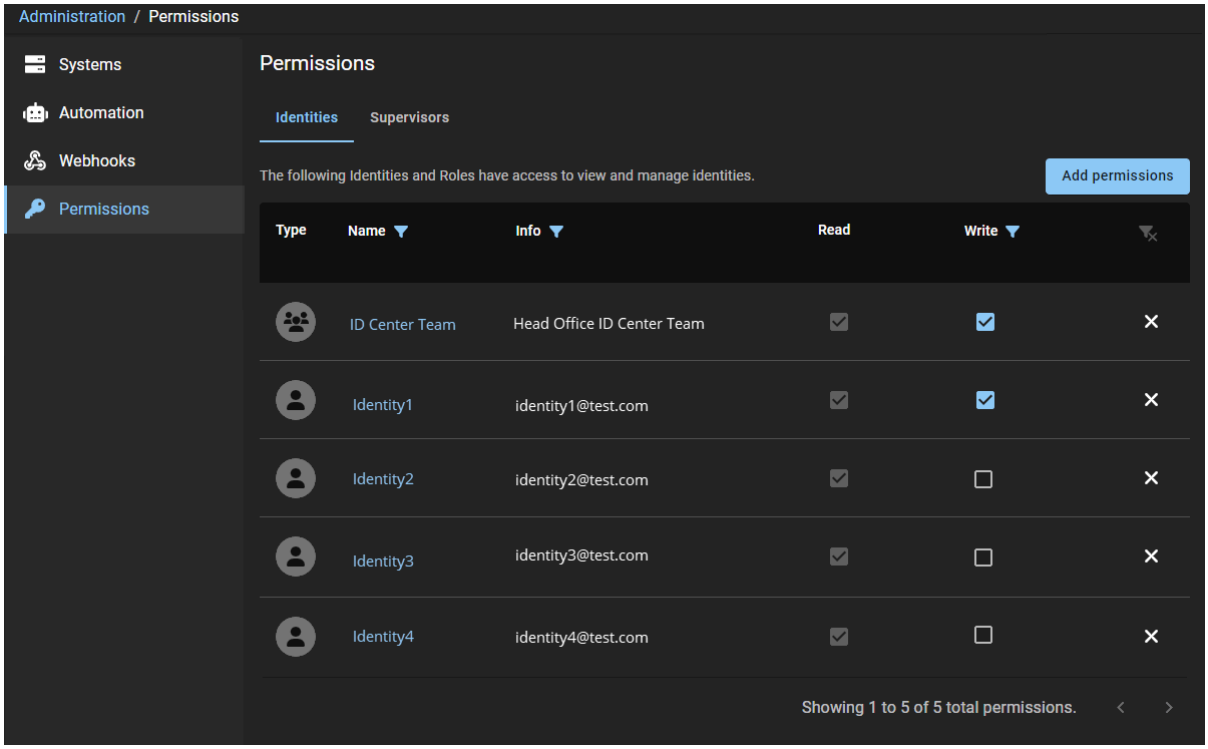
À savoir

Seul un administrateur de compte peut modifier des autorisations d'identité et de rôle.

Procédure

Pour modifier des autorisations d'identité et de rôle :

1 Sur la page *Accueil*, cliquez sur **Administration** > **Autorisations**.



Dans la colonne **Type**, chaque ligne possède un identificateur visuel qui indique si l'entrée est un rôle ou une identité.

2 Dans la colonne **Nom**, cliquez sur pour filtrer les résultats par nom d'identité ou de rôle.

3 Dans la colonne **Info**, cliquez sur pour filtrer les résultats par adresse e-mail ou saisissez les mots à rechercher dans les informations d'autorisation.

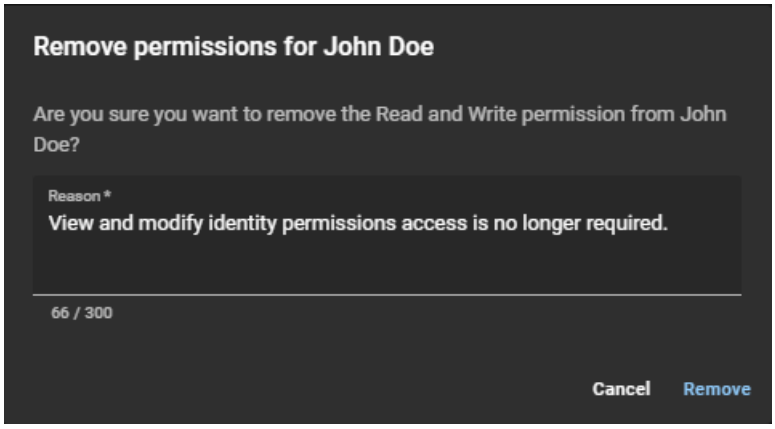
4 Dans la colonne **Écrire**, cliquez sur pour filtrer les résultats par autorisation. Par exemple, pour voir quelles identités ont des autorisations de **Lecture et d'Écriture**.

5 (Facultatif) Cliquez sur **Effacer les filtres** () pour réinitialiser les filtres et restaurer la vue de page par défaut.

6 (Facultatif) Dans la colonne **Écrire**, cochez ou décochez la case en regard d'une identité ou d'un rôle pour ajouter ou supprimer leur accès en **Écriture**.

a) Cliquez sur **Enregistrer** pour soumettre vos modifications.

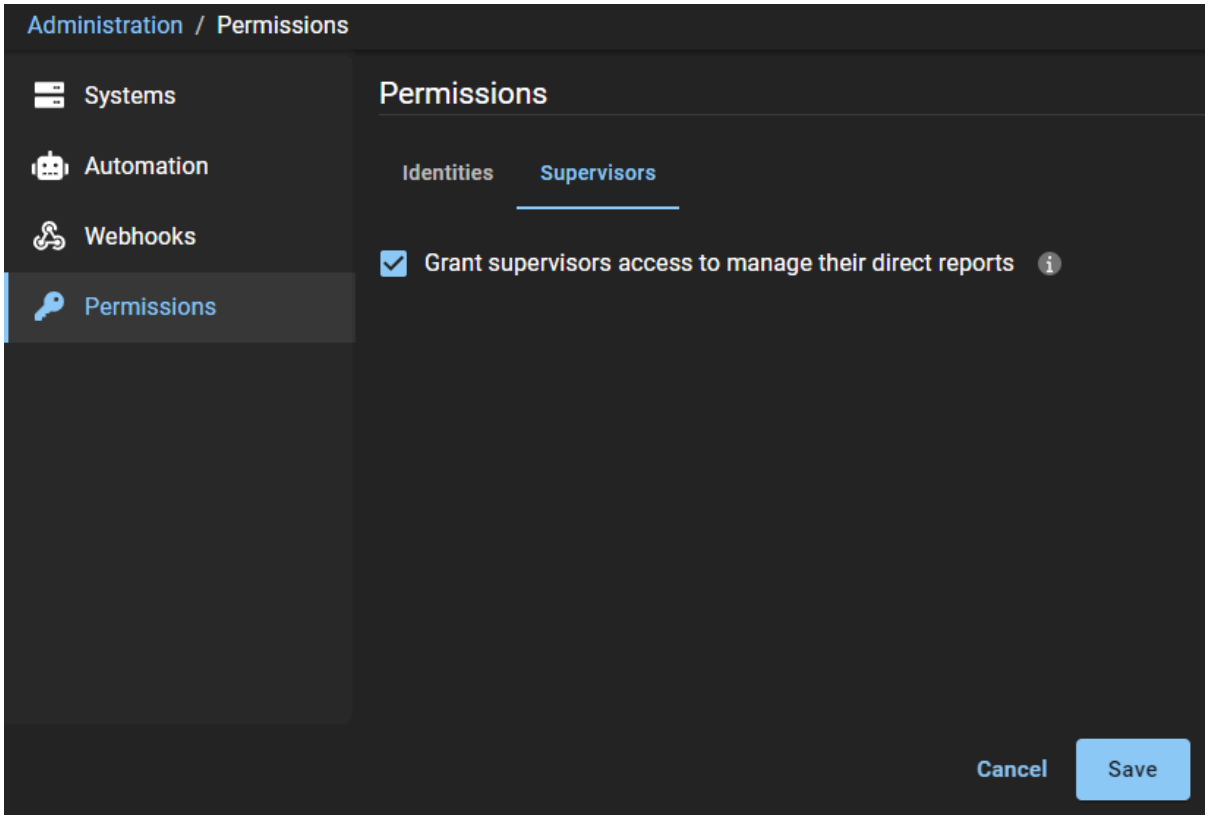
7 (Facultatif) Cliquez sur ✕ en regard d'une identité ou d'un rôle pour supprimer les autorisations supplémentaires (**Lecture** et **Écriture**) qui ne sont plus nécessaires.



a) Saisissez une `Raison`.
b) Cliquez sur **Supprimer**.

Pour modifier les autorisations du superviseur :

1 (Facultatif) Cliquez sur l'onglet **Superviseurs** pour modifier les autorisations du superviseur.



a) Apportez les modifications souhaitées et cliquez sur **Enregistrer**.

Afficher les identités

Vous pouvez afficher les identités dans Genetec ClearID[MC] pour examiner l'état du contrôle d'accès, des informations générales ou vérifier si des superviseurs ont été désignés.

Avant de commencer

Créez vos identités.

À savoir

Seuls les administrateurs de compte, les identités ou les rôles disposant des autorisations requises peuvent afficher les identités.

Procédure

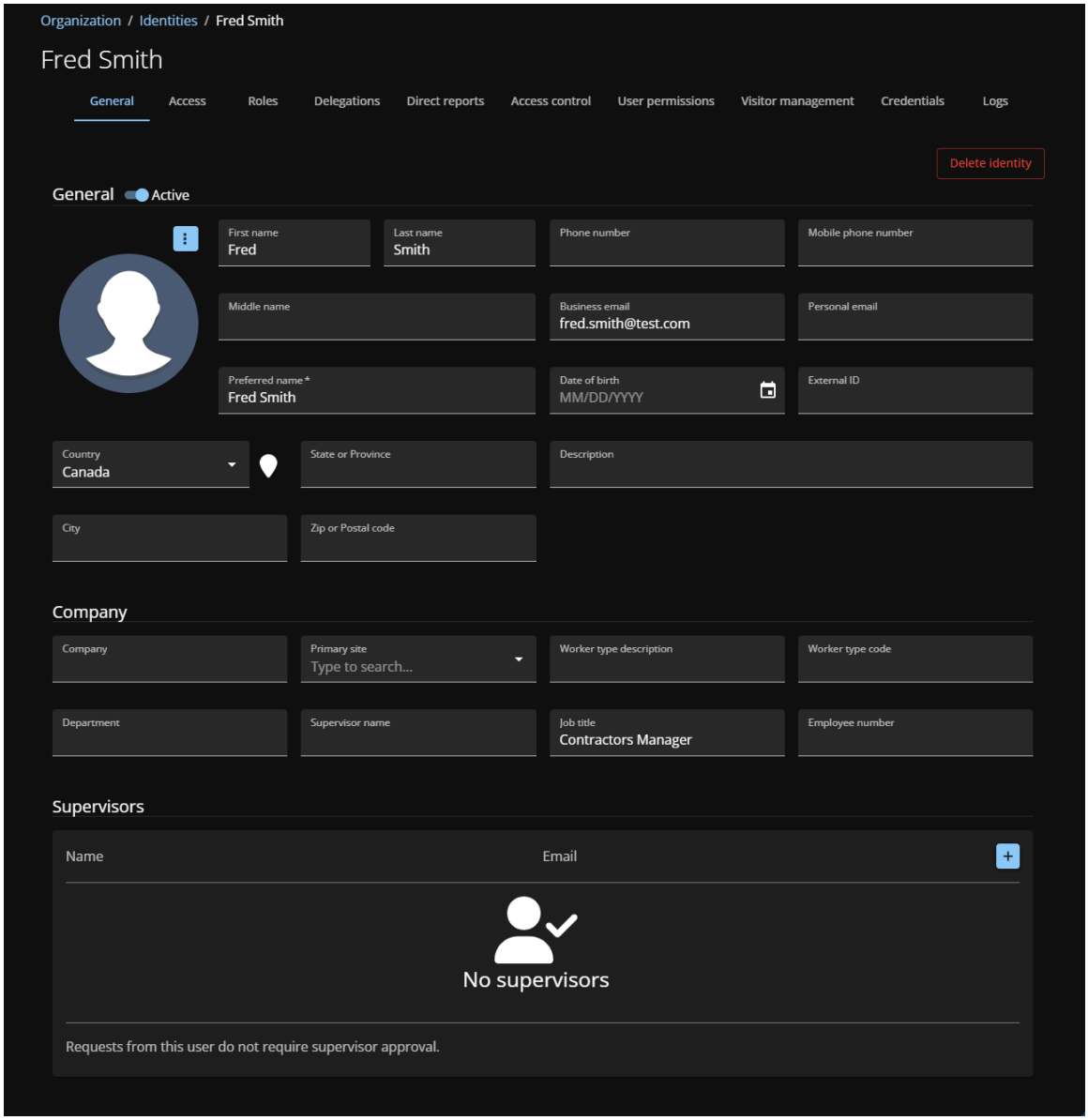
1 Sur la page *d'accueil*, cliquez sur **Organisation** > **Identités**.

2 Sélectionnez une option dans le menu déroulant pour afficher les identités dont vous avez besoin. Choisissez l'une des options suivantes :

- **Actif :** Affiche les identités actives.
- **Inactif :** Affiche les identités inactives.
- **Tous :** Affiche toutes les identités actives et inactives.

3 Dans le champ **Rechercher**, saisissez des critères de recherche et appuyez sur entrée.

4 Sélectionnez une identité dans la liste pour afficher les détails de l'identité.



5 Dans l'onglet **Général**, examinez les informations sur l'identité, comme les superviseurs associés ou l'état de l'identité (actif ou inactif).

6 (Facultatif) Des onglets supplémentaires permettent d'examiner d'autres informations et options associées à l'identité sélectionnée :

- **Champs personnalisés :** Champs personnalisés associés à l'identité sélectionnée.
- **Accès :** Accès associés à l'identité sélectionnée.
- **Rôles :** Rôles associés à l'identité sélectionnée, ajoutés manuellement ou par une règle de provisionnement.
- **Délégations :** Délégations associées à l'identité sélectionnée.
- **Subordonnés :** Subordonnés associés à l'identité sélectionnée.
- **Contrôle d'accès :** Contrôles d'accès associés à l'identité sélectionnée, comme le délai d'accès prolongé, l'activation de titulaire de cartes, les attributs de provisionnement et les titulaires de cartes associés.
- **Autorisations utilisateur :** Autorisations d'accès au portail web des utilisateurs ou administrateurs associées à l'identité sélectionnée.
- **Gestion des visiteurs :** Liste des sites où l'identité sélectionnée peut inviter des visiteurs.
- **Identifiants :** Identifiants synchronisés associés à l'identité sélectionnée.

  CONSEIL : Vous pouvez également synchroniser les identifiants au niveau d'une identité individuelle. Sélectionnez une identité, cliquez sur l'onglet **Identifiants**, puis cliquez sur **Synchroniser**.
- **Journaux :** Journaux d'événements d'identité associés à l'identité sélectionnée.

Lorsque vous avez terminé

Modifier vos identités.

Modifier les identités

Après avoir ajouté des identités, vous devrez peut-être modifier les détails de l'identité. Vous pouvez désactiver ou activer une identité, ou modifier les détails de l'identité à la suite d'une modification de l'intitulé du poste, du service, de l'entreprise, des superviseurs, des informations personnelles, etc.

Avant de commencer

Créez vos identités.

À savoir

- Seuls les administrateurs de compte, les superviseurs, les identités ou les rôles disposant des autorisations requises peuvent modifier les identités.
- Seul un administrateur de compte peut supprimer les identités.

IMPORTANT : Si vous effectuez des mises à jour d'identités synchronisées avec une source de données externe, vos modifications peuvent être écrasées par la synchronisation.

Procédure

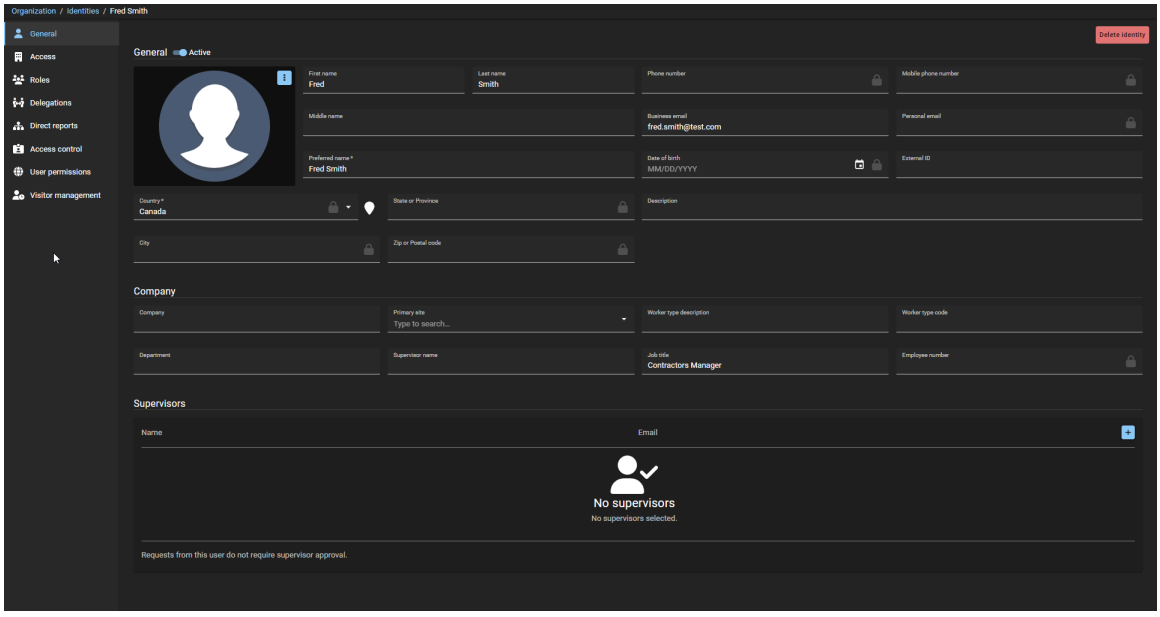
1 Sur la page *d'accueil*, cliquez sur **Organisation** > **Identités**.

2 Sélectionnez une option dans le menu déroulant pour afficher les identités dont vous avez besoin. Choisissez l'une des options suivantes :

- **Actif :** Affiche les identités actives.
- **Inactif :** Affiche les identités inactives.
- **Tous :** Affiche toutes les identités actives et inactives.

3 Dans le champ **Rechercher**, saisissez vos critères de recherche et appuyez sur entrée.

4 Sélectionnez une identité dans la liste pour afficher les détails de l'identité.



5 Modifiez les paramètres, ou désactivez ou activez une identité selon vos besoins.

Par exemple, à la suite d'une modification de l'intitulé du poste, du service, de l'entreprise, des superviseurs, des informations personnelles, et ainsi de suite.

6 Cliquez sur **Enregistrer** pour soumettre vos modifications.

Lorsque vous avez terminé

Supprimez les identités obsolètes ou qui ne sont plus nécessaires.

Rubriques connexes

Synchroniser les photos d'identité ClearID avec Security Center, page 134

Supprimer des identités

Un administrateur peut supprimer les identités obsolètes ou qui ne sont plus nécessaires. Par exemple, lorsqu'une personne quitte l'organisation ou lorsqu'une identité a été créée par erreur.

Avant de commencer

Des identités prêtes à être supprimées doivent avoir été créées préalablement.

À savoir

Seul un administrateur de compte peut supprimer les identités.

- Les fonctions de recherche et les données d'historique sont conservées après la suppression d'une identité, pour que vous puissiez voir quand l'accès de la personne a été révoqué et pourquoi.
- L'identité est également supprimée de toutes les listes des approbateurs, propriétaires et responsables, et le cas échéant des demandes d'identité.

Procédure

1 Sur la page *d'accueil*, cliquez sur **Organisation** > **Identités**.

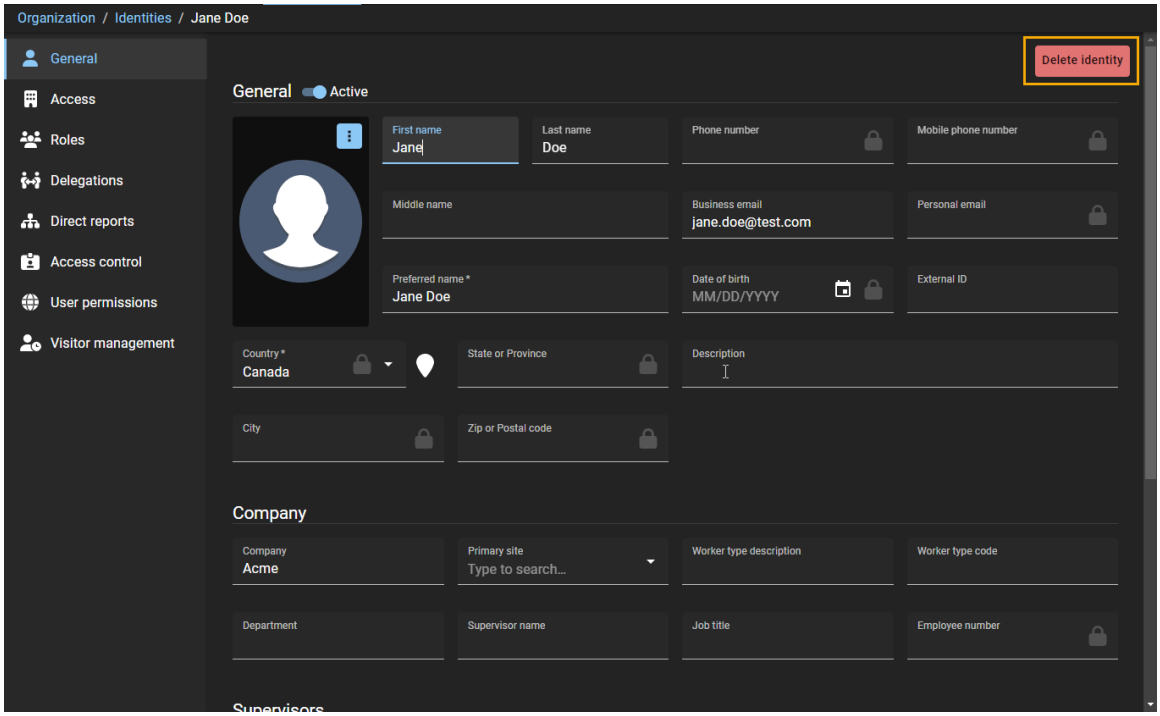
2 Sélectionnez une option dans le menu déroulant pour afficher les identités dont vous avez besoin. Choisissez l'une des options suivantes :

- **Actif :** Affiche les identités actives.
- **Inactif :** Affiche les identités inactives.
- **Tous :** Affiche toutes les identités actives et inactives.

3 Dans le champ **Rechercher**, saisissez vos critères de recherche et appuyez sur entrée.

4 Sélectionnez une identité dans la liste pour afficher les détails de l'identité.

5 Cliquez sur **Supprimer une identité**.



6 Cliquez sur **Supprimer** pour confirmer la suppression.

Synchroniser les photos d'identité ClearID avec Security Center

Pour gérer les photos d'identités et de titulaires de cartes de manière centralisée, les *administrateurs de comptes* peuvent configurer Genetec ClearID[MC] en tant que source de données officielle pour toutes les photos de titulaires de cartes dans Security Center.

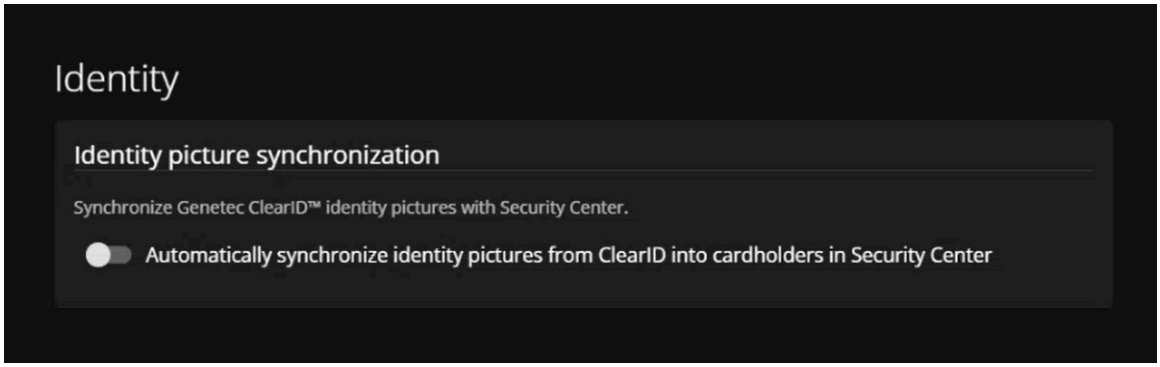
Avant de commencer

Vérifiez que Security Center est connecté à ClearID.

Procédure

1 Sur le portail web ClearID, cliquez sur **Administration** > **Configuration du compte**.

2 Dans la section *Identité*, activez l'option **Synchronisation des photos d'identité**.



3 Les photos d'identité ClearID sont synchronisées automatiquement avec Security Center, et remplacent les photos de titulaires de cartes existantes. Si une photo de titulaire de cartes est modifiée dans Security Center lorsque la synchronisation des photos d'identité est activée, les modifications sont remplacées par ClearID.

REMARQUE : En l'absence de photos d'identité dans ClearID lors de la première activation de la synchronisation, les photos ne sont pas remplacées dans Security Center.

Rubriques connexes

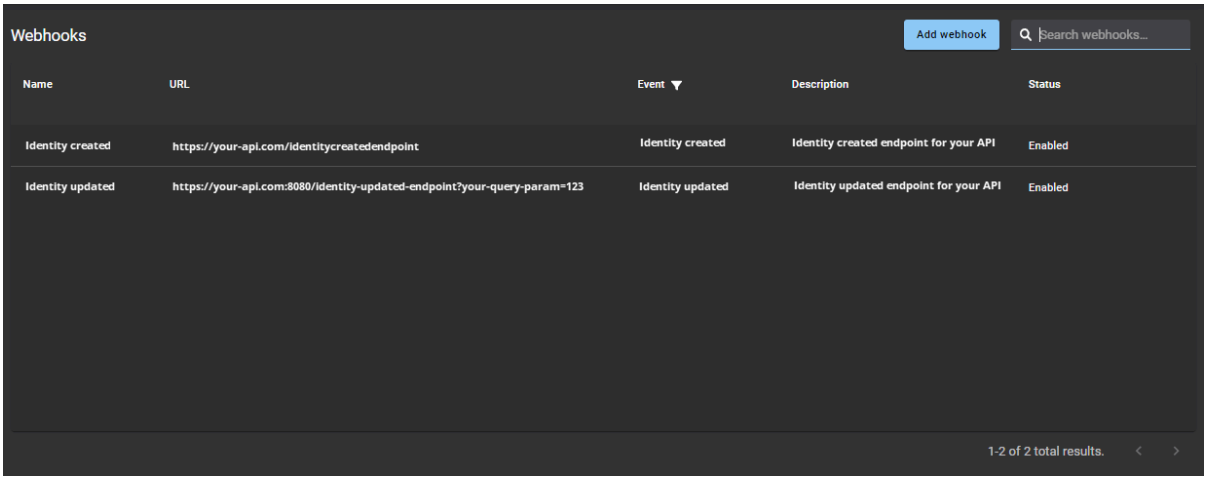
Connecter Security Center à ClearID, page 91
À propos des relations entre les titulaires de carte et les identités, page 87
Examiner les informations de titulaires de cartes et d'identifiants, page 92
Modifier les identités, page 130

À propos des points d'ancrage

Un point d’ancrage est un lien de rappel HTTP défini par l’utilisateur. Un point d’ancrage peut être déclenché par un événement dans une application Web et être utilisé pour envoyer des données ou des notifications à une interface de programmation (API) tierce.

Points d'ancrage dans Genetec ClearID[MC]

Dans ClearID, les points d'ancrage peuvent être créés et utilisés pour notifier les API tierces qu'un événement particulier est survenu.



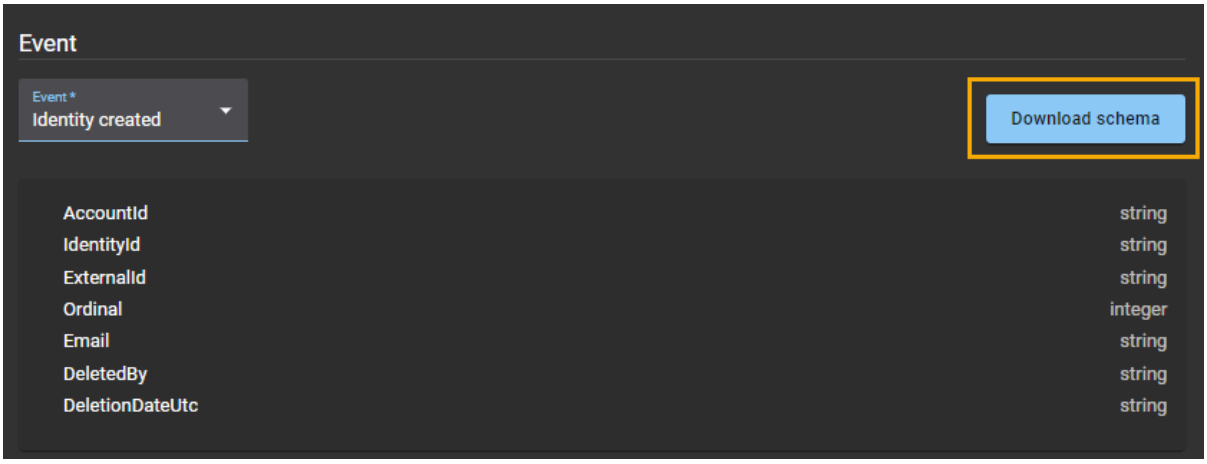
Par exemple, une notification contenant un lien vers des informations détaillées concernant une identité peut être envoyée par e-mail lorsqu’un évènement **Identité mise à jour** se produit, ou si vous souhaitez que d’autres parties prenantes soient notifiées après un évènement **Demandes d’identité créées** ou **Demandes d’identité mises à jour**.

Traitement de point d’ancrage

Une fois que le point d'ancrage est créé, le service webhook reste à l'écoute d'un sous-ensemble d’événements spécifiés provenant d'autres services ClearID. Lorsque l’évènement spécifié se produit, le service point d’ancrage notifie l’API spécifiée dans le champ **URL** de la section *Détails du point d’ancrage*.

Schémas d’évènement du point d’ancrage

Le schéma décrit l’objet qui est envoyé via le point d’ancrage et le contenu du schéma varie en fonction du type d’évènement spécifié. Le schéma d’évènement du point d’ancrage peut être téléchargé à partir de la section *Évènement* du point d’ancrage pour vous aider à comprendre la structure de données des évènements afin qu’ils puissent être récupérés et traités correctement du côté utilisateur de l’intégration du point d’ancrage.



Pour en savoir plus sur le téléchargement de schéma, voir Créer des points d'ancrage , page 138.

Journaux du point d'ancrage

Les propriétaires d'API tierces peuvent utiliser les journaux de point d'ancrage pour vérifier l'état de chaque demande de rappel HTTP envoyée à l'URL tierce et résoudre les problèmes liés aux points d'ancrage non reçus ou autres problèmes associés. Il peut s'agir, par exemple, de problèmes d'expéditeur, de problèmes de destinataire, etc.

Les journaux de point d'ancrage incluent les éléments suivants :

- **Date de rappel :** Date à laquelle le rappel a été envoyé (inclut des filtres de plage de dates).
- **URL :** URL utilisée pour transférer la notification d'évènement de point d'ancrage à l'API (programme ou application) tierce correspondante.
- **Réponse :** L'état de la réponse indique si le rappel HTTP a été reçu avec succès ou non par l'API tierce. L'état peut, par exemple, être accepté, requête incorrecte, erreur de serveur interne, etc.

REMARQUE : La section *Journaux* du point d'ancrage s'affiche uniquement à la fin des détails du point d'ancrage après le premier rappel.

Créer des points d'ancrage

Vous pouvez créer des points d'ancrage dans Genetec ClearID[MC] pour intégrer des API de solutions tierces, afin de pouvoir notifier les parties prenantes lorsque certains événements surviennent.

Avant de commencer

En savoir plus sur les points d’ancrage.

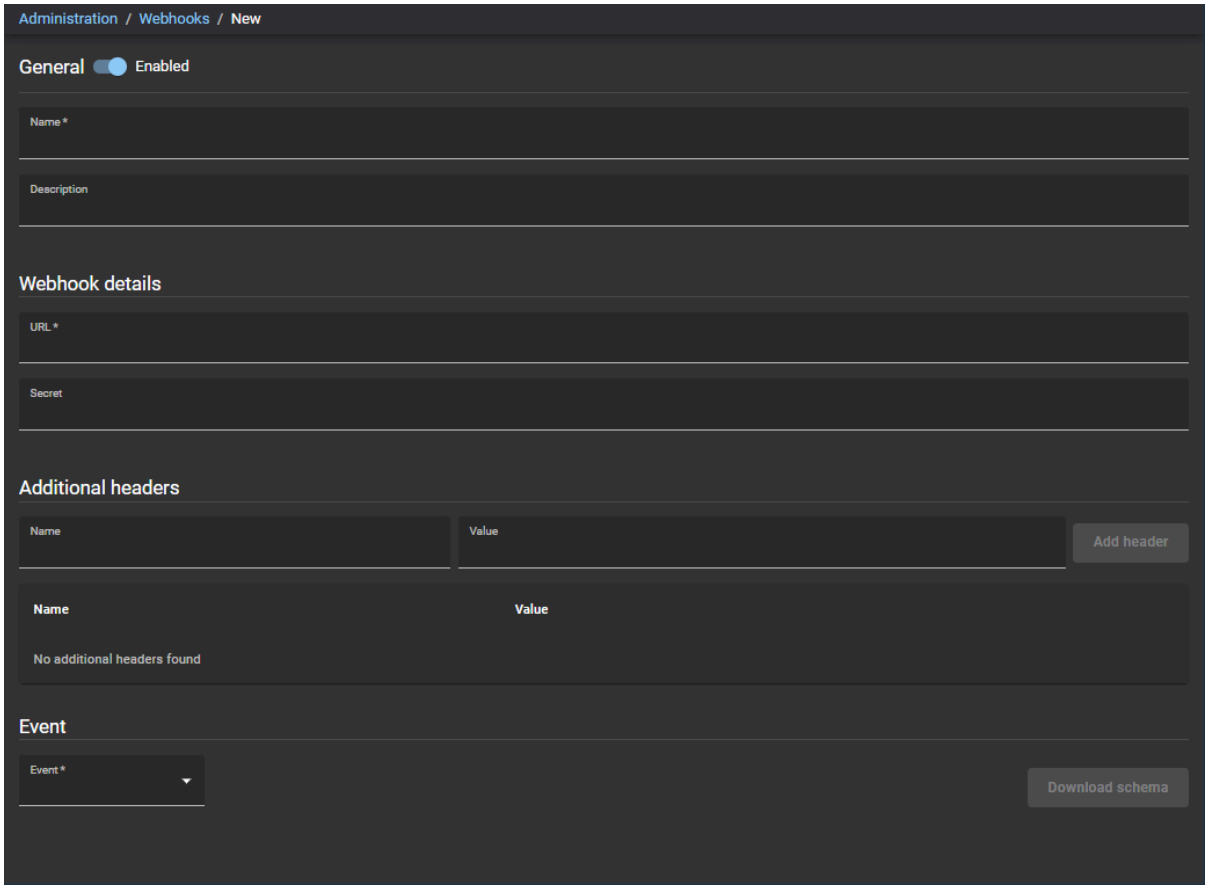
À savoir

- Seul un administrateur de compte peut créer des points d'ancrage dans ClearID.
- Les organisations externes développent leurs propres API pour solutions tierces (programmes ou applications) qui exploitent les notifications (par callback) des points d’ancrage ClearID.

Procédure

1 Sur la page *Accueil*, cliquez sur **Administration** > **Points d’ancrage**.

2 Cliquez sur **Ajouter un point d’ancrage**.



3 Dans la section *Général*, remplissez les champs :

a) (Facultatif) Déplacez le curseur **Activé** pour activer ou désactiver le point d'ancrage.

REMARQUE : Lorsque le point d'ancrage est *désactivé*, le rappel HTTP ne se produit pas.

b) Dans le champ **Nom**, saisissez un `Nom` représentatif afin de pouvoir facilement identifier votre point d'ancrage ultérieurement.

Par exemple, **Identité mise à jour** ou **Point d'ancrage Demandes d'identité créées**, etc.

c) Dans le champ **Description**, saisissez un `texte` qui décrit l'objectif du point d'ancrage.

Par exemple, à quoi sert le point d'ancrage et quelle API (programme ou application) il notifie lorsque des évènements se produisent.

4 Dans la section *Détails du point d'ancrage*, remplissez les champs :

a) Saisissez une *URL* HTTPS : `/ /` valide pour votre API (programme ou application).

Les URL peuvent inclure des ports et des paramètres de requête comme suit :

- Exemple 1 : *https://my-api.com/identityupdatedendpoint*
- Exemple 2 : *https://my-api.com:8080/identity-updated-endpoint?my-query-param=123*

Cette URL est utilisée pour transférer la notification d'évènement de point d'ancrage à l'API (programme ou application) tierce correspondante.

REMARQUE : Votre organisation est chargée de fournir l'URL vers laquelle vous souhaitez que les notifications d'évènements de point d'ancrage soient transférées.

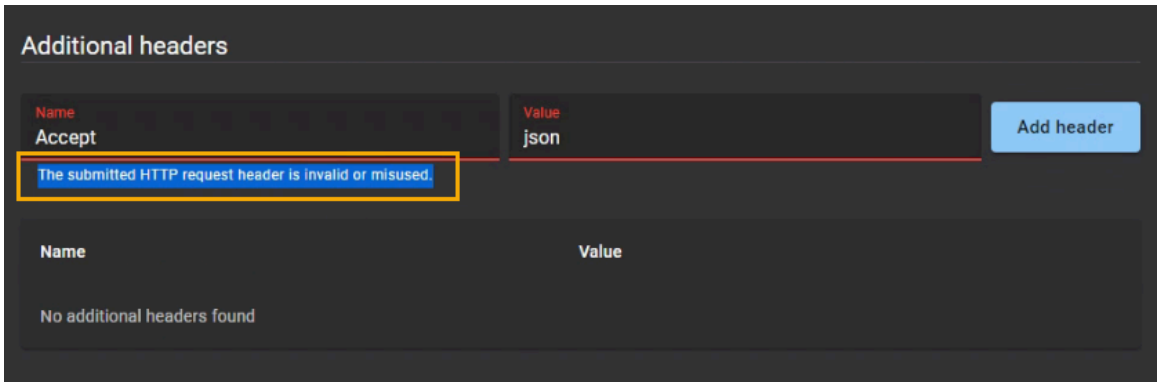
b) (Facultatif) Saisissez le Code `secret` (clé d'application) si l'API tierce l'exige.

Le code secret (la clé d'application) sert à authentifier les communications entre le point d'ancrage ClearID et l'API tierce de votre organisation.

5 (Facultatif) Dans la section *En-têtes supplémentaires*, remplissez les champs :

Des en-têtes HTTP personnalisés supplémentaires peuvent être ajoutés à la demande de rappel HTTP afin qu'ils puissent être utilisés par l'API tierce du côté utilisateur de l'intégration.

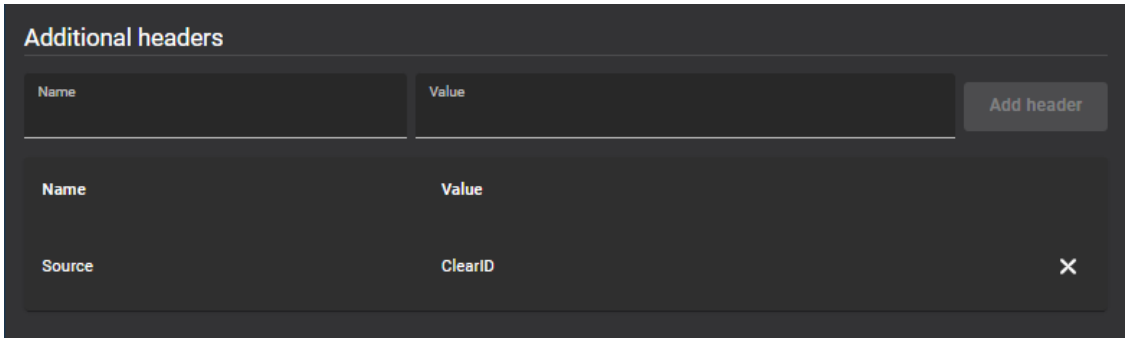
REMARQUE : Si vous saisissez un en-tête non valide ou réservé, le message suivant s'affiche L'en-tête de la requête HTTP soumis est incorrect ou mal utilisé.



a) Saisissiez le `Nom` du paramètre d'en-tête.

Par exemple, si un événement provient de plusieurs sources, des en-têtes de requêtes HTTP supplémentaires peuvent servir à indiquer la provenance de l'événement (ClearID ou une API externe).

Exemple:



b) Saisissiez la `Valeur` du paramètre d'en-tête.

c) (Facultatif) Cliquez sur **Ajouter un en-tête** pour ajouter des en-têtes de requête HTTP supplémentaires selon les besoins.

Par exemple, si votre API attend ou requiert un ensemble spécifique d'en-têtes (hôte, origine, langue, et ainsi de suite).

d) (Facultatif) Cliquez sur ✕ pour supprimer les en-têtes qui ne sont plus nécessaires.

6 Dans la section **Évènement**, configurez les paramètres dont vous avez besoin :

a) Dans la liste **Évènement**, sélectionnez un évènement que ce point d'ancrage doit écouter.

b) Cliquez sur **Télécharger le schéma** et suivez les invites de votre navigateur.

BONNE PRATIQUE : Utilisez les informations relatives au schéma téléchargé pour comprendre la structure de données des évènements afin qu'ils puissent être récupérés et traités correctement du côté utilisateur de l'intégration.

L'exemple suivant montre un extrait d'un fichier *schema-identitycreated.json* :

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "IdentityDeletedCallbackModel",
  "type": "object",
  "additionalProperties": false,
  "required": [
    "AccountId",
    "IdentityId",
    "DeletedBy",
    "DeletionDateUtc"
  ],
  "properties": {
    "AccountId": {
      "type": "string",
      "description": "The account id for which this identity is member of.",
      "minLength": 1
    },
    "IdentityId": {
      "type": "string",
      "description": "A unique id to identify the identity.",
      "minLength": 1
    },
    "ExternalId": {
      "type": [
        "null",
        "string"
      ],
      "description": "External ID"
    },
    "Ordinal": {
      "type": [
        "integer",
        "null"
      ],
      "description": "Commit ordinal in the storage.",
      "format": "int64"
    },
    "Email": {
      "type": [
        "null",
        "string"
      ],
```

7 Cliquez sur **Enregistrer**.

Votre point d'ancrage est maintenant configuré pour s'intégrer à une API tierce (programme ou application) afin de notifier les parties intéressées lorsque des évènements spécifiques se produisent.

Lorsque vous avez terminé

À l'aide du schéma téléchargé, configurez votre API tierce pour recevoir et traiter les notifications du point d'ancrage.

Modifier les points d'ancrage

Après avoir créé vos points d’ancrage, vous devrez peut-être modifier les détails du point d’ancrage. Vous pouvez désactiver ou activer un point d’ancrage et modifier les détails du point d’ancrage ou le type d’évènement si nécessaire.

Avant de commencer

Créer vos points d’ancrage.

À savoir

Seul un administrateur de compte peut modifier les points d'ancrage dans Genetec ClearID[MC].

Procédure

1 Sur la page *Accueil*, cliquez sur **Administration** > **Points d’ancrage**.

2 Sélectionnez le point d’ancrage que vous souhaitez modifier.

CONSEIL : Si la liste est longue, utilisez le champ **Rechercher** pour trouver le point d’ancrage dont vous avez besoin.

3 Dans la section *Général*, modifiez les champs selon vos besoins.

a) (Facultatif) Déplacez le curseur **Activé** pour activer ou désactiver le point d’ancrage.

REMARQUE : Lorsque le point d’ancrage est *désactivé*, le rappel HTTP ne se produit pas.

4 Dans la section *Détails du point d’ancrage*, modifiez les champs selon vos besoins :

5 (Facultatif) Dans la section *En-têtes supplémentaires*, modifiez les champs selon vos besoins :

6 Dans la section *Évènement*, modifiez les paramètres dont vous avez besoin.

7 Cliquez sur **Enregistrer**.

Consulter les journaux de points d'ancrage

Pour résoudre les problèmes de points d’ancrage non reçus ou d’autres problèmes associés, les propriétaires d’une interface de programmation (API) tierce peuvent utiliser les journaux de points d’ancrage pour vérifier l’état de chaque demande de rappel HTTP envoyée à l’URL tierce.

Avant de commencer

Créer vos points d’ancrage.

À savoir

- Seul un administrateur de compte ou le propriétaire d'une API tierce peut consulter les journaux de points d'ancrage dans Genetec ClearID[MC].
- La section *Journaux* du point d’ancrage s’affiche uniquement à la fin des détails du point d’ancrage après le premier rappel.

Procédure

1 Sur la page *Accueil*, cliquez sur **Administration** > **Points d’ancrage**.

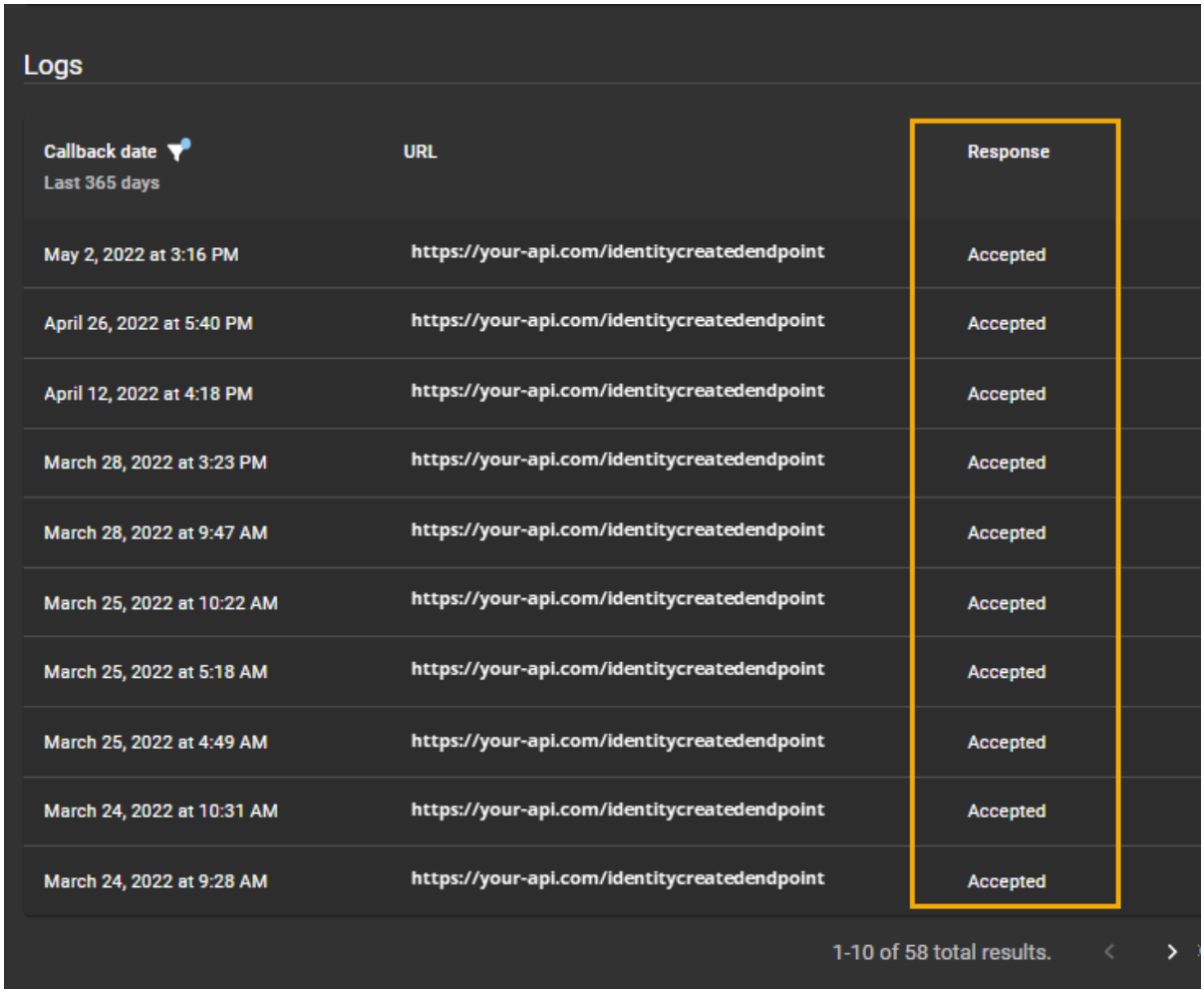
2 Sélectionnez le point d’ancrage que vous souhaitez dépanner.

CONSEIL : Si la liste des **Points d’ancrage** est longue, vous pouvez utiliser le champ **Rechercher** pour trouver le point d’ancrage dont vous avez besoin.

3 Dans la colonne **Date de rappel** de la section *Journaux*, cliquez sur pour sélectionner une plage spécifiée ou utilisez le sélecteur de **Plage de dates** pour spécifier votre propre plage.

REMARQUE : La période de la plage de données de rappel est limitée à un maximum de 1 an et les informations de rappel sont affichées dans l'ordre chronologique inverse.

L'image suivante montre les journaux de rappel contenant les réponses *Acceptées*.



L'image suivante montre les journaux de rappel contenant les réponses *RequêteIncorrecte*.

4 Consultez les informations des **Journaux** comme suit :

a) Dans la colonne **Date de rappel**, consultez la date à laquelle le rappel a été envoyé (inclut des filtres de plage de dates).

b) Dans la colonne **URL**, consultez l'URL utilisée pour transférer la notification d'évènement du point d'ancrage indiquant qu'un évènement spécifié s'est produit à l'API tierce (programme ou application) correspondante.

c) Dans la colonne **Réponse**, consultez les états pour vérifier si le rappel HTTP a été reçu avec succès ou non par l'API tierce. Les états peuvent, par exemple, être **Accepté**, **RequêteIncorrect**, **ErreurServeurInterne**, etc.

d) (Facultatif) Naviguez dans les journaux de rappel (vers l'avant ou vers l'arrière dans le temps) en cliquant sur les icônes **Page suivante** ou **Page précédente**.

Accorder l’accès au portail Web

Pour qu'un utilisateur puisse accéder au portail Web Genetec ClearID[MC], vous devez lui accorder les autorisations d'accès *Utilisateur* ou *Administrateur*.

Avant de commencer

L'identité à laquelle vous souhaitez accorder l'accès doit exister dans le système.

À savoir

- Pour accorder l’accès *Utilisateur* ou *Administrateur* au site web, vous devez être un administrateur de compte.

Procédure

- Choisissez l'une des options suivantes :
  - Pour accorder l’accès au portail web :
  - Accorder un accès Administrateur au portail web

L'identité sélectionnée a désormais accès au portail web avec les privilèges **Utilisateur** ou **Administrateur**.

Lorsque vous avez terminé

Connectez-vous au portail web.

Rubriques connexes

Afficher les sites où un utilisateur peut inviter des visiteurs, page 272

Accorder un accès utilisateur au portail Web

Pour qu'un utilisateur puisse accéder au portail Web Genetec ClearID[MC], vous devez lui accorder les autorisations d'accès nécessaires.

Avant de commencer

L'identité à laquelle vous souhaitez accorder l'accès doit exister dans le système.

À savoir

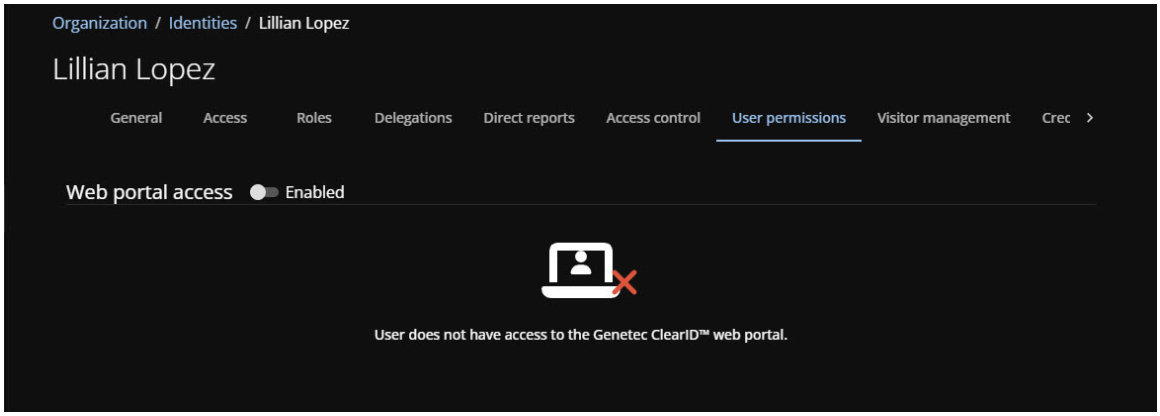
- Pour accorder des autorisations utilisateur pour accéder au site Web, vous devez être un administrateur de compte.

Procédure

1 Cliquez sur **Organisation** > **Identités**.

2 Recherchez un utilisateur ou sélectionnez-en un dans la liste Identités.

3 Cliquez sur **Autorisations utilisateur**.



4 Dans la section *Autorisations, d'utilisateur*, cliquez ou déplacez le curseur **Accès au portail web** vers **Activé** pour autoriser l'accès au portail web.

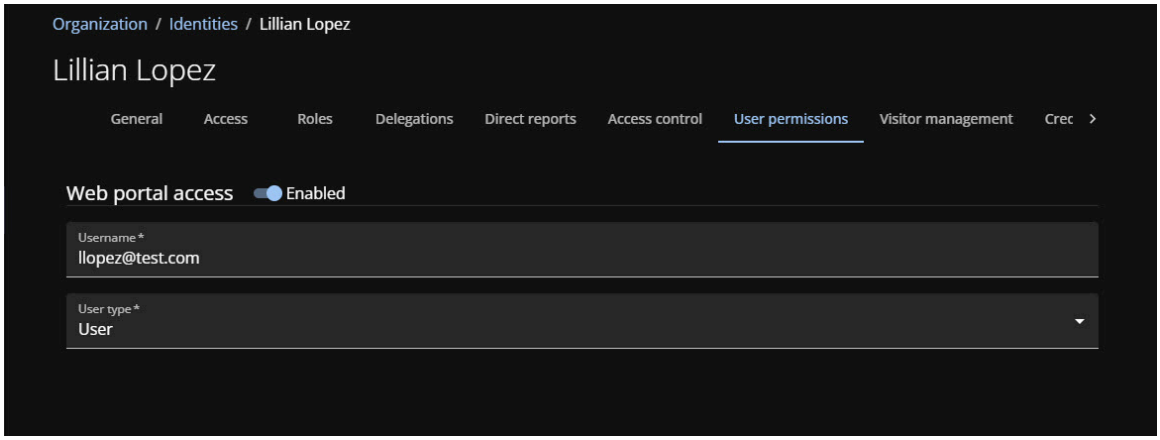
Si le curseur est désactivé, l'identité ne peut pas accéder au portail web.

REMARQUE : Certaines organisations n'activent pas l'accès au portail web pour toutes les identités, car leurs employés n'ont pas besoin de faire de demandes ou d'accéder au portail.

5 Dans le champ **Nom d'utilisateur**, entrez une adresse e-mail valable.

6 Dans la liste **Type d'utilisateur**, sélectionnez **Utilisateur** pour accorder un accès utilisateur par défaut au portail web.

7 Cliquez sur **Enregistrer** pour confirmer vos modifications.



L'identité sélectionnée a désormais accès au portail web avec les privilèges **Utilisateur**.

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles.

Lorsque vous avez terminé

Connectez-vous au portail web.

Accorder un accès administrateur au portail Web

Pour qu'un administrateur puisse accéder au portail Web Genetec ClearID[MC], vous devez lui accorder les autorisations d'accès nécessaires.

Avant de commencer

L'identité à laquelle vous souhaitez accorder l'accès doit exister dans le système.

À savoir

- Pour accorder l'accès administrateur au site Web, vous devez être un administrateur de compte.

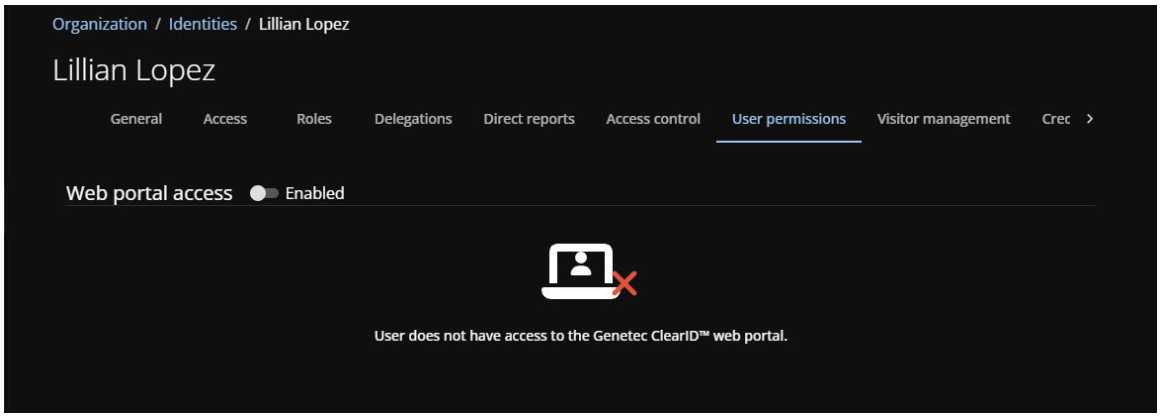
IMPORTANT : Lorsqu'un compte est créé, un utilisateur final désigné en tant qu'administrateur de compte reçoit une notification par e-mail Bienvenue à Genetec ClearID[MC] et Nouveau compte ClearID - NOMDUCOMPTE. Par défaut, un accès administrateur est accordé à l'utilisateur final qui reçoit l'e-mail. Si un intégrateur système ou une autre identité doit disposer d'un accès administrateur, l'utilisateur final (l'administrateur de compte) doit lui accorder.

Procédure

1 Cliquez sur **Organisation** > **Identités**.

2 Recherchez un utilisateur ou sélectionnez-en un dans la liste Identités.

3 Cliquez sur **Autorisations utilisateur**.



4 Dans la section *Autorisations, d'utilisateur*, cliquez ou déplacez le curseur **Accès au portail web** vers **Activé** pour autoriser l'accès au portail web.

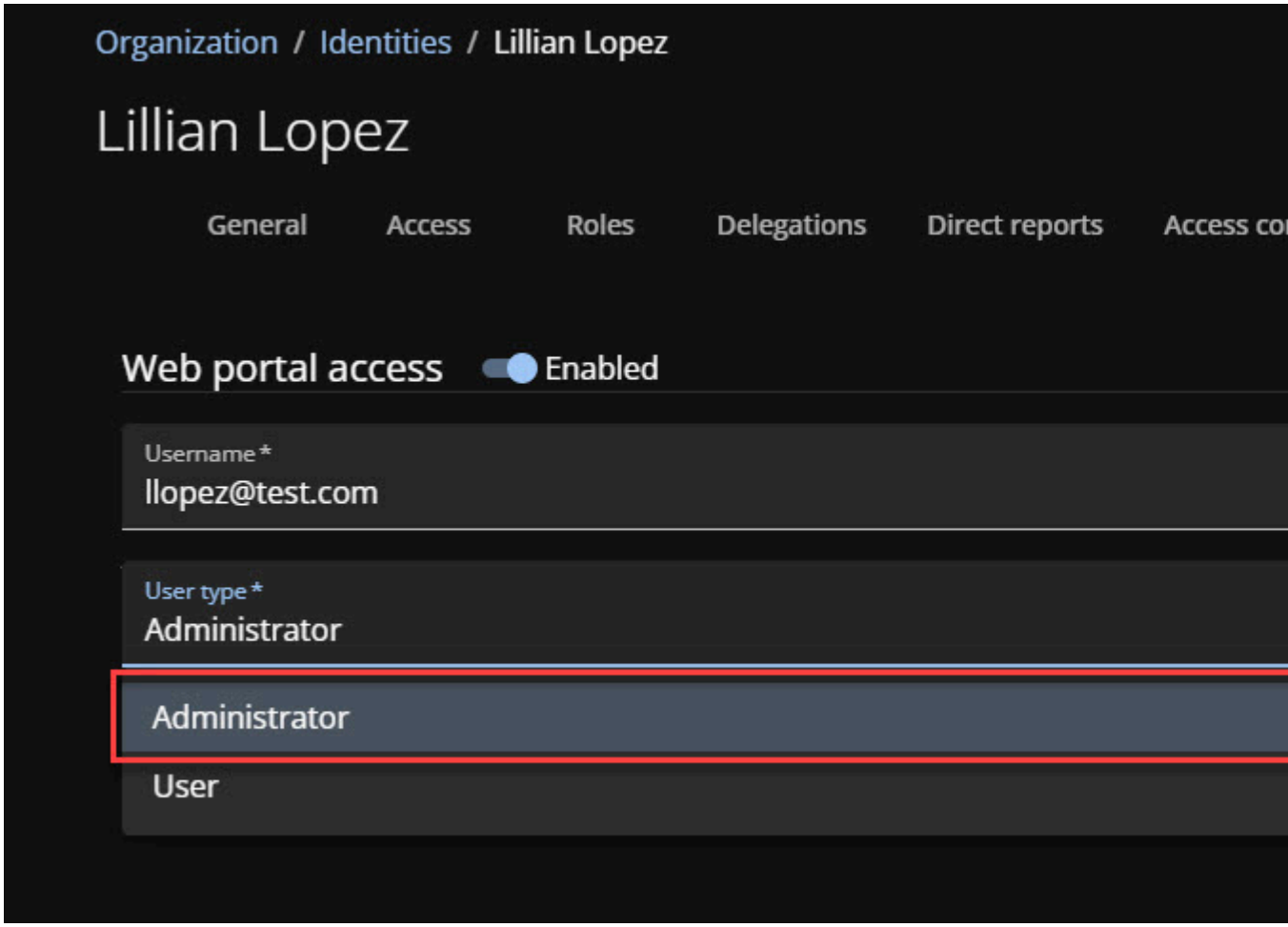
Si le curseur est désactivé, l'identité ne peut pas accéder au portail web.

REMARQUE : Certaines organisations n'activent pas l'accès au portail web pour toutes les identités, car leurs employés n'ont pas besoin de faire de demandes ou d'accéder au portail.

5 Dans le champ **Nom d'utilisateur**, entrez une adresse e-mail valable.

6 Dans la liste **Type d'utilisateur**, sélectionnez **Administrateur** pour accorder un accès administrateur au portail web.

7 Cliquez sur **Enregistrer** pour confirmer vos modifications.



L'identité a désormais accès au portail web avec les privilèges **Administrateur**.

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles.

Lorsque vous avez terminé

Connectez-vous au portail web.

Consulter votre profil

Vous pouvez utiliser la page *Profil* pour consulter votre profil et vérifier vos accès ou vos rôles dans Genetec ClearID[MC].

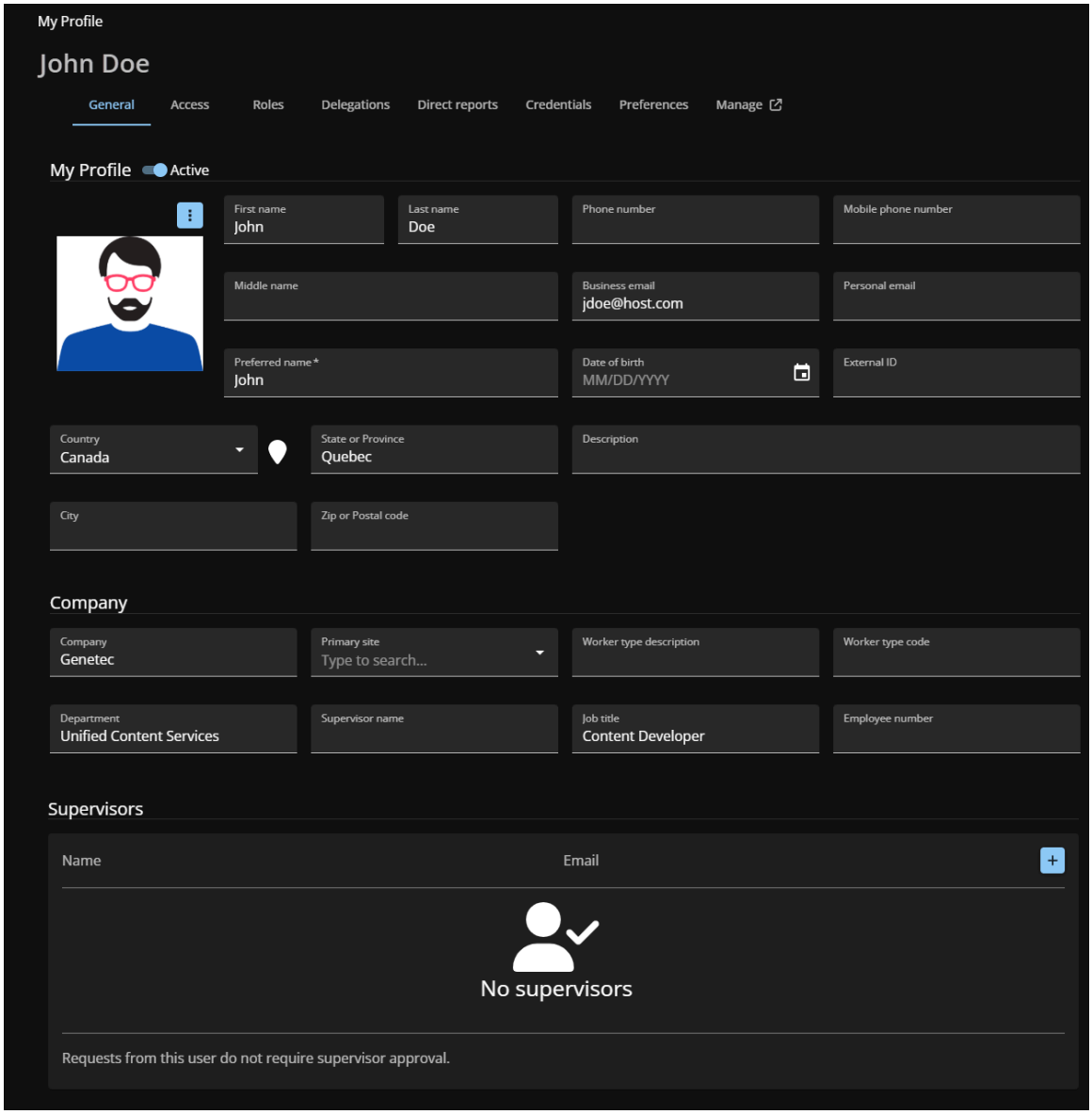
À savoir

- Le profil dans ClearID est présenté à l'employé en mode lecture seule. Le profil contient le site, la description du type de travailleur, le nom du superviseur et d'autres informations.
- Un *employé* peut consulter son profil à tout moment, afin de savoir quelles informations à son propos sont stockées dans ClearID. Il peut également voir si les informations sont obsolètes et demander leur mise à jour.

CONSEIL : Vérifiez votre intitulé de poste ou votre service après un changement de poste pour confirmer que vous avez les bons accès.

Procédure

1 Sur la page d'accueil, cliquez sur **Mon profil**.



2 Dans l'onglet **Général**, examinez vos informations d'identité, comme les superviseurs associés ou l'état de l'identité (actif ou inactif).

3 (Facultatif) Des onglets supplémentaires permettent d'examiner d'autres informations et options associées votre identité :

- **Champs personnalisés :** Champs personnalisés associés à votre identité.
- **Accès :** Accès associés à votre identité.
- **Rôles :** Rôles associés à votre identité, ajoutés manuellement ou par une règle de provisionnement.
- **Délégations :** Délégations associées à votre identité.
- **Subordonnés :** Subordonnés associés à votre identité.
- **Contrôle d'accès :** Contrôles d'accès associés à votre identité, comme le délai d'accès prolongé, l'activation de titulaire de cartes, les attributs de provisionnement et les titulaires de cartes associés.
- **Autorisations utilisateur :** Autorisations d'accès au portail web des utilisateurs ou administrateurs associées à votre identité.
- **Gestion des visiteurs :** Liste des sites où votre identité peut inviter des visiteurs.
- **Identifiants :** Identifiants synchronisés associés à votre identité.
- **Journaux :** Journaux d'événements d'identité associés votre identité.

Lorsque vous avez terminé

Consultez vos accès aux secteurs et au site.

Configurer les préférences du thème du portail

Vous pouvez personnaliser le thème de votre portail Genetec ClearID[MC] en fonction de vos préférences personnelles en choisissant entre le mode clair et le mode sombre.

À savoir

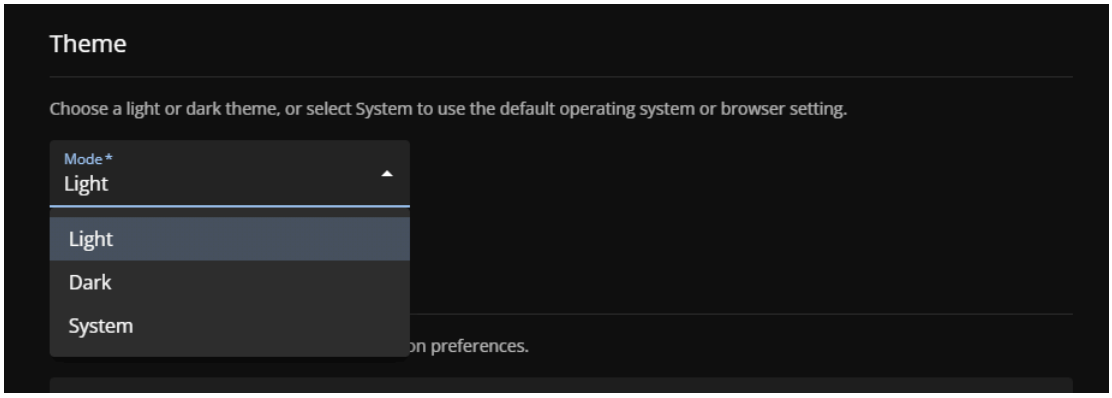
Vos préférences de thème ne s'appliquent qu'à votre profil utilisateur. Si vous ne configurez pas de thème personnel, votre thème correspond au thème du portail configuré par l'*administrateur* .

Procédure

1 Sur le portail web ClearID, cliquez sur **Mon profil** > **Préférences**.

2 Dans la section *Thème*, configurez vos préférences de thème.

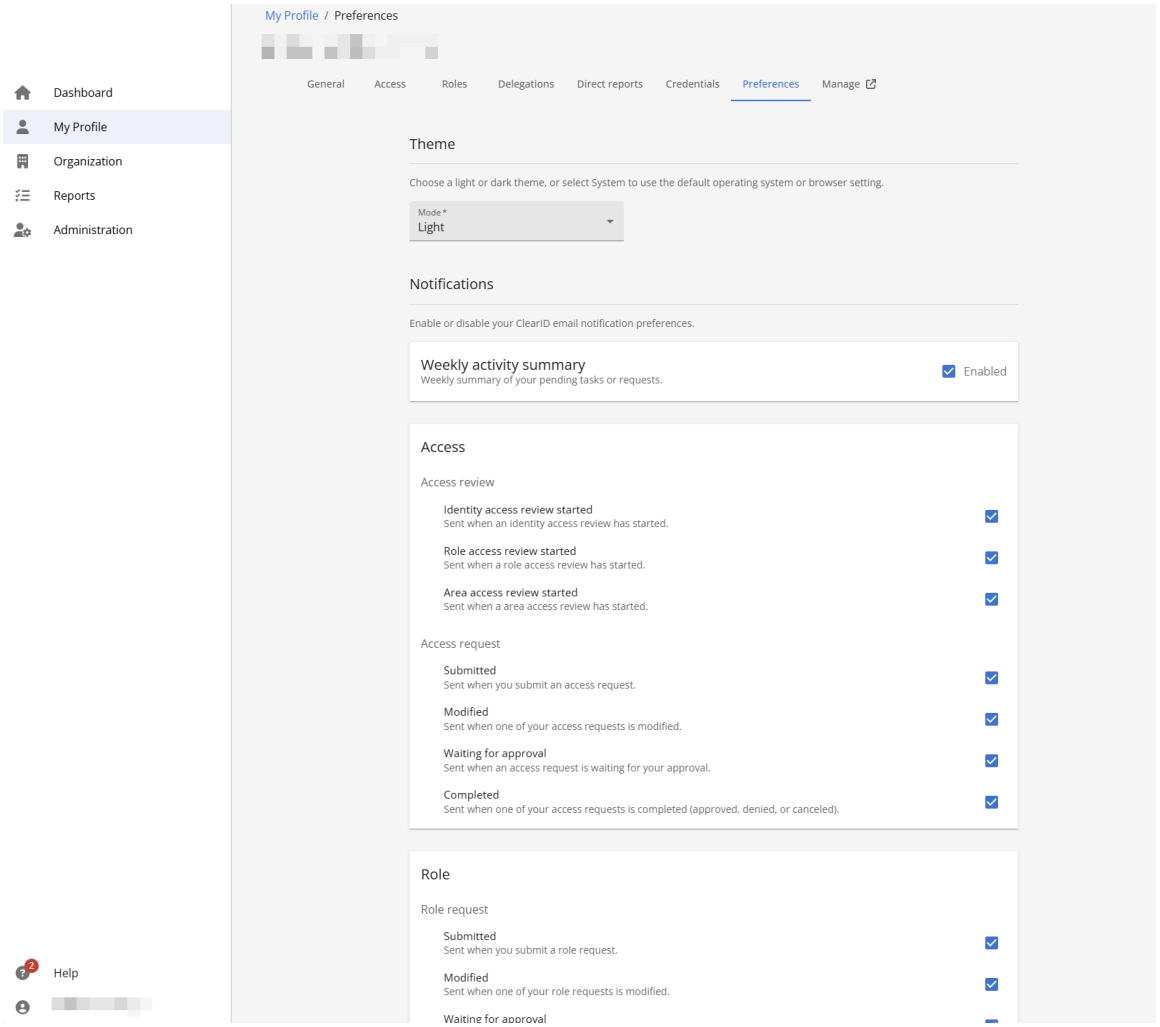
a) Dans la liste **Mode**, choisissez entre **Clair**, **Sombre**et **Système**.



REMARQUE : La sélection **Système** utilise les paramètres par défaut de votre système d'exploitation ou de votre navigateur.

3 Cliquez sur **Enregistrer**.

Portail ClearID d'un utilisateur avec le mode clair sélectionné :


Dashboard
My Profile
Organization
Reports
Administration
Help
My Profile / Preferences
General
Access
Roles
Delegations
Direct reports
Credentials
Preferences
Manage
Theme
Choose a light or dark theme, or select System to use the default operating system or browser setting.
Mode*
Light
Notifications
Enable or disable your ClearID email notification preferences.
Weekly activity summary
Weekly summary of your pending tasks or requests.
Enabled
Access
Access review
Identity access review started
Sent when an identity access review has started.
Role access review started
Sent when a role access review has started.
Area access review started
Sent when a area access review has started.
Access request
Submitted
Sent when you submit an access request.
Modified
Sent when one of your access requests is modified.
Waiting for approval
Sent when an access request is waiting for your approval.
Completed
Sent when one of your access requests is completed (approved, denied, or canceled).
Role
Role request
Submitted
Sent when you submit a role request.
Modified
Sent when one of your role requests is modified.
Waiting for approval

Consulter vos accès aux sites et aux secteurs

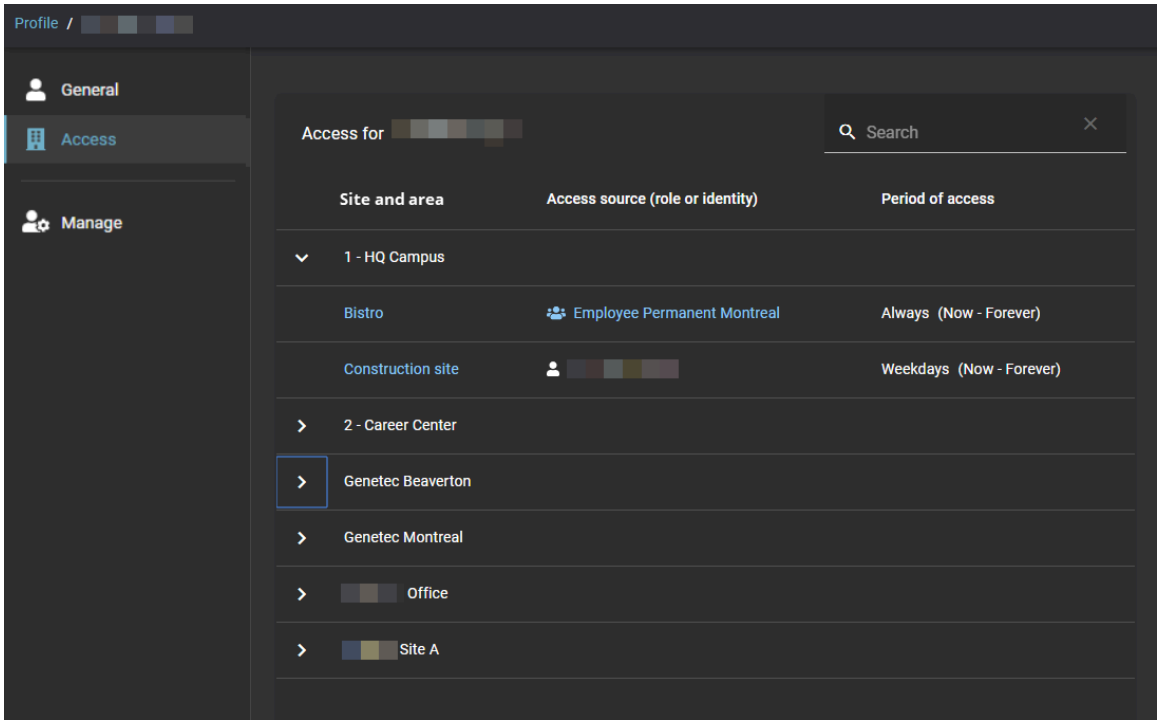
Utilisez la page *Accès* du profil pour consulter vos accès aux sites et aux secteurs. Cette information vous permet de voir si vous devez demander des accès supplémentaires à votre site principal ou à d'autres sites.

À savoir

La page Secteurs affiche tous les sites et secteurs auxquels l'utilisateur connecté a accès, ainsi que la source et la durée des accès.

Procédure

1 Sur la page d'*accueil*, cliquez sur **Mon profil** > **Accès**.



Les sites et les secteurs auxquels vous avez accès sont affichés dans la colonne **Site et secteur**.

2 (Facultatif) Cliquez sur le texte en bleu dans la colonne **Site et secteur** pour basculer vers la page *Accès*.

3 (Facultatif) Cliquez sur le texte en bleu dans la colonne **Source d'accès** pour basculer vers la page *Rôles*.

Lorsque vous avez terminé

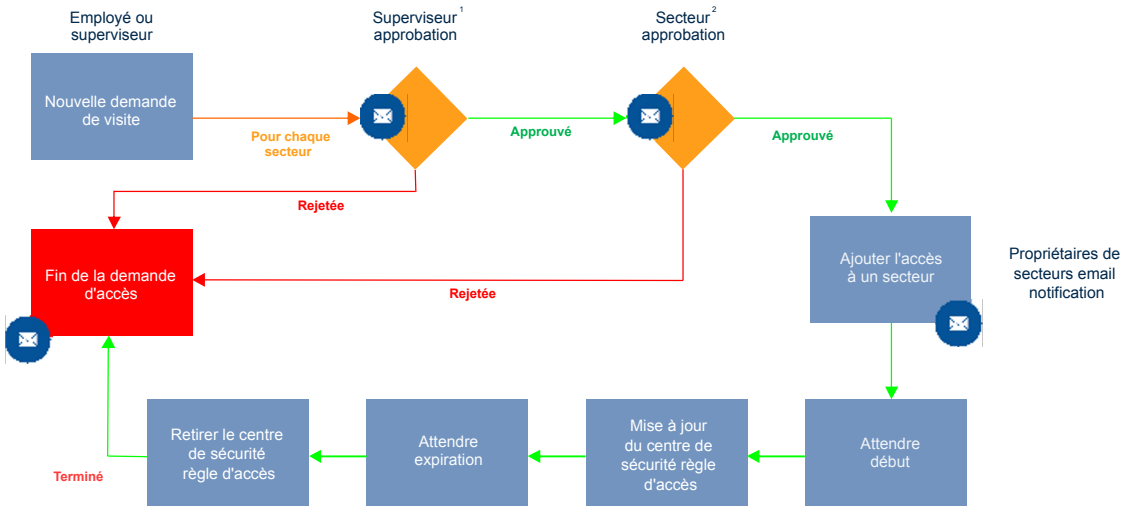
Envoyez des demandes d'accès à d'autres secteurs en cas de besoin.

À propos du processus de demande d'accès

Un processus de demande d'accès est une série d'activités effectuées par le système ou par des personnes habilitées au cours du cycle de vie d'une demande d'accès. Les activités peuvent modifier l'état et les propriétés des demandes d'accès, affecter d'autres entités du système, ou attendre qu'une condition soit réunie.

Le processus permet d'automatiser les tâches liées aux demandes d'accès, comme l'approbation ou le rejet des demandes d'accès, afin que les personnes chargées de l'examen et de l'approbation puissent se concentrer sur d'autres tâches.

Le diagramme suivant illustre le *processus de demande d'accès* exécuté dans Genetec ClearID[MC] et Synergis[MC].



[1] (Facultatif) L'approbation du superviseur peut être activée pour le secteur.

[2] (Facultatif) L'approbation du secteur peut être activée pour le secteur.

REMARQUE : Par défaut, les demandes d'accès sont limitées à l'accès minimum requis. Cela limite les actions qu'un utilisateur peut réaliser avec une carte d'accès.

Rubriques connexes

À propos des processus, page 12

Demander un accès

Pour demander un accès pour vous-même, une autre identité ou un membre de l'équipe, vous pouvez utiliser le portail Genetec ClearID[MC] en libre-service. L'utilisation d'un portail en libre-service avec des approbateurs de secteur spécifiés simplifie le processus d'approbation et évite d'interrompre une chaîne de personnes qui ne sont pas forcément les bons approbateurs.

Avant de commencer

- Familiarisez-vous avec les processus.

À savoir

Les employés, les responsables et les superviseurs de différents secteurs sécurisés peuvent demander l'accès pour eux-mêmes ou leurs employés à l'aide d'un portail Web en libre-service.

REMARQUE : Dans le passé, la plupart des solutions de contrôle d'accès des sites ne consignaient et n'enregistraient pas les raisons pour lesquelles l'accès était requis.

Dans ClearID, la demande d'accès comprend les informations suivantes : demandeur, site, secteur, quand et le motif de la demande.

- Des demandes d'accès et des processus d'approbation distincts sont créés pour chaque demande d'accès à un secteur.
- Une fois le récapitulatif de la demande validé, la demande est automatiquement affectée aux personnes pertinentes pour approbation.
- Une fois le processus d'approbation terminé, le demandeur reçoit un e-mail lui indiquant si la demande d'accès a été approuvée ou rejetée.

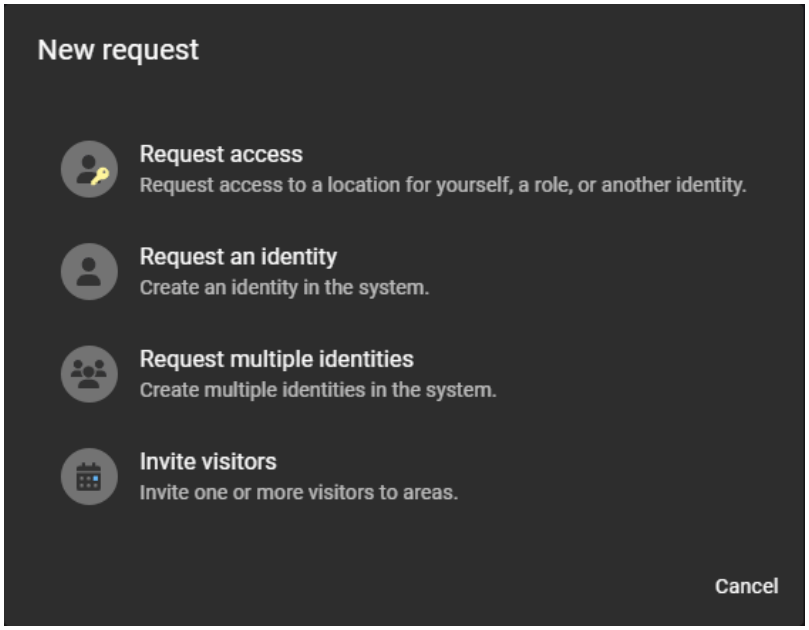
Procédure

1 Connectez-vous au portail en libre-service.

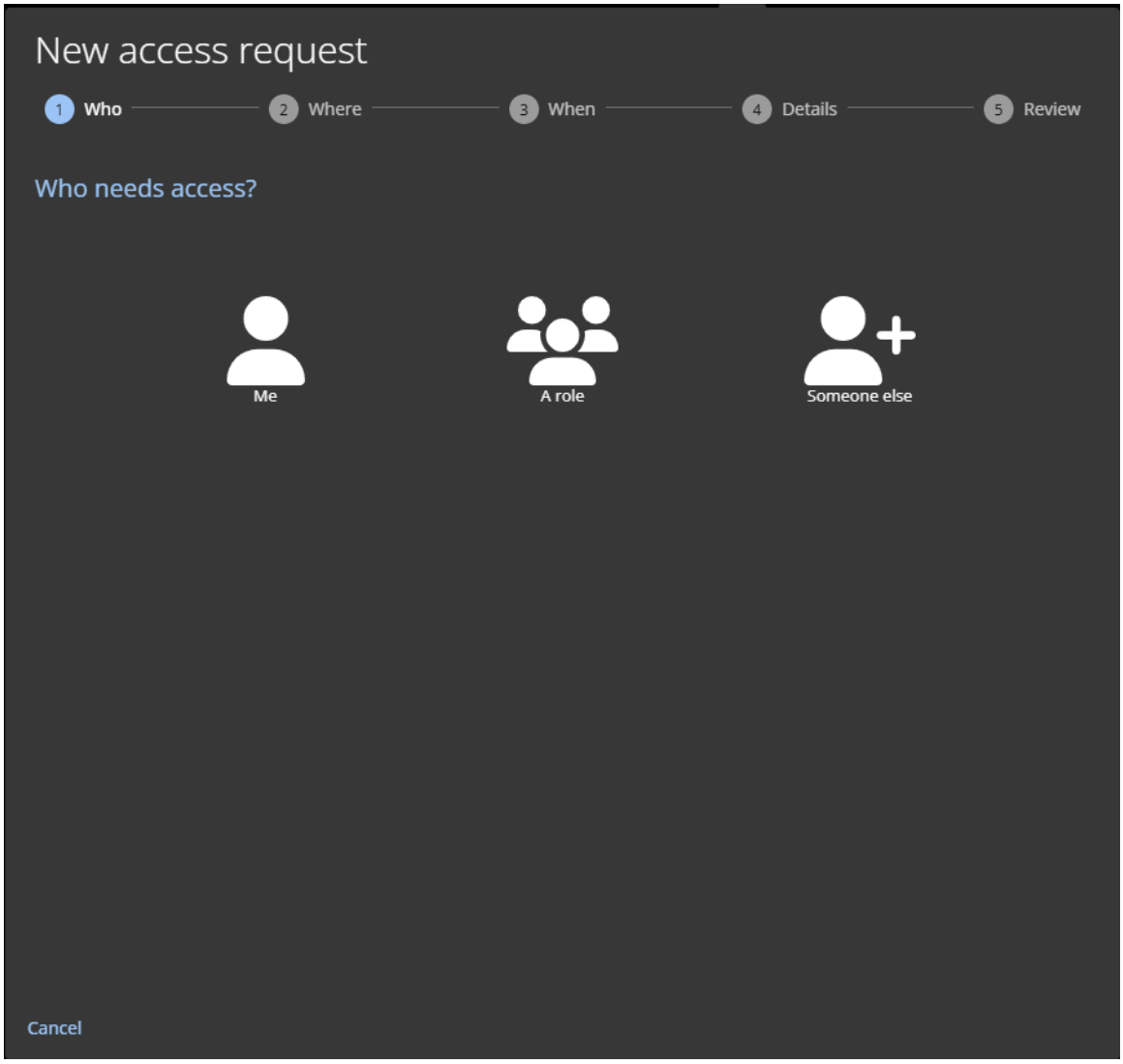
2 Cliquez sur **Tableau de bord** > **Mes demandes**.

3 Cliquez sur **Nouvelle demande**.

4 Dans la boîte de dialogue **Nouvelle demande**, cliquez sur **Demander l'accès**.



5 Dans la section *Qui* de la boîte de dialogue *Nouvelle demande d'accès*, cliquez sur une option pour choisir qui a besoin d'un accès :



a) (Facultatif) Si vous avez sélectionné **Moi**, l'assistant *Nouvelle demande d'accès* est automatiquement mis à jour pour inclure les informations de l'utilisateur actuellement connecté.

b) (Facultatif) Si vous avez sélectionné **Un rôle**, recherchez ou sélectionnez un rôle dans la liste.

L'assistant *Nouvelle demande d'accès* est mis à jour pour inclure les informations du rôle sélectionné.

IMPORTANT : Seul un *propriétaire de rôle* ou un *responsable de rôle* peut afficher et demander l'accès pour les rôles. Ils peuvent uniquement demander l'accès pour les rôles qu'ils gèrent.

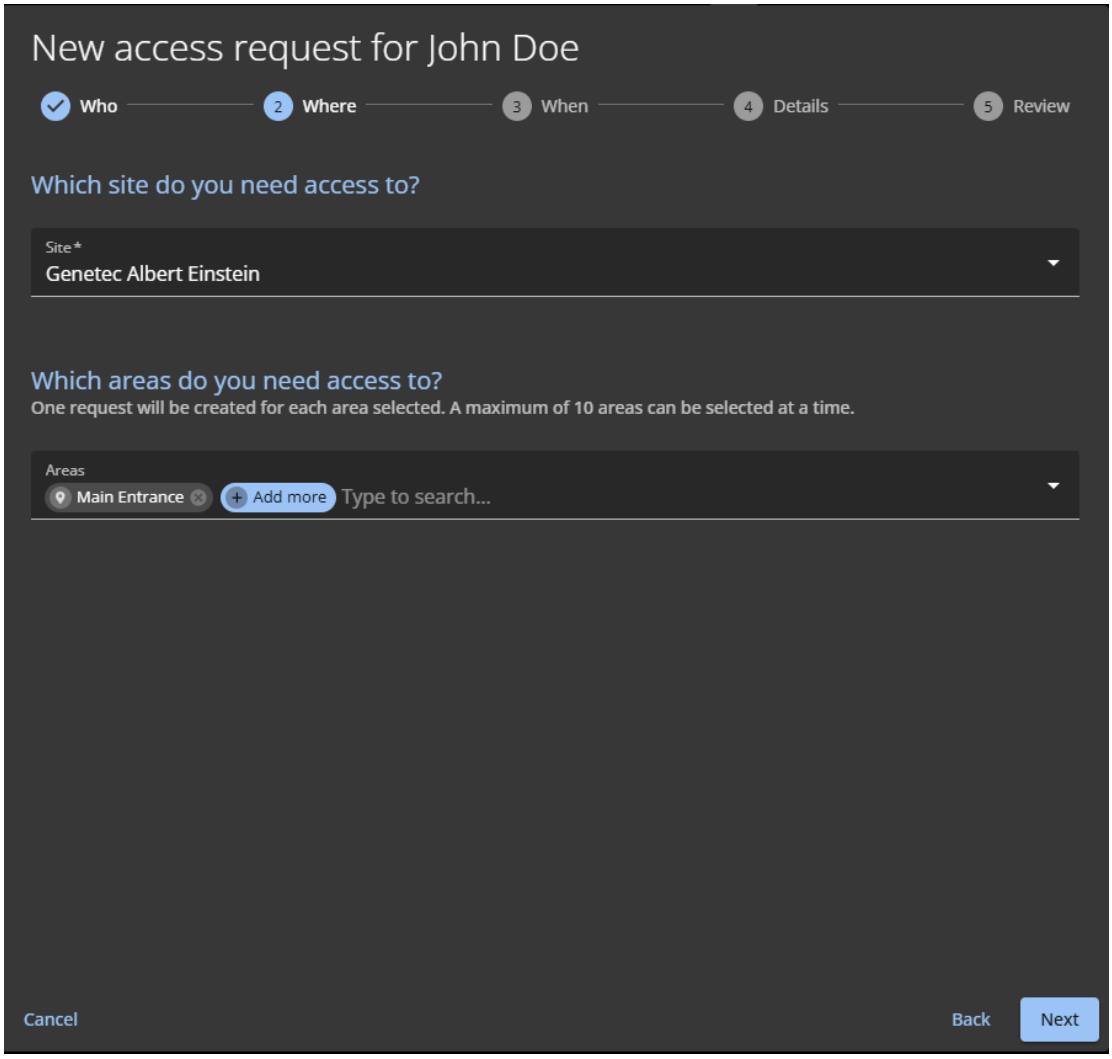
c) (Facultatif) Si vous avez sélectionné **Quelqu'un d'autre**, recherchez ou sélectionnez une personne dans la liste.

L'assistant *Nouvelle demande d'accès* est mis à jour pour inclure les informations de la personne sélectionnée.

REMARQUE : Un superviseur ou un chef d'équipe peut demander l'accès pour une personne de son équipe, de son groupe ou de son service.

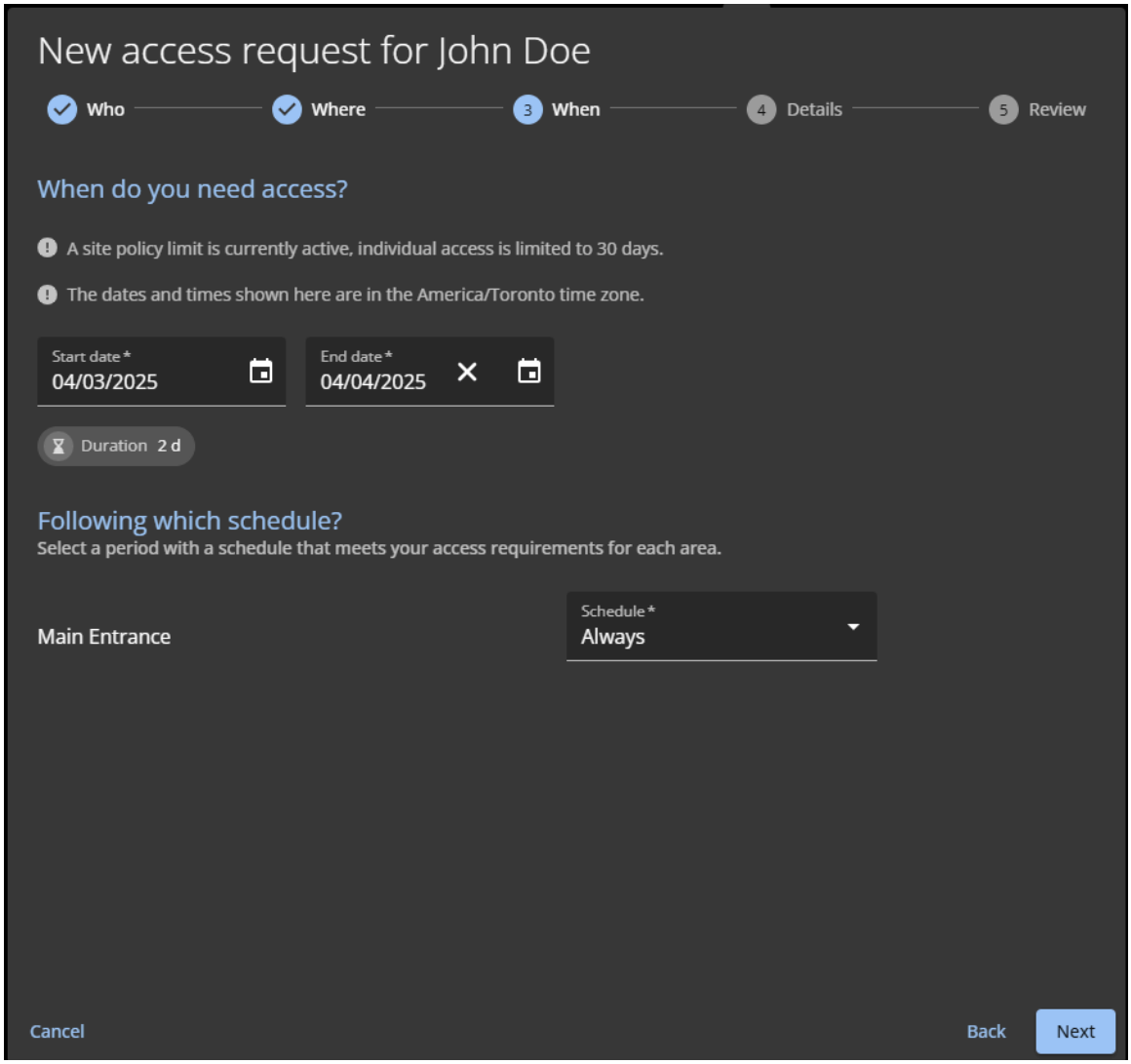
6 Dans la section *Où* de la boîte de dialogue *Nouvelle demande d'accès*, sélectionnez un site dans la liste des sites.

a) Recherchez ou sélectionnez un ou plusieurs secteurs et cliquez sur **Suivant**.



REMARQUE : Seuls les secteurs créés avec une visibilité **publique** sont affichés dans cette liste.

7 Dans la section *Quand* de la boîte de dialogue *Nouvelle demande d'accès*, saisissez les dates souhaitées ou sélectionnez-les à l'aide du sélecteur de calendrier.



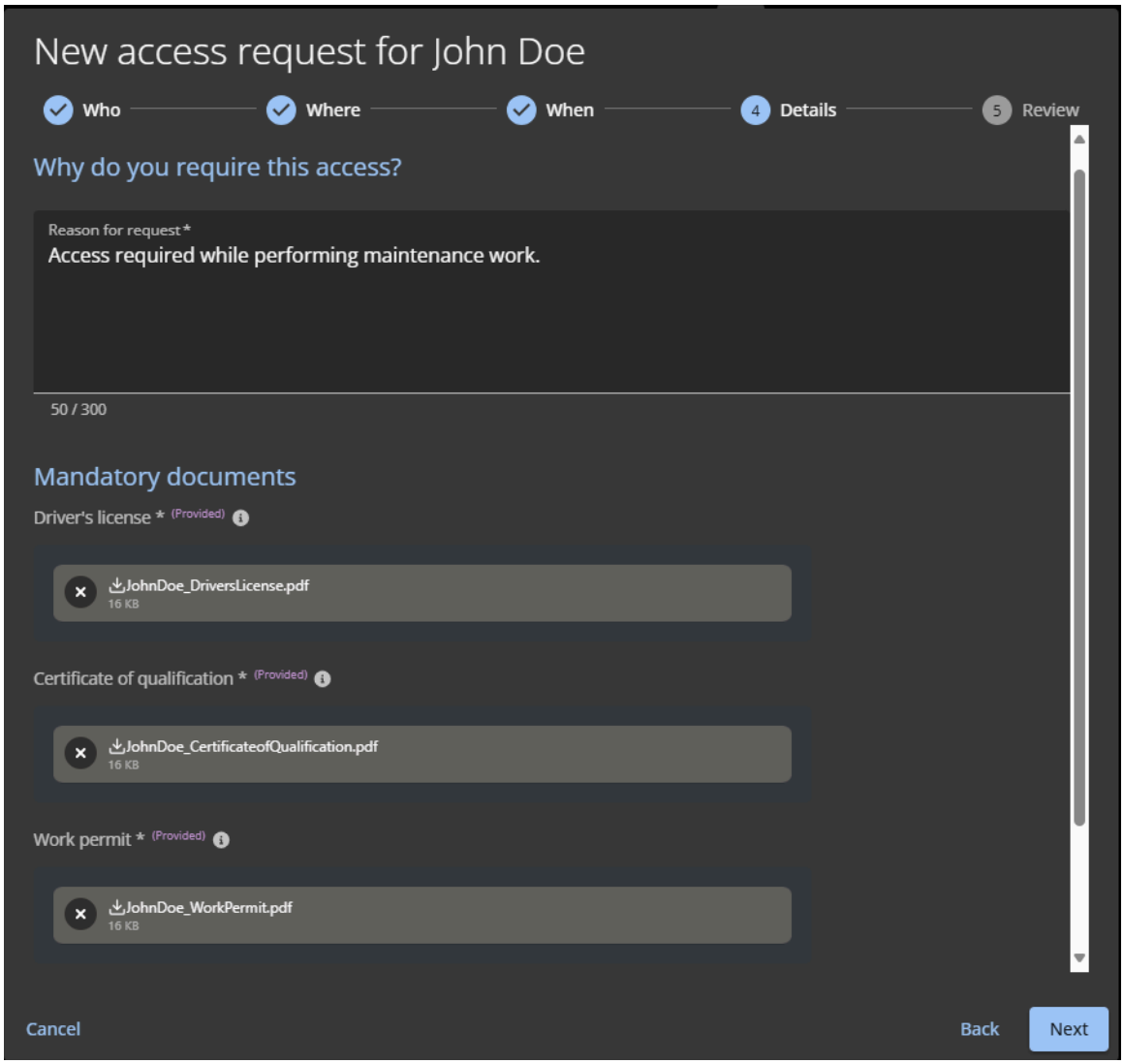
a) Sélectionnez l'horaire nécessaire pour chaque secteur et cliquez sur Suivant.

IMPORTANT : Si une durée d'accès au site a été activée, vous ne pouvez pas sélectionner une durée supérieure à la limite définie dans la configuration de l'accès au site.

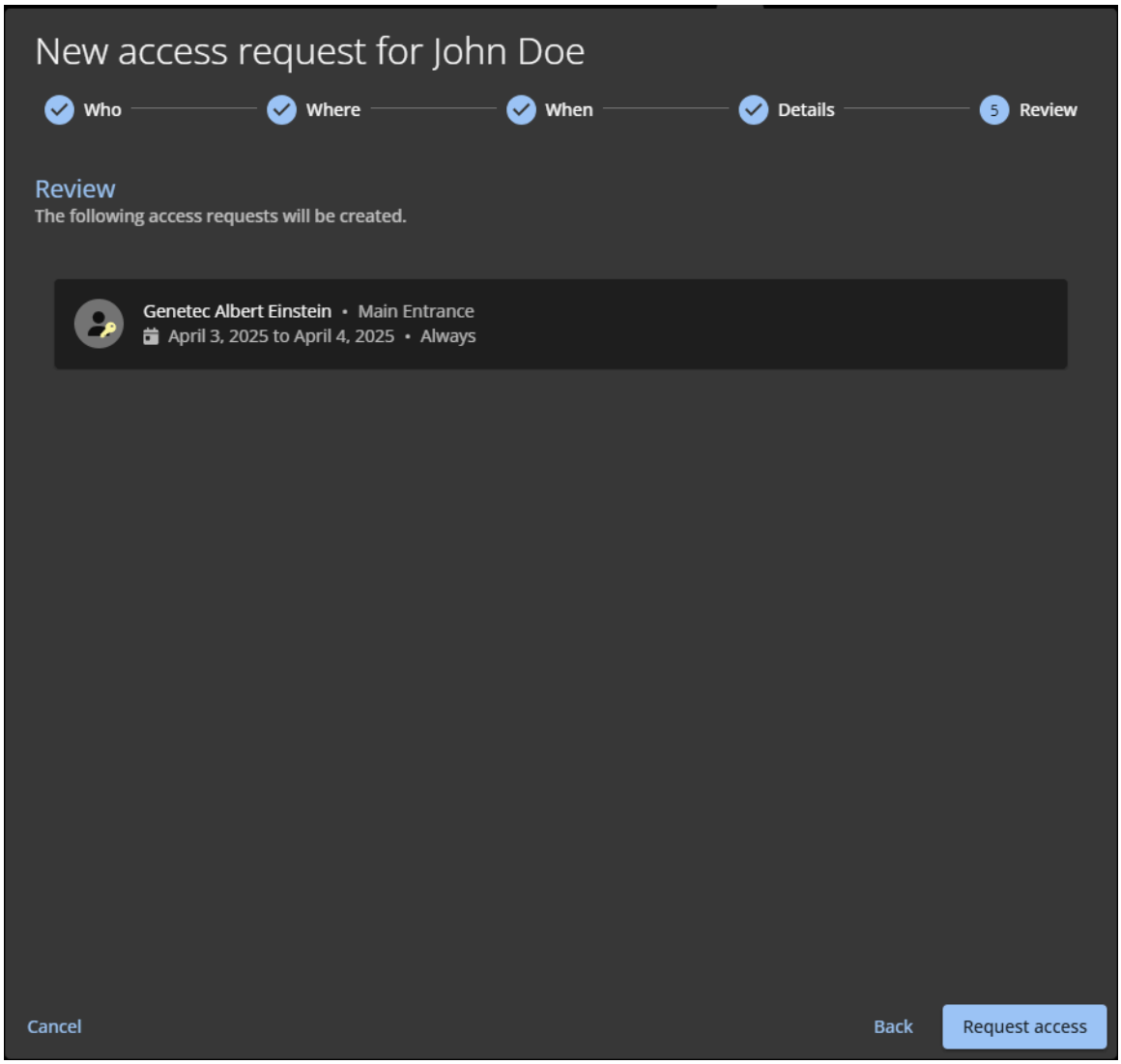
8 Dans la section *Détails* de la boîte de dialogue *Nouvelle demande d'accès*, saisissez le motif de la demande d'accès.

REMARQUE : Motif de la demande est un champ obligatoire et le motif est stocké à des fins d'audit de l'analyse d'accès.

a) Chargez les pièces justificatives vers la demande d'accès et cliquez sur **Suivant**.

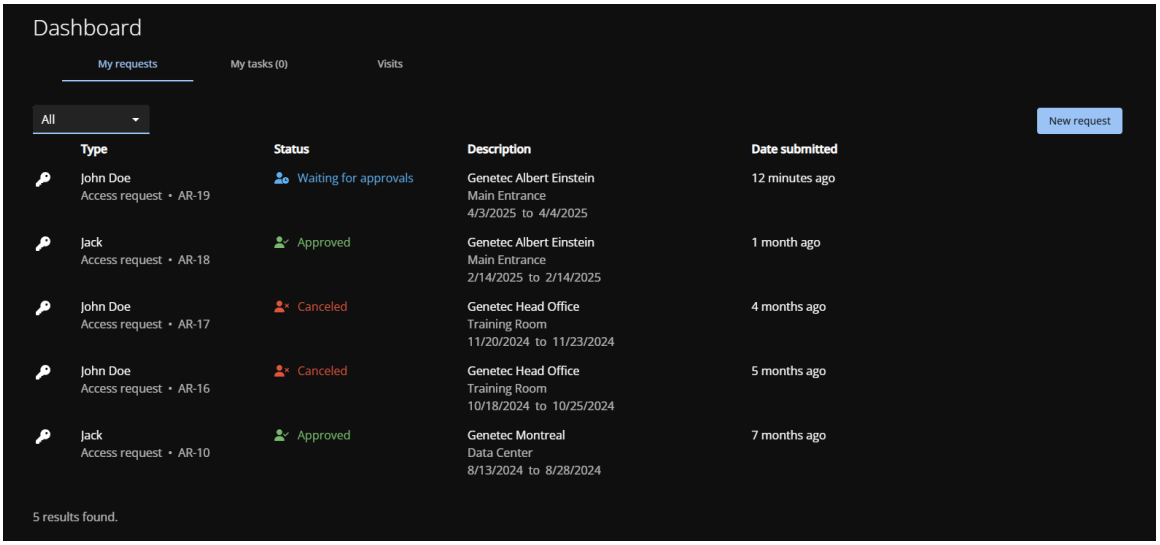


9 Passez en revue la synthèse de la demande.



a) Si des modifications sont nécessaires, cliquez sur **Retour** et modifiez les paramètres.
b) Vérifiez les informations, puis cliquez sur **Demander accès** pour envoyer la demande d'accès.
c) Cliquez sur **Terminé** pour revenir à *Mes demandes*.

Votre demande d'accès a été soumise et attend les approbations requises. Selon votre configuration, la demande est automatiquement approuvée ou en attente des approbations requises. Dans certaines situations, la demande d'accès peut également être annulée ou rejetée manuellement ou automatiquement.



Lorsque vous avez terminé

Confirmez si la demande a été approuvée ou rejetée :

- Recherchez un e-mail *Accès approuvé* dans votre boîte de réception.
- Consultez **Mes demandes** dans ClearID.

Rubriques connexes

Définir la durée maximale d'accès à un site, page 275
À propos des notifications par e-mail, page 186
Vérifier l'état des demandes d'accès, page 329
Note sur la fonction de demande d'accès (2 pages)

Ajouter des superviseurs manuellement

Pour vous aider à gérer les demandes de vos subordonnés, vous pouvez ajouter des superviseurs manuellement aux profils d'identité pertinents, afin de pouvoir utiliser le processus d'approbation par un superviseur.

Avant de commencer

Créez vos identités.

À savoir

Cette procédure concerne les Superviseurs qui ont des subordonnés.

- Pour ajouter des superviseurs manuellement à un profil d'identité, vous devez être un administrateur de compte.

Procédure

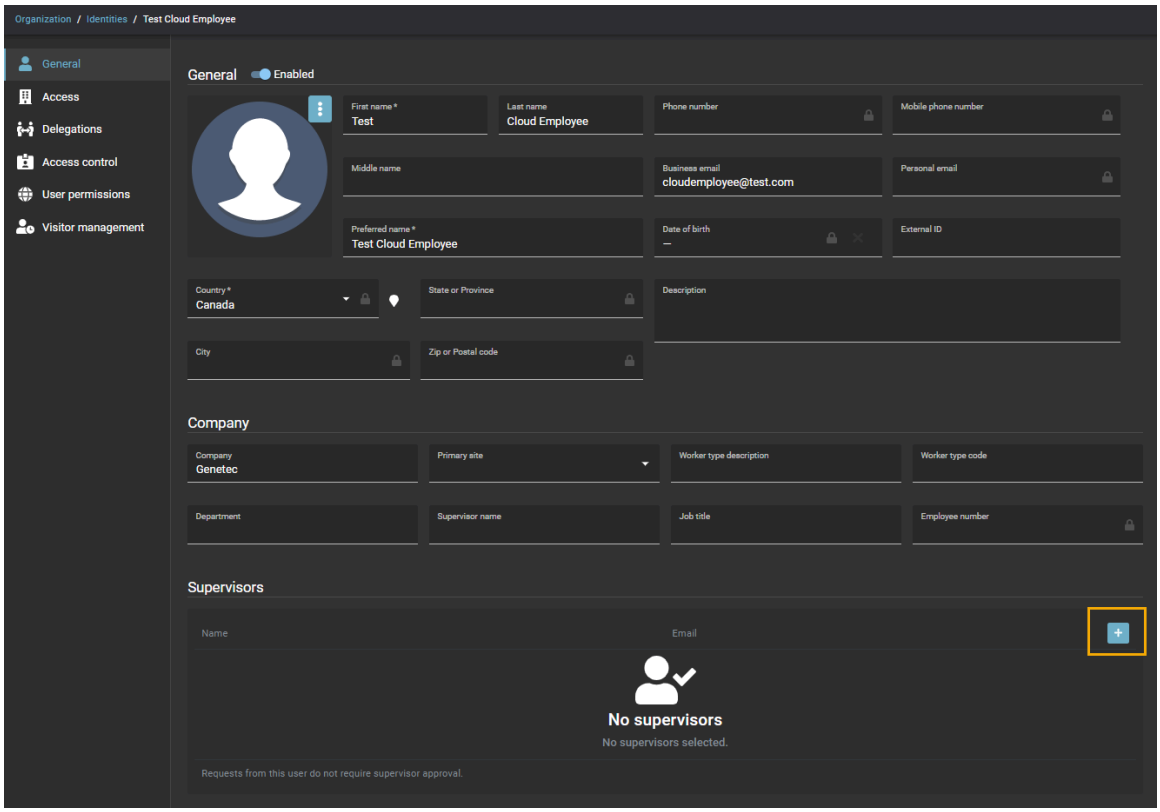
1 Sur la page d'accueil, cliquez sur **Organisation** > **Identités**.

2 Recherchez ou sélectionnez une identité dans la liste.

a) (Facultatif) Utilisez les filtres **Actif**, **Inactif** ou **Tous les filtres** pour affiner votre recherche.

3 Cliquez sur l'identité qui vous intéresse.

4 Dans la section **Superviseurs**, cliquez sur +.



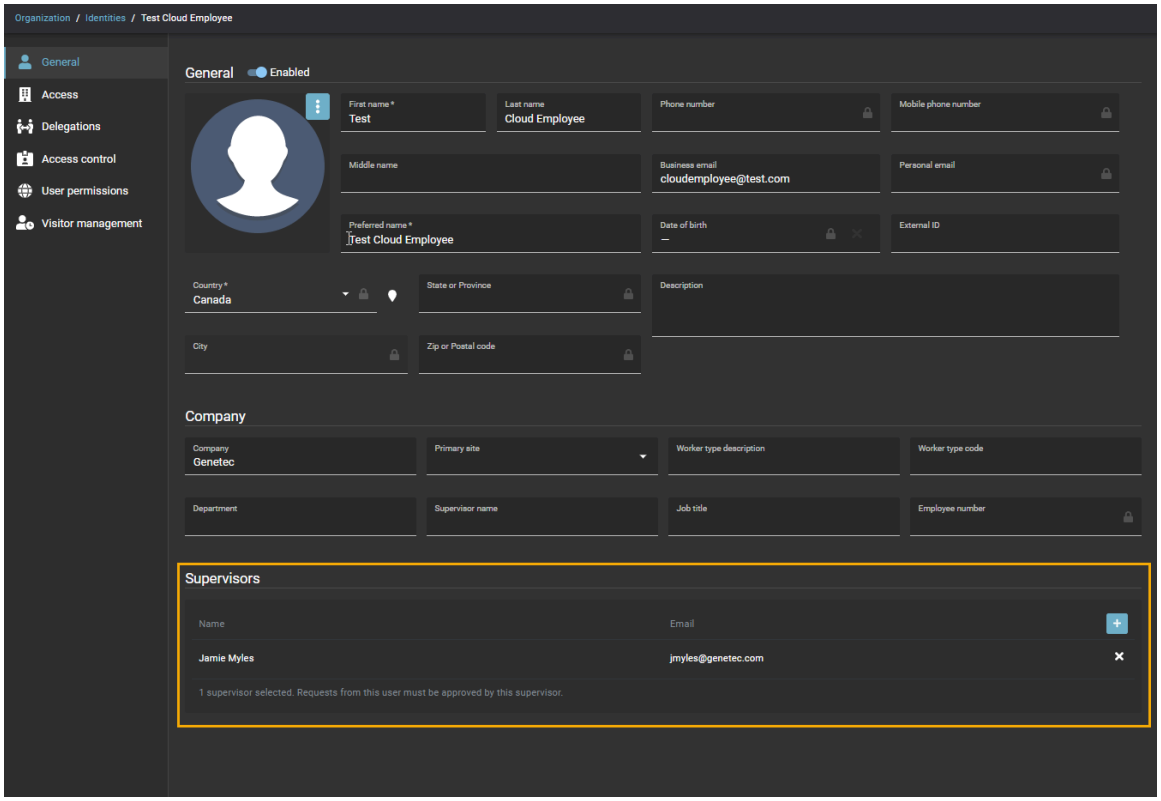
5 Recherchez ou sélectionnez un ou plusieurs utilisateurs dans la liste, et cliquez sur **Ajouter** pour confirmer votre sélection.

REMARQUE : Ajouter plusieurs superviseurs est utile en cas de roulement des employés ou des superviseurs. Dans ce type de situation, il est courant de désigner plusieurs superviseurs pour différents employés qui ne travaillent pas les mêmes jours.

6 (Facultatif) Cliquez sur pour supprimer les superviseurs qui ne sont plus nécessaires.

7 Cliquez sur **Enregistrer** pour confirmer vos modifications.

Les superviseurs que vous avez sélectionnés sont ajoutés à la liste des superviseurs pour l'identité concernée.



Lorsque vous avez terminé

Affichez vos subordonnés.

Afficher les subordonnés

En tant que *superviseur*, vous pouvez vérifier l'état du contrôle d'accès et les informations générales d'identité de vos rapports directs. Vous pouvez également utiliser la liste des subordonnés directs à des fins d'examen de sécurité ou d'audit.

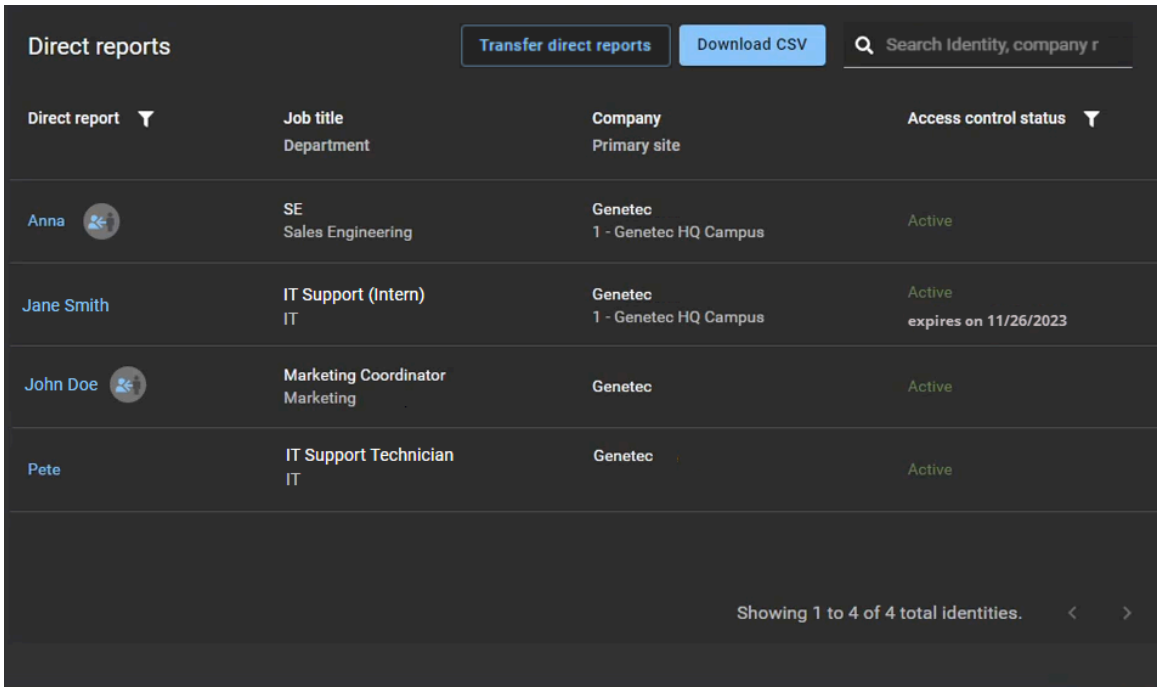
Avant de commencer

Pour voir les *subordonnés*, vous devez être un *superviseur* ou un *administrateur de compte*.

- Un *superviseur* peut consulter les informations générales sur ses subordonnés à tout moment, afin de savoir quelles informations sont stockées dans Genetec ClearID[MC] à leur propos. Il peut également voir si les informations sont obsolètes et demander leur mise à jour.
- Un *administrateur de comptes* peut consulter les subordonnés d'une identité pour valider le lien hiérarchique et d'autres informations.

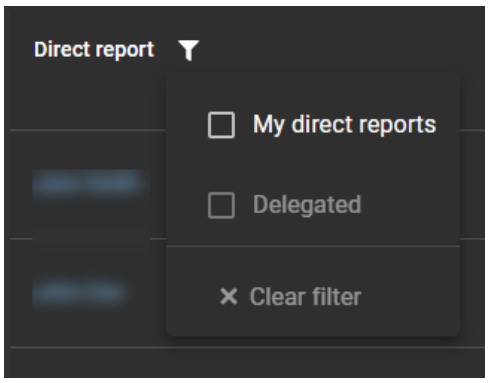
Procédure

1 Sur la *page d'accueil*, cliquez sur **Mon profil** > **Subordonnés**.



2 Filtrez la liste en fonction de vos critères requis :

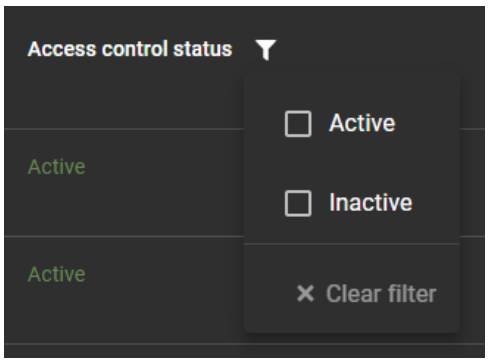
- **Subordonnés :** Cliquez sur l'icône de filtre de **subordonné** ( ) pour filtrer la liste. Sélectionnez **Mes subordonnés**, **Délégué** ou les deux.



- **Mes subordonnés :** Affiche les employés qui sont vos subordonnés.
- **Délégué :** Affiche les employés délégués (parce qu'un autre utilisateur vous a délégué ses tâches).

  REMARQUE : Les employés délégués sont indiqués dans la liste par une icône .
- **Effacer le filtre :** Cliquez sur **Effacer le filtre** (✕) pour supprimer les filtres sélectionnés.

- **État du contrôle d'accès :** Cliquez sur l'icône de filtre **d'état de Contrôle d'accès** (▼) pour filtrer la liste. Sélectionnez **Actif**, **Inactif** ou les deux.



  - **Actif :** Affiche les subordonnés avec un statut de contrôle d'accès **actif**.
  - **Inactif :** Affiche les subordonnés avec un statut de contrôle d'accès **inactif**.
  - **Effacer le filtre :** Cliquez sur **Effacer le filtre** (✕) pour supprimer les filtres sélectionnés.

- **Rechercher :** Utilisez la barre de recherche pour rechercher une identité par prénom, nom ou entreprise.

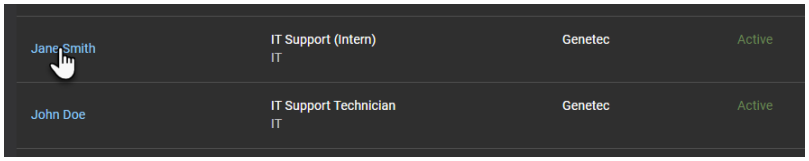
3 Cliquez sur **Télécharger CSV** pour télécharger une copie de la liste des subordonnés au format CSV. Le rapport peut ensuite être utilisé à des fins d'audit, pour conserver un exemplaire physique, pour le joindre à une demande d'audit, pour une analyse hors ligne ou encore pour traiter ou consolider les données dans un tableur pour d'autres publics.

a) Suivez les instructions dans votre navigateur pour télécharger le fichier exporté.

Le fichier est exporté sous forme de fichier *.CSV* vers l' emplacement|lieu de téléchargement par défaut de votre navigateur (*ClearID Direct reports.csv*).

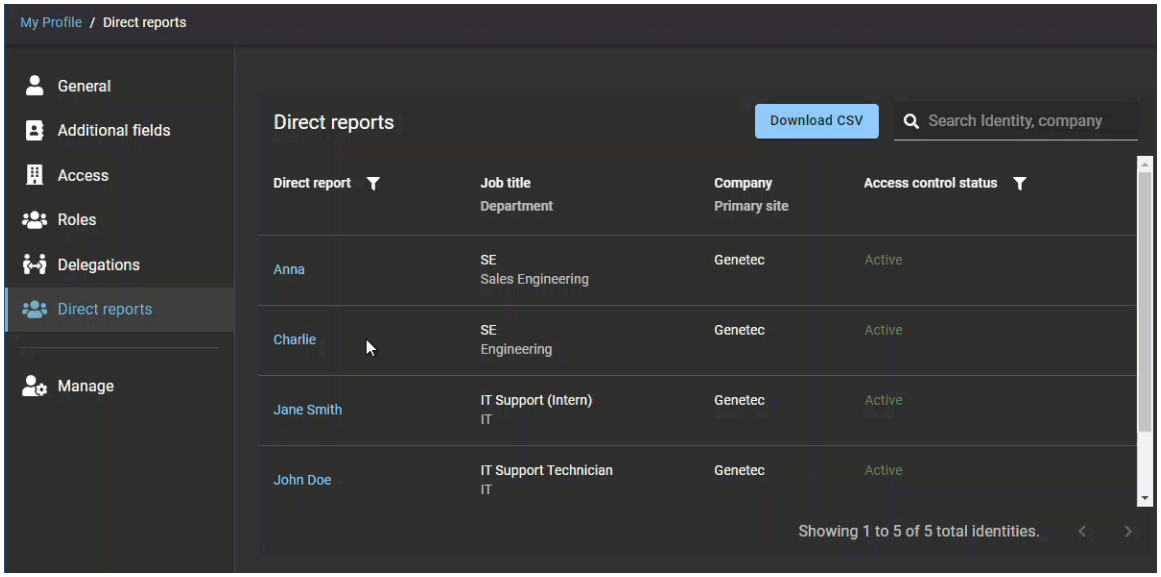
REMARQUE : Les colonnes et les entrées dans le fichier CSV peuvent varier en fonction des filtres sélectionnés au moment de télécharger le rapport.

4 (Facultatif) Cliquez sur le nom d'un subordonné dans la liste (lien hypertexte bleu) pour afficher les détails de son profil d'identité.



Vous pouvez également afficher des informations complémentaires sur l'identité en consultant les pages suivantes du profil d'identité :

- Général
- Accès
- Rôles
- Délégations
- Contrôle d'accès
- Autorisations utilisateur
- Gestion des visiteurs



Lorsque vous avez terminé

Gérez l'accès et les rôles des subordonnés si nécessaire.

Rubriques connexes

Ajouter des superviseurs manuellement, page 164
Créer des identités, page 113
À propos du rapport Subordonnés, page 182

Gérer les subordonnés

Les superviseurs peuvent gérer les accès de leurs subordonnés. Il peut s'agir d'informations générales sur l'identité, d'accès à des secteurs, de modification ou de suppression de rôles, de délégation de tâches et de contrôle d'accès.

Avant de commencer

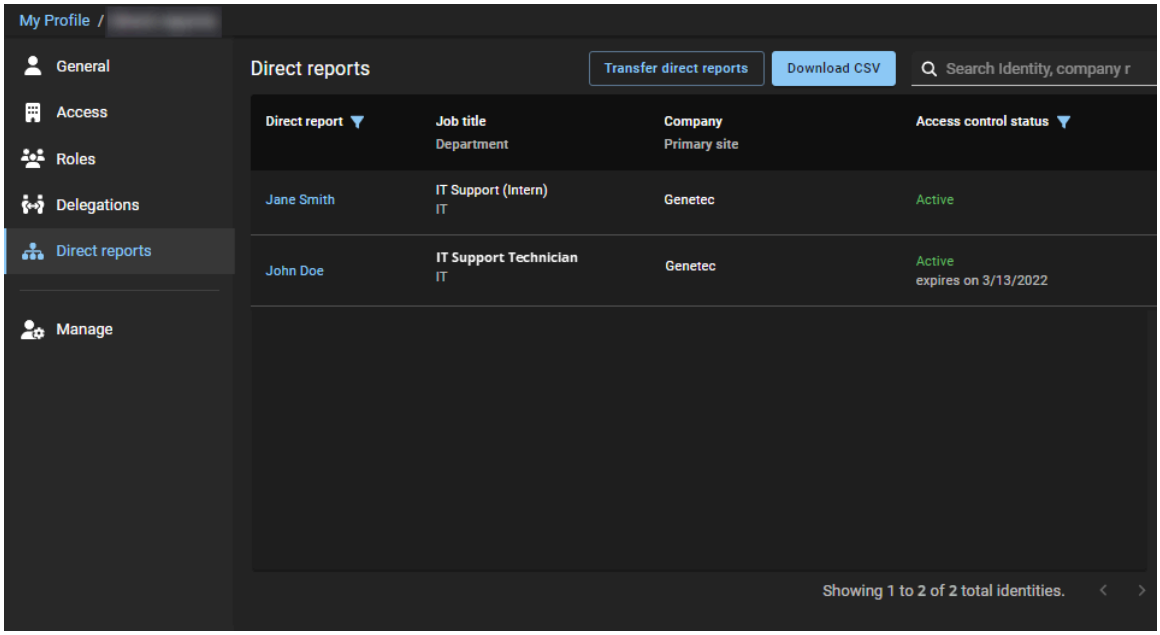
- Ajouter des superviseurs manuellement , page 164.
- (Facultatif) Ajoutez un accès superviseur pour gérer les subordonnés.

À savoir

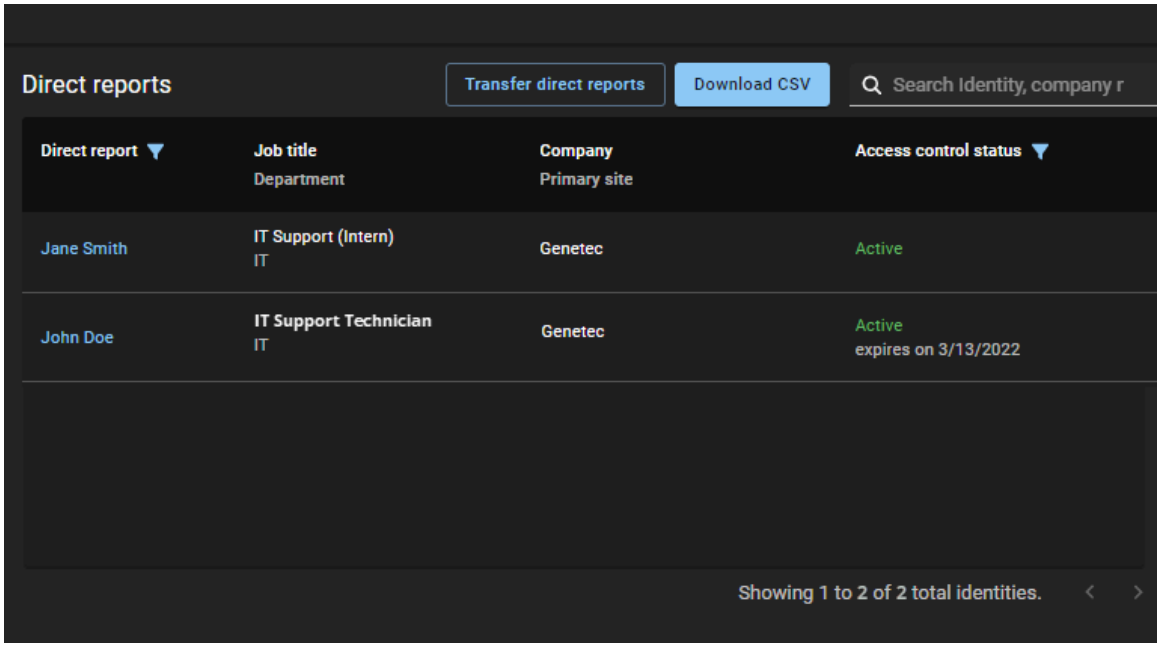
- Vous devez être un superviseur pour gérer les *subordonnés*.
- Pour modifier les informations d'identité **générales** ou les paramètres de **contrôle d'accès** d'un subordonné, vous devez être un superviseur disposant de l'autorisation de gérer les subordonnés.

Procédure

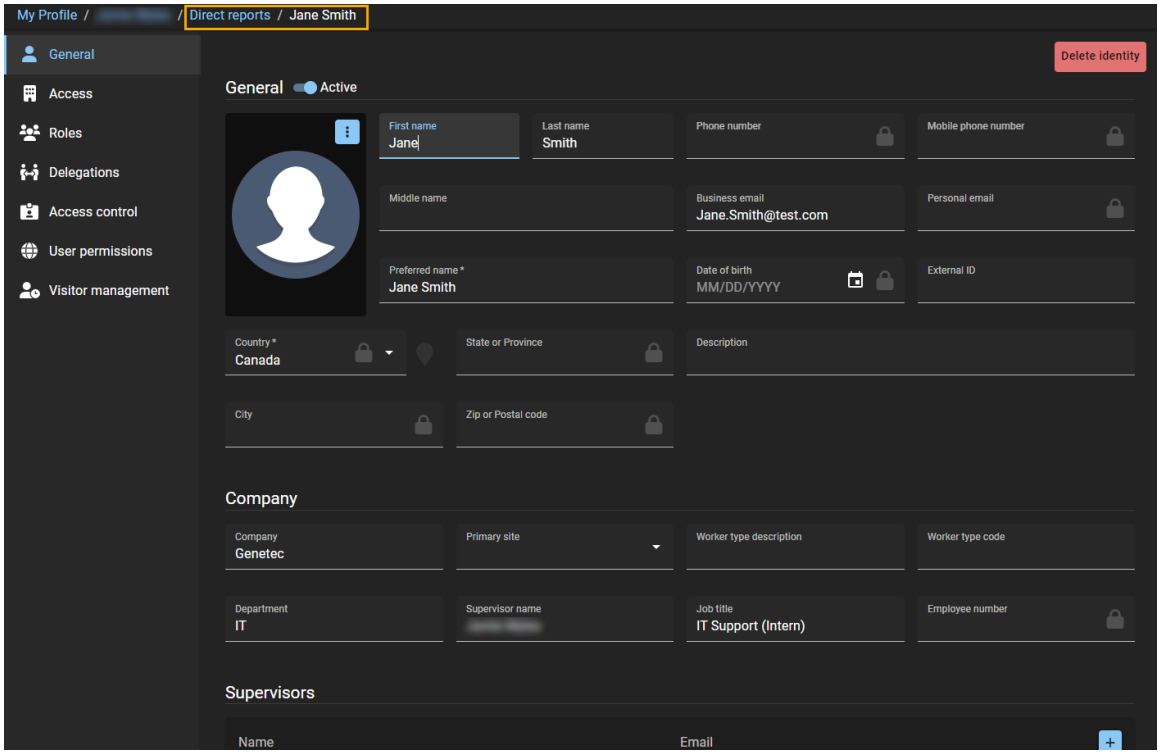
1 Sur la *page d'accueil*, cliquez sur **Mon profil** > **Subordonnés**.



2 Dans la liste **Subordonnés**, sélectionnez le subordonné que vous souhaitez modifier.



CONSEIL : Utilisez les filtres décrits dans Afficher les subordonnés , page 166 pour rechercher et sélectionner le subordonné souhaité.

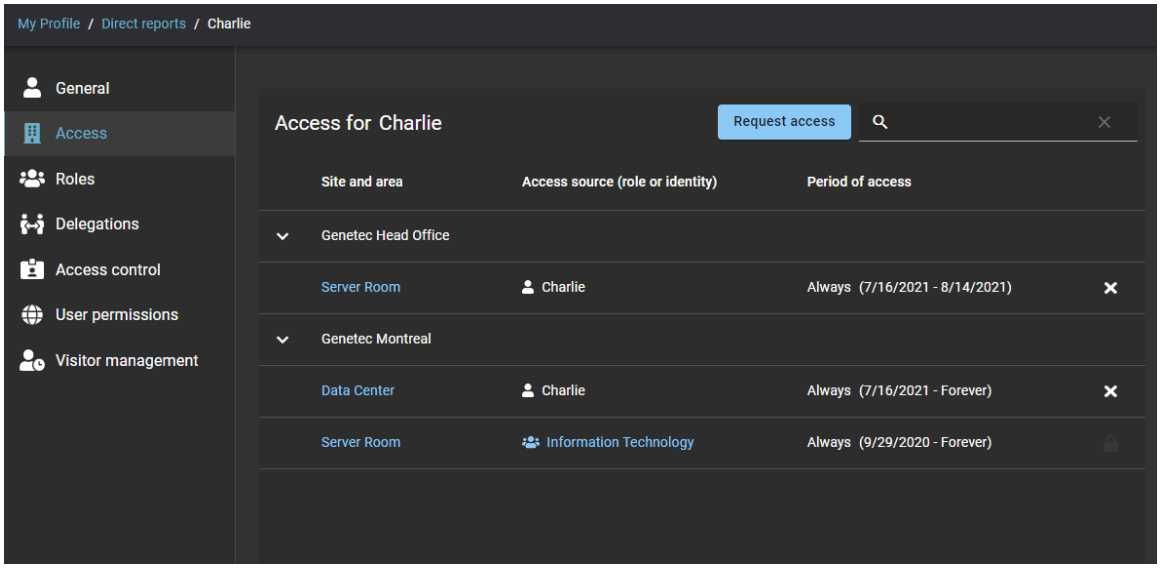


IMPORTANT : Les attributs d'informations d'identité **générales** sont généralement synchronisés depuis une source de données externe pour renseigner les informations d'identité générales. Si vous effectuez

des mises à jour d'identités synchronisées avec une source de données externe, vos modifications peuvent être écrasées par la synchronisation.

- Un superviseur disposant des permissions par défaut ne peut modifier aucune des informations d'identité **générales** de ses subordonnés.
- Un superviseur ayant la permission de gérer les subordonnés peut modifier les informations d'identité **générales** si nécessaire. Cette autorisation renforcée est généralement utilisée pour gérer les contractants ou les travailleurs temporaires qui ne sont pas synchronisés à partir d'une source de données externe.

3 Cliquez sur la page **Accès** pour demander ou modifier l'accès à un secteur pour votre subordonné.

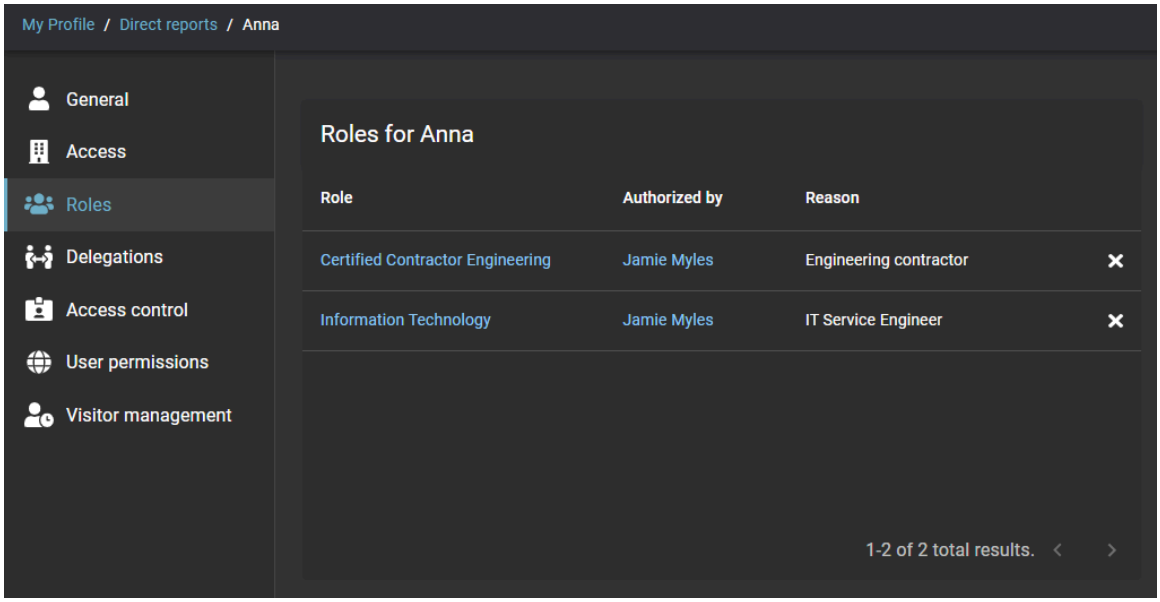


a) Cliquez sur **Demander l'accès** pour demander l'accès à un ou plusieurs secteurs.

b) Cliquez sur pour supprimer tout accès à un secteur qui n'est plus requis, puis sur **Révoquer** pour confirmer la suppression.

REMARQUE : Vous pouvez uniquement supprimer les accès aux secteurs créés manuellement. L'accès au secteur qui a été ajouté à l'aide d'une stratégie de provisionnement est identifié par l'icône verrouillée ( ) et ne peut pas être modifié.

4 Cliquez sur la page **Rôles** pour modifier ou supprimer les accès de rôle pour votre subordonné.

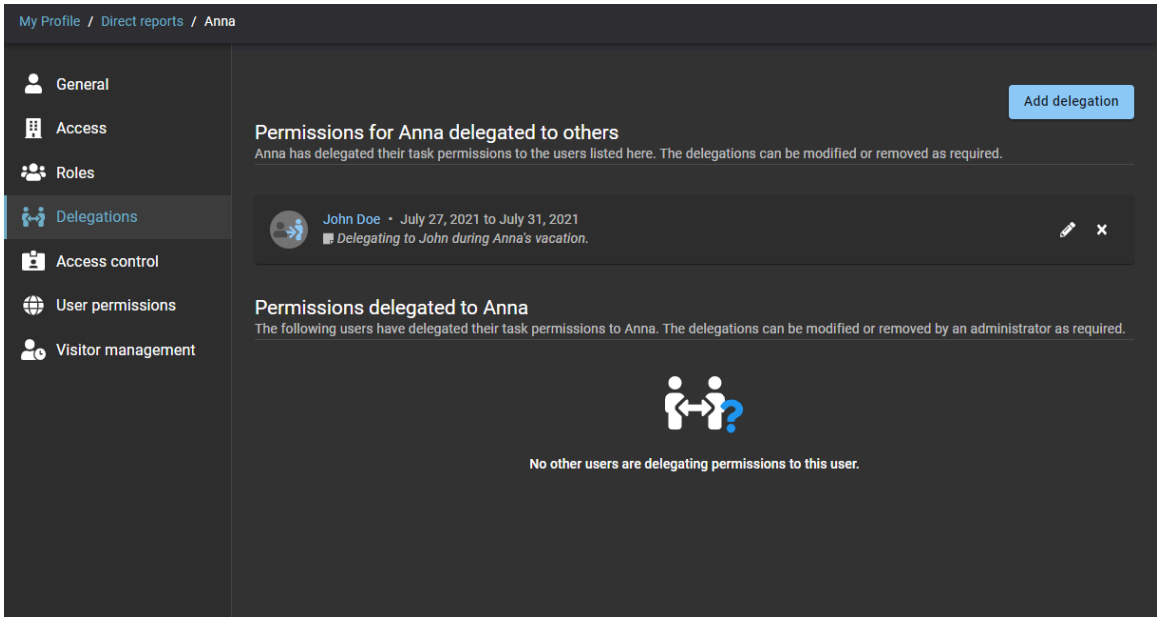


a) Cliquez sur l'hyperlien d'un rôle pour afficher les détails du rôle.

b) Cliquez sur ✕ à côté d'un rôle pour supprimer tout accès de rôle qui n'est plus requis, puis cliquez à nouveau sur **Supprimer** pour confirmer la suppression.

REMARQUE : Vous pouvez uniquement supprimer les accès de rôle créés manuellement. Les rôles qui ont été ajoutés à l'aide d'une politique de provisionnement sont identifiés par l'icône verrouillée (🔒) et ne peut pas être modifié.

5 Cliquez sur la page **Délégations** pour afficher ou modifier les délégations pour votre subordonné.

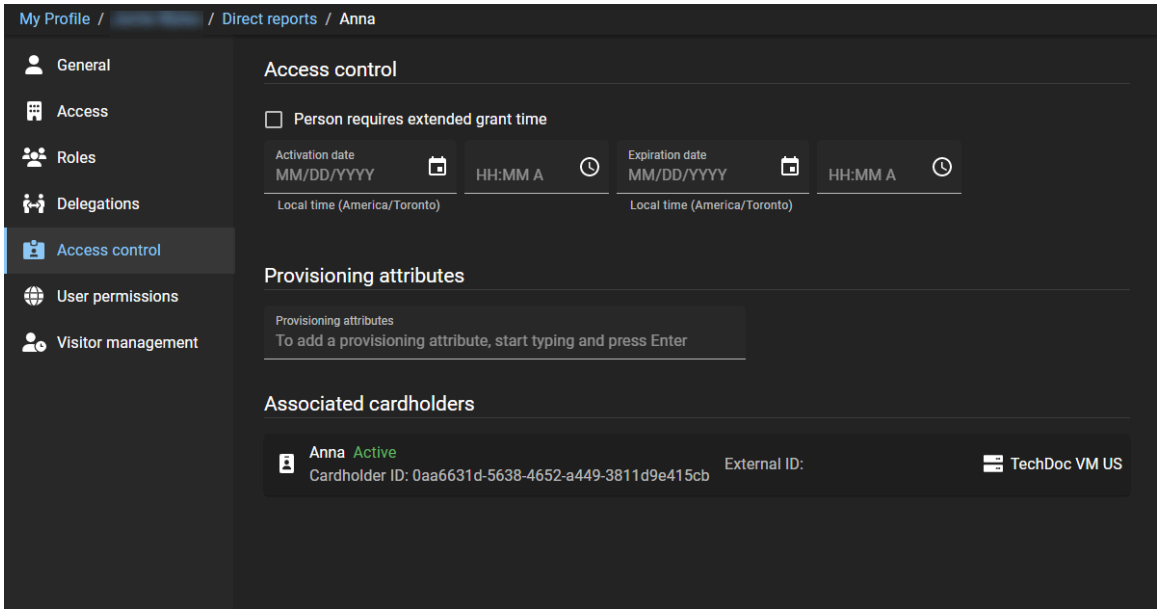


a) Cliquez sur **Ajouter une délégation** pour déléguer des tâches à un autre utilisateur.

b) Cliquez sur le ✎ à côté d'une délégation pour modifier les paramètres.

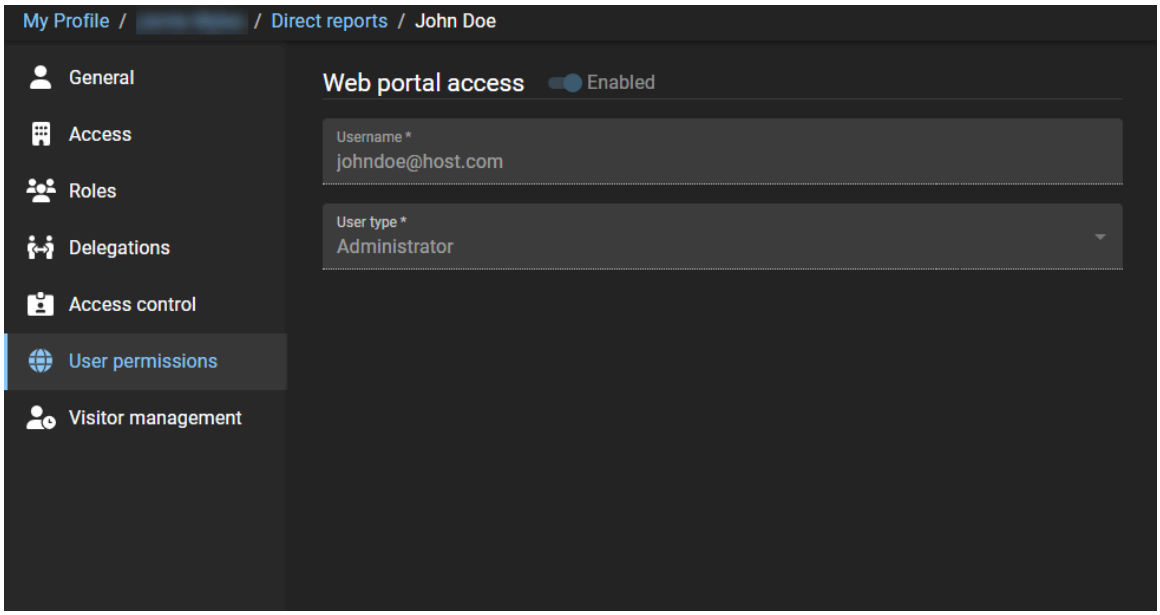
c) Cliquez sur ✕ en regard d'une délégation pour supprimer une délégation qui n'est plus requise.

6 Cliquez sur la page **Contrôle d'accès** pour afficher les paramètres de contrôle d'accès pour votre subordonné.

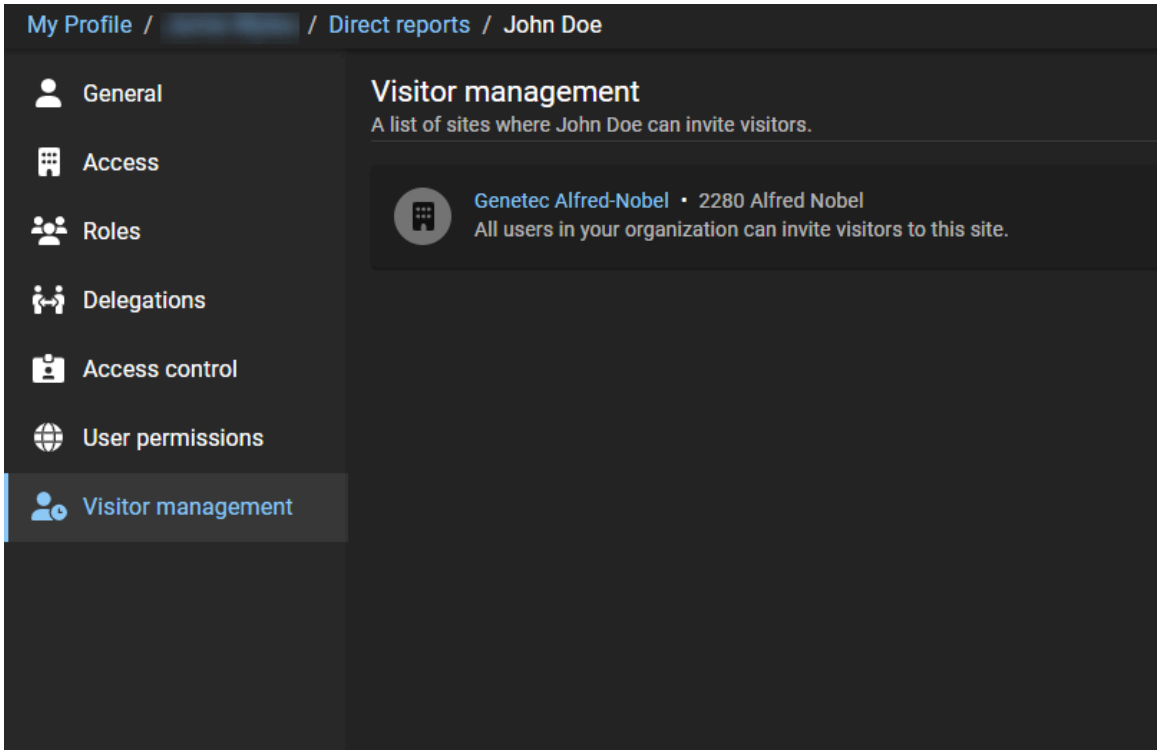


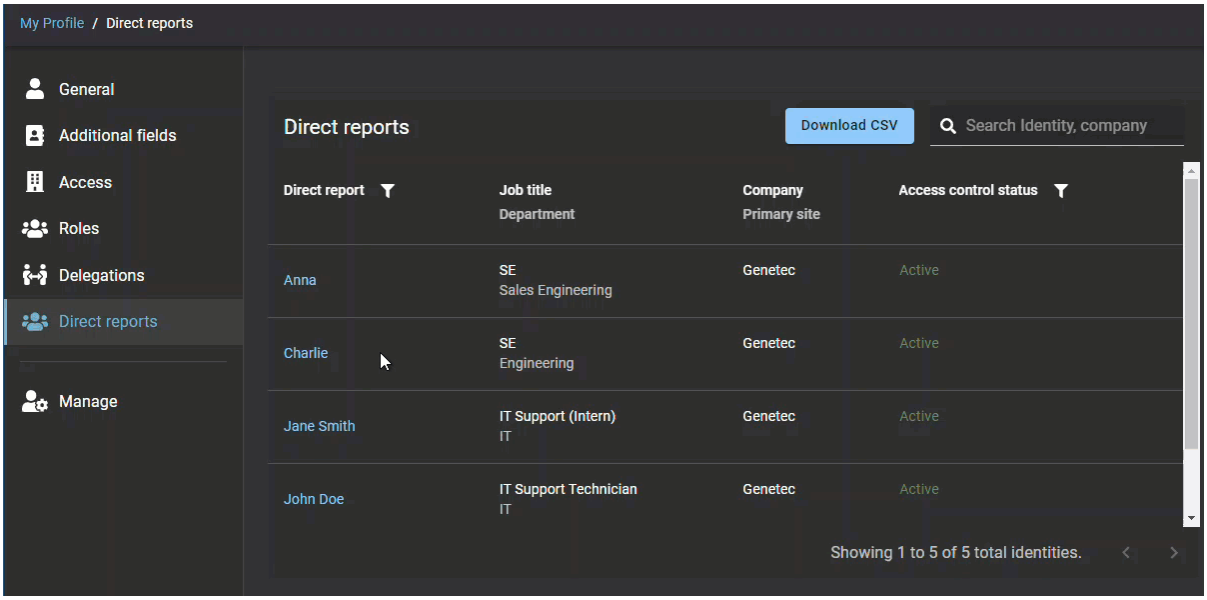
a) (Facultatif) Un superviseur ayant l'autorisation de gérer les subordonnés peut modifier les paramètres de **Contrôle d'accès** si nécessaire.

7 Cliquez sur la page **Autorisations utilisateur** pour afficher les autorisations d'accès des utilisateurs au portail Web pour votre subordonné.



8 Cliquez sur la page **Gestion des visiteurs** pour afficher les paramètres de gestion des visiteurs pour votre subordonné.





Rubriques connexes

Accorder des autorisations supplémentaires à des superviseurs, page 121

Transférer les subordonnés

Un superviseur, un administrateur de comptes ou une identité souhaitera parfois transférer des subordonnés, par exemple, pour transférer un subordonné à un nouveau responsable ou en cas de changement de superviseur.

Avant de commencer

Vous devez disposer d'un superviseur ou d'une identité qui a des subordonnés prêts à être transférés.

À savoir

Pour transférer des *subordonnés*, vous devez être un superviseur ou une identité avec des autorisations d'écriture avancées pour les identités ou un administrateur de comptes.

- Vous pouvez transférer les subordonnés à une autre identité (quelles que soient ses autorisations).
- Vous pouvez ajouter jusqu'à 20 superviseurs lorsque vous transférez des subordonnés.

IMPORTANT : Cette fonctionnalité est conçue pour les identités qui sont gérées en local dans Genetec ClearID[MC]. Si les identités sont gérées à l'aide d'une source de données externe, le transfert de subordonnés sera remplacé.

Procédure

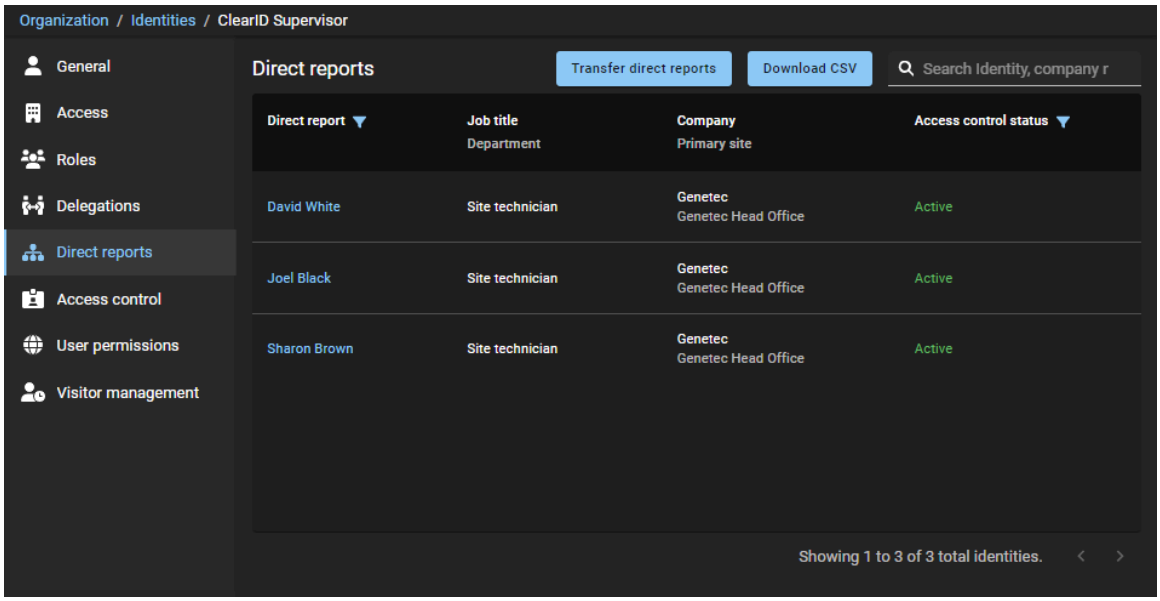
Pour transférer des subordonnés (effectué par un administrateur de comptes ou une identité) :

1 Sur la page d'*accueil*, cliquez sur **Organisation** > **Identités**.

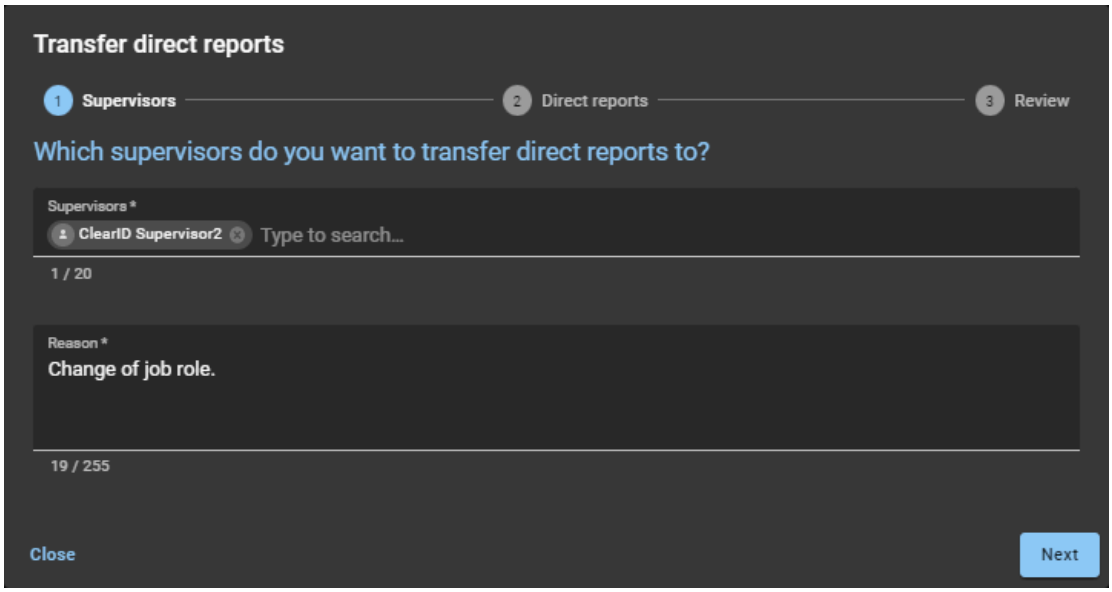
2 Sélectionnez l'identité dont vous souhaitez transférer des subordonnés.

3 Cliquez sur **Subordonnés**.

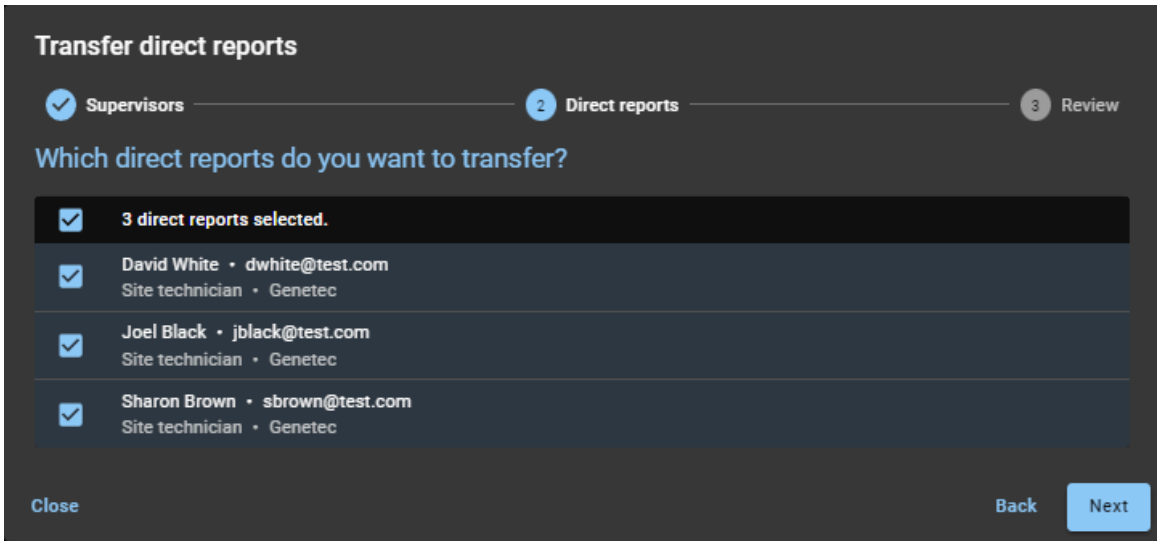
4 Cliquez sur **Transférer des subordonnés**.



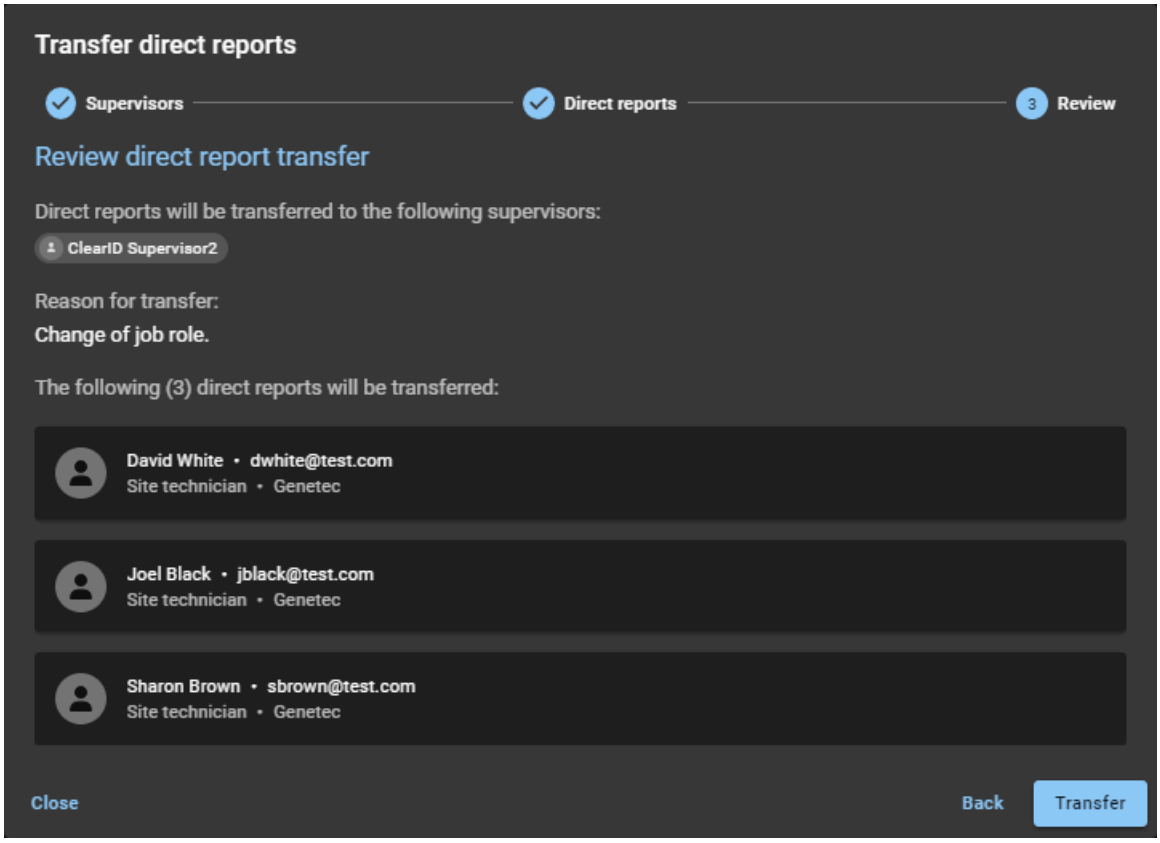
5 Renseignez les champs dans la section *Superviseurs* de la boîte de dialogue *Transférer des subordonnés*.
   a) Recherchez ou sélectionnez un ou plusieurs superviseurs.
   b) Indiquez le motif du transfert des subordonnés puis cliquez sur **Suivant**.



6 Dans la section *Subordonnés*, sélectionnez les subordonnés que vous souhaitez transférer, puis cliquez sur **Suivant**.



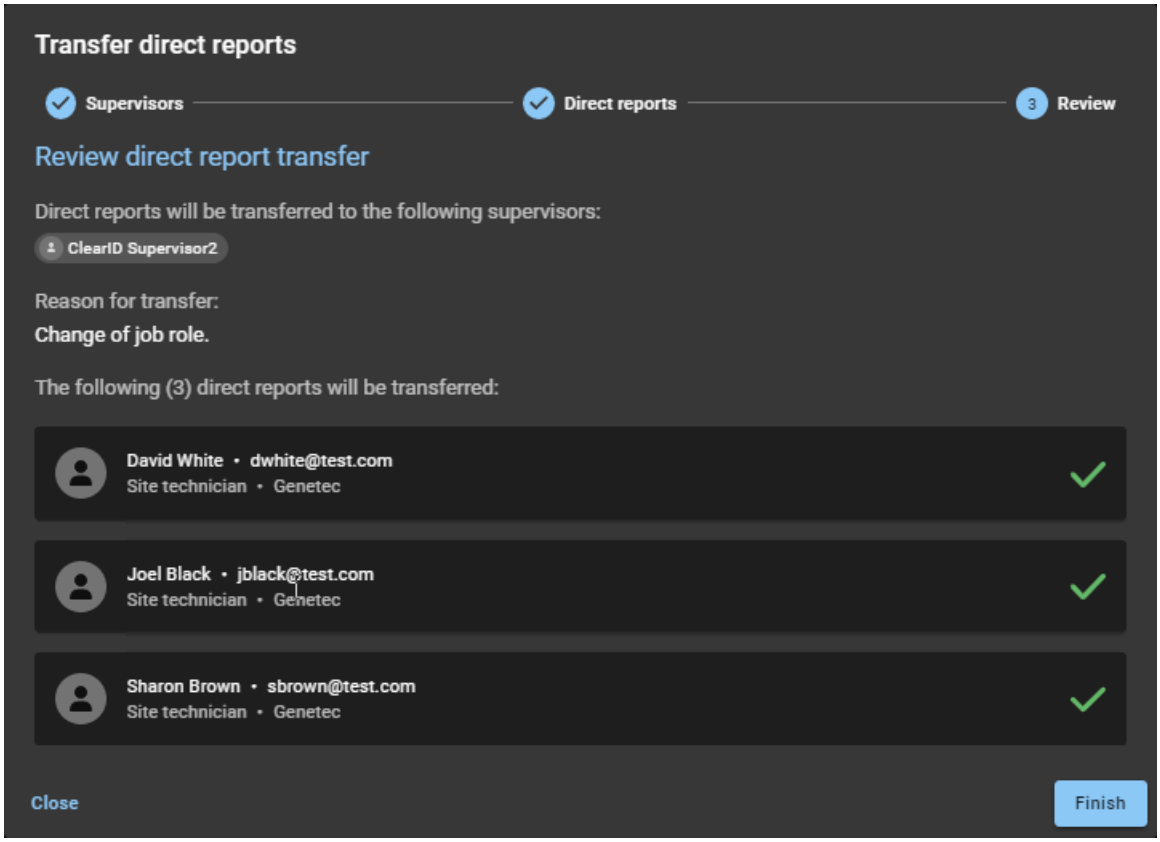
7 Dans la section **Examen**, vérifiez les informations sur les subordonnés que vous souhaitez transférer.



a) (Facultatif) Si vous souhaitez effectuer des ajouts ou des modifications, cliquez sur **Précédent** pour revenir à l'étape précédente.

b) Si aucune modification n'est nécessaire, cliquez sur **Transférer**.

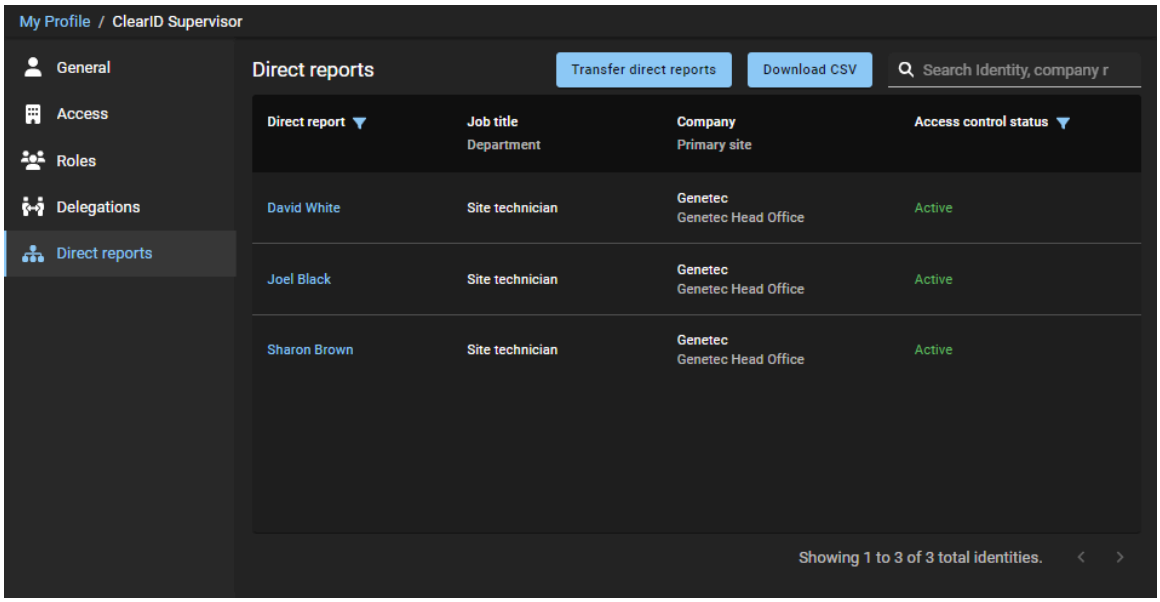
8 Cliquez sur **Terminer** pour clore la demande de transfert.



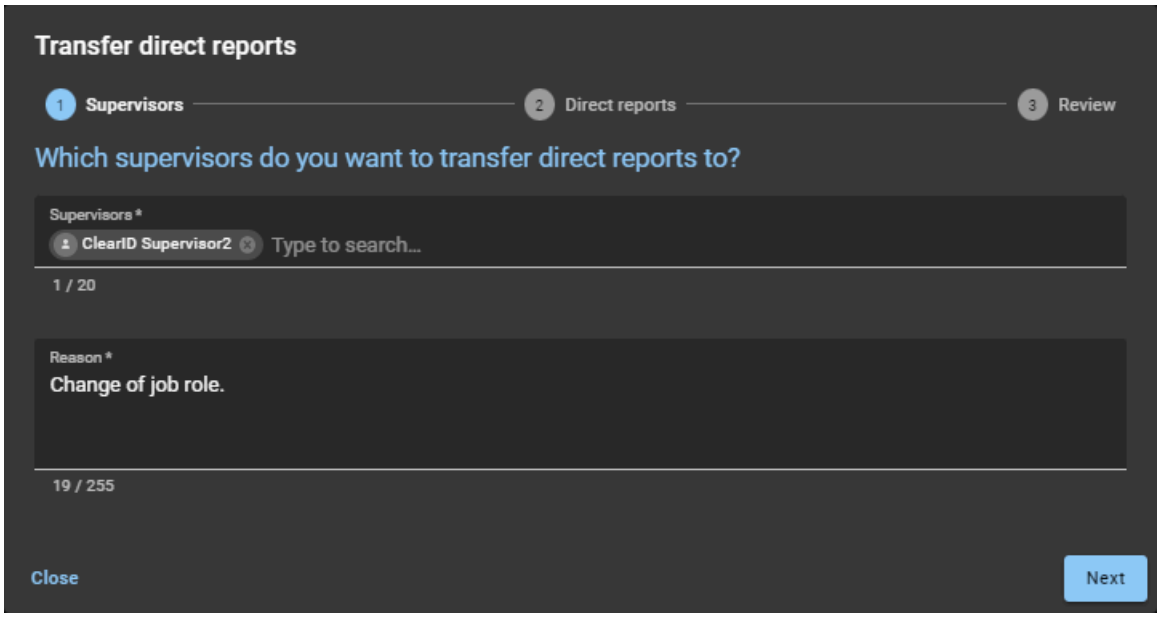
Pour transférer des subordonnés (par un superviseur) :

1 Sur la *page d'accueil*, cliquez sur **Mon profil** > **Subordonnés**.

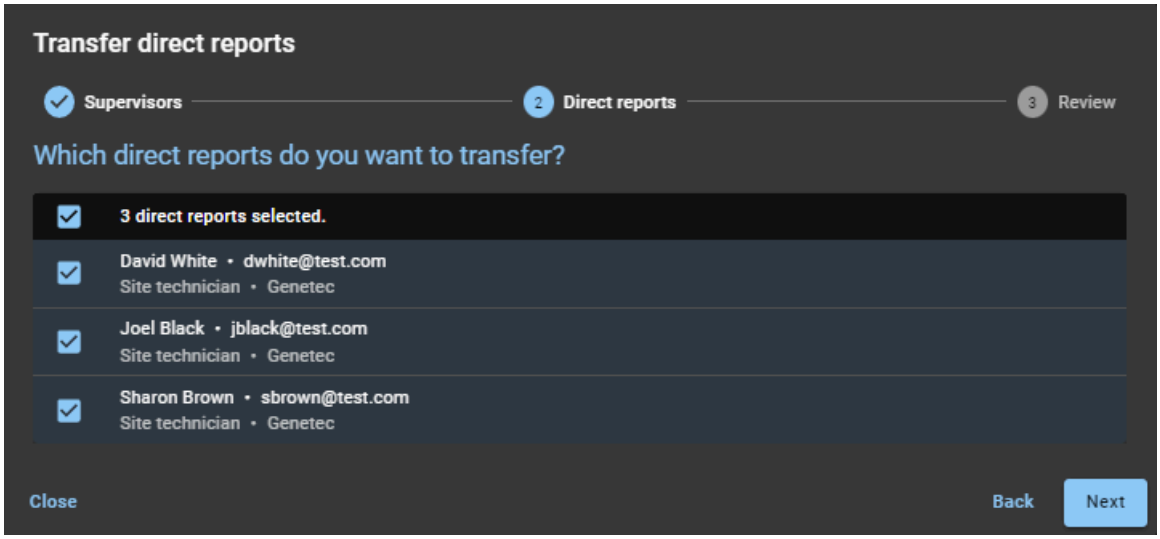
2 Cliquez sur **Transférer des subordonnés**.



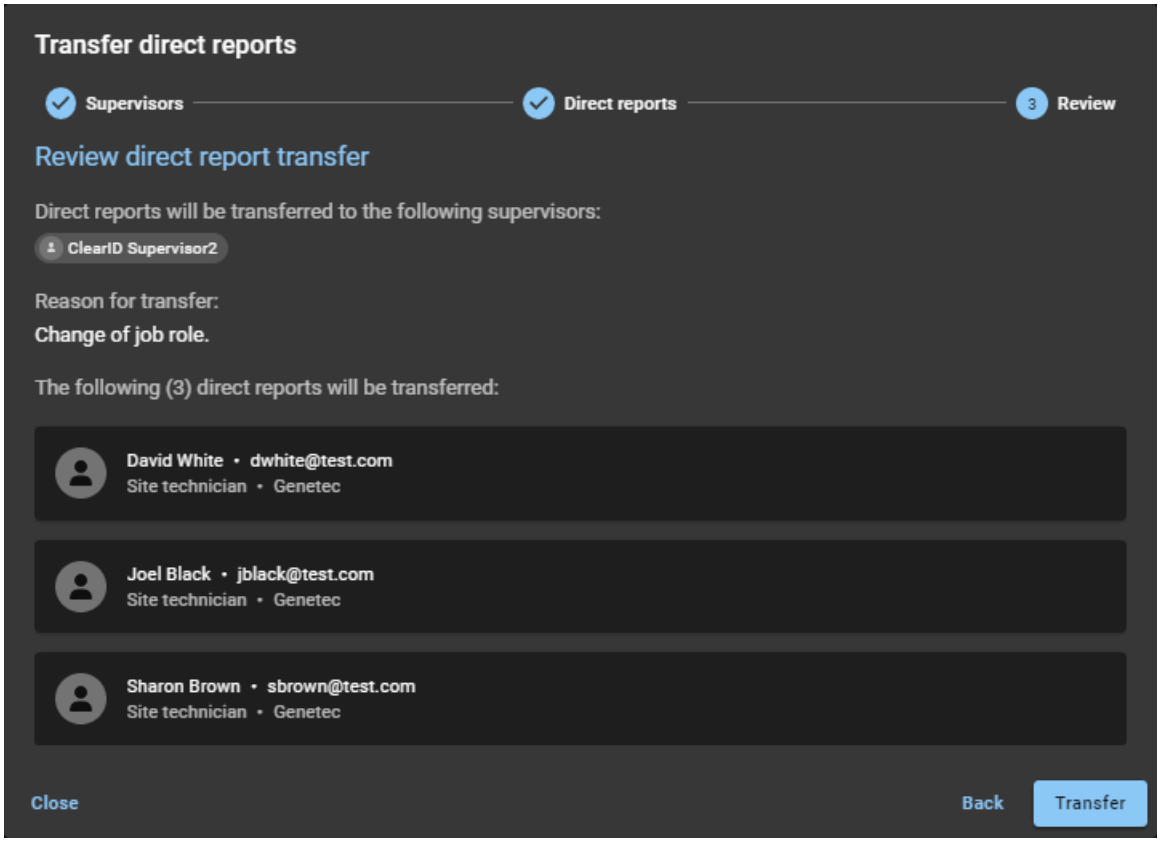
3 Renseignez les champs dans la section *Superviseurs* de la boîte de dialogue *Transférer des subordonnés*.
   a) Recherchez ou sélectionnez un ou plusieurs superviseurs.
   b) Indiquez le motif du transfert des subordonnés puis cliquez sur **Suivant**.



4 Dans la section *Subordonnés*, sélectionnez les subordonnés que vous souhaitez transférer, puis cliquez sur **Suivant**.



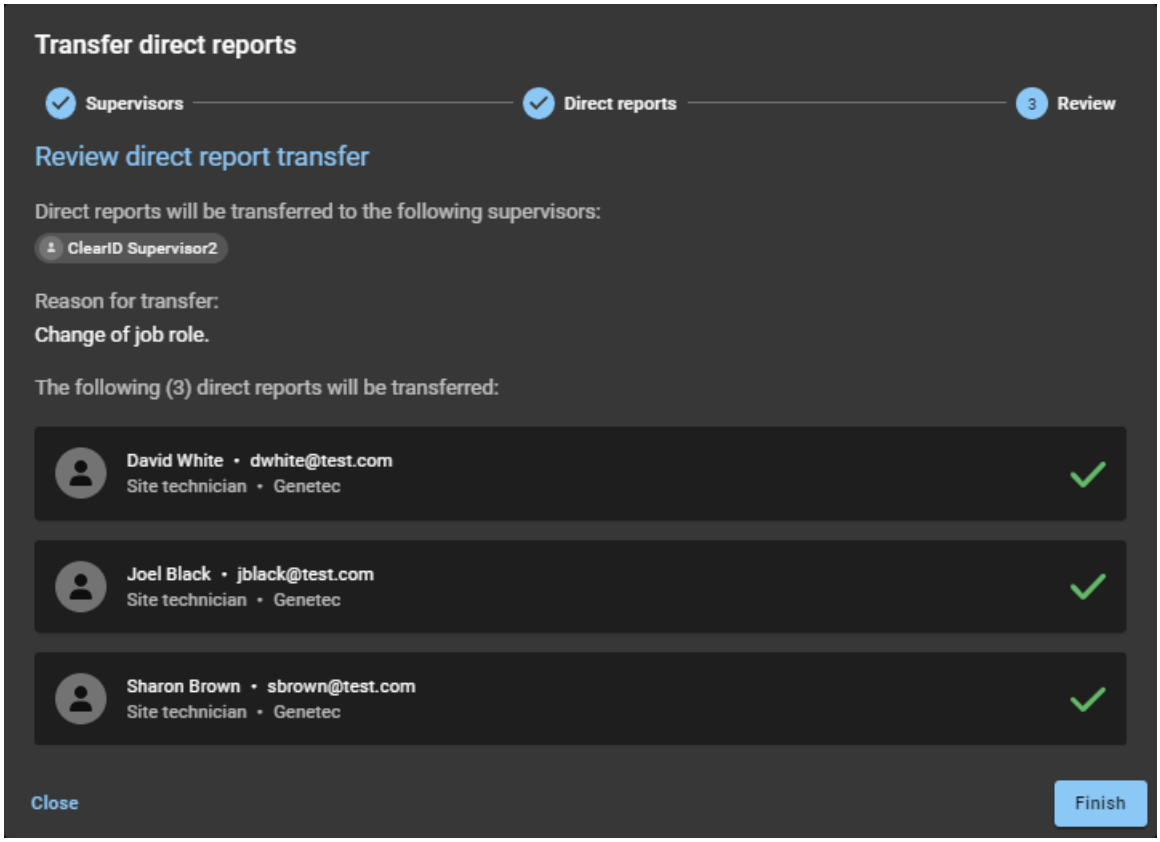
5 Dans la section **Examen**, vérifiez les informations sur les subordonnés que vous souhaitez transférer.



a) (Facultatif) Si vous souhaitez effectuer des ajouts ou des modifications, cliquez sur **Précédent** pour revenir à l'étape précédente.

b) Si aucune modification n'est nécessaire, cliquez sur **Transférer**.

6 Cliquez sur **Terminer** pour clore la demande de transfert.



Lorsque vous avez terminé

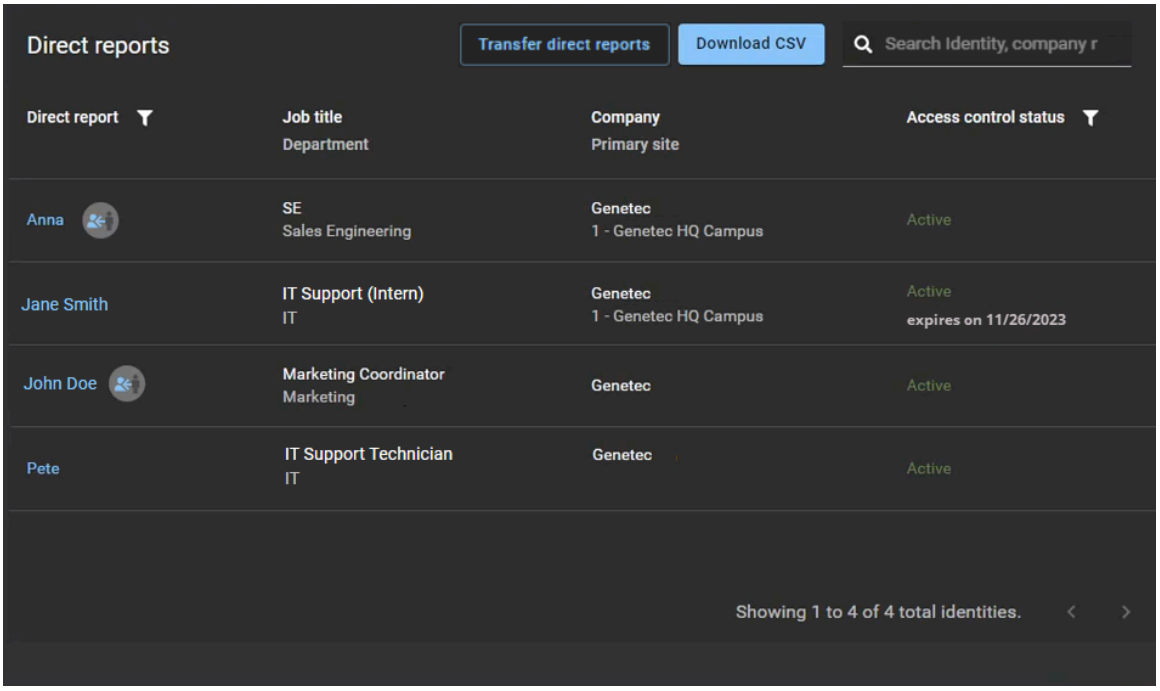
Affichez l'identité des nouveaux superviseurs pour vérifier que les subordonnés ont bien été transférés.

Rubriques connexes

Accorder des autorisations supplémentaires à des identités et des rôles, page 117
Accorder des autorisations supplémentaires à des superviseurs, page 121

À propos du rapport Subordonnés

Dans Genetec ClearID[MC], le rapport Subordonnés renvoie une liste d'identités d'employés qui rendent des comptes à un superviseur. Le rapport contient des informations sur les subordonnés, les subordonnés délégués, les intitulés de poste, les sociétés et l'état du contrôle d'accès.



Le rapport Subordonnés est utilisé par les superviseurs pour afficher leurs subordonnés, dont l'état du contrôle d'accès et des informations d'identité générales. Le rapport peut également servir à fournir des informations sur les subordonnés dans le cadre d'un audit.

Des filtres sont disponibles pour affiner le résultat de la recherche par subordonné (ou subordonné délégué) et par état du contrôle d'accès (actif ou inactif).

Illustration 1 : Rapport Subordonnés

Rubriques connexes

Afficher les subordonnés, page 166

Réinitialiser les mots de passe utilisateur

Si vous ne parvenez pas à vous authentifier lors de la connexion à un compte géré par Genetec ClearID[MC], vous pouvez réinitialiser votre mot de passe.

À savoir

La réinitialisation du mot de passe n'est disponible que pour les utilisateurs dont les comptes sont gérés par ClearID. Utilisez les bonnes pratiques du secteur pour créer des mots de passe fiables.

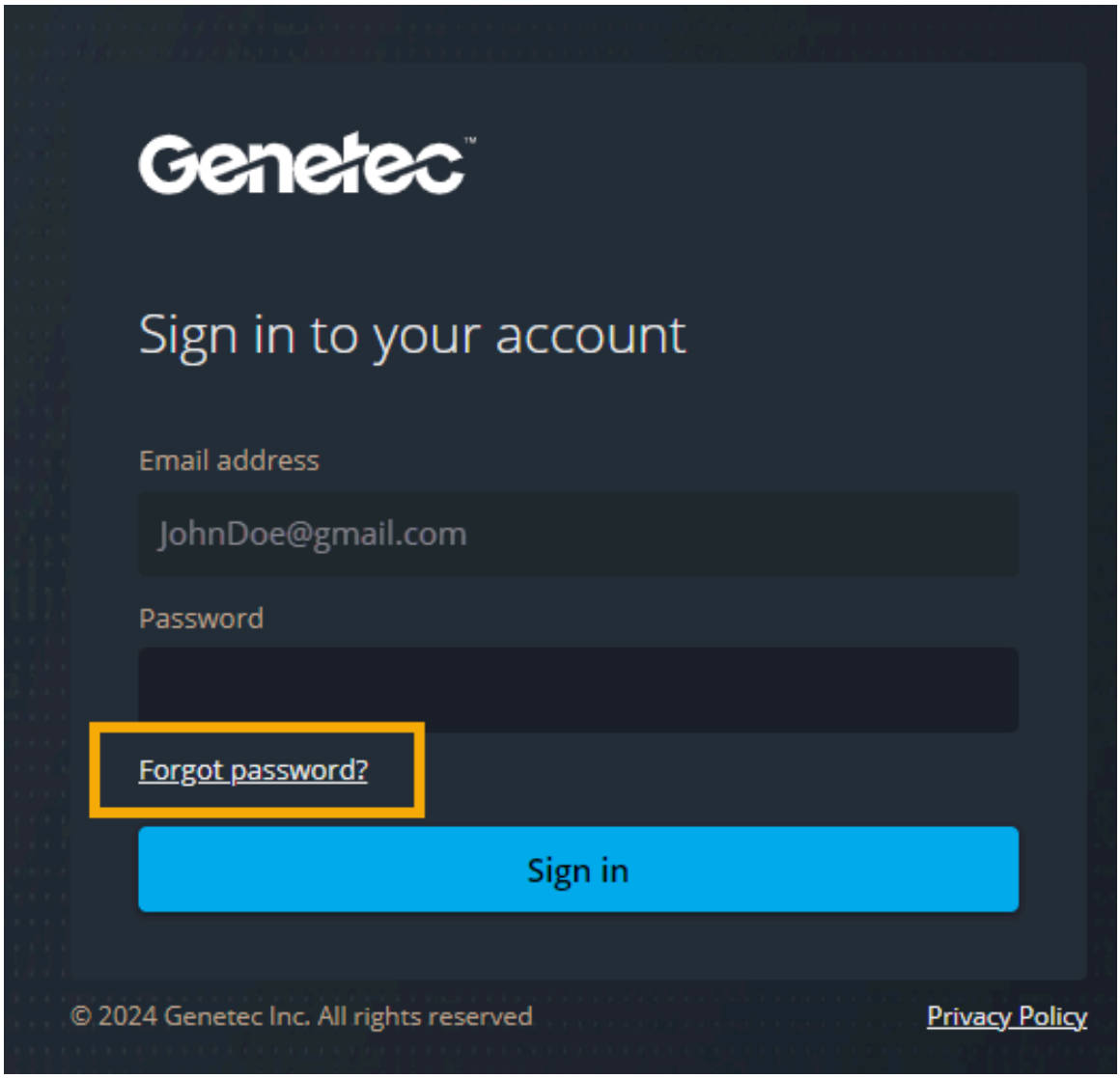
REMARQUE : Cette procédure ne concerne pas les utilisateurs de l'authentification unique d'entreprise.

Procédure

1 Dans un navigateur Web, effectuez l'une des opérations suivantes :

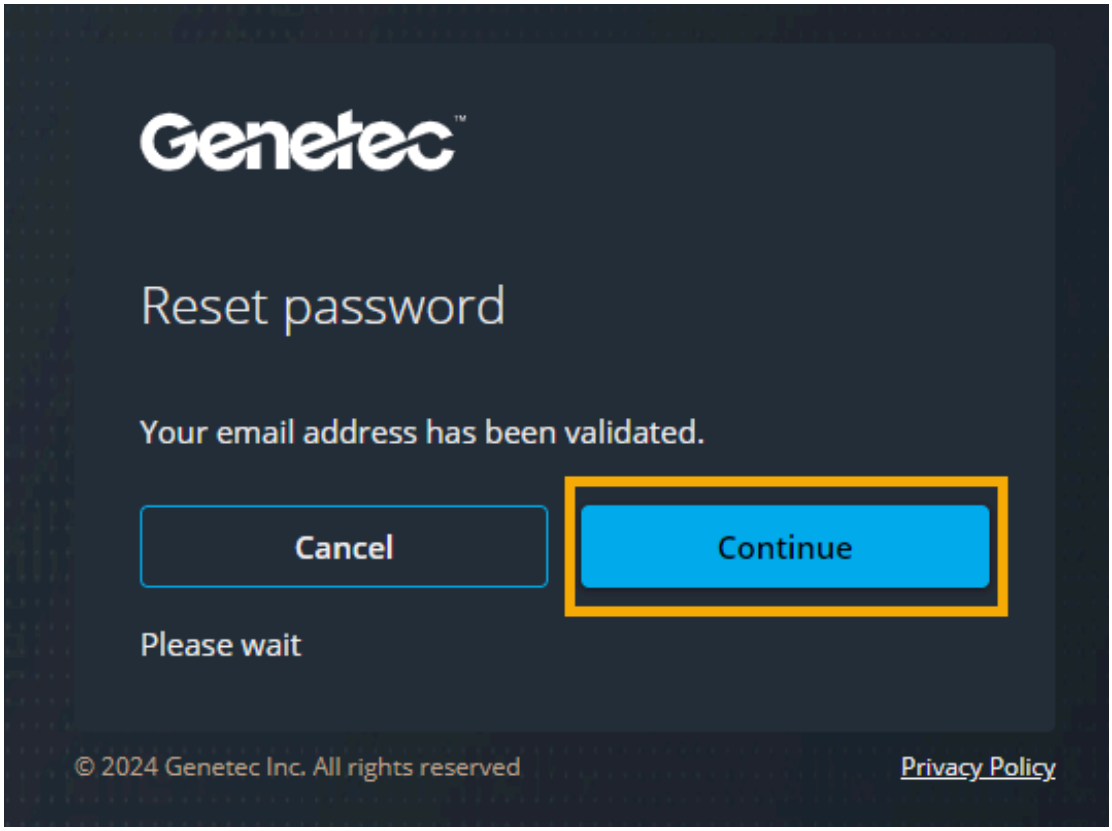
- Si vous avez un compte en production, allez à https://portal.clearid.io.
- Si vous avez un compte de démo ou de test, allez à https://demo.clearid.io.

2 Entrez votre adresse e-mail et cliquez sur **Se connecter**.
Vous êtes redirigé vers la nouvelle page de connexion de Genetec[MC].



3 Cliquez sur **Mot de passe oublié ?**.
Vous êtes redirigé vers la page *Réinitialiser le mot de passe*.

4 Sur la page *Réinitialiser le mot de passe*, cliquez sur **Envoyer un code** pour recevoir un code de vérification par e-mail.
   a) Entrez le code dans le champ **Code de vérification** de la page *Réinitialiser le mot de passe*.
   b) Cliquez sur **Vérifier le code**.
   c) Une fois que votre e-mail est validé, cliquez sur **Continuer**.



5 Entrez et confirmez votre nouveau mot de passe, puis cliquez sur **Continuer**.

Vous pouvez à présent accéder à ClearID à l'aide du mot de passe que vous avez créé.

À propos des notifications par e-mail

Genetec ClearID[MC] envoie des notifications par e-mail pour informer les utilisateurs d'événements système particuliers associés aux accès, identités, rôles et visites.

Les notifications par e-mail sont envoyées par *noreply@clearid.io*. Si vous ne recevez pas les notifications dans votre boîte de réception ou votre dossier de courrier indésirable, contactez *l'administrateur de votre compte*.

Pour vous désabonner ou vous réabonner aux notifications par e-mail, voir Configurer vos préférences de notification par e-mail, page 190

Les événements suivants peuvent déclencher les notifications par e-mail :

Événement déclencheur de la notification	Destinataires potentiels de la notification
Résumé d'activité	
Résumé d'activité hebdomadaire **REMARQUE :** • Le résumé d'activité hebdomadaire contient toutes les tâches ou requêtes en attente concernant les événements de visite, les demandes d'identité ou les demandes d'accès à un secteur qui nécessitent une approbation. En l'absence de tâches ou de requêtes en attente, vous ne recevez pas ces notifications. • Les e-mails de résumé d'activité hebdomadaire sont envoyés tous les lundis matins à 9h00, basé sur l'heure du site principal de l'identité. Si aucun site principal n'est défini, l'e-mail est envoyé à 9h00 GMT.	• Demandeurs • *Approbateurs de visite* • *Superviseurs* • *Approbateurs d'identité* • *Propriétaires de secteurs* • *Gestionnaires de secteur* • *Gestionnaires de rôles*
Accès pour une identité	
Compte créé pour une identité **IMPORTANT :** Si une connexion d'entreprise (authentification unique à l'aide de Microsoft Office 365 ou similaire) est utilisée, le compte est automatiquement activé et aucun e-mail d'activation n'est reçu.	• Identité • *Administrateurs de comptes*
La demande d'accès à un secteur pour une identité a été envoyée	• Demandeur d'identité
La demande d'accès à un secteur pour une identité a été supprimée	• Demandeur d'identité • *Gestionnaires de secteur* • *Propriétaires de secteurs*
La demande d'accès à un secteur pour une identité nécessite une approbation ou un refus **CONSEIL :** • Aucun e-mail n'est envoyé si la demande est approuvée automatiquement.	• *Superviseurs* • *Gestionnaires de secteur*

Événement déclencheur de la notification	Destinataires potentiels de la notification
• Le destinataire de l'e-mail dépend des réglages des processus du système.	
La demande d'accès à un secteur pour une identité est approuvée ou refusée **REMARQUE :** Si la personne qui envoie une demande d'accès et l'identité de la demande d'accès sont différentes, les deux reçoivent l'e-mail.	• Identité • *Propriétaires de secteurs*
La demande d'accès à un secteur pour une identité est accordée	• Identité • *Superviseurs d'identité*
L'accès à un secteur pour une identité est révoqué (ou a expiré) **REMARQUE :** Les e-mails d'expiration d'accès sont envoyés à minuit selon le fuseau horaire spécifié pour le site.	• Identité • *Superviseurs d'identité*
Accès pour un rôle	
Demande d'accès envoyée pour un rôle **REMARQUE :** Les *propriétaires de rôles* et les *gestionnaires de rôles* peuvent demander l'accès pour les rôles. La personne qui effectue la demande reçoit l'e-mail.	• *Gestionnaires de rôles* • *Propriétaires de rôle*
La demande d'accès pour un rôle nécessite une approbation ou un refus	• *Superviseurs* • *Gestionnaires de secteur*
La demande d'accès pour un rôle est approuvée ou refusée **REMARQUE :** Un *superviseur* ou *un gestionnaire de secteur* doit approuver ou refuser la demande.	Approuvé : • *Gestionnaires de secteur* Refusé : • Tous les *gestionnaires de rôles*
L'accès au secteur est accordé au rôle **REMARQUE :** Les *gestionnaires de secteur* peuvent approuver les demandes d'accès à un secteur pour les rôles, ou les demandes peuvent être acceptées automatiquement. L'accès d'un rôle à un secteur peut également être accordé manuellement.	• Tous les *gestionnaires de rôles*
L'accès au secteur est révoqué pour un rôle	• Tous les *gestionnaires de rôles*
Identité ajoutée aux membres du rôle	• Identité
Identité supprimée des membres du rôle	• Identité
Demandes d'identité	

Événement déclencheur de la notification	Destinataires potentiels de la notification
Identité demandée **REMARQUE :** Si l'une des identités demandées est annulée, tous les approbateurs configurés sont ajoutés à la liste **cc** dans l'e-mail d'approbation de la demande d'identité. L'objet de l'e-mail est : « La demande d'identité pour *identité* a été mise à jour ».	• Demandeur • *Superviseurs* (si configuré dans le modèle d'identité) • *Approbateurs d'identité* (si configuré dans le modèle d'identité)
Événements de visite	
Visite créée	• Demandeur • Hôtes
La visite nécessite une approbation ou un refus **REMARQUE :** Aucun e-mail n'est envoyé si la demande est approuvée automatiquement.	• *Superviseurs*
Visite approuvée ou refusée	• Demandeur • Hôtes
Confirmation du visiteur	• Visiteur
La demande de visite nécessite une approbation ou un refus **REMARQUE :** Aucun e-mail n'est envoyé si la visite est approuvée automatiquement.	• *Gestionnaires de secteur* (en fonction du processus) • *Approbateurs de visite* (en fonction du processus)
Visiteur inscrit	• Hôtes
Alerte de liste de surveillance de visiteurs (notifier ou bloquer)	• *Gestionnaires de listes de surveillance*
Examens d'accès	
Examens d'accès en attente	• *Gestionnaires de secteur* • *Gestionnaires de rôles*

Rubriques connexes

Configurer vos préférences de notification par e-mail, page 190

Personnaliser la bannière d'e-mail d'un site

Vous pouvez personnaliser la bannière graphique affichée dans les e-mails de notification de demande d'accès ou de demande de visiteur envoyés pour le site.

Avant de commencer

Configurer l'iPad de la borne en libre-service, page 582

CONSEIL : Vérifiez que votre bannière répond aux exigences spécifiées dans l'infobulle sur la page **Images** du portail web Genetec ClearID[MC].

À savoir

Seul un propriétaire de site ou un administrateur de comptes peut personnaliser les bannières d’e-mail.

- Les modifications de bannières d’e-mail sont synchronisées avec la borne toutes les 60 secondes.

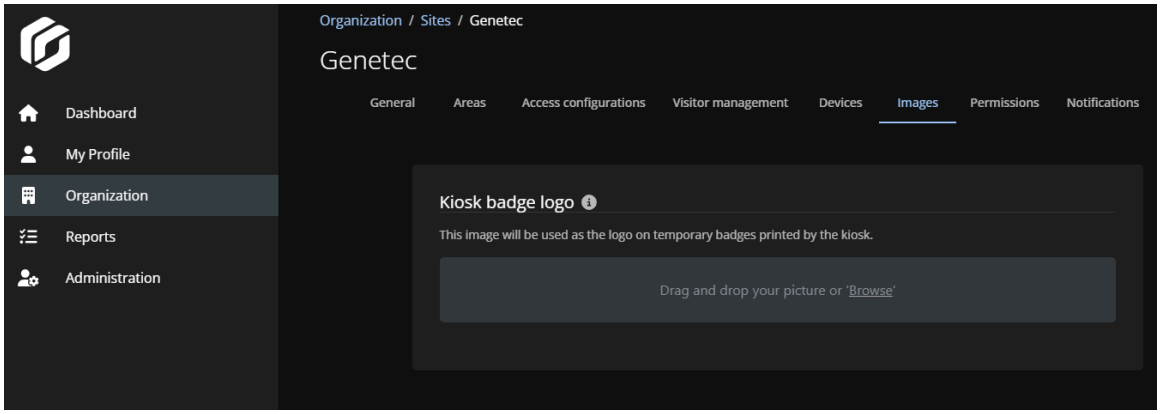
BONNE PRATIQUE : Pour un résultat optimal, utilisez des images *.PNG* transparentes pour personnaliser votre bannière d’e-mail.

Procédure

1 Sur le portail Web ClearID, cliquez sur **Organisation** > **Sites**.

2 Recherchez et sélectionnez un site.

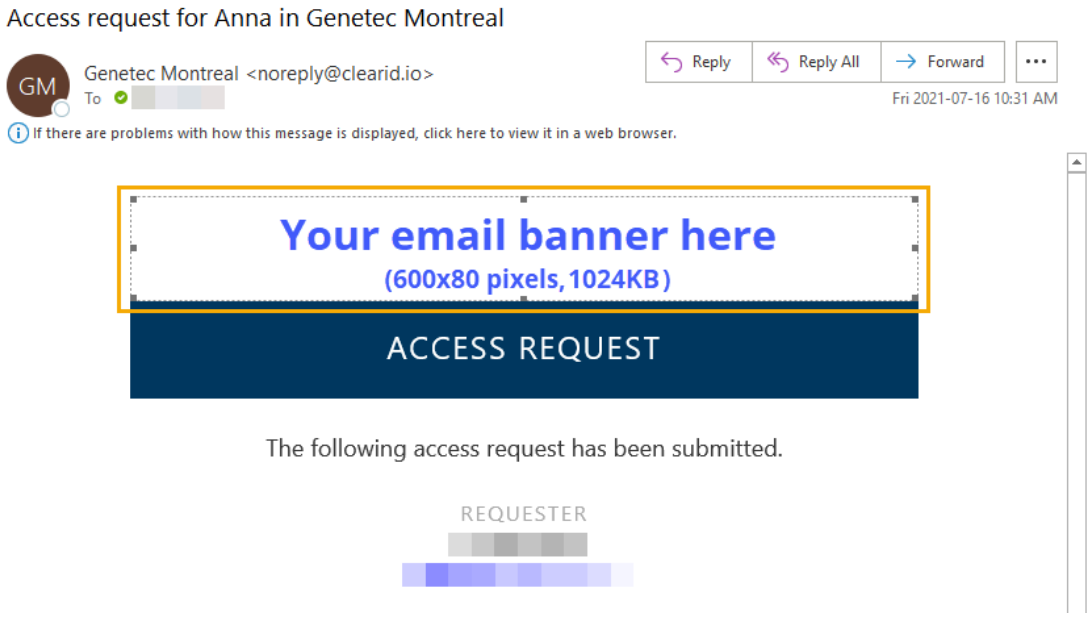
3 Cliquez sur **Images**.



a) Dans la section *Bannière d'e-mail*, faites un glisser-déposer de votre image ou parcourez vos fichiers pour sélectionner l'image de **Bannière d'e-mail**.

b) Cliquez sur **Enregistrer**.

Voici un exemple d'image de bannière d'e-mail personnalisée.



Configurer vos préférences de notification par e-mail

Vous recevez des notifications par e-mail pour les demandes de visite, les demandes d'accès ou divers résumés d'activité depuis Genetec ClearID[MC]. Vous pouvez décider quelles notifications vous souhaitez recevoir et configurer vos préférences de notification en conséquence.

À savoir

Vos préférences de notification ne s'appliquent qu'à votre profil d'utilisateur. Toutes les notifications par e-mail sont activées par défaut.

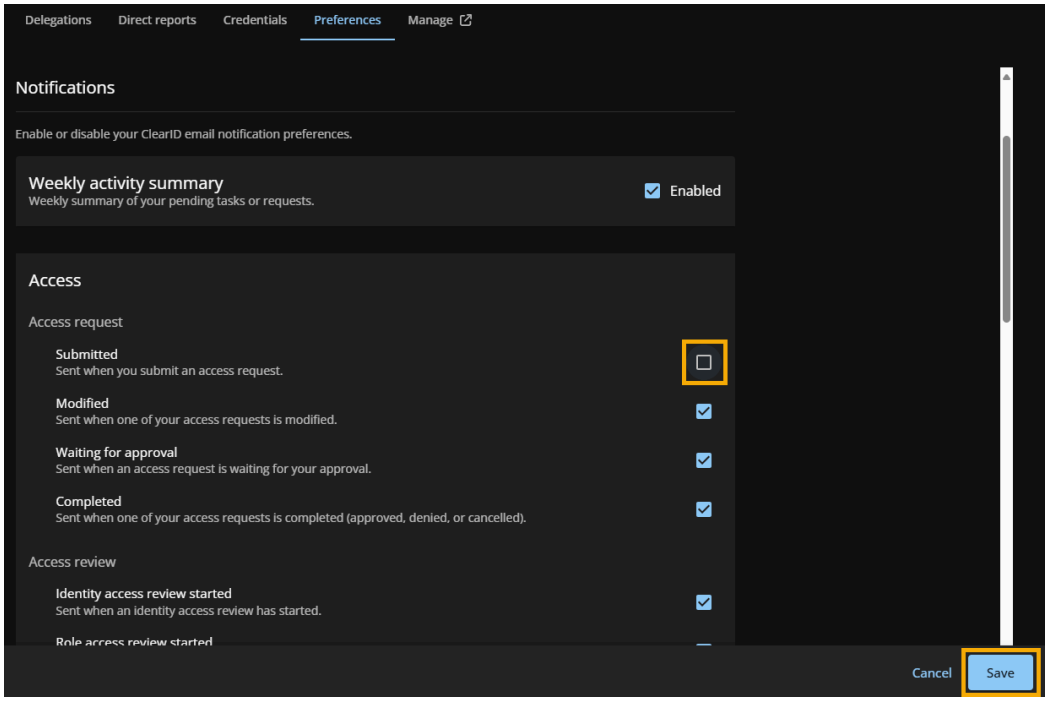
CONSEIL : Utilisez le résumé d'activité hebdomadaire pour suivre vos demandes et vos tâches en attente.

Procédure

1 Sur le portail web ClearID, cliquez sur **Mon profil** > **Préférences**.

2 Dans la section *Notifications*, configurez les préférences selon vos besoins.

a) Décochez la case en regard de chaque notification que vous ne souhaitez pas recevoir.



3 Cliquez sur **Enregistrer**.

Rubriques connexes

À propos des notifications par e-mail, page 186

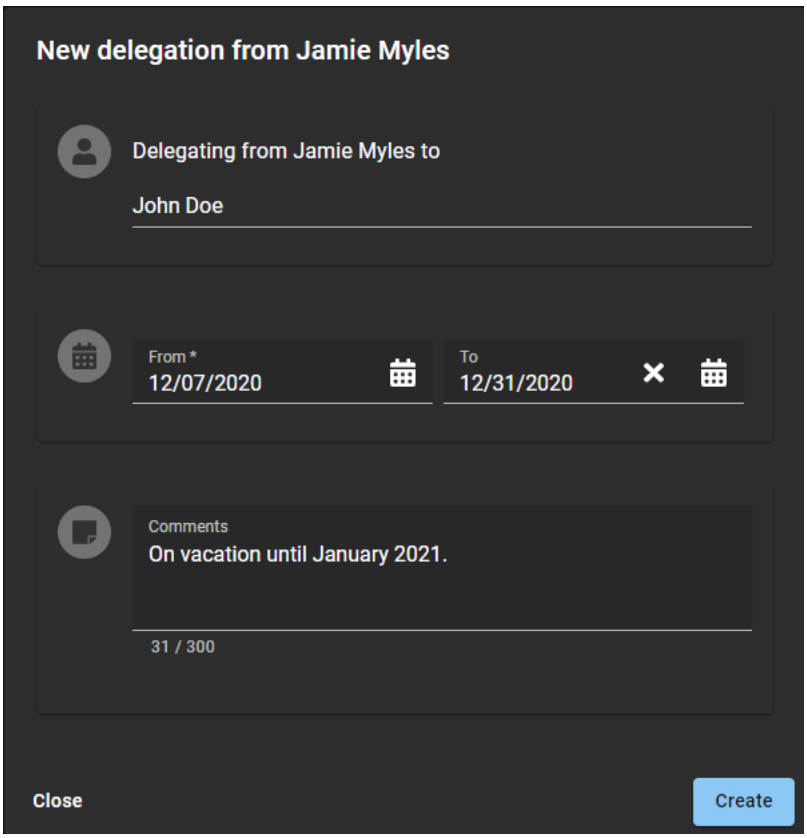
À propos de la délégation

Dans Genetec ClearID[MC], la délégation est le processus consistant à transférer des tâches Genetec ClearID[MC] de propriétaires de sites, propriétaires de secteurs, approbateurs de secteurs, responsables de rôles et approbateurs d'événements de visite à quelqu'un d'autre au sein de votre organisation. Par exemple, à l'occasion de vacances prévues, de congés sabbatiques, etc.

Délégation planifiée

Dans ce cas, le besoin de délégation est connue à l'avance et est planifiée par le propriétaire de l'autorisation. Par exemple, un congé planifié, un congé sabbatique ou un congé de maternité.

Un délégué reçoit alors temporairement les mêmes autorisations que la personne déléguant la responsabilité afin de pouvoir gérer les tâches déléguées.

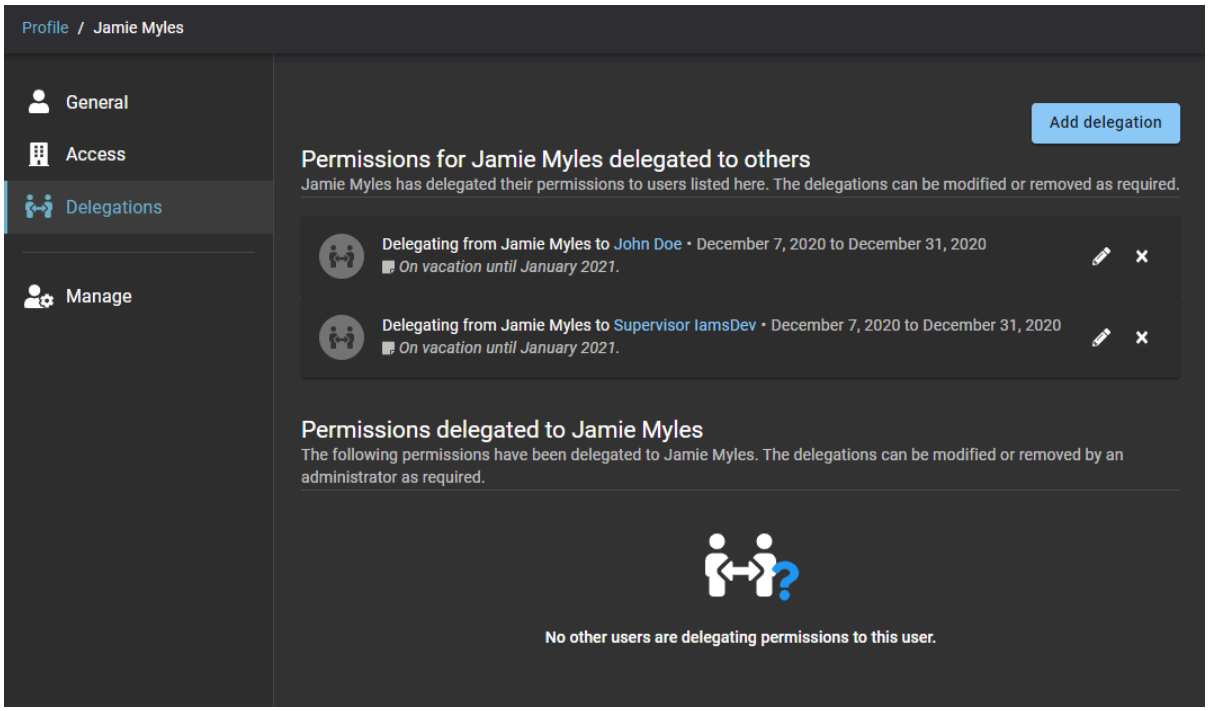


Par exemple, si un approbateur de secteur vous délègue des tâches, vous êtes temporairement autorisé à effectuer ces tâches d'approbateurs de secteur. Les tâches déléguées sont ensuite affichées dans la section **Mes tâches** de votre **tableau de bord**.

Autorisations d'*utilisateur* déléguées à d'autres

- Si nécessaire, vous pouvez déléguer à plus d'une personne. Cette possibilité peut s'avérer utile lorsque les tâches sont effectuées par plusieurs personnes. Par exemple, différents superviseurs ou collaborateurs d'équipe.
- Vous ne pouvez pas déléguer des tâches qui vous ont été déléguées, car cela pourrait créer un conflit d'approbation. Lorsque vous créez une délégation, vous ne déléguez que vos propres tâches.

- La période de délégation peut être modifiée ( ) ou désactivée ( ) tôt si vos exigences de délégation changent.



Autorisations déléguées à *utilisateur*

Les autorisations peuvent également vous être déléguées par une autre personne.

REMARQUE : Vous ne pouvez pas déléguer des autorisations à un utilisateur qui vous délègue déjà. Dans ce cas, le message d'erreur suivant s'affiche : L'utilisateur spécifié vous délègue déjà des autorisations. Cette délégation doit être supprimée avant que vous puissiez leur en déléguer.

Délégation non planifiée

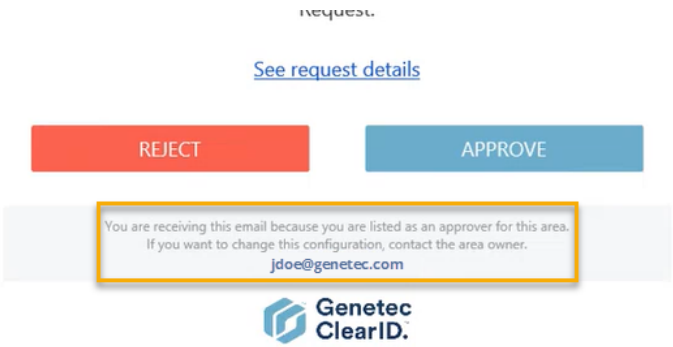
Quelquefois, une délégation non planifiée peut s'avérer nécessaire car le délégant n'est pas disponible pour définir la délégation. Par exemple, en cas d'absence imprévue ou de période d'indisponibilité. Dans ce cas, un administrateur de compte peut effectuer une délégation au nom d'un délégateur indisponible. L'administrateur de compte peut également modifier ou supprimer une délégation si nécessaire.

IMPORTANT : Les autorisations d'administrateur ne peuvent pas être déléguées. Vous ne pouvez attribuer des autorisations d'administrateur qu'au moyen de canaux officiels standard.

Notifications par e-mail de délégation

Toutes les notifications par e-mail associées aux tâches déléguées sont envoyées au propriétaire de l'autorisation d'origine et au délégué. À l'aide de ces notifications par e-mail ou de la page **Mes tâches**, le délégué peut accéder aux tâches déléguées et les exécuter.

Les notifications par e-mail envoyées aux délégués comprennent les coordonnées du contact dans le pied de page des notifications par e-mail afin que le délégué puisse contacter le propriétaire de l'autorisation s'il souhaite demander des modifications par rapport à la configuration de la délégation.


See request details
REJECT
APPROVE
You are receiving this email because you are listed as an approver for this area.
If you want to change this configuration, contact the area owner.
jdoe@genetec.com
Genetec
ClearID.

Déléguer des tâches à un autre utilisateur

Les propriétaires de sites, les propriétaires de secteurs, les approbateurs de secteurs, les propriétaires de rôles, les responsables de rôles, les superviseurs et les approbateurs d'événements de visite peuvent déléguer à titre temporaire leurs tâches Genetec ClearID[MC] à une autre personne de leur organisation. Par exemple, à l'occasion de vacances prévues, de congés sabbatiques, etc.

Avant de commencer

En savoir plus sur la délégation.

BONNE PRATIQUE : Avant de déléguer vos tâches, pensez à contacter le délégué potentiel pour lui faire part de la délégation et confirmer sa disponibilité.

À savoir

- Seul un utilisateur connecté peut déléguer ses tâches ClearID à une ou plusieurs autres personnes.
- La période de délégation peut être modifiée ( ) ou désactivée ( ) tôt si vos exigences de délégation changent.
- Un administrateur de compte peut également effectuer une délégation non planifiée au nom d'un délégant indisponible. Par exemple, en cas d'absence imprévue ou de période d'indisponibilité.

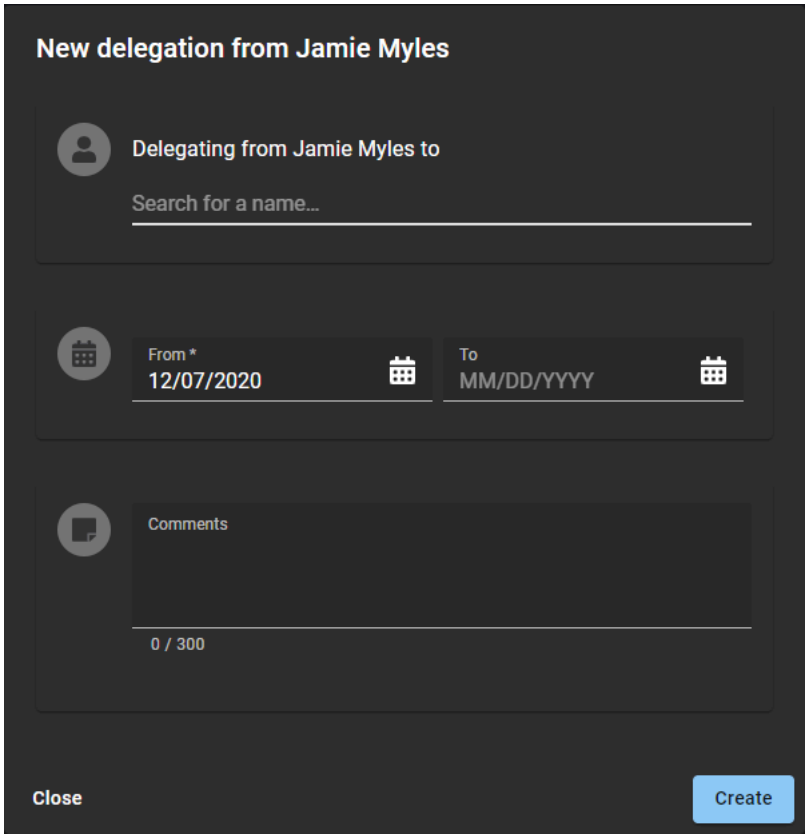
IMPORTANT : Les autorisations d'administrateur ne peuvent pas être déléguées. Vous ne pouvez attribuer des autorisations d'administrateur qu'au moyen de canaux officiels standard.

Procédure

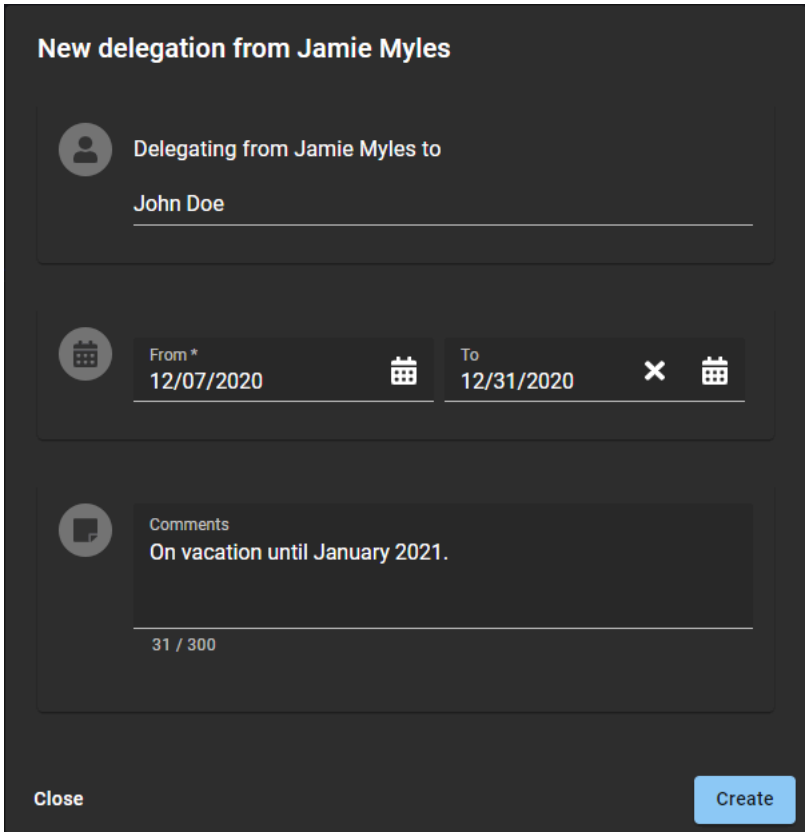
1 Depuis le *tableau de bord*, cliquez sur **Mon profil** > **Délégations**.

2 Cliquez sur **Ajouter une délégation**.

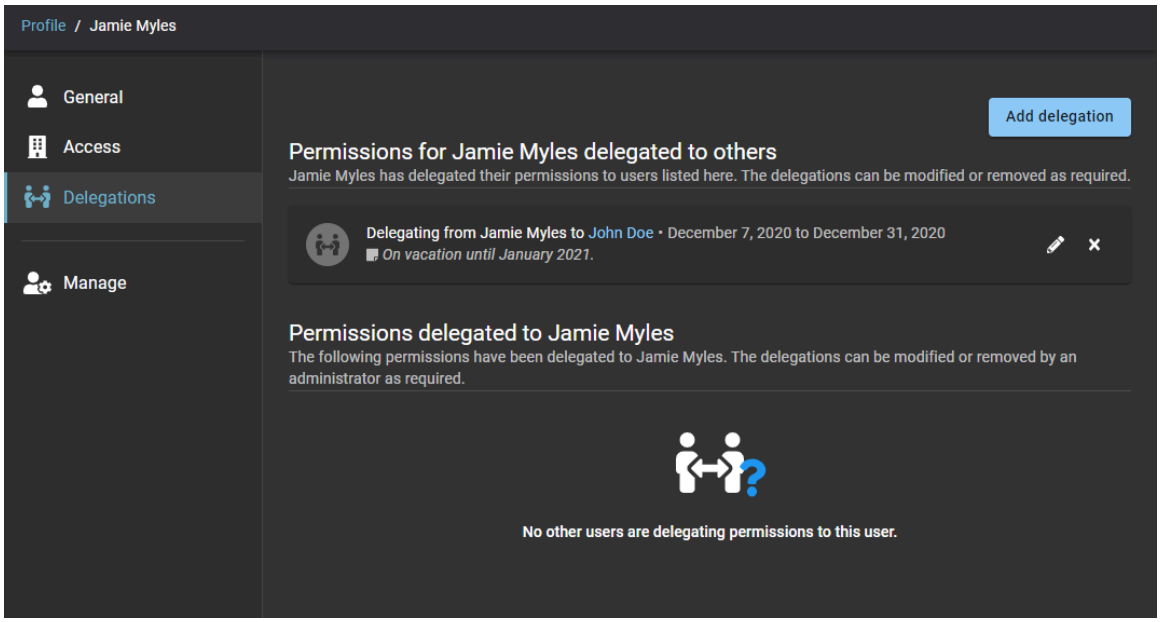
3 Renseignez les champs.



a) Recherchez ou saisissez le nom de l'utilisateur auquel vous souhaitez déléguer vos tâches ClearID.
b) Saisissez les dates **de début** et **de fin** de la période pendant laquelle vous souhaitez que la délégation soit en vigueur.
c) Dans le champ **Commentaires**, ajoutez une explication sur la raison pour laquelle vous déléguez vos tâches à d'autres utilisateurs.



4 Cliquez sur **Créer**.



5 (Facultatif) Dans la section **Autorisations de *nom d'utilisateur* déléguées à d'autres**, cliquez sur pour modifier une délégation active.

a) Saisissez les dates **de début** et **de fin** de la période pendant laquelle vous souhaitez que la délégation soit en vigueur.

b) Dans le champ **Commentaires**, ajoutez une explication sur les raisons pour lesquelles vous déléguez vos tâches à d'autres utilisateurs.

c) Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Votre délégation est désormais active et expirera automatiquement à la date indiquée.

6 (facultatif) Cliquez sur pour supprimer une délégation.

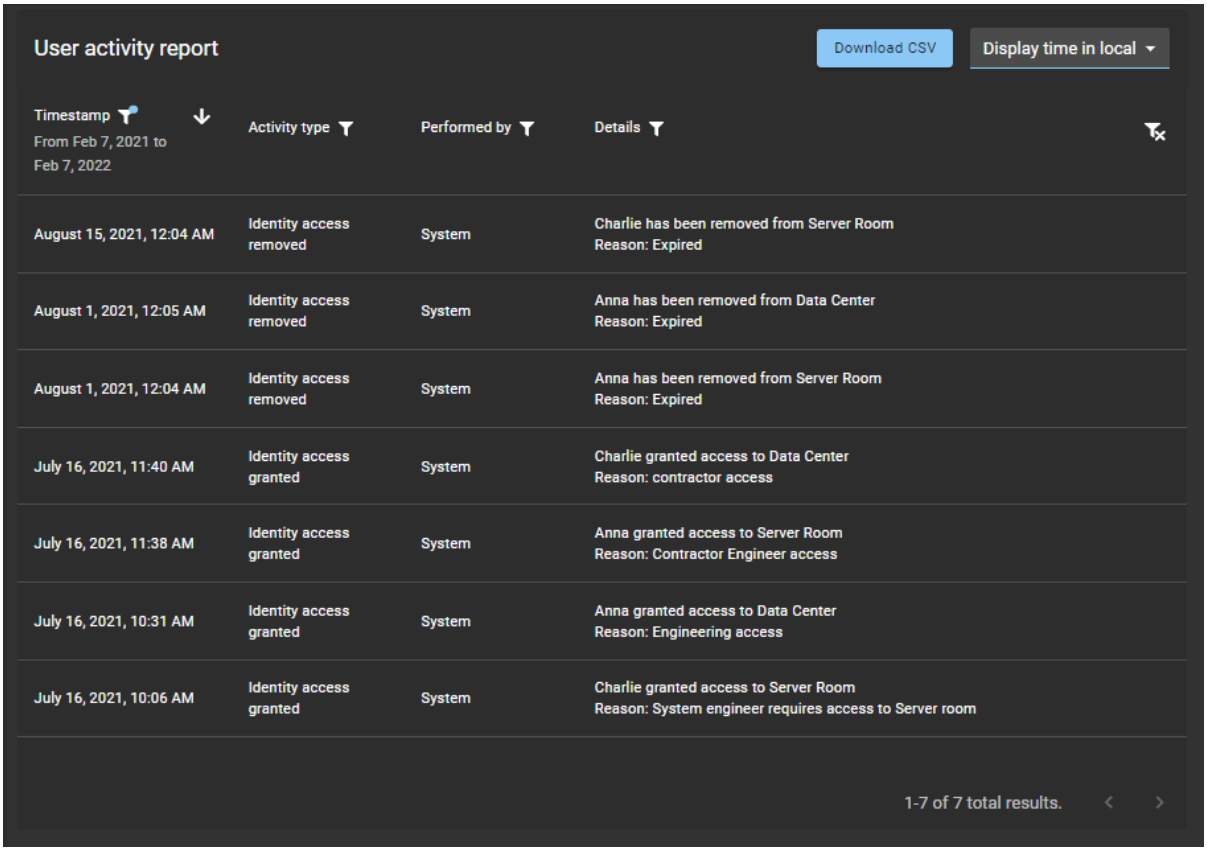
a) Dans la boîte de dialogue **Supprimer la délégation**, cliquez sur **Supprimer** pour confirmer que la délégation n'est plus requise.

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles.

À propos du rapport d'activité d'utilisateurs

Dans Genetec ClearID[MC], le rapport d'activité d'utilisateurs est un historique de toutes les activités associées aux utilisateurs. Le rapport contient des informations d'horodatage, de type d'activité, sur les personnes ayant effectué l'activité, ainsi qu'une section détails qui contient des informations de motif.

Rapport d'activité d'utilisateurs



En tant qu'administrateur de compte, vous pouvez utiliser ce rapport pour afficher toutes les données correspondant aux activités suivantes :

- Propriétaire de secteur ajouté ou supprimé
- Approbateur de secteur ajouté ou supprimé
- Accès d'identité accordé ou supprimé
- Accès au rôle accordé ou supprimé
- Propriétaire de rôle ajouté ou supprimé
- Gestionnaire de rôle ajouté ou supprimé
- Membre de rôle ajouté ou supprimé
- Superviseur ajouté ou supprimé
- Identité créé, mise à jour, ou supprimé
- Champ personnalisé créé, mise à jour, ou supprimé
- Section de champ personnalisé créé, mise à jour, ou supprimé

Vous pouvez utiliser des filtres pour affiner le résultat de la recherche du rapport par horodatage, type d'activité, effectué par et détails.

Rubriques connexes

Afficher un rapport d'activité d'utilisateurs, page 201

Afficher un rapport d'activité d'utilisateurs

Vous pouvez consulter le *Activité utilisateur* pour examiner toutes les activités associées aux utilisateurs. Utilisez le rapport à des fins d'audit, téléchargez une copie à joindre à une demande d'audit pour l'examiner hors ligne, ou manipulez ou consolidez les données dans une feuille de calcul pour d'autres publics.

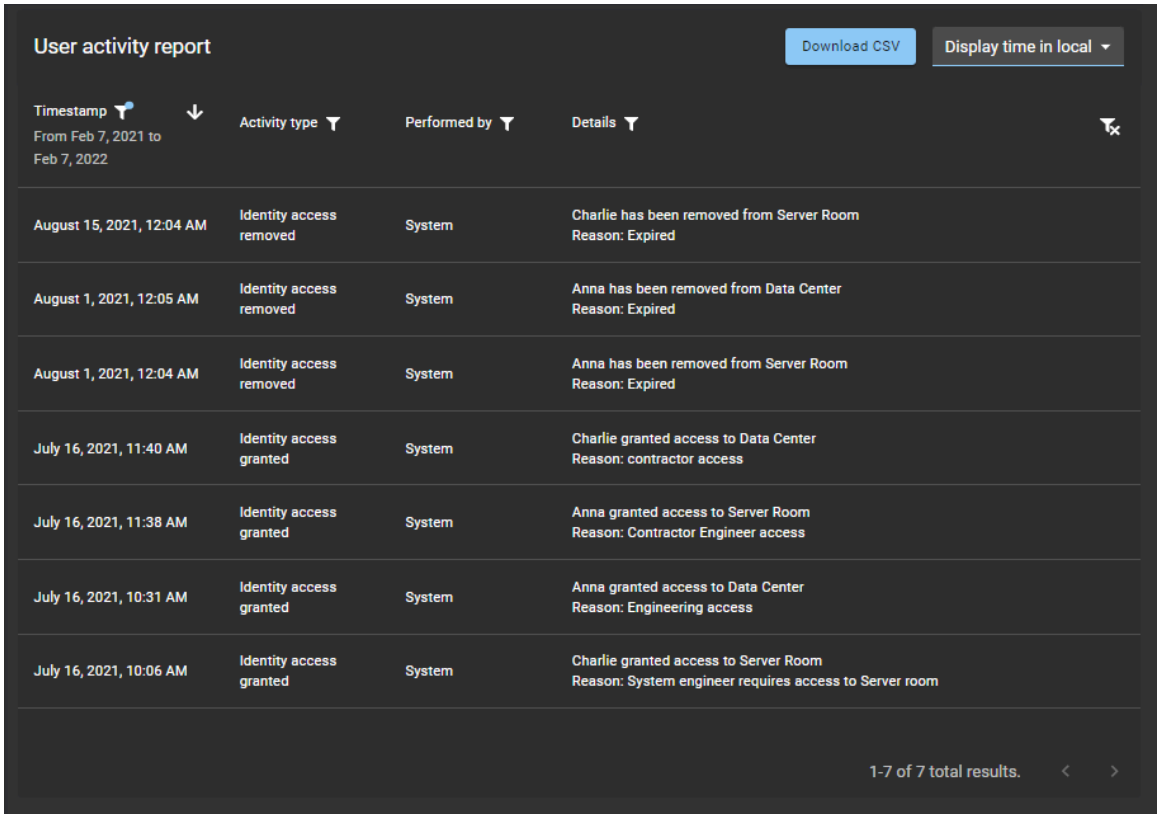
Avant de commencer

Pour afficher le *Activité utilisateur* créez des rapports et examinez les informations de l'historique de configuration, assurez-vous d'être un administrateur de compte.

REMARQUE : Le *Activité utilisateur* le rapport est vide si aucune activité n'est enregistrée par responsables de secteur, gestionnaires de rôlesou membres du rôle dans votre système Genetec ClearID[MC].

Procédure

1 Depuis le *Accueil* page, cliquez sur **Rapports** > **Activité utilisateur**.

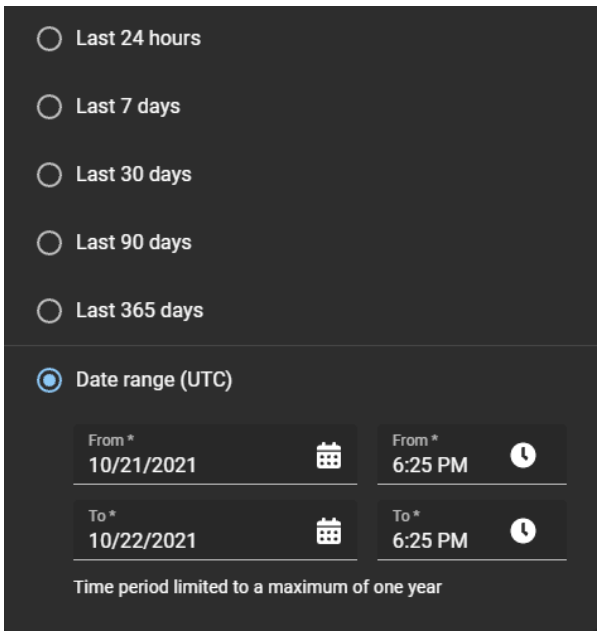


2 Dans le *Activité utilisateur* dans l'onglet de rapport, sélectionnez le réglage d'heure d'affichage dont vous avez besoin.

- **Heure d'affichage locale :** Les heures d'affichage sont affichées via l'heure du système de l'ordinateur de l'utilisateur connecté.
- **Heure d'affichage UTC :** Les heures du rapport sont affichées au format UTC (temps universel coordonné).

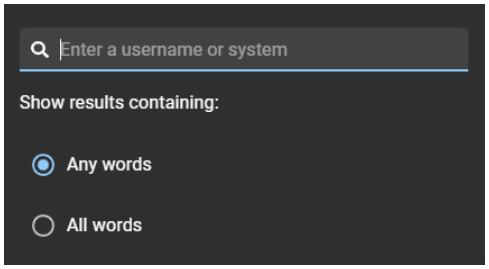
3 Filtrez le rapport en fonction de vos critères :

- **Horodatage :** Dans la colonne **Horodatage**, cliquez sur pour filtrer le résultat par date. Sélectionnez une plage de dates prédéfinie parmi les choix disponibles, ou spécifiez une plage particulière à l'aide du sélecteur de plage de dates.

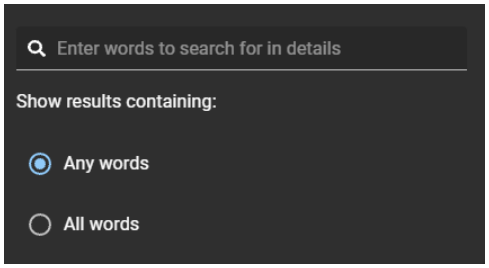


(Facultatif) Utilisez les icônes de tri (et) pour afficher les résultats en ordre croissant ou décroissant.

- **Type d'activité :** Dans la colonne **Type d'activité**, cliquez sur pour filtrer les résultats par type d'activité :
  - Propriétaire de secteur ajouté ou supprimé
  - Approbateur de secteur ajouté ou supprimé
  - Accès d'identité accordé ou supprimé
  - Accès au rôle accordé ou supprimé
  - Propriétaire de rôle ajouté ou supprimé
  - Gestionnaire de rôles ajouté ou supprimé
  - Membre de rôle ajouté ou supprimé
  - Superviseur ajouté ou supprimé
  - Identité créée, mise à jour ou supprimée
  - Champ personnalisé créé, mis à jour ou supprimé
  - Section champ personnalisé créée, mise à jour ou supprimée
- **Effectué par :** Dans la colonne **Effectué par**, cliquez sur pour ouvrir une boîte de dialogue de recherche et filtrer les résultats sur la personne ayant effectué une activité. Par exemple, recherchez les tâches effectuées par un utilisateur particulier, ou les tâches effectuées automatiquement par le système.



- **Détails :** Dans la colonne **Détails**, cliquez sur pour ouvrir une boîte de dialogue qui permet de rechercher dans les détails ou les motifs à l'aide de critères de recherche.



- **(Facultatif) :** Cliquer pour réinitialiser les sélections de filtres.

4 Cliquer **Télécharger un fichier CSV** pour télécharger une copie du *Activité utilisateur* rapport.
Suivez les instructions dans votre navigateur pour télécharger le fichier exporté.

Le fichier est exporté sous la forme d'un fichier *.CSV* dans le dossier de téléchargement par défaut de votre navigateur. Par défaut, le fichier exporté est créé d'après le nom du rapport et la date de téléchargement. Par exemple, *UserActivities_2022-02-14.csv*.

REMARQUE : Les colonnes et les entrées dans le fichier CSV peuvent varier en fonction des filtres sélectionnés au moment de télécharger le rapport.

Rubriques connexes

À propos du rapport d'activité d'utilisateurs, page 199

Niveaux utilisateur

Les informations suivantes vous aident à comprendre les actions que les utilisateurs ou les rôles peuvent effectuer dans Genetec ClearID[MC].

Gestion des identités

Actions	Propriétaires de compte (et clé API)	Propriétaires de sites	Propriétaires de secteurs	Approbateurs de secteur	Superviseurs d'identité	Utilisateurs authentifiés
Créer des identités	✓[1]					
Mettre à jour les identités	✓[1]					
Afficher les informations privées sur les identités	✓[1]					
Répertorier les identités lors de l'ajout à une secteur ou à un rôle	✓[1]	✓	✓	✓	✓	✓
Créer des sites	✓[1]					
Supprimer les identités	✓[1]					
Voir les subordonnés	✓[1]				✓	
Gérer les subordonnés	✓[1]				✓	
Transférer les subordonnés	✓[1]				✓	

[1] Les utilisateurs affectés en tant que délégué pour un autre utilisateur n'héritent pas de l'autorisation.

Gestion de secteurs

Actions	Propriétaires de compte (et clé API)	Propriétaires de sites	Propriétaires de secteurs	Approbateurs de secteur	Superviseurs d'identité	Utilisateurs authentifiés
Créer et supprimer des sites	✓[1]					

Actions	Propriétaires de compte (et clé API)	Propriétaires de sites	Propriétaires de secteurs	Approbateurs de secteur	Superviseurs d'identité	Utilisateurs authentifiés
Modifier les informations du site	✓[1]	✓				
Attribuer des propriétaires de site	✓[1]	✓[1]				
Créer et supprimer des secteurs	✓[1]	✓				
Modifier les attributs de provisionnement automatique du secteur	✓[1]	✓				
Modifier le nom du secteur	✓[1]	✓				
Afficher tous les secteurs privés d'un site	✓[1]	✓				
Affecter les propriétaires de secteurs	✓[1]	✓				
Affecter les approbateurs de secteurs	✓[1]	✓	✓[1]			
Modifier la visibilité du secteur (public ou privé)	✓[1]	✓	✓			
Modifier le processus d'approbation	✓[1]	✓	✓			
Modifier les horaires du secteur	✓[1]		✓			
Afficher la configuration du secteur et la liste d'accès	✓[1]	✓	✓	✓		
Ajouter des personnes ou	✓[1]		✓	✓		

Actions	Propriétaires de compte (et clé API)	Propriétaires de sites	Propriétaires de secteurs	Approbateurs de secteur	Superviseurs d'identité	Utilisateurs authentifiés
des rôles à des secteurs						
Supprimer des personnes ou des rôles de secteurs	✓[1]		✓	✓		
Approuver une demande d'accès à un secteur	✓[1]			✓	✓	
Modifier la période et l'horaire avant d'approuver la demande d'accès	✓[1]			✓	✓	
Planifier des analyses d'accès au secteur	✓	✓				
Recevoir et effectuer les analyses d'accès au secteur	✓[1]	✓	✓	✓		
Consulter un rapport d'examen d'accès	✓	✓				

[1] Les utilisateurs affectés en tant que délégué pour un autre utilisateur n'héritent pas de l'autorisation.

Gestion des rôles

Actions	Propriétaires de compte (et clé API)	Propriétaires de sites	Propriétaires de rôle	Responsables de rôles	Superviseur d'identité	Tout utilisateur du compte
Créer et supprimer des rôles	✓[1]					
Affecter les propriétaires de rôles	✓[1]					

Actions	Propriétaires de compte (et clé API)	Propriétaires de sites	Propriétaires de rôle	Responsables de rôles	Superviseur d'identité	Tout utilisateur du compte
Affecter les responsables de rôles	✓[1]		✓[1]			
Modifier les règles de provisionnement automatique et la configuration d'un rôle	✓[1]		✓			
Modifier le nom, la description et les notes d'un rôle	✓[1]		✓			
Répertorier les rôles lors de l'ajout à un secteur ou à une demande d'accès	✓[1]		✓	✓		
Ajouter ou supprimer manuellement une personne d'un rôle	✓[1]		✓	✓		
Soumettre une demande d'accès pour le compte d'un rôle			✓	✓		
Recevoir et effectuer les analyses d'accès du rôle			✓	✓		
Supprimer des identités d'un rôle	✓[1]		✓	✓		

[1] Les utilisateurs affectés en tant que délégué pour un autre utilisateur n'héritent pas de l'autorisation.

Gestion des visiteurs

Actions	Propriétaires de compte (et clé API)	Demandeur de visite	Superviseur du demandeur	Propriétaires de sites	Hôtes de visite	Approbateurs de secteur
Événement de visite						
Créer un événement de visite		✓ 1				
Ajouter des invités à un événement ou les supprimer d'un événement		✓ 1			✓1	
Approuver ou rejeter un événement de visite			✓			
Approuver ou refuser l'accès invité spécifique à un secteur						✓
Créer un événement (copier un événement) à partir d'un événement existant		✓1	✓		✓1	
Annuler l'événement		✓1			✓1	
Voir la liste des événements à venir		✓ 1			✓1	
Afficher les détails de l'événement		✓ 1	✓		✓1	✓
Configuration de la gestion des visiteurs						
Modifier la configuration de la gestion	✓ 1			✓		

Actions	Propriétaires de compte (et clé API)	Demandeur de visite	Superviseur du demandeur	Propriétaires de sites	Hôtes de visite	Approbateurs de secteur
des visiteurs (secteur)						
Modifier la configuration de la gestion des visiteurs (site)	✓ [1]			✓		

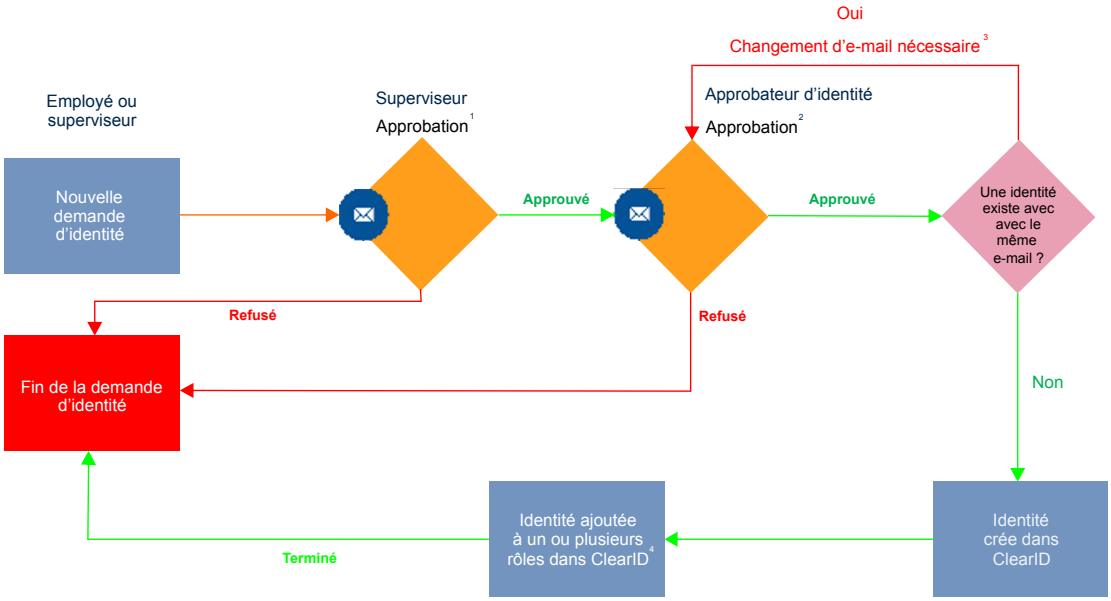
[1] Les utilisateurs affectés en tant que délégué pour un autre utilisateur n'héritent pas de l'autorisation.

À propos du processus de demande d'identité

Un processus de demande d'identité est une série d'activités effectuées par le système ou par des personnes habilitées au cours du cycle de vie d'une demande d'identité. Ces activités peuvent créer une identité individuelle ou plusieurs identités en important un fichier CSV, et ajouter chaque nouvelle identité à un rôle afin d'hériter des accès pertinents sur une période donnée.

Ce processus permet d'automatiser les tâches de demande d'identité, comme approuver ou refuser les demandes, afin que les personnes impliquées dans le processus d'examen et d'approbation puissent se consacrer à d'autres tâches.

Le diagramme suivant illustre le *processus de demande d'identité* exécuté dans Genetec ClearID[MC] et Synergis[MC].



[1] (Facultatif) L'approbation par un superviseur peut être activée ou désactivée pour chaque modèle d'identité.

[2] (Facultatif) L'approbation par un approbateur d'identité peut être activée ou désactivée pour chaque modèle d'identité.

[3] (Facultatif) L'adresse e-mail doit être unique au sein du système.

[4] (Si applicable) Le titulaire de cartes est ajouté au groupe de titulaires de cartes correspondant dans Security Center.

Rubriques connexes

À propos des processus, page 12

Note sur la fonction de demande d'identité (2 pages)

Créer un modèle d'identité

Avant d’envoyer une demande d’identité, vous devez créer vos modèles d'identité.

Avant de commencer

- Familiarisez-vous avec les processus.
- Créez les rôles qui seront autorisés à demander des identités.
- (Facultatif) Créez les rôles dotés des accès qui seront utilisés par vos modèles d'identité.
- (Facultatif) Si vous souhaitez utiliser les approbations par des superviseurs, ajoutez un superviseur à chaque identité pouvant faire l’objet d'une demande.

À savoir

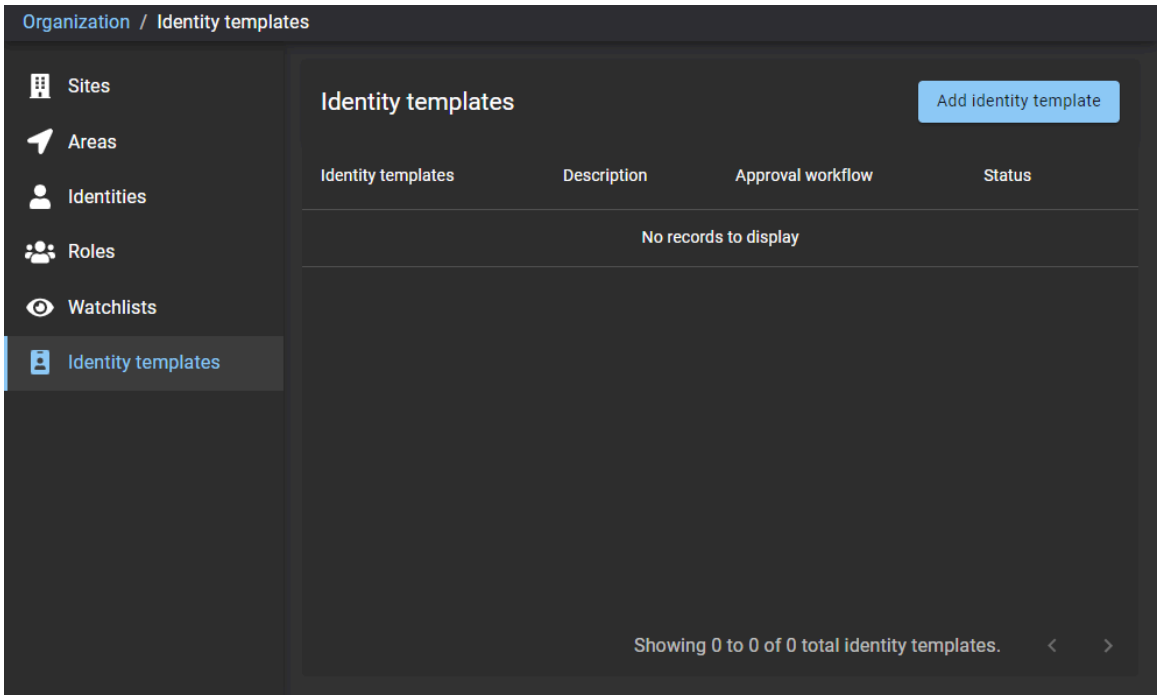
Seul un administrateur de compte peut créer un modèle d'identité.

Créez des modèles d'identité pour gérer les demandes d’identité les plus fréquentes dans votre organisation.

- Vous pouvez créer des modèles d'identité avec des accès de rôles prédéfinis pour répondre à différentes exigences. Par exemple, des demandes d’identité pour différents types de fournisseurs, ou pour des groupes d’employés particuliers qui doivent pouvoir accéder à un site ou un bâtiment particulier.
- Lorsqu'une demande d’identité est envoyée à l'aide d'un modèle d'identité, l’identité est ajoutée en tant que membre aux rôles associés au modèle, et elle hérite des accès associés aux rôles.

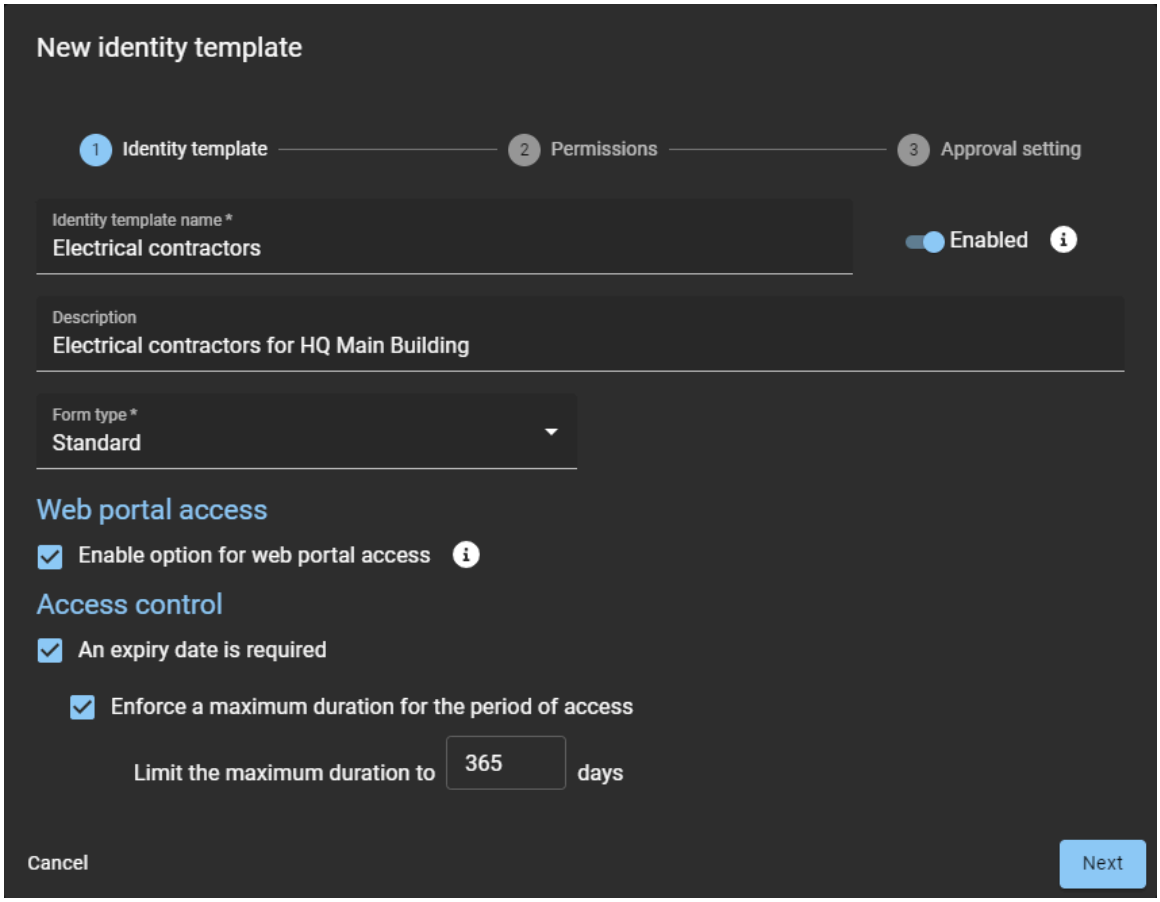
Procédure

1 Cliquez sur **Organisation** > **Modèles d'identité**.



2 Cliquez sur **Ajouter un modèle d’identité**.

3 Dans la section *Modèle d'identité*, renseignez les champs ou configurez les options nécessaires :



- **Nom du modèle d'identité :** Entrez un nom qui décrit le type de demande d'identité que le modèle doit traiter. Par exemple, Prestataires électriciens.
- **Description :** Entrez une description claire de l'objectif du modèle. Par exemple, Prestataires électriciens pour le bâtiment principal du siège.
- **Type de formulaire :** Standard est la valeur par défaut.
- **Activé :** Réglez le curseur en position **Activé** pour que ce modèle soit disponible lors d'une demande d'identité. Activé est la valeur par défaut.

a) Dans la section *Accès au portail web*, configurez les options nécessaires :

- **Activer l'option d'accès au portail web :** Cochez la case si vous souhaitez afficher l'option d'accès au portail web lors de la demande d'identité.

  REMARQUE : En cas de demande d'identités multiples, la disponibilité de l'option d'accès au portail web dépend de la configuration de votre modèle.

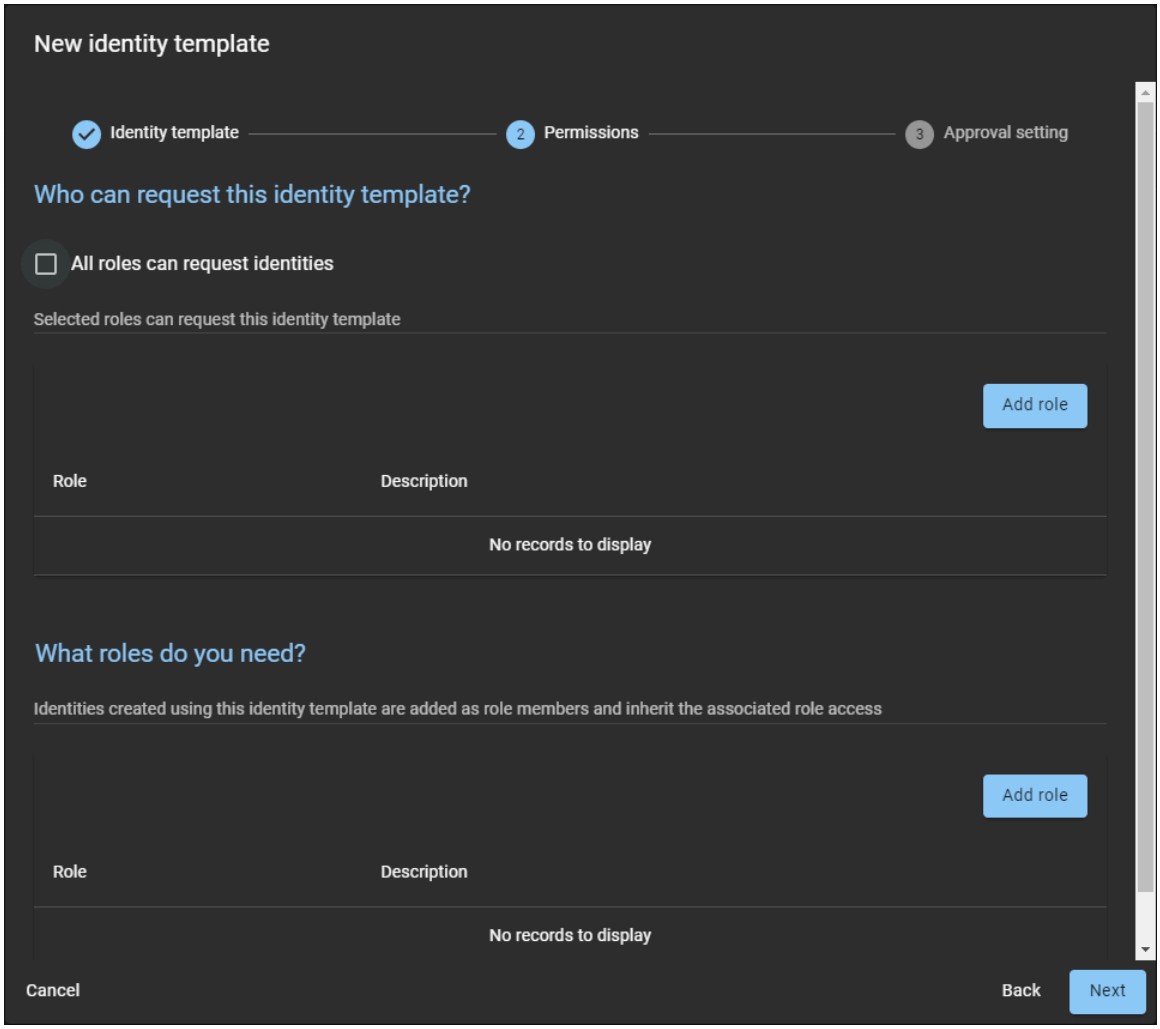
  - Si votre modèle ne contient pas l'option d'accès au portail web, les champs associés sont ignorés.
  - Si votre modèle contient l'option d'accès au portail web, les champs associés sont traités.

b) Dans la section *Contrôle d'accès*, configurez les options nécessaires :

- **Une date d'expiration est requise :** Cochez la case si vous souhaitez appliquer une date d'expiration lorsque vous créez des demandes d'identité.
  - **Appliquer une durée maximale à la période d'accès :** Cochez la case si vous souhaitez appliquer une durée maximale lorsque vous créez des demandes d'identité.
    - **Limiter la durée à *nnn* jours :** Spécifiez la durée maximale. Par exemple, 365 jours.

c) Cliquez sur **Suivant**.

4 Dans la section **Autorisations**, configurez les options ou ajoutez les rôles nécessaires :



a) Dans la section **Qui peut demander ce modèle d'identité ?**, procédez de l'une des manières suivantes :

- Si vous souhaitez que tous les utilisateurs puissent sélectionner ce modèle d'identité, cochez la case **Tous les utilisateurs peuvent demander une identité** .
- Si vous souhaitez sélectionner des rôles particuliers, cliquez sur **Ajouter un rôle**.

REMARQUE : Si vous avez sélectionné **Tous les utilisateurs peuvent demander une identité** , passez à l'étape 6.

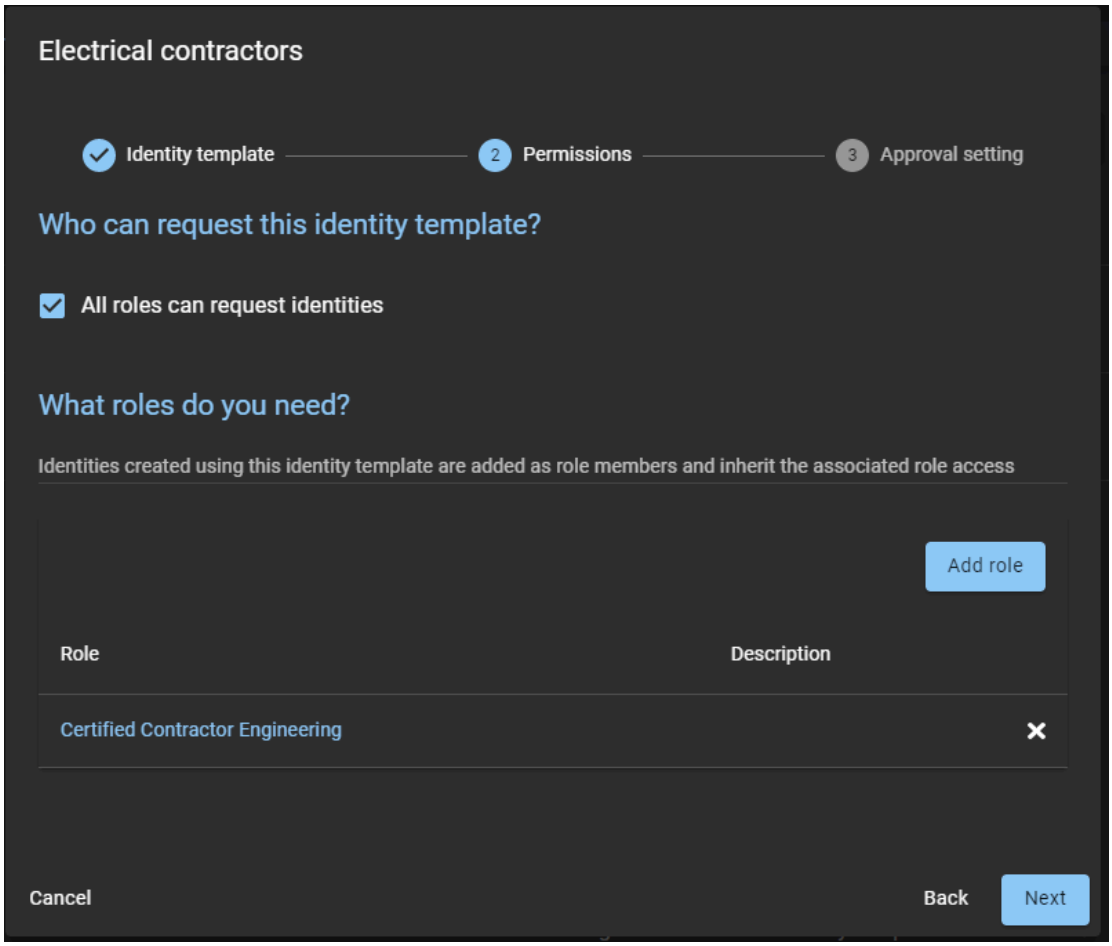
5 Si vous avez cliqué sur **Ajouter un rôle**, recherchez ou sélectionnez un ou plusieurs rôles, puis cliquez sur **Ajouter**.

REMARQUE : Les rôles que vous ajoutez dans la section **Qui peut demander ce modèle d'identité ?** déterminent qui peut demander des identités à l'aide de ce modèle. Par exemple, vous pouvez ajouter un rôle afin que seuls les *Responsables de fournisseurs* puissent demander des identités. Ou si par exemple vous avez des bâtiments et des locataires, vous pourriez créer des *Responsables de locataires*.

6 (Facultatif) Dans la section **Rôles nécessaires**, ajoutez les rôles selon vos besoins.

a) Cliquez sur **Ajouter un rôle**.

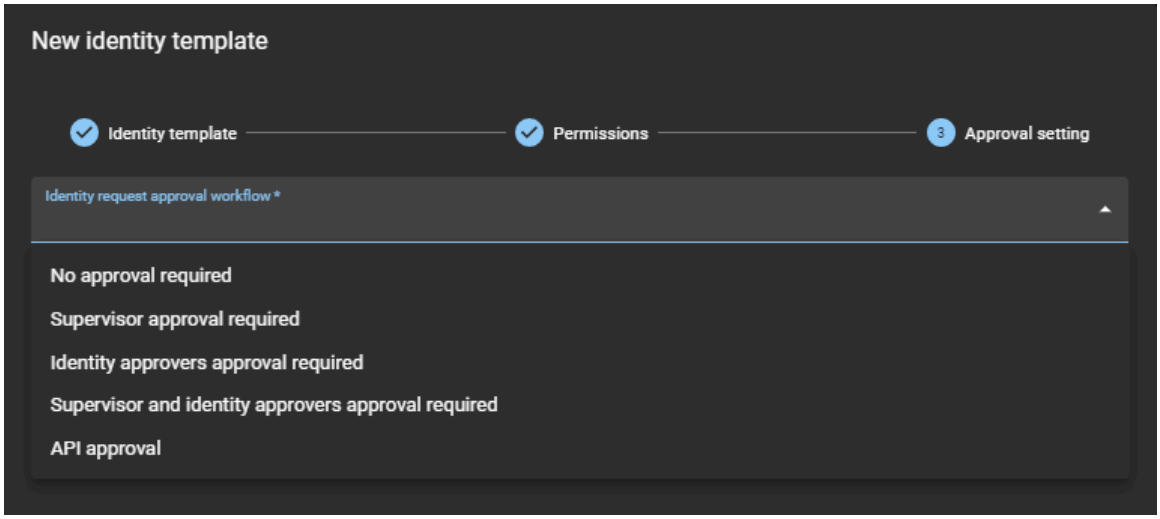
b) Recherchez ou sélectionnez un ou plusieurs rôles, puis cliquez sur **Ajouter**.



REMARQUE : Les rôles que vous ajoutez dans la section **Rôles nécessaires** déterminent les accès hérités par les identités lorsqu'une identité est demandée à l'aide de ce modèle. Par exemple, vous pouvez créer un rôle pour les électriciens, qui leur accorde un accès aux infrastructures électriques.

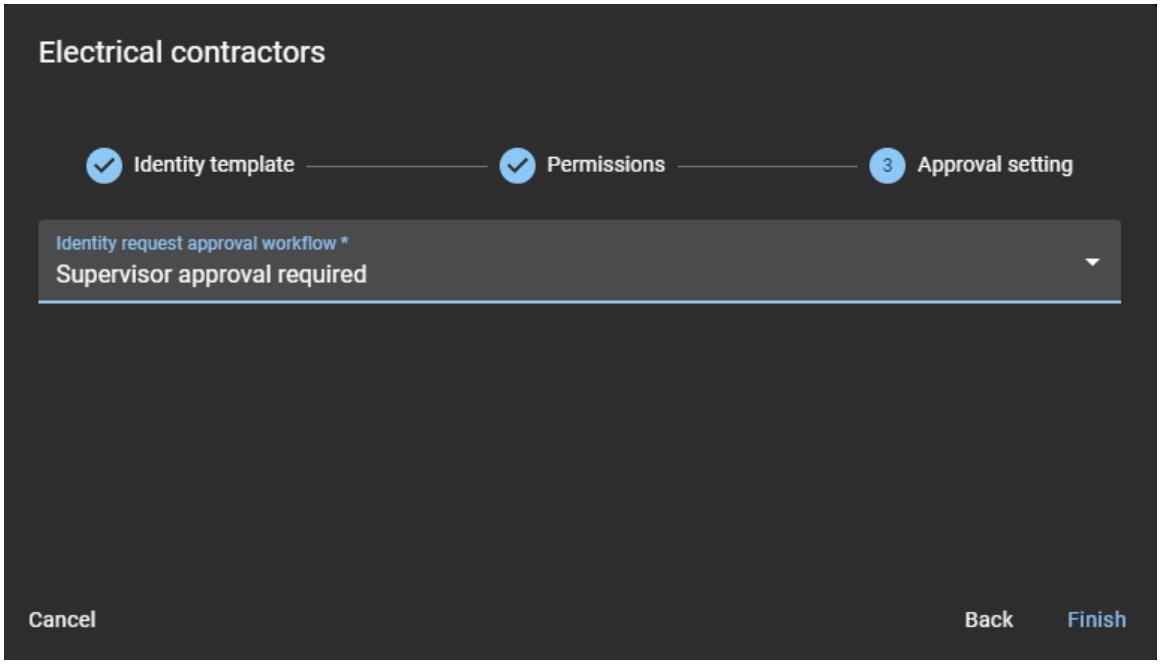
c) Cliquez sur **Suivant**.

7 Dans la section **Réglages d'approbation**, sélectionnez le **Processus d'approbation de demande d'identité** nécessaire.



- **Aucune approbation nécessaire :** Approuvée automatiquement.
- **Approbation par un superviseur nécessaire :** Approuvé par le superviseur du demandeur.
  REMARQUE : Si le demandeur n'a pas de superviseur (ou est un demandeur de confiance), l'étape d'approbation par le superviseur est ignorée.
- **Approbation par un approbateur d'identité requise :** Lorsque cette option est sélectionnée, des approbateurs d'identité doivent être ajoutés.
  a. Cliquez sur **Ajouter** et sélectionnez **Ajouter des identités** ou **Ajouter des rôles**.
  b. Suivez les instructions pour effectuer les étapes.
- **Approbation par un superviseur et un approbateur d'identité requise :** Lorsque cette option est sélectionnée, les superviseurs sont déjà associés à l'identité, mais les approbateurs d'identité doivent être ajoutés, comme indiqué plus haut.
  REMARQUE : Si le demandeur n'a pas de superviseur (ou est un demandeur de confiance), l'étape d'approbation par le superviseur est ignorée.
- **Approbation d'API :** L'approbation d'API n'est utilisée que lorsque le processus d'approbation de demande d'identité est personnalisé pour traiter les demandes émanant d'un service externe.
  Par exemple, Genetec ClearID[MC] LDAP Synchronization Agent, Genetec ClearID[MC] One Identity Synchronization Tool ou un processus d'API pour l'intégration d'un module externe. Dans ce cas, les approbations de demandes ne sont pas affichées dans l'interface utilisateur de ClearID.

REMARQUE : Si un utilisateur crée une demande d'identité à l'aide du portail Web ClearID, cet utilisateur verra toujours ses demandes dans le tableau de bord **Mes demandes**.



8 Cliquez sur **Terminer**.

Votre modèle est opérationnel.

Lorsque vous avez terminé

Demandez une identité.

Rubriques connexes

Note sur la fonction de demande d'identité (2 pages)

Modifier un modèle d'identité

Lorsque vous avez créé un modèle d'identité, vous pouvez modifier ses réglages ou le supprimer si nécessaire.

Avant de commencer

Créez vos modèles d'identité.

À savoir

Seul un administrateur de compte peut modifier un modèle d'identité.

Procédure

1 Cliquez sur **Organisation** > **Modèles d'identité**.

2 (Facultatif) Si vous n’avez plus besoin d'un modèle, cliquez sur **Supprimer** (✖) pour supprimer le modèle.
3 Cliquez sur un modèle dans la liste.
4 Dans la section *Modèle d'identité*, apportez les modifications nécessaires, puis cliquez sur **Suivant**.
5 Dans la section *Autorisations*, apportez les modifications nécessaires, puis cliquez sur **Suivant**.
6 Dans la section *Approbations*, apportez les modifications nécessaires, puis cliquez sur **Terminer**.

Demander des identités

Vous pouvez utiliser le portail Genetec ClearID[MC] en libre-service pour demander une identité individuelle ou pour demander plusieurs identités à la fois en passant par l'importation d'un fichier CSV. L'utilisation du portail en libre-service avec le workflow d'approbateur optionnel simplifie le processus d'approbation en ne notifiant que les approbateurs spécifiés.

Avant de commencer

- Familiarisez-vous avec les processus.

À savoir

Toute personne dotée des autorisations nécessaires peut envoyer une demande d'identité.

REMARQUE : Auparavant, la plupart des solutions de contrôle d'accès ne suivaient pas et ne consignaient pas les motifs de demande d'identité.

Dans ClearID, la demande d'identité inclut : qui demande l'identité, quand, et pour quelle raison.

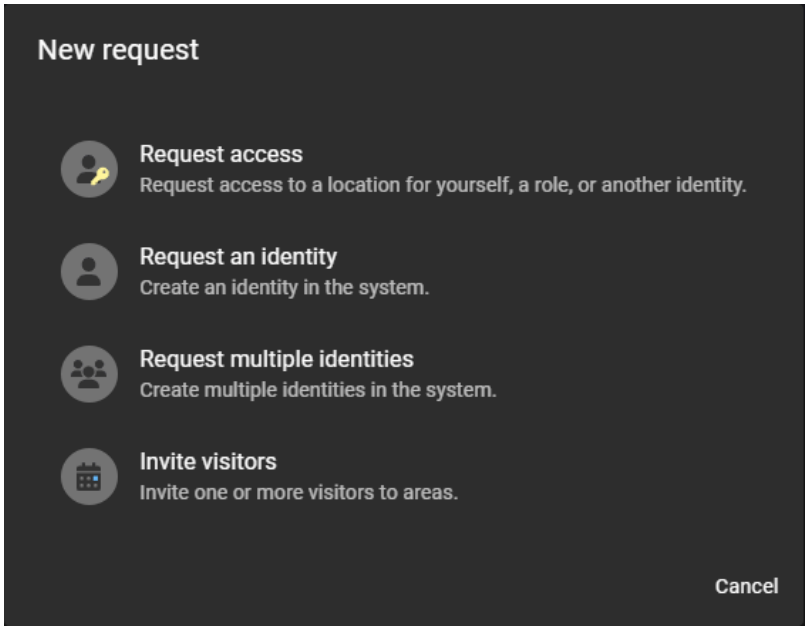
- Des demandes d'identité et des processus d'approbation distincts sont créés pour chaque demande d'identité.
- Une fois le récapitulatif de la demande validé, la demande est automatiquement affectée aux personnes pertinentes pour approbation.
- Une fois le processus d'approbation terminé, le demandeur reçoit un e-mail lui indiquant si la demande d'identité a été approuvée ou rejetée.

Procédure

1 Connectez-vous au portail en libre-service.

2 Cliquez sur **Tableau de bord**.

3 Cliquez sur **Nouvelle demande**.



4 Dans l'onglet *Nouvelle demande*, procédez de l'une des manières suivantes :
   - Demander une identité, page 219
   - Demander des identités multiples à l'aide de l'importation CSV, page 223

5 Cliquez sur **Terminer**.

Lorsque vous avez terminé

En fonction du modèle d'identité que vous avez sélectionné, vos demandes d'identité sont soit approuvées automatiquement, soit examinées par des approbateurs, qui les approuvent (ou les refusent).

Rubriques connexes

Note sur la fonction de demande d'identité (2 pages)
Vérifier l'état des demandes d'identité, page 242

Demander une identité

Vous pouvez utiliser le portail Genetec ClearID[MC] en libre-service pour demander une identité. La demande ajoute une personne (en tant qu'identité) qui n'existe pas encore au sein du système. L'utilisation du portail en libre-service avec le processus d'approbateur facultatif simplifie le processus d'approbation en ne notifiant que les approbateurs spécifiés.

Avant de commencer

- Familiarisez-vous avec les processus.

À savoir

Toute personne dotée des autorisations nécessaires peut envoyer une demande d'identité.

Cette rubrique décrit l'utilisation de l'assistant de demande d'identité sur le portail web. Le demandeur peut utiliser l'assistant pour ajouter quelqu'un (en tant qu'identité) qui n'existe pas encore au sein du système.

REMARQUE : Auparavant, la plupart des solutions de contrôle d'accès aux sites ne suivaient pas et ne consignaient pas les motifs de demande d'identité.

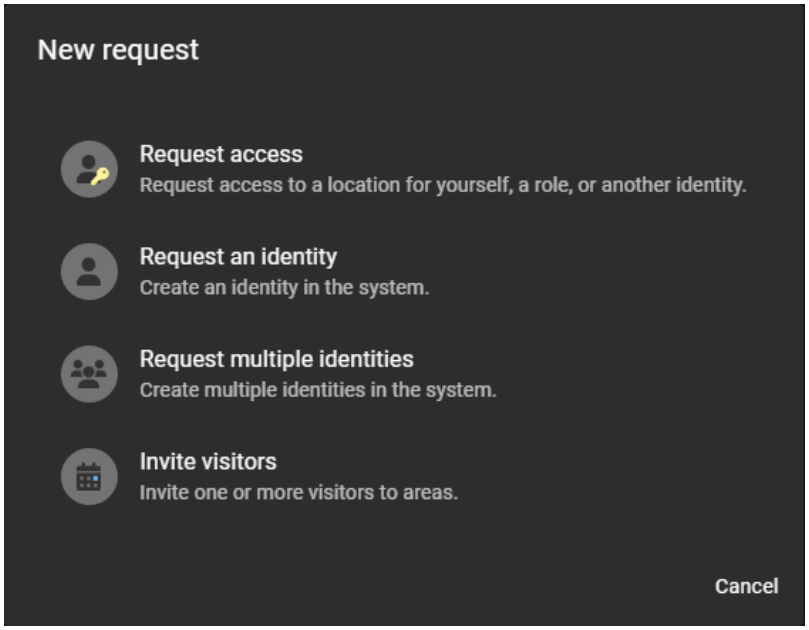
Dans ClearID, la demande d'identité inclut : qui demande l'identité, quand, et pour quelle raison.

- Des demandes d'identité et des processus d'approbation distincts sont créés pour chaque demande d'identité.
- Une fois le récapitulatif de la demande validé, la demande est automatiquement affectée aux personnes pertinentes pour approbation.
- Une fois le processus d'approbation terminé, le demandeur reçoit un e-mail lui indiquant si la demande d'identité a été approuvée ou rejetée.

Procédure

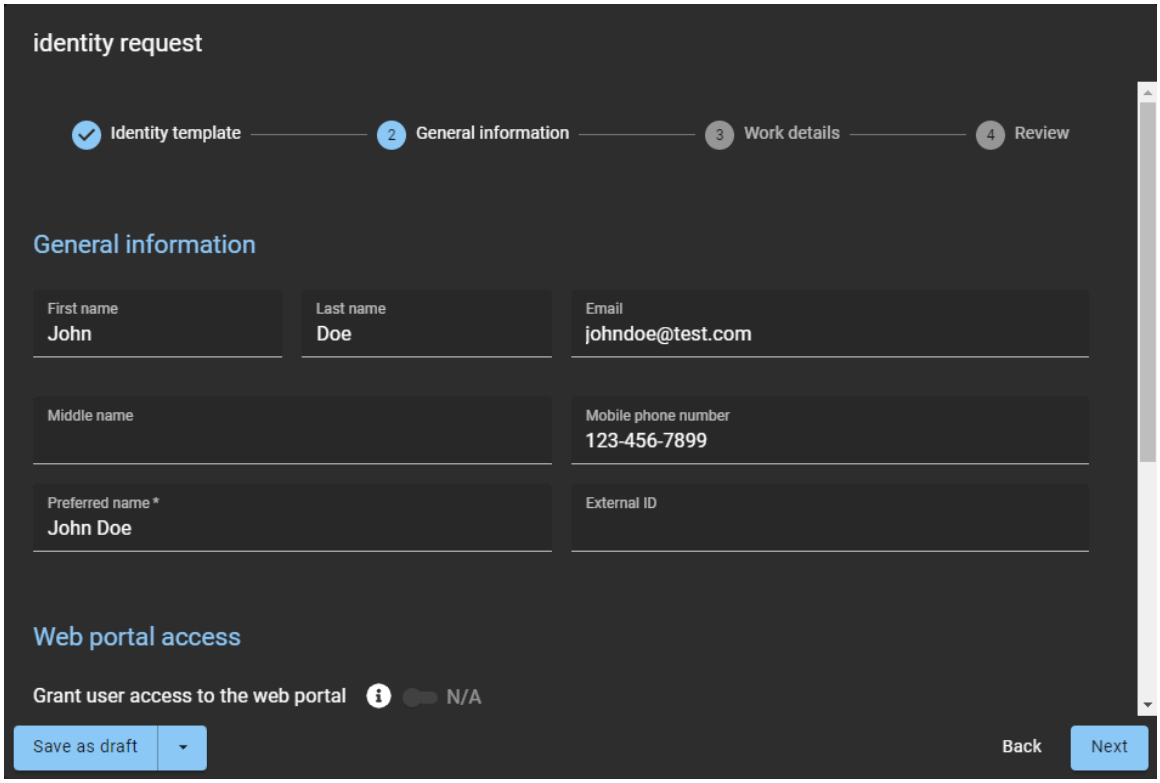
1 Connectez-vous au portail en libre-service.
2 Cliquez sur **Tableau de bord**.
3 Cliquez sur **Nouvelle demande**.

4 Dans la boîte de dialogue **Nouvelle demande**, cliquez sur **Demander une identité**.



5 Dans l'assistant *Nouvelle demande d'identité*, sélectionnez un **Modèle d'identité** dans la liste, et cliquez sur **Suivant**.

6 Renseignez les champs dans la section *Informations générales*.



CONSEIL : Pendant la création de la demande, vous pouvez à tout moment cliquer sur **Enregistrer un brouillon** pour enregistrer une demande incomplète (en attendant des informations manquantes). Vous pouvez aussi cliquer sur **Supprimer** si la demande n'est plus d'actualité. Vos brouillons sont disponibles dans l'onglet **Mes demandes** du Tableau de bord.

7 (Facultatif) Dans la section *Accès au portail Web*, **Activez** l'option **Accorder l'accès au portail Web** si vous souhaitez que l'identité demandée puisse se connecter au portail Web ClearID et l'utiliser.

REMARQUE : L'option **Accorder l'accès au portail web** est désactivée si le modèle d'identité que vous utilisez n'intègre pas l'accès au portail web.

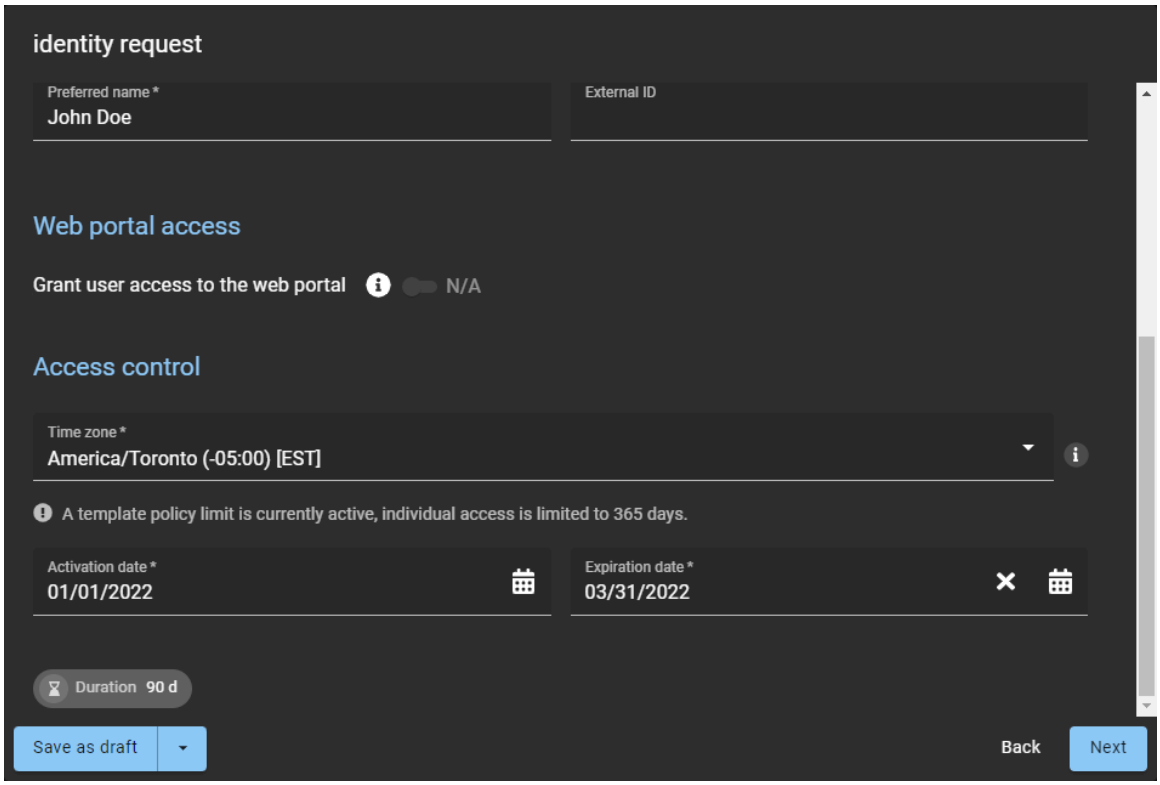
a) Si vous activez l'accès au portail web, entrez un nom d'utilisateur.

REMARQUE : Le nom d'utilisateur doit être une adresse e-mail valable.

8 Renseignez les champs dans la section *Contrôle d'accès*. Les champs obligatoires sont indiqués par un astérisque (*).

- **Fuseau horaire :** Sélectionnez le fuseau horaire pertinent.
- **Date d'activation :** Sélectionnez la date à laquelle l'identité demandée doit être activée.
- **Date d'expiration :** Sélectionnez la date à laquelle l'identité demandée doit être désactivée.

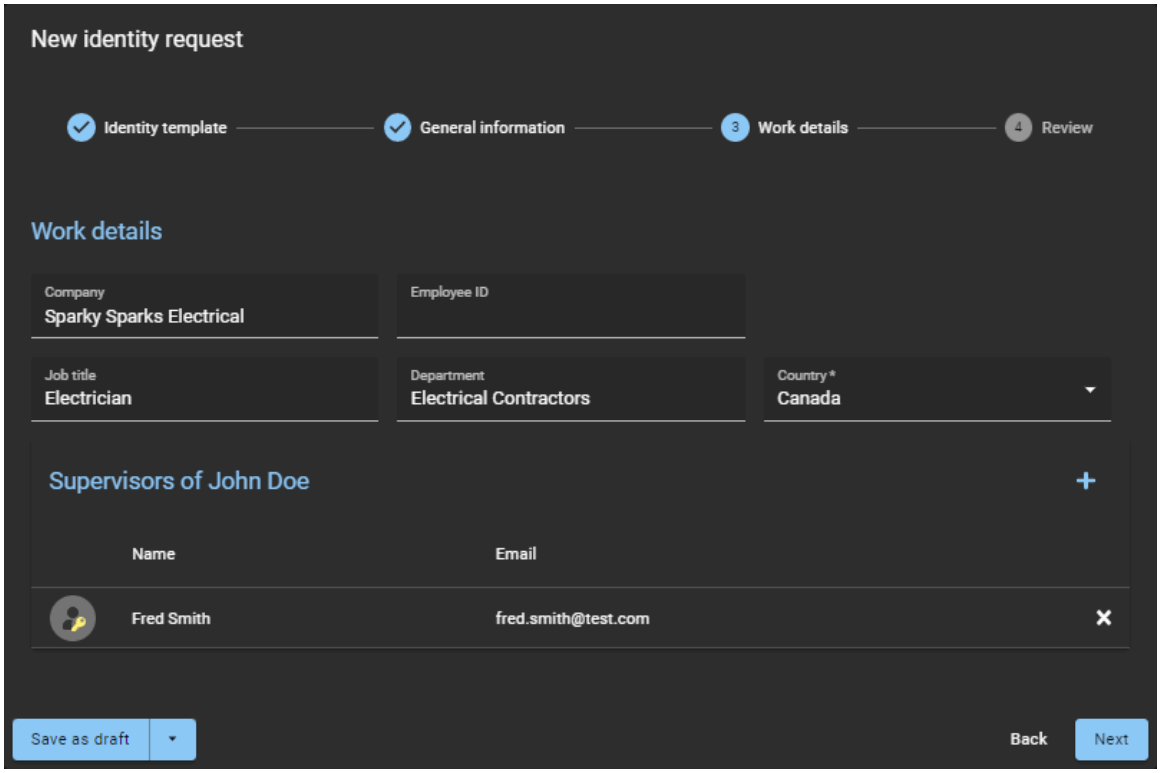
  REMARQUE : Selon le modèle d'identité sélectionné, une date d'expiration ne sera pas forcément obligatoire.



REMARQUE : Les heures d'activation et d'expiration de l'identité dépendent et sont déclenchées par les horaires de la période d'accès spécifiée dans la demande d'identité et par l'heure dans le fuseau horaire sélectionné. Si une *durée maximale* d'accès a été spécifiée et activée dans le modèle d'identité, un message indique la durée d'accès maximale que vous pouvez spécifier.

a) Cliquez sur **Suivant**.

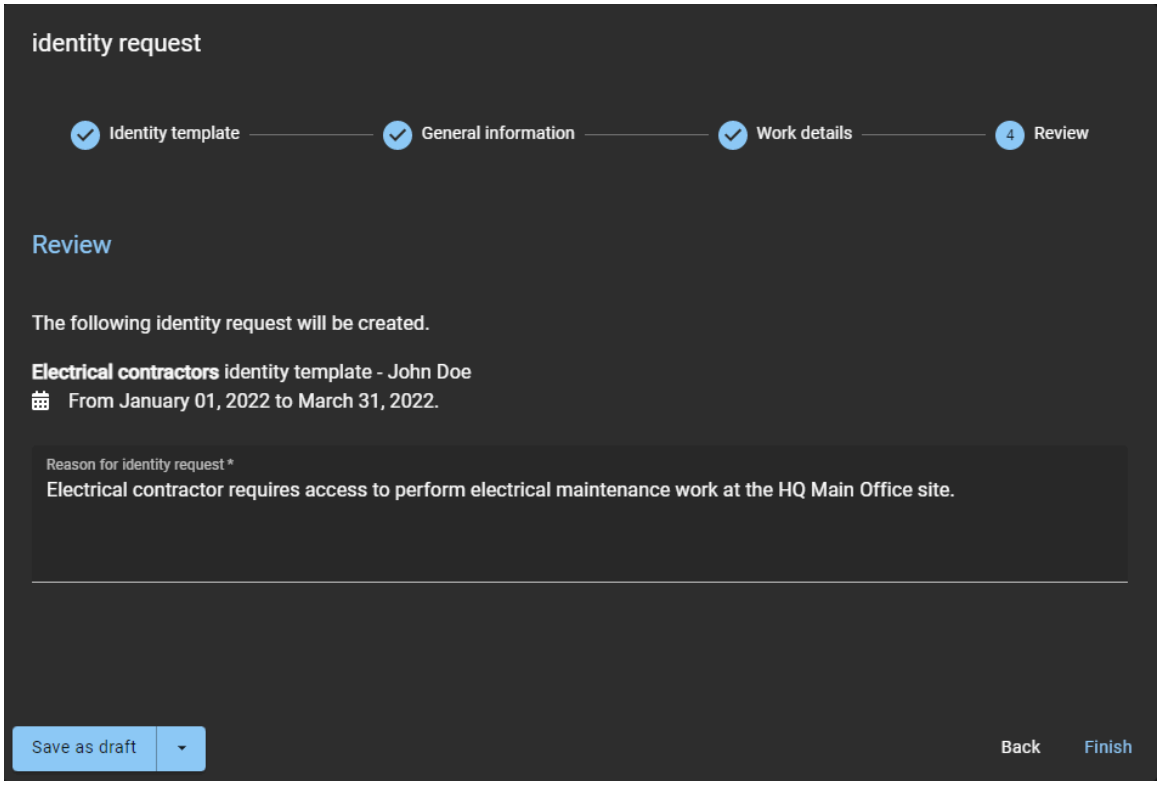
9 Renseignez les champs dans la section *Détails professionnels*.



- **Société :** Saisissez le nom de l'entreprise.
- **ID d'employé :** Entrez l'ID de l'employé.
- **Intitulé du poste :** Entrez un intitulé de poste.
- **Département :** Entez un département.
- **Pays :** Sélectionnez un pays dans la liste. Le pays n'est utilisé que par le formulaire *Standard*.
  CONSEIL : Entrez la première lettre du pays pour faire défiler la liste des pays.

a) Dans la section *Superviseurs de*, cliquez sur pour ajouter des superviseurs.
   REMARQUE : Les superviseurs spécifiés ici sont ceux de l'identité en cours de création. Par défaut, le demandeur est ajouté automatiquement à la liste **Superviseurs de**.
b) (Facultatif) Ajoutez des superviseurs selon vos besoins.
c) (Facultatif) Cliquez sur pour supprimer les superviseurs qui ne sont plus nécessaires. Par exemple, si vous avez demandé des identités pour quelqu'un d'autre, vous pouvez vous supprimer de la liste une fois que les superviseurs nécessaires ont été ajoutés.
d) Cliquez sur **Suivant**.

10 Dans la section *Examen*, vérifiez que les informations de la demande d'identité sont exactes.



11 Si les informations sont exactes, ajoutez un motif à la demande, et cliquez sur **Terminer**.
Une notification est envoyée par e-mail aux approbateurs (le cas échéant).

Lorsque vous avez terminé

En fonction du modèle d'identité que vous avez sélectionné, vos demandes d'identité sont soit approuvées automatiquement, soit examinées par des approbateurs, qui les approuvent (ou les refusent).

Rubriques connexes

Note sur la fonction de demande d'identité (2 pages)

Demander des identités multiples à l'aide de l'importation CSV

Vous pouvez utiliser le portail Genetec ClearID[MC] en libre-service pour demander plusieurs identités à la fois. La demande ajoute plusieurs personnes (en tant qu'identités) qui n'existent pas encore au sein du système. L'utilisation du portail en libre-service avec le processus d'approbateur facultatif simplifie le processus d'approbation en ne notifiant que les approbateurs spécifiés.

Avant de commencer

- Familiarisez-vous avec les processus.

À savoir

Toute personne dotée des autorisations nécessaires peut envoyer une demande d'identité.

Cette rubrique décrit l'utilisation de l'assistant de demande d'identité sur le portail web pour demander plusieurs identités à la fois via l'importation d'un fichier CSV. Le demandeur peut utiliser l'assistant pour ajouter des gens (en tant qu'identités) qui n'existent pas encore au sein du système.

REMARQUE : Auparavant, la plupart des solutions de contrôle d'accès ne suivaient pas et ne consignaient pas les motifs de demande d'identité.

Dans ClearID, la demande d'identité inclut : qui demande l'identité, quand, et pour quelle raison.

- Des demandes d'identité et des processus d'approbation distincts sont créés pour chaque demande d'identité.
- Une fois le récapitulatif de la demande validé, la demande est automatiquement affectée aux personnes pertinentes pour approbation.
- Une fois le processus d'approbation terminé, le demandeur reçoit un e-mail lui indiquant si la demande d'identité a été approuvée ou rejetée.

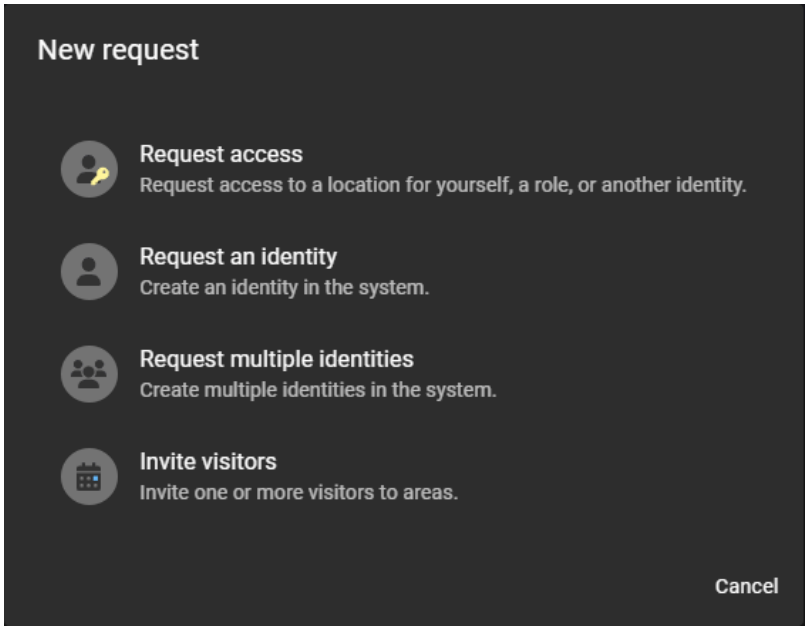
Procédure

1 Connectez-vous au portail en libre-service.

2 Cliquez sur **Tableau de bord**.

3 Cliquez sur **Nouvelle demande**.

4 Dans la boîte de dialogue **Nouvelle demande**, cliquez sur **Demander des identités multiples**.



5 Renseignez les champs dans la section **Informations de base** de l'assistant *Demander des identités multiples*.

a) Dans le champ **Nom** de la section *Nom de la demande*, donnez un nom descriptif à votre demande.

Avec un nom descriptif, la demande sera facilement identifiable dans les tableaux de bord **Mes demandes** et **Mes tâches**.

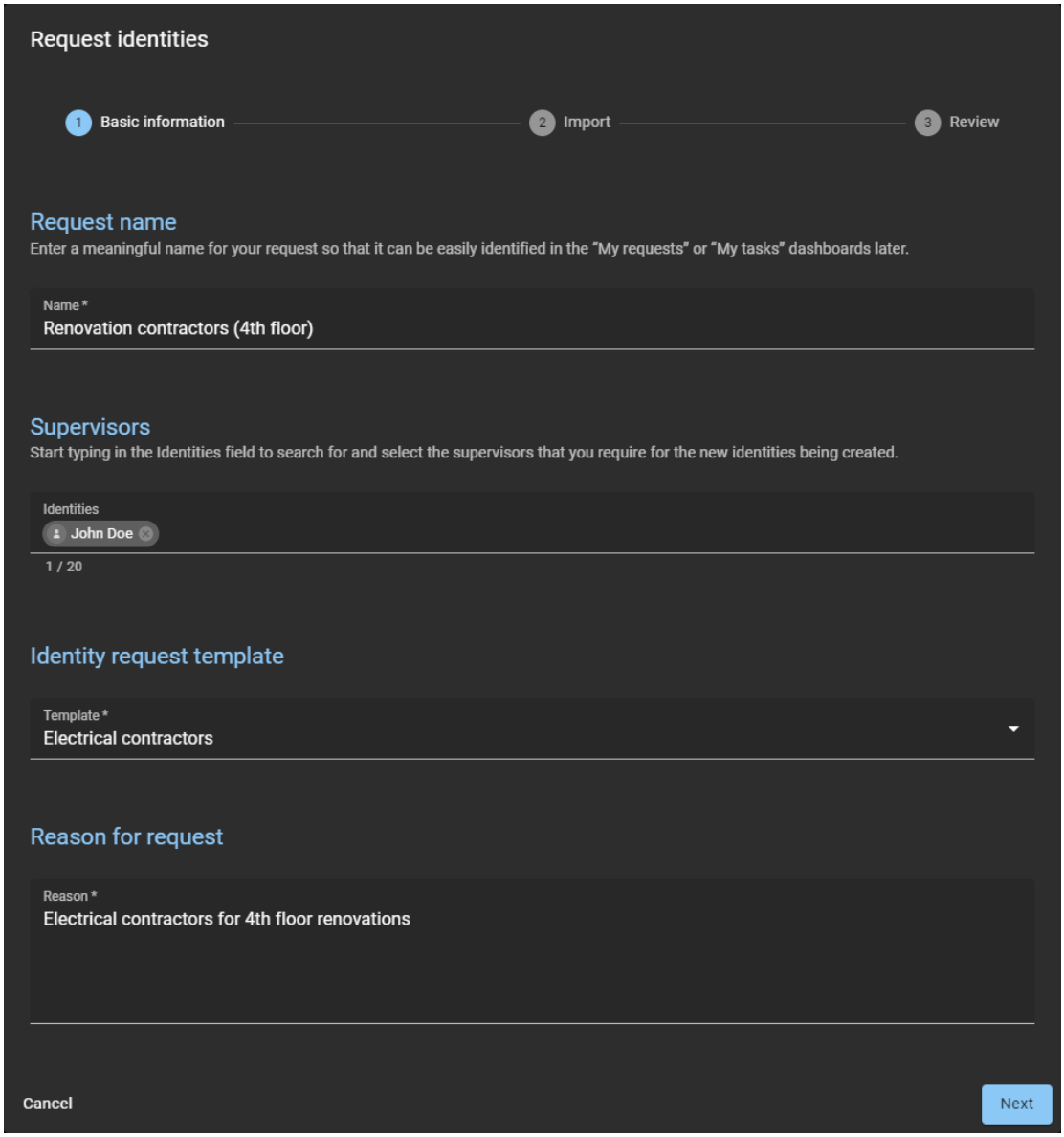
b) Dans la section **Superviseurs**, recherchez et sélectionnez une ou plusieurs identités pour les désigner en tant que superviseurs des identités importées.

Vous pouvez affecter un maximum de 20 superviseurs.

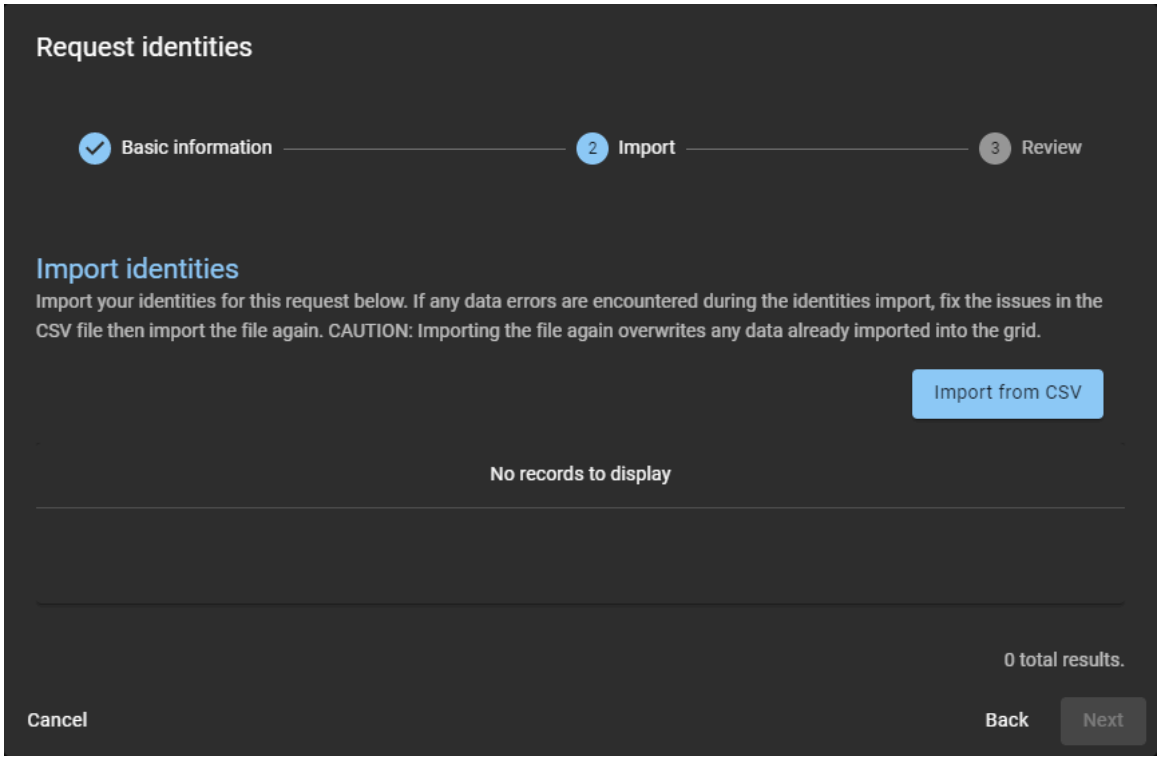
REMARQUE : Les superviseurs spécifiés ici sont ceux des identités en cours de création. Par défaut, le demandeur est ajouté automatiquement à la liste **Superviseurs**.

c) Dans la section *Modèle de demande d'identité*, sélectionnez un modèle dans la liste.

d) Dans la section *Motif de la demande*, motivez la demande, et cliquez sur **Suivant**.



6 Dans la section **Importer**, cliquez sur **Importer d'un fichier CSV**.



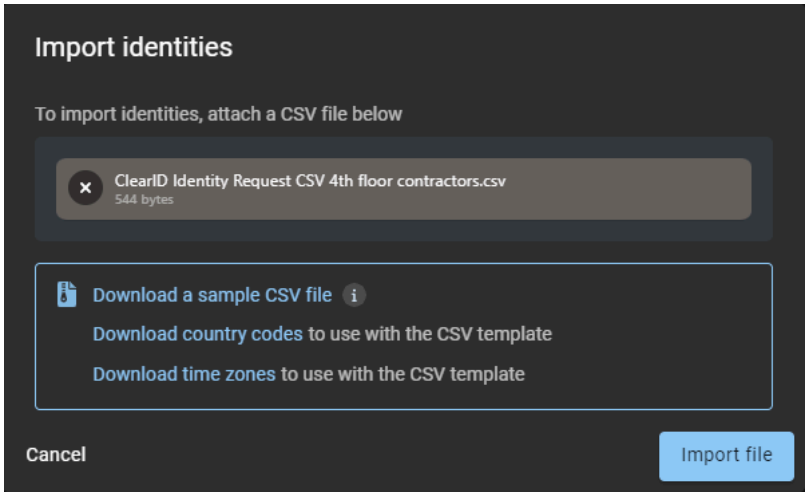
REMARQUE : Vous pouvez importer un maximum de 1000 identités par demande d'identités.

7 Choisissez l'une des options suivantes :

- Utiliser un fichier CSV existant.
- Télécharger un exemple de fichier CSV.

8 Si vous avez choisi d'utiliser un fichier CSV existant, procédez comme suit :

a) Faites un glisser-déposer du fichier CSV contenant les identités, ou cliquez sur **Parcourir** et sélectionnez le fichier.



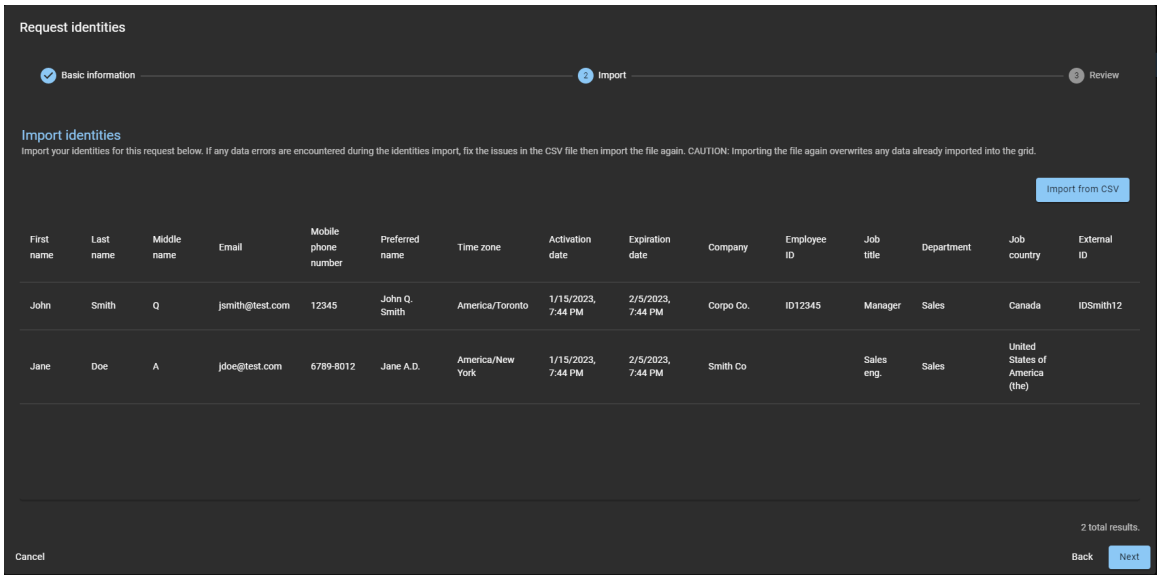
b) Cliquez sur **Importer un fichier** pour importer la liste des identités.

9 Examinez les données d'identité importées et vérifiez qu'il n'y a pas d'erreurs.

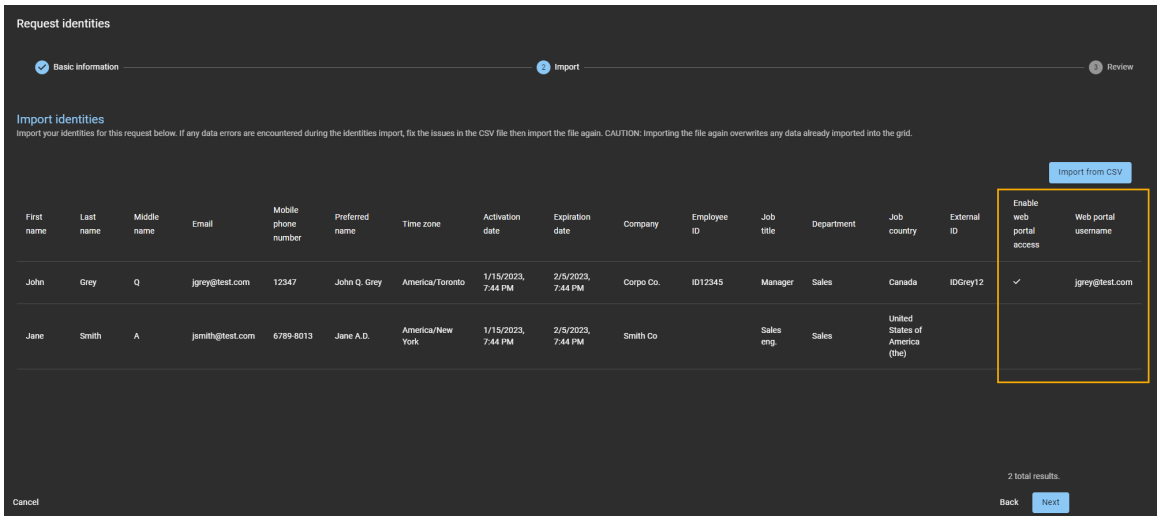
REMARQUE : En cas de demande d'identités multiples, la disponibilité de l'option d'accès au portail web dépend de la configuration de votre modèle.

- Si votre modèle ne contient pas l'option d'accès au portail web, les champs associés sont ignorés.
- Si votre modèle contient l'option d'accès au portail web, les champs associés sont traités.

L'exemple suivant montre des identités importées qui n'ont pas accès au portail Web.



L'exemple suivant montre des identités importées qui ont accès au portail Web.



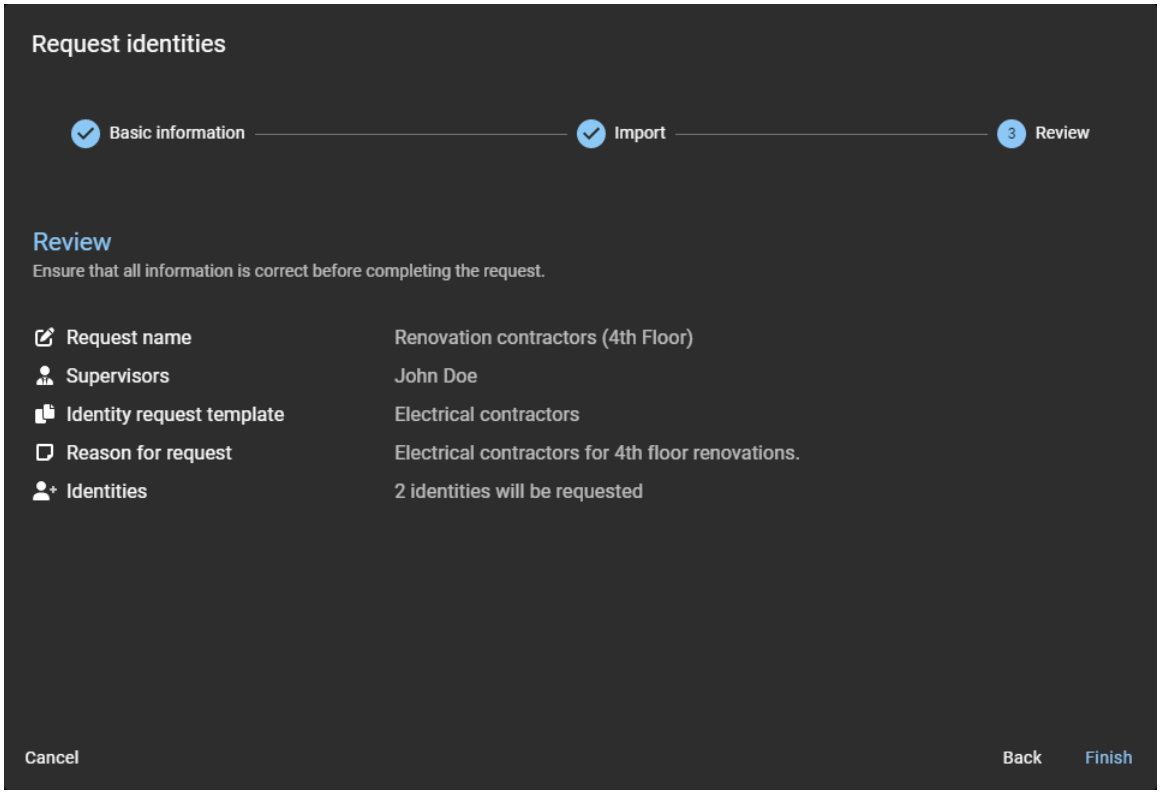
Les erreurs détectées dans le fichier CSV importé sont indiquées en rouge. Vous devez corriger les erreurs dans le fichier CSV, puis le réimporter.

ATTENTION : La correction d'erreurs remplace toutes les données déjà importées dans la grille.

a) (Facultatif) Si votre liste d'identités est longue, vous pouvez activer l'option **N'afficher que les erreurs**.

b) Cliquez sur **Suivant**.

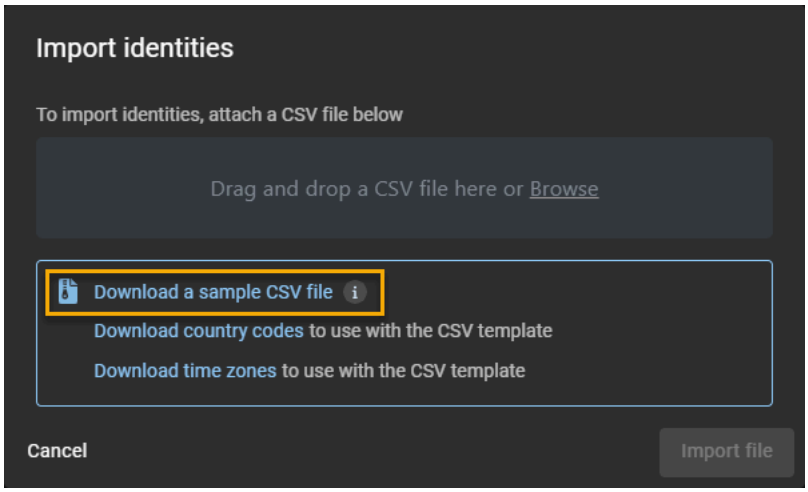
10 Dans la section **Examen**, vérifiez que les informations sont exactes.



a) Si les informations dans la section *Examen* semblent exactes, cliquez sur **Terminer**.

11 Si vous avez choisi **Télécharger un exemple de fichier CSV**, procédez comme suit :

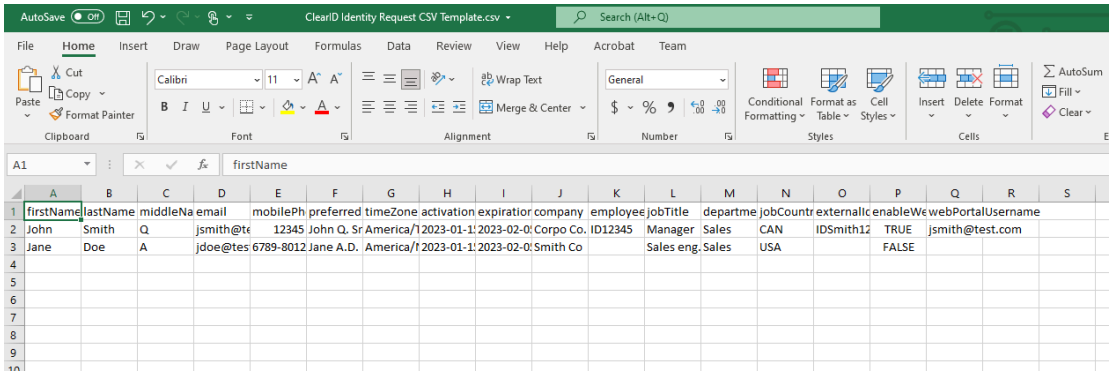
a) Cliquez sur **Télécharger un modèle de fichier CSV**.



b) Sélectionnez et ouvrez le fichier CSV téléchargé.

CONSEIL : Téléchargez les exemples de *codes de pays* et de *fuseaux horaires* si les *codes de pays* et les *fuseaux horaires* qui vous intéressent ne figurent pas dans le modèle téléchargé.

c) Pour chaque identité, saisissez une ligne complète d'informations dans le modèle de fichier CSV.

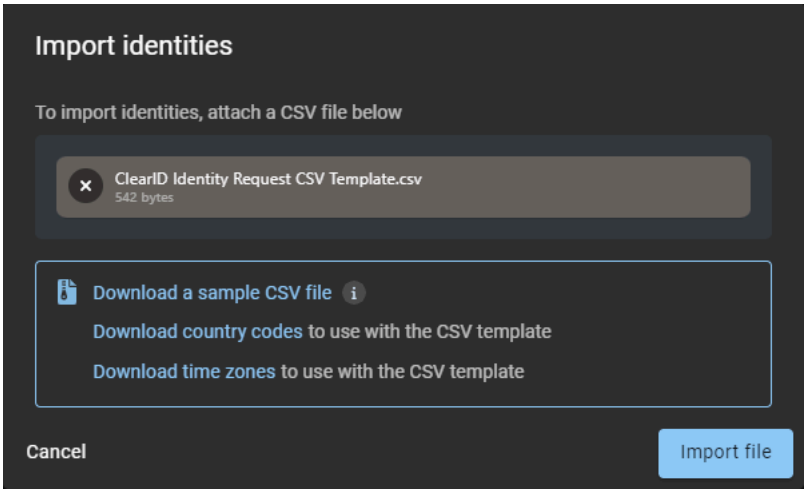


REMARQUE : Les colonnes du modèle CSV peuvent varier en fonction des paramètres de configuration de votre site.

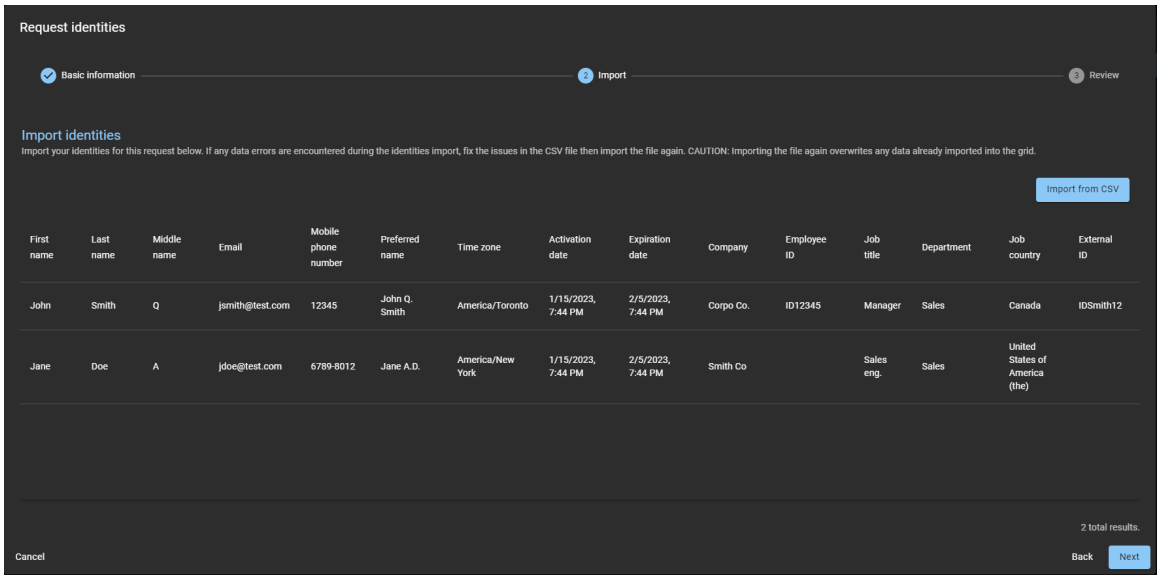
d) Enregistrez la liste d'identités sous forme de fichier CSV.

e) Revenez à la boîte de dialogue *Importer des identités*, et faites un glisser-déposer ou cliquez sur **Parcourir** pour sélectionner le fichier que vous venez de créer.

f) Cliquez sur **Importer un fichier** pour importer la liste des identités.



12 Examinez les données d'identité importées et vérifiez qu'il n'y a pas d'erreurs.



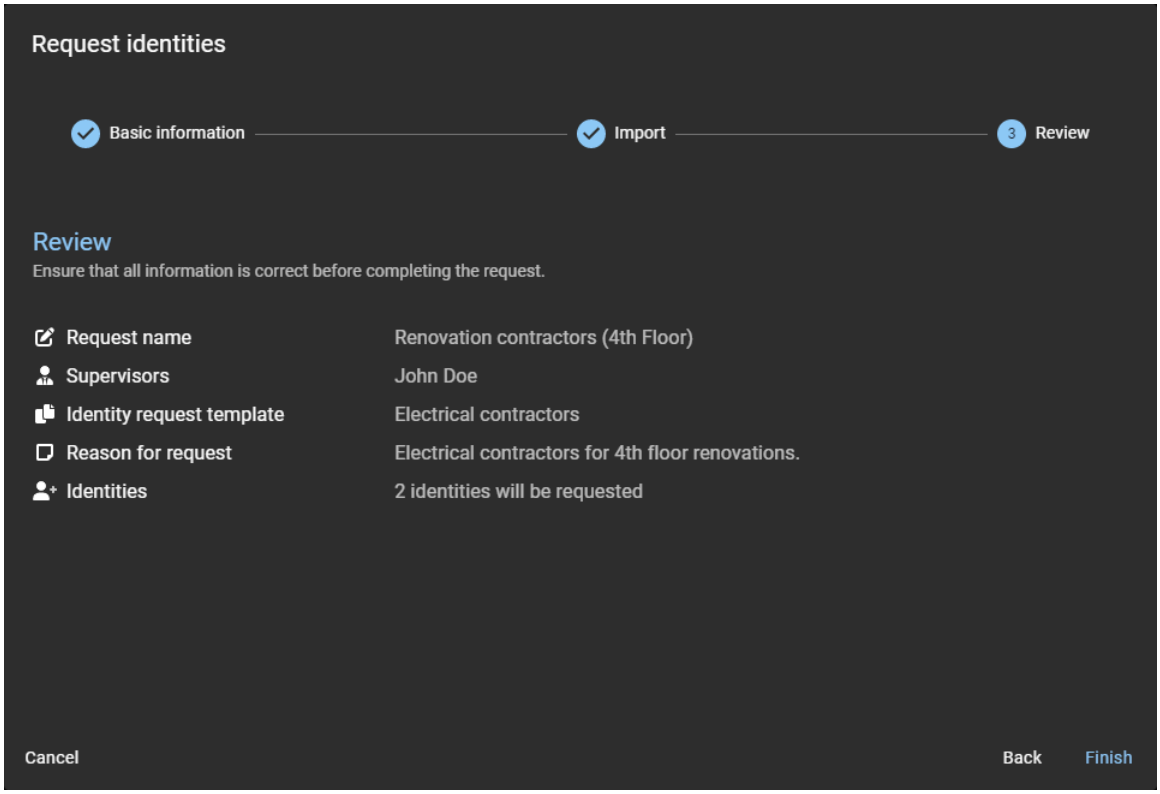
Les erreurs détectées dans le fichier CSV importé sont indiquées en rouge. Vous devez corriger les erreurs dans le fichier CSV, puis le réimporter.

ATTENTION : La correction d'erreurs remplace toutes les données déjà importées dans la grille.

a) (Facultatif) Si votre liste d'identités est longue, vous pouvez activer l'option **N'afficher que les erreurs**.

b) Cliquez sur **Suivant**.

13 Dans la section **Examen**, vérifiez que les informations sont exactes.



a) Si les informations dans la section *Examen* semblent exactes, cliquez sur **Terminer**.

Lorsque vous avez terminé

En fonction du modèle d'identité que vous avez sélectionné, vos demandes d'identité sont soit approuvées automatiquement, soit examinées par des approbateurs, qui les approuvent (ou les refusent).

Rubriques connexes

Note sur la fonction de demande d'identité (2 pages)

Annuler les demandes d'identité

Pour annuler les demandes d'identité, le demandeur d’identité doit consulter les demandes en attente, puis décider quelles demandes annuler.

Avant de commencer

Vérifiez que des demandes d’identité ont déjà été envoyées.

À savoir

Seuls les demandeurs d’identités peuvent annuler les demandes d’identité.

- Seules les demandes en attente peuvent être annulées.
- Les demandes déjà traitées ne peuvent pas être annulées.

REMARQUE : Si l’une des identités demandées est annulée, tous les approbateurs configurés sont ajoutés à la liste **.cc** dans l’e-mail de notification pour l’approbation de la demande d’identité intitulée : « La demande d’identité pour *identité* a été mise à jour ».

Procédure

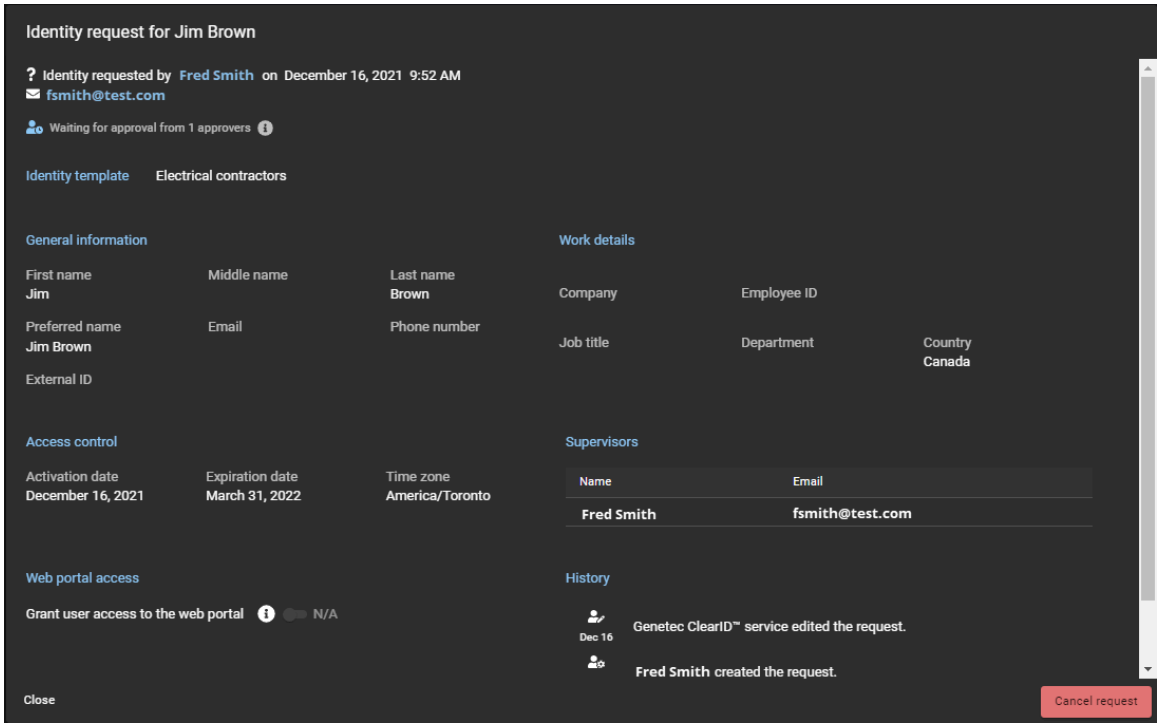
Pour annuler une demande d’identité :

1 Cliquez sur **Tableau de bord** > **Mes demandes**.

2 Dans la liste **État**, filtrez les demandes qui sont affichées :

- **État :** Sélectionnez un état parmi les suivants :
  - **Tous :** Affiche toutes les tâches en attente ou terminées.
  - **En attente :** Affiche les tâches en attente d'approbation.
  - **Terminé :** Affiche les tâches terminées et leur état. Par exemple, approuvé, terminé, refusé ou annulé.

3 Dans la liste **Mes demandes**, cliquez sur une demande d'identité pour afficher des informations complémentaires sur celle-ci.



REMARQUE : Les boutons disponibles dans les détails de la demande d'identité varient selon que vous êtes le demandeur, un superviseur ou un approbateur.

4 Vérifiez que la demande d'identité est exacte et complète.

5 Si la demande d'identité n'est plus d'actualité, cliquez sur **Annuler la demande**.

a) Indiquez le motif de l'annulation et cliquez sur **Confirmer**.

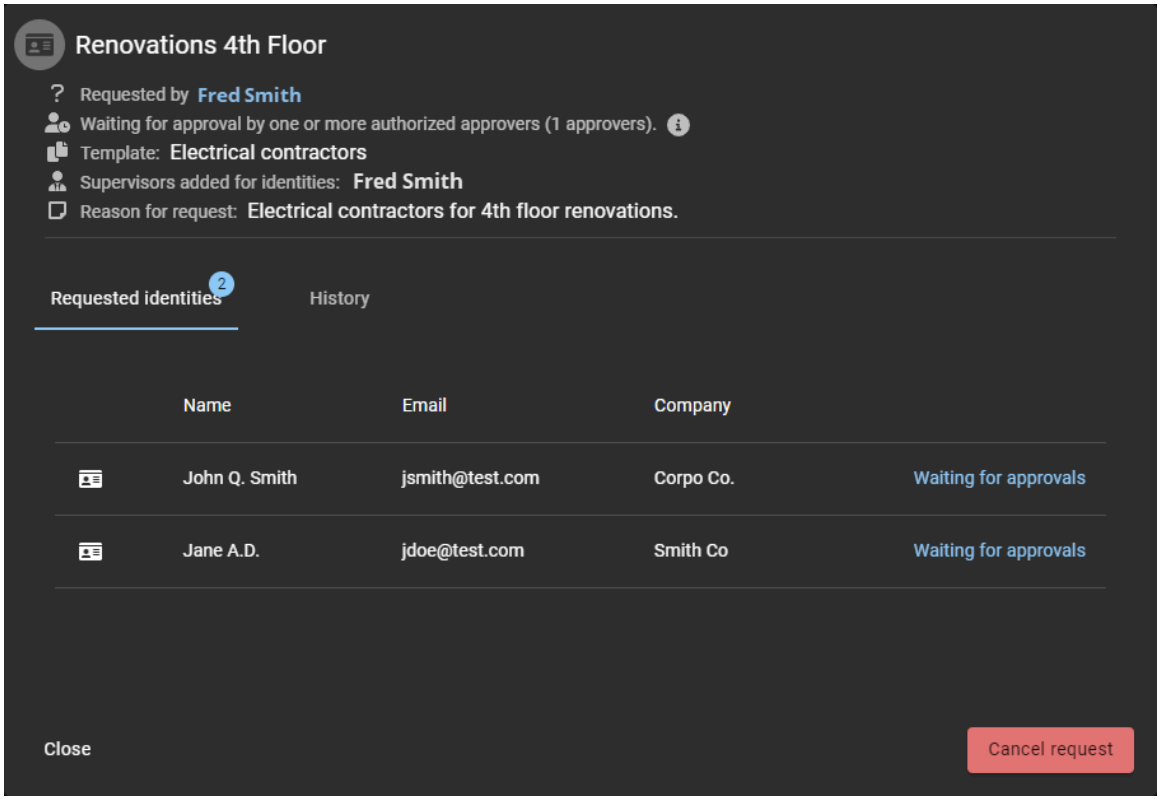
Pour annuler des identités multiples importées depuis un fichier CSV :

1 Cliquez sur **Tableau de bord** > **Mes demandes**.

2 Dans la liste **État**, filtrez les demandes qui sont affichées :

- **État :** Sélectionnez un état parmi les suivants :
  - **Tous :** Affiche toutes les tâches en attente ou terminées.
  - **En attente :** Affiche les tâches en attente d'approbation.
  - **Terminé :** Affiche les tâches terminées et leur état. Par exemple, approuvé, terminé, refusé ou annulé.

3 Dans la liste **Mes demandes**, cliquez sur une demande d’identités en attente d'approbation pour afficher des informations complémentaires sur celle-ci.



REMARQUE : Les boutons disponibles dans les détails de la demande d’identité varient selon que vous êtes le demandeur, un superviseur ou un approbateur.

4 Vérifiez que la demande d’identité est exacte et complète.

5 Si la demande d'identité n’est plus d'actualité, cliquez sur **Annuler la demande**.

a) Indiquez le motif de l’annulation et cliquez sur **Confirmer**.

La demande d’identité est à présent annulée.

Approuver les demandes d'identité

Pour approuver les demandes d'identité, un superviseur ou un approbateur d'identité doit examiner les approbations en attente, puis décider quelles demandes approuver.

Avant de commencer

Vérifiez que des demandes d’identité ont déjà été envoyées.

À savoir

Seuls les superviseurs et les approbateurs d'identité peuvent approuver les demandes d’identité.

Procédure

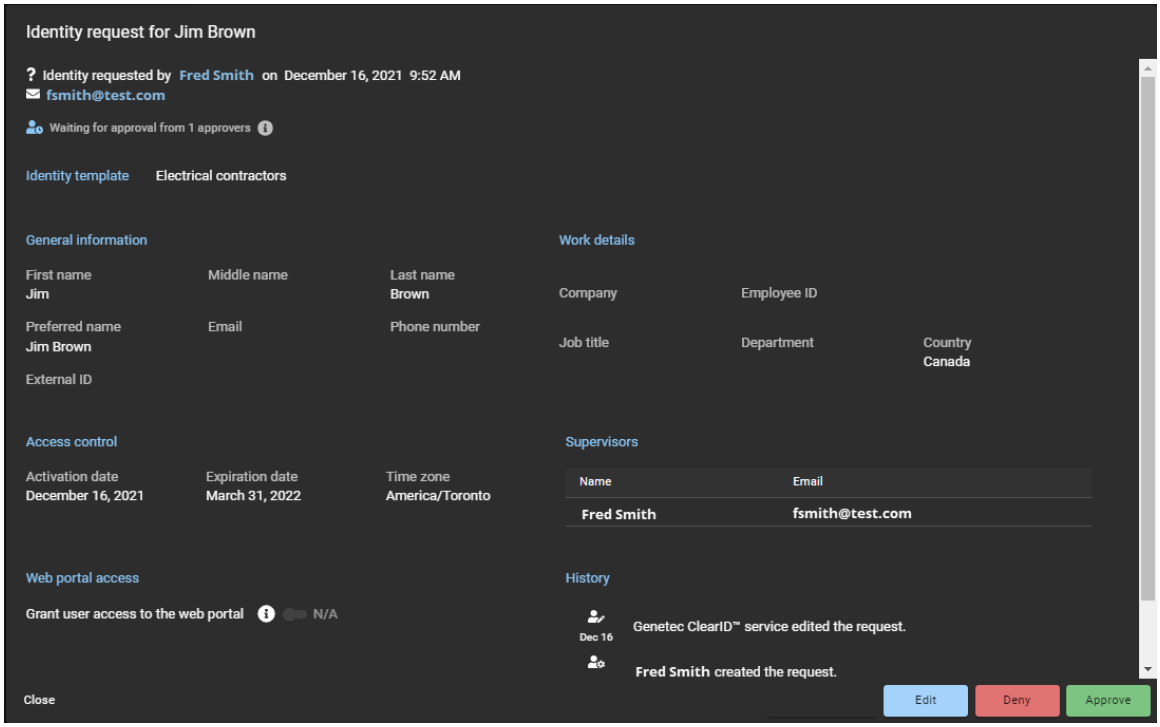
Pour approuver une demande d’identité :

1 Cliquez sur **Tableau de bord** > **Mes tâches**.

2 Dans la liste **État**, filtrez les tâches qui sont affichées :

- **État :** Sélectionnez un état parmi les suivants :
  - **Tous :** Affiche toutes les tâches en attente ou terminées.
  - **En attente :** Affiche les tâches en attente d'approbation.
  - **Terminé :** Affiche les tâches terminées et leur état. Par exemple, approuvé, terminé, refusé ou annulé.

3 Dans la liste **Mes tâches**, cliquez sur une demande d’identité pour afficher des informations complémentaires sur celle-ci.



REMARQUE : Les boutons disponibles dans les détails de la demande d’identité varient selon que vous êtes le demandeur, un superviseur ou un approbateur.

4 Vérifiez que la demande d'identité est exacte et complète.

5 (Facultatif) Si vous voulez modifier la demande d'identité, cliquez sur **Modifier** et apportez les modifications nécessaires.

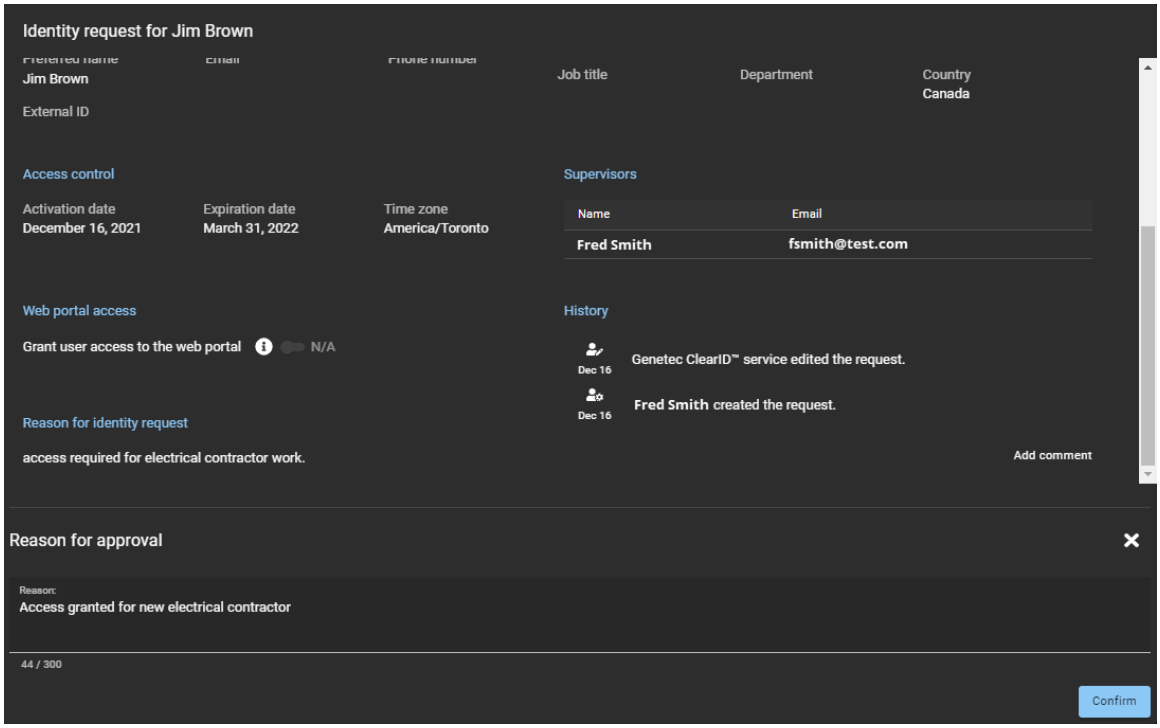
   a) Cliquez sur **Enregistrer**.

6 Si la demande n'est pas recevable ou contient des informations inexactes, cliquez sur **Refuser**.

   a) Indiquez le motif du refus et cliquez sur **Confirmer**.

7 Si la demande est recevable et ne contient pas d'erreurs, cliquez sur **Approuver**.

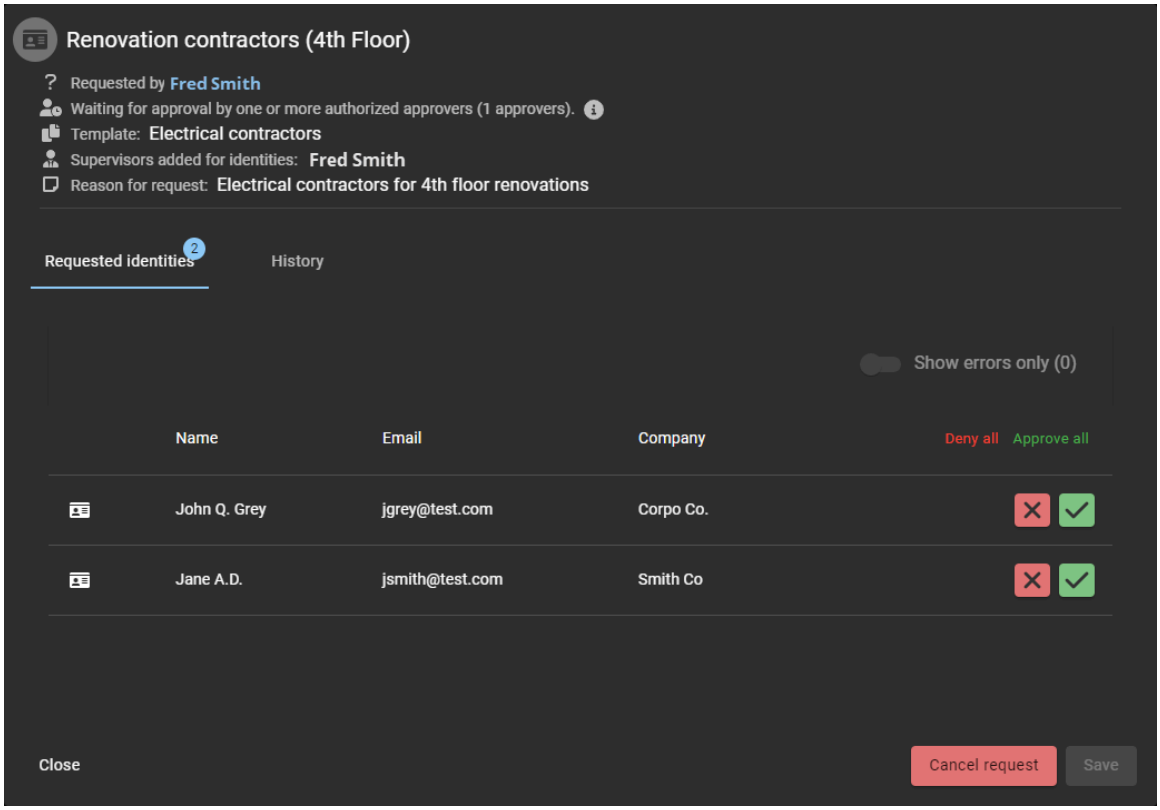
8 Dans le champ **Motif d'approbation**, entrez les informations nécessaires, puis cliquez sur **Confirmer**.



Pour approuver des identités importées depuis un fichier CSV :

1 Cliquez sur **Tableau de bord** > **Mes tâches**.

2 Dans la liste **Mes tâches**, cliquez sur une demande d'identités pour afficher des informations complémentaires sur celle-ci.



REMARQUE : Les boutons disponibles dans les détails de la demande d'identité varient selon que vous êtes le demandeur, un superviseur ou un approbateur.

3 Vérifiez que la demande d'identités est exacte et complète.
   a) Si toutes les identités de la demande sont recevables, cliquez sur **Approuver tout**, puis cliquez sur **Enregistrer**.
   b) Si les identités de la demande ne sont pas toutes recevables, cliquez sur **Refuser tout**, puis cliquez sur **Enregistrer**.

4 (Facultatif) Si vous souhaitez modifier une identité, cliquez sur **Afficher les détails de la demande d'identité** ( ) dans la ligne correspondante pour afficher les détails de la demande.
   a) Cliquez sur **Modifier** pour apporter les modifications nécessaires.
   b) Cliquez sur **Enregistrer**.

5 Si la demande n'est pas recevable ou contient des informations inexactes, cliquez sur **Refuser** ( ) sur la ligne correspondante.
   a) Indiquez le motif du refus et cliquez sur **Confirmer**.

6 Si la demande est recevable et ne contient pas d'erreurs, cliquez sur **Approuver** ( ) sur la ligne correspondante.
   a) Cliquez sur **Enregistrer**.
   b) Dans le champ **Motif d'approbation**, entrez les informations nécessaires, puis cliquez sur **Confirmer**.

La demande d'identité est à présent approuvée. L'identité est créée et hérite le cas échéant des accès du rôle associé aux secteurs durant la période spécifiée dans la demande d'identité.

REMARQUE : (Facultatif) D'autres informations peuvent être fournies par votre organisation pour savoir où et comment récupérer un badge d'accès (si nécessaire) pour la nouvelle identité.

Lorsque vous avez terminé

Rubriques connexes

Note sur la fonction de demande d'identité (2 pages)

Modifier une demande d’identité

Pour modifier les demandes d'identité, un superviseur ou un approbateur d'identité doit examiner les approbations en attente, puis décider quelles demandes approuver.

Avant de commencer

Vérifiez que des demandes d’identité ont déjà été envoyées.

À savoir

Seuls les superviseurs et les approbateurs d'identité peuvent modifier les demandes d’identité.

Procédure

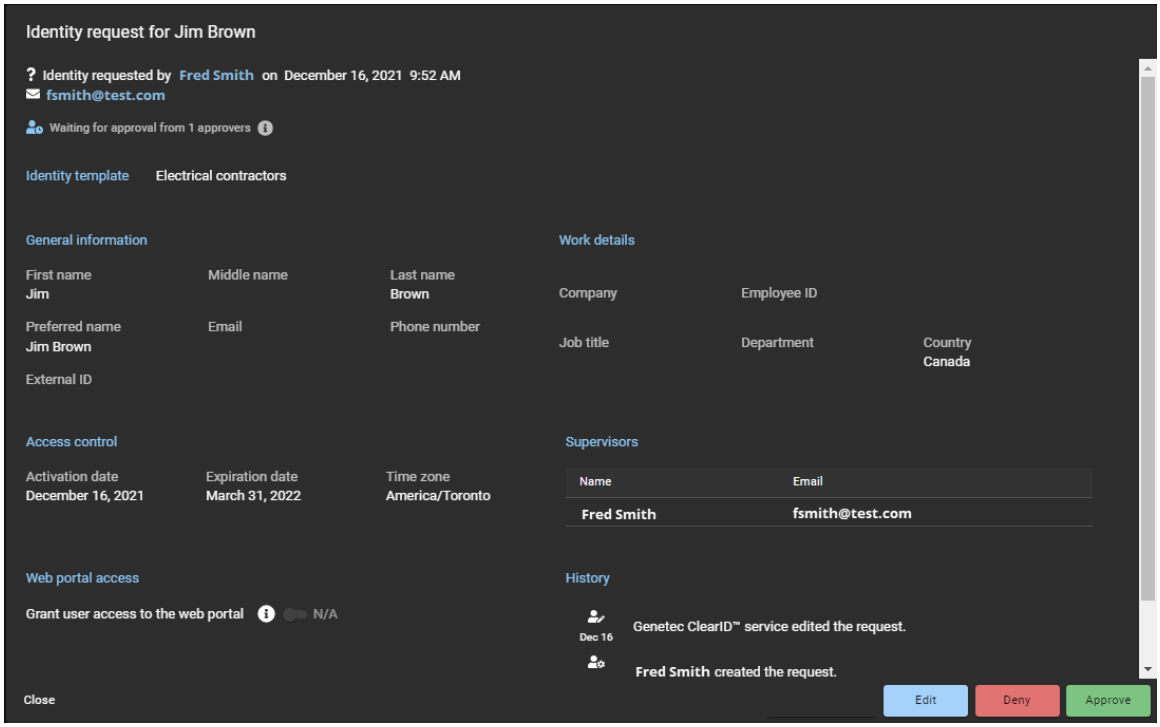
Pour modifier une demande d’identité :

1 Cliquez sur **Tableau de bord** > **Mes tâches**.

2 Dans la liste **État**, filtrez les tâches qui sont affichées :

- **État :** Sélectionnez un état parmi les suivants :
  - **Tous :** Affiche toutes les tâches en attente ou terminées.
  - **En attente :** Affiche les tâches en attente d'approbation.
  - **Terminé :** Affiche les tâches terminées et leur état. Par exemple, approuvé, terminé, refusé ou annulé.

3 Dans la liste **Mes tâches**, cliquez sur une demande d'identité en attente d'approbation pour afficher des informations complémentaires sur celle-ci.



4 Vérifiez que la demande d'identité est exacte et complète.

5 Pour modifier la demande d'identité, cliquez sur **Modifier** et apportez les modifications nécessaires.

a) Cliquez sur **Enregistrer**.

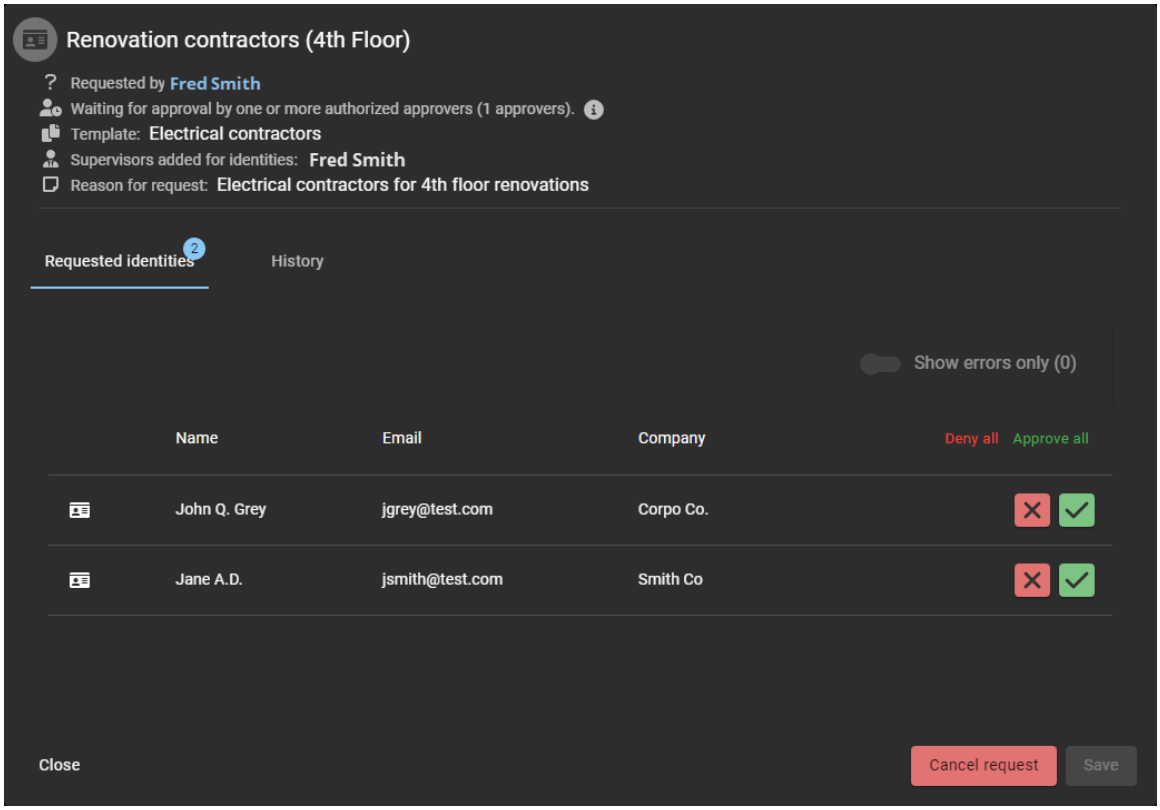
Pour modifier des identités multiples demandées à l'aide d'un fichier CSV :

1 Cliquez sur **Tableau de bord** > **Mes tâches**.

2 Dans la liste **État**, filtrez les tâches qui sont affichées :

- **État :** Sélectionnez un état parmi les suivants :
  - **Tous :** Affiche toutes les tâches en attente ou terminées.
  - **En attente :** Affiche les tâches en attente d'approbation.
  - **Terminé :** Affiche les tâches terminées et leur état. Par exemple, approuvé, terminé, refusé ou annulé.

3 Dans la liste **Mes tâches**, cliquez sur une demande d'identités en attente d'approbation pour afficher des informations complémentaires sur celle-ci.



4 (Facultatif) Si vous souhaitez modifier une identité, cliquez sur **Afficher les détails de la demande d'identité** ( ) dans la ligne correspondante pour afficher les détails de la demande.

a) Vérifiez que la demande d'identité est exacte et complète.

b) Cliquez sur **Modifier** pour apporter les modifications nécessaires.

c) Cliquez sur **Enregistrer**.

Lorsque vous avez terminé

Approuvez vos demandes d'identité.

À propos du rapport de demandes d'identités

Dans Genetec ClearID[MC], le rapport de demandes d’identités renvoie une liste de demandes d'identités pour votre compte ClearID. Le rapport contient des informations sur la date de la demande d'identité, le demandeur, le nom, le modèle d'identité, l’état et les évaluateurs.

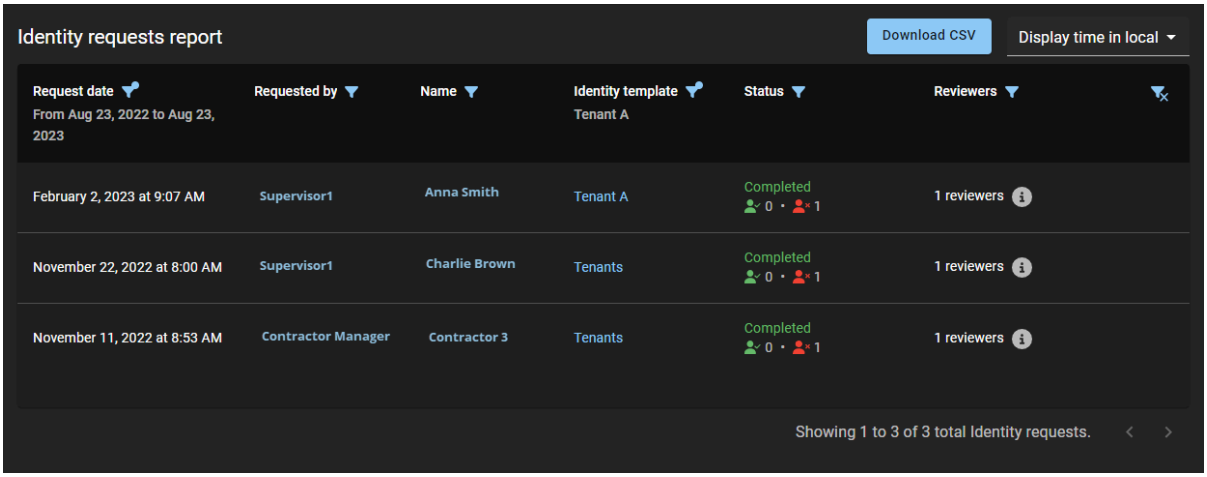


Illustration 2 : Rapport de demandes d'identité

Le rapport Demandes d'identités permet aux administrateurs de consulter l’état de toutes les demandes d'identités au niveau des comptes. Le rapport peut également servir à fournir des informations sur les demandes d’identités dans le cadre d'un audit.

Des filtres permettent d'affiner le résultat de la recherche par date de la demande, demandeur, nom, modèle d'identité, état et évaluateur.

Rubriques connexes

Vérifier l’état des demandes d'identité, page 242

Vérifier l’état des demandes d'identité

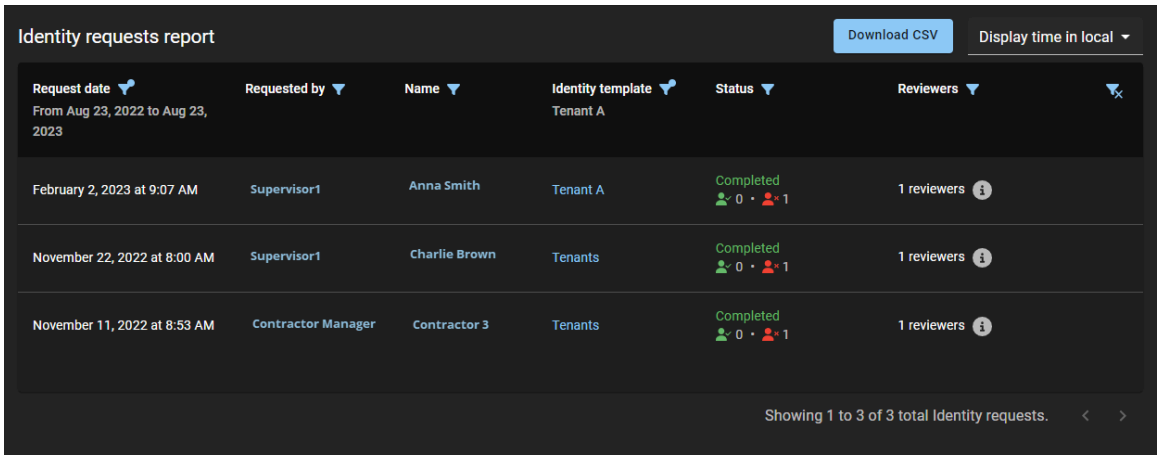
En tant *qu'administrateur de comptes*, vous pouvez vérifier l'état des demandes d'identité pour vous assurer que l'organisation est conforme aux normes de sécurité, prête pour l'audit et que les demandes sont traitées en temps opportun.

Avant de commencer

Vous devez être *administrateur de comptes* pour afficher le **rapport sur les demandes d’identité** et vérifier l’état ou la progression des demandes d’identité.

Procédure

1 Sur la page d'accueil, cliquez sur **Rapports** > **Demandes d’identité**.



2 Dans la page du rapport *Demandes d’identité*, sélectionnez le format d’heure d’affichage requis.

- **Heure d'affichage locale :** Les heures d'affichage sont affichées via l'heure du système de l'ordinateur de l'utilisateur connecté.
- **Heure d'affichage UTC :** Les heures du rapport sont affichées au format UTC (temps universel coordonné).

3 Filtrez le rapport en fonction de vos critères requis :

- **Date de la demande :** Dans la colonne **Date de la demande**, cliquez sur l'icône pour filtrer les résultats par date.

  Si vous sélectionnez **Plage de dates**, utilisez le calendrier pour indiquer la plage de dates désirée.

  REMARQUE : La plage de la **Date de la demande** est limitée à une année.
- **Demandé par :** Dans la colonne **Demandeur**, cliquez sur l'icône pour filtrer les résultats par demandeur d’identité.
  - Entrez un nom d'utilisateur ou une adresse e-mail dans le champ de recherche.
  - (Facultatif) Cliquez sur le lien **Demandeur** pour afficher des informations synthétiques sur celui-ci.
- **Nom :** Dans la colonne **Nom**, cliquez sur pour entrer une chaîne de recherche et filtrer le résultat par **N'importe quel mot** ou **Tous les mots**.
  - **(Facultatif) :** Cliquez sur l’hyperlien **Nom** pour afficher la demande d’identité.

REMARQUE : Si vous êtes un approbateur, vous pouvez **Approuver** ou **Refuser** la demande d'identité en attente que vous consultez.

- **Modèle d'identité :** Dans la colonne **Modèle d'identité**, cliquez sur l'icône pour filtrer les résultats par type de modèle d'identité.
- **État :** Dans la colonne **État**, cliquez sur l'icône pour filtrer les résultats par état.
  - Cochez une ou plusieurs **cases** pour filtrer le résultat en fonction des états souhaités (Envoyé, En attente d'approbation, Refusé, Approuvé, Annulé ou Terminé).
- **Réviseurs :** Dans la colonne **Évaluateurs**, cliquez sur l'icône pour filtrer les résultats par identité, par rôle ou les deux.
- **(Facultatif) :** Cliquez pour réinitialiser les sélections de filtre.

4 Cliquez sur **Télécharger CSV** pour télécharger une copie du rapport des demandes d'identité au format CSV. Le rapport peut ensuite être utilisé à des fins d'audit, pour conserver un exemplaire physique, pour le joindre à une demande d'audit, pour une analyse hors ligne ou encore pour traiter ou consolider les données dans un tableur pour d'autres publics.

a) Suivez les instructions dans votre navigateur pour télécharger le fichier exporté.

Le fichier est exporté sous la forme d'un fichier *.CSV* dans le dossier de téléchargement par défaut de votre navigateur. Par défaut, le fichier exporté est créé d'après le nom de votre site. Par exemple, *IdentityRequestReport_fromdate*_to_*todate*_SiteActivityReport.csv (*IdentityRequestReport_2024-09-24.csv*).

REMARQUE : Les colonnes et les entrées dans le fichier CSV peuvent varier en fonction des filtres sélectionnés au moment de télécharger le rapport.

Lorsque vous avez terminé

Approuvez ou refusez les demandes d'identité :

- Approuver les demandes d'identité, page 235

Rubriques connexes

À propos du rapport de demandes d'identités, page 241
Demander des identités, page 218

6

Synchronisation d'identifiant

Cette section aborde les sujets suivants:

- " Configurer la duplication d’identifiants ", page 245
- " Consulter les journaux de synchronisation des identifiants ", page 247
- " Forcer la synchronisation des identifiants ", page 249

Configurer la duplication d’identifiants

Pour dupliquer des identifiants compatibles sur plusieurs systèmes Synergis[MC], vous devez configurer les réglages de duplication d’identifiants sur le portail Genetec ClearID[MC].

Avant de commencer

- En savoir plus sur les relations entre les titulaires de carte et les identités.
- Vérifiez que ClearID gère les modifications de vos titulaires de cartes et identifiants.

À savoir

Seul un administrateur de compte peut configurer la duplication des identifiants.

Cette fonctionnalité est conçue pour la duplication d’*identifiants* sur plusieurs systèmes Synergis. Pour que la duplication fonctionne correctement, vous devez utiliser toutes les fonctionnalités de gestion des identités fournies par ClearID. Les modifications d'identifiants effectuées sur un système secondaire ne sont pas dupliquées sur les autres systèmes.

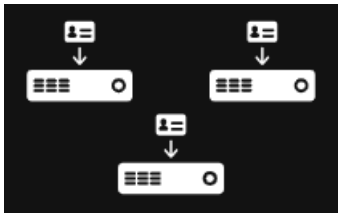
REMARQUE : Les identifiants ne sont pas envoyés aux systèmes sur lesquels la gestion des titulaires de cartes et des identifiants est en mode lecture seule. Dans ce cas, le système de contrôle d'accès est signalé dans la liste avec l’icône **La gestion des titulaires de cartes et des identifiants est désactivée** ( ).

Procédure

1 Sur la page d'accueil, cliquez sur **Administration** > **identifiants**.

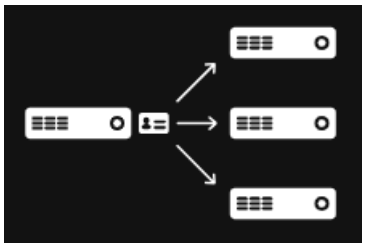
2 Dans la section *Mode de duplication des identifiants*, sélectionnez un mode de duplication dans la liste **Mode**.

a) Option 1 : **Pas de duplication entre systèmes de contrôle d'accès**.



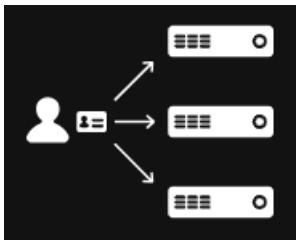
Chaque système de contrôle d'accès fonctionne indépendamment, sans synchroniser les identifiants avec d'autres systèmes. Les identifiants créés sur un système sont propres à ce système et ne sont pas synchronisés automatiquement ni utilisés par d'autres systèmes.

b) Option 2 : **Utiliser un système de contrôle d'accès particulier en tant que source de synchronisation des identifiants**.



Les modifications apportées sur le système sélectionné sont synchronisées avec tous les autres systèmes sur lesquels l'identité est associée à un titulaire de cartes.

c) Option 3 : **Utiliser le système associé au site principal de l'identité en tant que source de synchronisation des identifiants**.



Les modifications apportées aux identifiants sur le système associé au site principal de l'identité sont dupliquées sur tous les autres systèmes sur lesquels l'identité est associée à un titulaire de cartes.

REMARQUE : Si vous sélectionnez **Pas de duplication entre systèmes de contrôle d'accès**, vous pouvez sauter l'étape suivante.

3 Dans la section *Types et formats d'identifiants*, sélectionnez les types d'identifiants que vous souhaitez synchroniser.

REMARQUE : Les options d'identifiants disponibles ici varient en fonction des informations récupérées depuis vos systèmes connectés. Les identifiants personnalisés ne sont pas pris en charge.

a) (Facultatif) Si votre organisation utilise plusieurs formats, vous voudrez parfois ne synchroniser que certains formats particuliers.

4 Cliquez sur **Enregistrer**.

Lorsque vous avez terminé

(Facultatif) Procédez de l'une ou de plusieurs des manières suivantes :

- Examinez les journaux de synchronisation d'identifiants.
- Forcez une synchronisation des identifiants.

Consulter les journaux de synchronisation des identifiants

Pour consulter l'état de la synchronisation des identifiants ou examiner un historique détaillé des activités pour tous les événements associés aux identifiants, consultez les journaux de synchronisation des identifiants dans Genetec ClearID[MC].

Avant de commencer

Configurez vos réglages de synchronisation des identifiants.

À savoir

Seul un administrateur de compte peut consulter les journaux de synchronisation des identifiants.

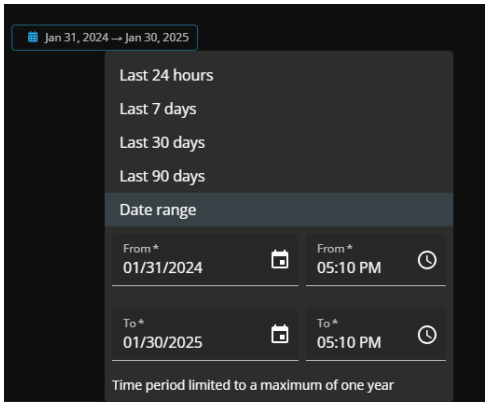
Procédure

1 Sur la page d'accueil, cliquez sur **Administration** > **identifiants**.

2 Dans la section *Journaux de duplication des identifiants*, cliquez sur **Afficher les journaux**.

3 (Facultatif) Utilisez les filtres pour affiner le résultat en fonction d'un ou de plusieurs des critères suivants :

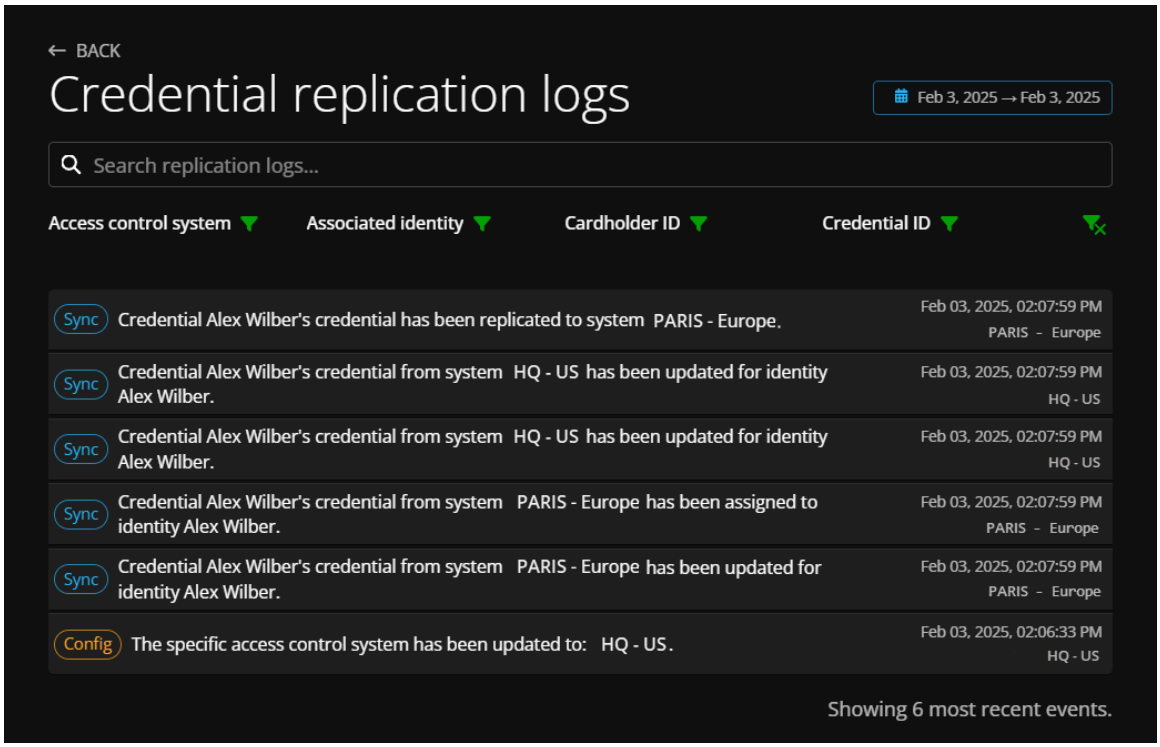
- **Plage de dates :** Sélectionnez une plage de dates prédéfinie parmi les choix disponibles, ou spécifiez une plage particulière à l'aide du sélecteur de plage de dates.



- **Champ de recherche :** Entrez un critère de recherche dans le champ de recherche.
- **Commandes de filtre :**
  - **Système de contrôle d'accès :** Recherchez un système SCA par nom, ou sélectionnez un ou plusieurs SCA dans la liste.
  - **Identité associée :** Recherchez une identité associée. Par exemple un prénom, nom, e-mail ou une autre chaîne de texte.
  - **ID du titulaire de cartes :** Seul un ID de titulaires de cartes au format alphanumérique en valeur HEX est accepté dans ce champ de saisie. Par exemple, `29abdafb-f124-401a-b143-3c88556ec3c1`.

REMARQUE : Ce filtre est pratique pour les utilisateurs qui exploitent principalement des informations provenant de Security Center.

- **ID de l'identifiant :** Seul un ID d'identifiant au format alphanumérique en valeur HEX est accepté dans ce champ de saisie. Par exemple, `fc6e4851-f429-40e5-bbe7-ba363c5cad1a`.



Lorsque vous avez terminé

(Facultatif) Forcez une synchronisation des identifiants.

Forcer la synchronisation des identifiants

Pour résoudre les problèmes liés aux identifiants, vous pouvez forcer une synchronisation pour remplacer tous les identifiants dans Genetec ClearID. Cette synchronisation forcée est déclenchée immédiatement et elle utilise les dernières valeurs de la source sélectionnée.

Avant de commencer

- Configurez vos réglages de synchronisation des identifiants.
- (Facultatif) Consultez les journaux de synchronisation des identifiants.

À savoir

Seul un administrateur de compte peut forcer la synchronisation des identifiants.

Une fois que vous avez configuré les réglages de synchronisation des identifiants, la synchronisation est automatique.

- Une synchronisation forcée peut être utilisée lors de la configuration initiale de manière préventive préventive pour s'assurer que tous les identifiants sont propagés correctement.
- Une synchronisation forcée est également lancée lors du changement du mode de synchronisation, d'un système particulier vers l'option site principal. Après un changement de mode, la synchronisation forcée garantit que les bons identifiants sont synchronisés immédiatement conformément au mode choisi.

Le débit de la synchronisation est d'environ 10 identifiants par seconde. Toutefois, ce débit peut varier en fonction du poste qui exécute le module externe Genetec ClearID^{MC} et du nombre d'identifiants affectés aux identités.

Si vous rencontrez des problèmes d'identifiants sur un site, contactez l'administrateur du compte pour consulter les journaux, effectuer un dépannage et le cas échéant, forcer une synchronisation.

REMARQUE : Si vous avez sélectionné **Pas de duplication entre systèmes de contrôle d'accès** lors de la configuration de la synchronisation des identifiants, la synchronisation forcée n'est pas disponible.

Procédure

1 Sur la page d'accueil, cliquez sur **Administration** > **identifiants**.

2 Dans la section *Forcer la synchronisation des identifiants*, cliquez sur **Synchroniser**.

3 Dans la boîte de dialogue *Synchroniser*, cliquez sur **Synchroniser**.

La demande de synchronisation des identifiants est lancée et le message Demande de synchronisation d'autres systèmes envoyée avec succès est affiché.

IMPORTANT : Aucune autre information n'est signalée dans l'onglet **Identifiants**.

Lorsque vous avez terminé

Examinez les **Journaux de duplication des identifiants** pour vérifier que les identifiants ont bien été mis à jour avec les dernières informations.

7

Gérer les sites

Découvrez comment gérer les sites.

Cette section aborde les sujets suivants:

- " À propos des sites ", page 251
- " Création de sites ", page 252
- " Modifier les sites ", page 273
- " Définir la durée maximale d'accès à un site ", page 275
- " Configurer les documents de demande d'accès pour les sites ", page 276
- " Personnaliser les notifications par e-mail pour un site ", page 279
- " À propos des examens d'accès ", page 283
- "Configuration de l’expiration automatique pour les examens d’accès", page 285
- " Configurer les examens d'accès à un secteur ", page 287
- " Configurer les examens d'accès d'identité ", page 293
- " Modifier les examens d'accès ", page 297
- " À propos du rapport d’examen d'accès ", page 298
- " Vérifier l’état des examens d'accès ", page 299
- " Terminer un examen d'accès à un secteur (propriétaire de site) ", page 302
- " Terminer un examen d'accès (approbateur de secteur ou responsable de rôle) ", page 311
- " Terminer un examen d’accès d’identité (superviseur) ", page 320
- " Générer un résumé d’examen d'accès ", page 326
- " À propos du rapport de demandes d'accès ", page 328
- " Vérifier l’état des demandes d'accès ", page 329
- " À propos du rapport d'activité de site ", page 332
- " Afficher un rapport d'activité de site ", page 333
- " À propos du rapport Propriétaires de sites et de secteurs ", page 336
- " Afficher le rapport Propriétaires de sites et de secteurs ", page 337

À propos des sites

Dans Genetec ClearID[MC], un site est une entité logique. Les sites incluent un ou plusieurs secteurs. Chaque site et chaque zone peuvent avoir un propriétaire différent.

Un site représente généralement un bâtiment ou un campus :

- Si plusieurs bâtiments sont gérés par une seule équipe de sécurité ou un seul ensemble de politiques pour les visiteurs, il est conseillé de les configurer à l'aide d'un seul site.
- Chaque site peut avoir son propre ensemble de règles et de propriétaires de sites.
- Si différents bâtiments sont répartis dans une ville, envisagez d'implémenter un site par bâtiment.
- Plusieurs sites peuvent être associés à un même système de contrôle d'accès Security Center.

IMPORTANT : Vos choix de mise en œuvre peuvent affecter le coût de la solution Genetec ClearID[MC]. Ces coûts peuvent varier selon les fonctions mises en œuvre, le nombre d'identités et le nombre de sites.

Création de sites

Avant de pouvoir configurer vos secteurs dans Genetec ClearID[MC], vous devez créer les sites auxquels vos secteurs seront associés.

Avant de commencer

- Ajoutez vos systèmes.

À savoir

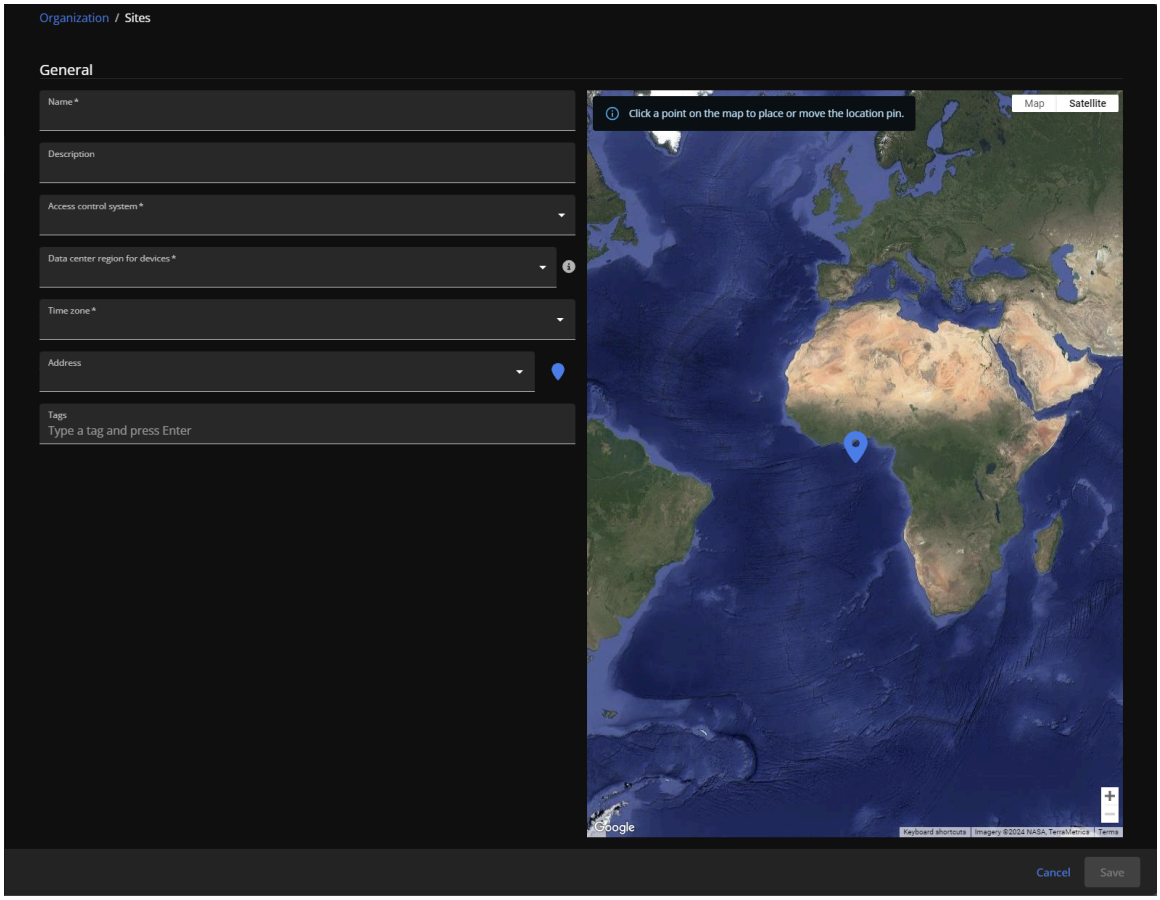
Pour créer des sites dans ClearID, vous devez être un *Administrateur de compte*.

- Un *Administrateur de compte* peut choisir les *propriétaires du site* et configurer la gestion des visiteurs pour le site.
- Un *site* est associé à un système de contrôle d'accès Security Center.
- Plusieurs sites peuvent être associés à un même système de contrôle d'accès Security Center.

Procédure

1 Cliquez sur **Organisation** > **Sites**.

2 Cliquez sur **Ajouter un site**.



3 Sur la page *Général*, renseignez les champs.

REMARQUE : Les champs obligatoires sont mis en évidence dans l'interface utilisateur avec un astérisque (*).

- **Nom :** Saisissez un nom pour votre site.
- **Description :** Entrez une description qui indique l'emplacement géographique du bâtiment ou l'emplacement physique du site.
- **Système de contrôle d'accès :** Sélectionnez le système dont vous avez besoin dans la liste **Système de contrôle d'accès**. .

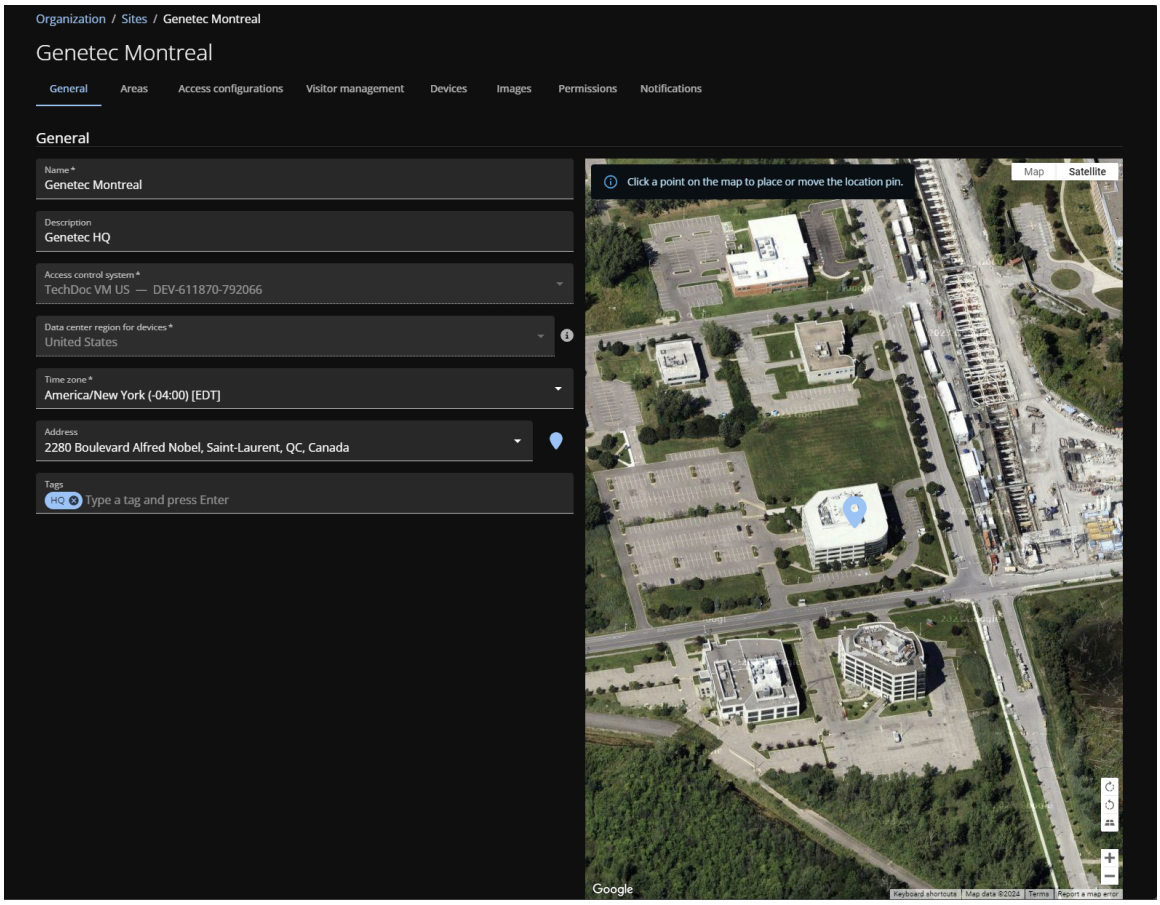
  REMARQUE : Ce système de contrôle d'accès sert à répercuter les modifications apportées à ClearID dans Security Center.
- **Région du centre de données pour les appareils :** Sélectionnez une région de centre de données dans la liste déroulante. Cette option est généralement définie sur la région du centre de données la plus proche de l'endroit où l'appareil sera utilisé. La région de centre de données sera utilisée pour la communication avec les appareils.

  REMARQUE : Ce réglage est définitif et ne peut pas être modifié après la création d'un site. L'option de centre de données n'est pas disponible si votre compte est déployé dans l'architecture Europe uniquement.
- **Fuseau horaire :** Sélectionnez un fuseau horaire dans la liste déroulante. Les options de fuseau horaire sont représentées au format IANA (Internet Assigned Numbers Authority).

  REMARQUE : Lorsqu'une demande d'accès ou une demande de visiteur est soumise depuis n'importe quel point dans le monde, le fuseau horaire de l'accès ou de la visite du site demandé est utilisé pour garantir que la date et l'heure correctes sont appliquées à la demande.
- **Address :** Entrez une adresse pour le site. Pendant la frappe, l'intégration Google Maps traite l’information et affiche les adresses disponibles.

- **Plan du centre :** Cliquez sur pour trouver l'adresse sur la carte et centrer la carte sur cette adresse.

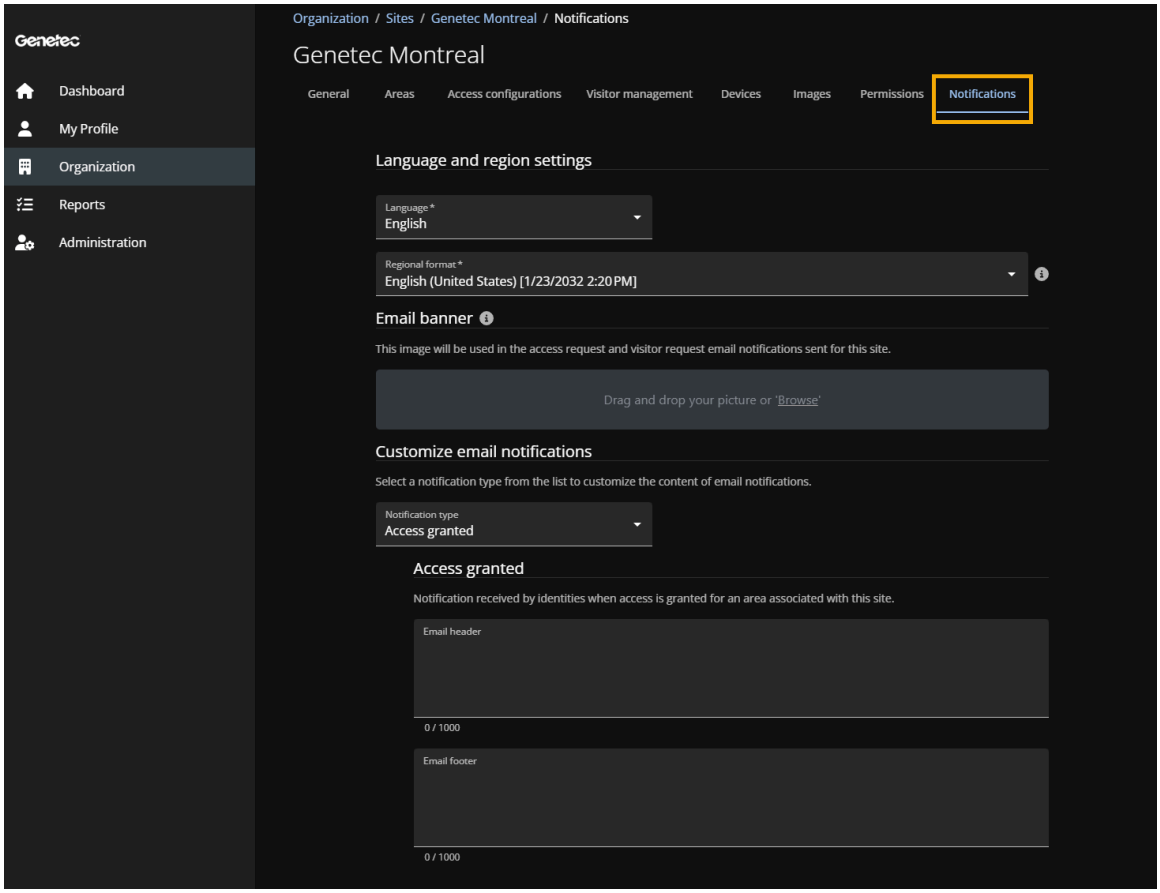
- **Étiquettes :** Saisissez d'autres mots clés ou catégories de termes de recherche qui pourraient être utilisés pour trouver le site.



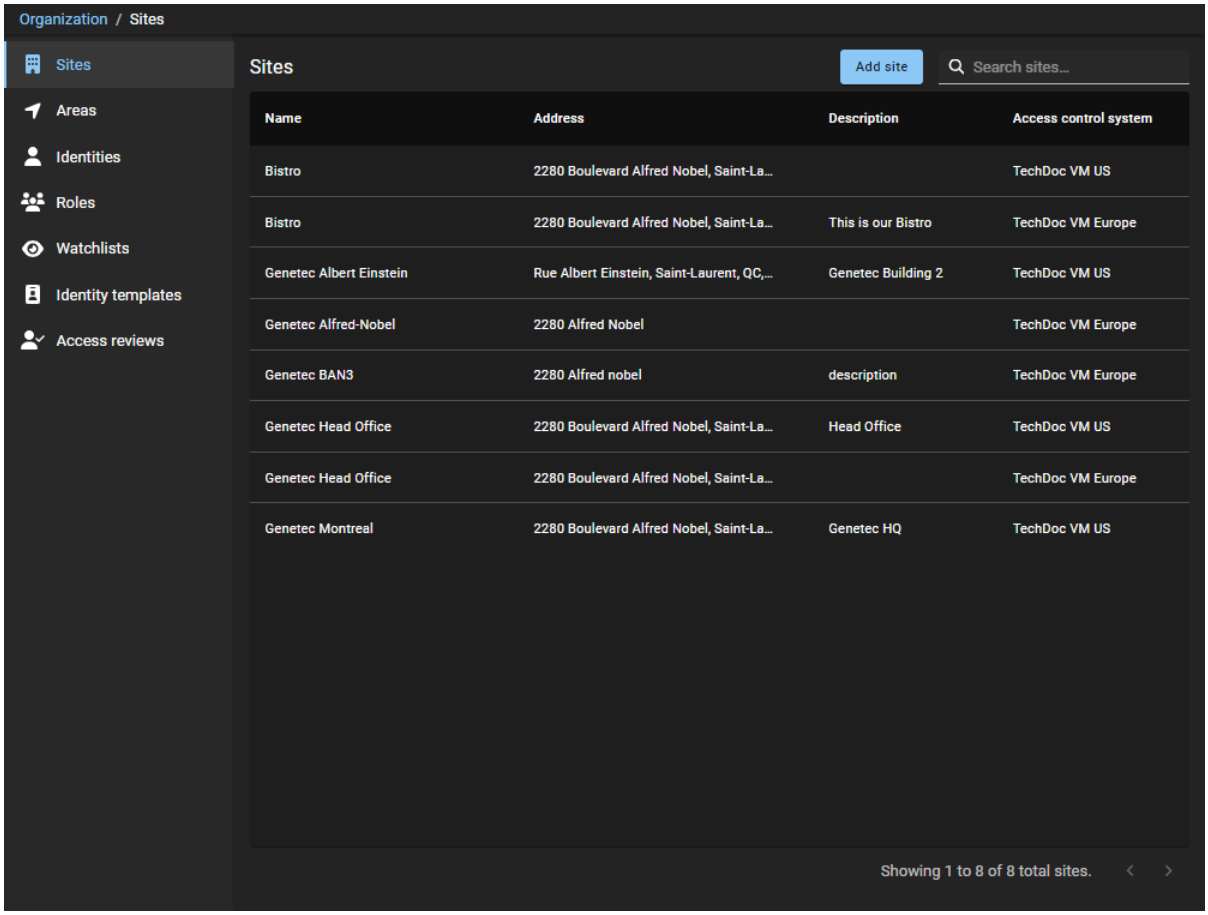
4 Sur la page *Notifications*, renseignez les champs.

- **Langue :** Sélectionnez une langue de notification dans la liste déroulante. Ce paramètre est utilisé pour les notifications par e-mail et les alertes SMS. La sélection de la langue des notifications est unique pour un site et vous pouvez choisir parmi les langues suivantes : français, espagnol, portugais, italien, allemand, néerlandais et japonais.
- **Format régional :** Sélectionnez un format régional de date et d'heure pour les e-mails de notification provenant de ce site. Le format régional par défaut est l'anglais des États-Unis (en-us). Par exemple, 1/23/2032 2:20 PM.

5 Cliquez sur **Enregistrer**.



Votre site a été créé dans ClearID.



Lorsque vous avez terminé

Ajoutez vos propriétaires de site.

Rubriques connexes

Modifier les sites, page 273
Base de données des fuseaux horaires IANA

Ajouter des propriétaires de sites

Dans Genetec ClearID[MC], un propriétaire de site est une identité qui a autorité sur les secteurs associés à un site particulier. Avant de pouvoir attribuer ou modifier des propriétaires de secteurs, configurer des paramètres de secteur spécifiques exclusifs aux propriétaires de site ou gérer les analyses d'accès au site, vous devez ajouter vos propriétaires de site.

Avant de commencer

Créez vos sites.

À savoir

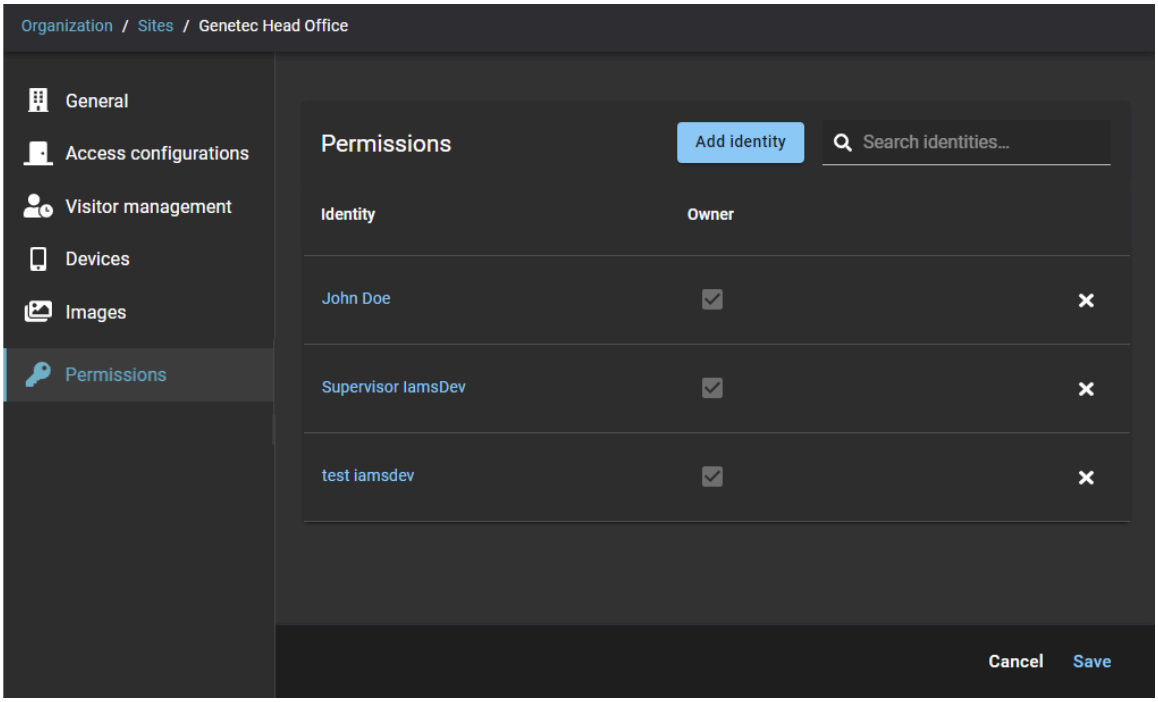
Pour ajouter des propriétaires de sites dans ClearID, vous devez être un administrateur de compte.

Procédure

1 Cliquez sur **Organisation** > **Sites**.

2 Sélectionnez votre site et cliquez sur **Autorisations**.

3 Cliquez sur **Ajouter une identité** pour ajouter des propriétaires de site à la liste des **autorisations** du site.



a) Recherchez ou sélectionnez les identités dont vous avez besoin et cliquez sur **Ajouter**.

CONSEIL : Cliquez sur le lien hypertexte d'identité dans la colonne **Identité** pour consulter les détails d'identité (entreprise, département, site d'origine, superviseur et e-mail) et vérifier que les bonnes identités figurent dans la liste.

b) (Facultatif) Cliquez sur ✕ pour supprimer toute autorisation de propriétaire de site qui n'est plus requise.

4 Cliquez sur **Enregistrer**.

Lorsque vous avez terminé

Créez vos secteurs

Activer la gestion des visiteurs pour un site

Avant que les utilisateurs puissent inviter des visiteurs, vous devez configurer les réglages de gestion des visiteurs pour votre site.

Avant de commencer

Créez vos sites.

À savoir

- La gestion des visiteurs est désactivée par défaut.

- Seuls les administrateurs de comptes ou les *propriétaires de sites* peuvent activer la gestion des visiteurs pour un site dans Genetec ClearID[MC].
- Les options affichées lors de la création d'une demande de visite varient en fonction des utilisateurs demandant l'accès et des paramètres que vous configurez ici.
- Seuls les administrateurs de comptes peuvent autoriser les utilisateurs à inviter des visiteurs à l'aide de rôles.
- Par défaut, les utilisateurs bénéficient automatiquement des autorisations *Inviter des visiteurs* pour leur site d'origine.

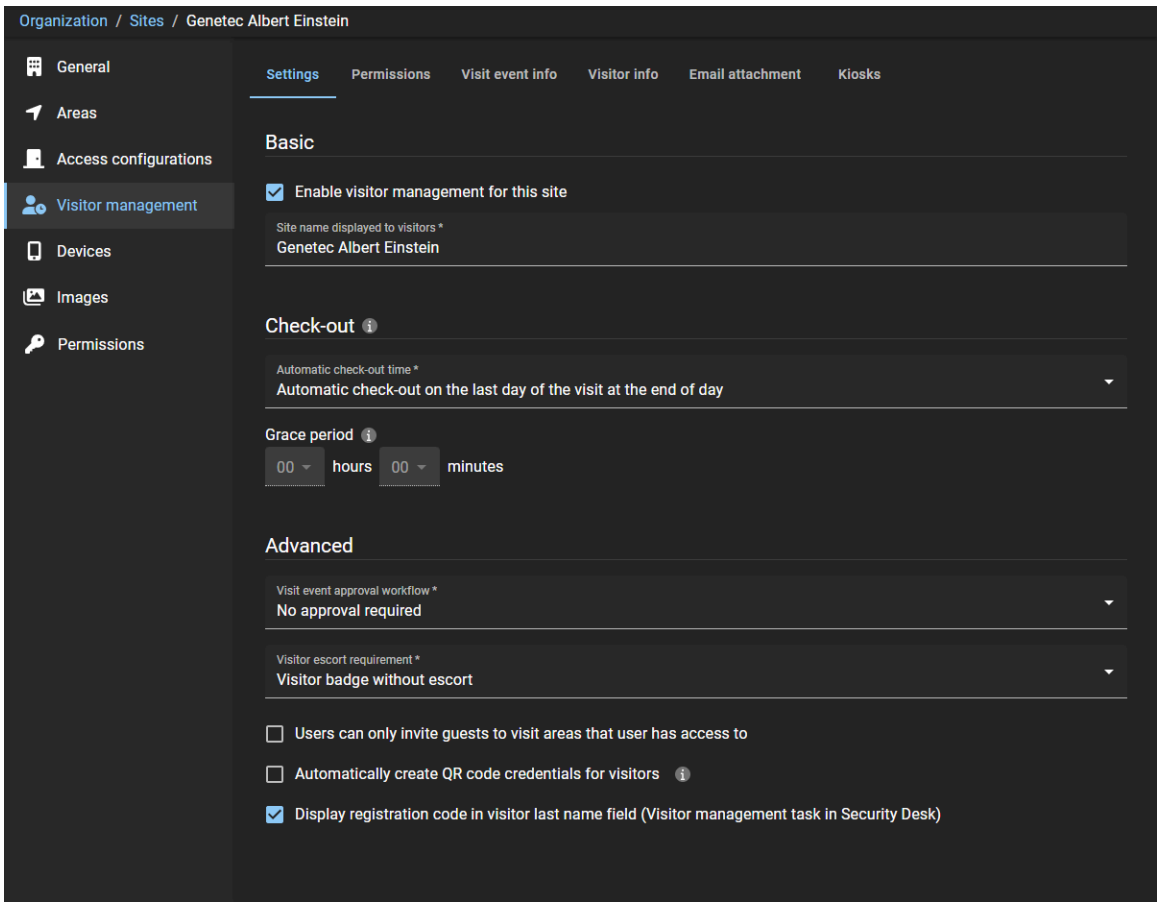
Procédure

1 Cliquez sur **Organisation** > **Sites**.

2 Recherchez et sélectionnez un site.

3 Cliquez sur **Gestion des visiteurs** pour configurer les options de gestion des visiteurs d'un site.

4 Cliquez sur l'onglet **Réglages**.



a) Dans la section *Paramètres de base*, configurez les options nécessaires :

- **Activer la gestion des visiteurs pour ce site :** Cochez cette case pour activer la gestion des visiteurs pour le site.
- **Nom du site affiché pour les visiteurs :** Saisissez le nom du site que vous souhaitez afficher en externe pour les visiteurs.

b) Dans la section *Radiation*, configurez les options nécessaires :

- **Heure de radiation automatique :**

- **Radiation automatique le dernier jour de la visite en fin de journée :** Le visiteur est radié automatiquement à minuit le dernier jour de la visite.
- **Radiation automatique à l'heure de fin programmée de la visite :** Le visiteur est radié à l'heure de fin spécifiée pour la visite.

  REMARQUE : Les droits d'accès temporaires du visiteur et le code QR d'identification sont désactivés durant la radiation automatique. Lorsqu'un délai de grâce est activé, les visiteurs sont radiés à l'issue du délai de grâce ajouté à l'heure de fin de la visite.

- **Délai de grâce :** Ajoute du temps supplémentaire à l'heure de fin programmée de l'événement de visite. À l'échéance du délai de grâce, le visiteur est radié.

c) (Facultatif) Dans la section *Avancé*, configurez les options nécessaires :

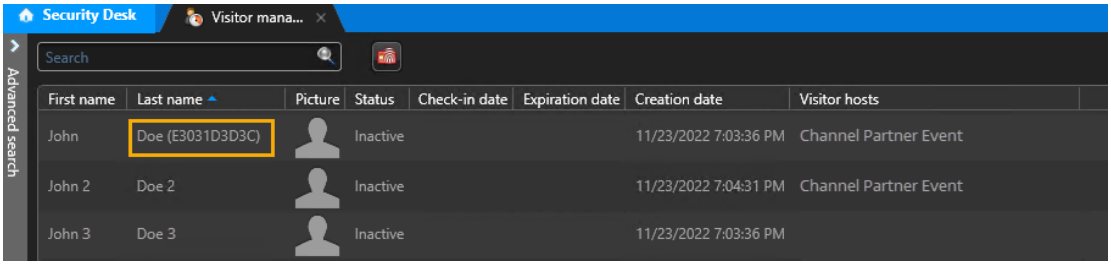
- **Processus d'approbation d'événement de visite :** Sélectionnez le processus d'approbation dont vous avez besoin :
  - **Aucune approbation nécessaire :** Aucune approbation n'est nécessaire pour faire approuver l'événement de visite. Par exemple, pour simplifier le fait pour les employés d'inviter des visiteurs à tout moment.
  - **Approbation par un superviseur nécessaire :** L'approbation du superviseur est nécessaire pour faire approuver l'événement de visite.
  - **Approbation nécessaire par l'approbateur de l'événement de visite :** L'approbation de l'approbateur de l'événement de visite est requise pour faire approuver l'événement de visite.

    REMARQUE : Si un secteur est sélectionné lors de la création de l'événement de visite, il peut déclencher son propre flux d'approbation.
- **Exigence d'escorte de visiteur :** Sélectionnez le type de badge dont vous avez besoin :
  - **Badge visiteur sans escorte :** Généralement utilisé pour les visiteurs qui ne nécessitent pas d'escorte ou d'accès aux portes des secteurs sécurisés ou sensibles.
  - **Badge visiteur avec escorte :** Généralement utilisé pour les visiteurs qui ont besoin d'une escorte ou d'accéder aux portes des secteurs sécurisés ou sensibles.

    REMARQUE : La **règle d'escorte de visiteur** doit également être activée pour les secteurs dans Synergis[MC]. Pour que l'escorte fonctionne correctement, l'option **Les groupes de titulaires de cartes peuvent escorter les visiteurs** doit également être activée dans les **Paramètres généraux** de la tâche *contrôle d'accès* dans Config Tool.
- **Les utilisateurs peuvent uniquement inviter des personnes à visiter les secteurs auxquels ils ont accès :**
  - Si la case est cochée, les utilisateurs peuvent uniquement convier les invités à visiter les secteurs auxquels l'utilisateur demandeur a accès. Ce paramètre est appliqué lorsqu'une demande de visite d'invité est créée.
  - Si la case est décochée, les utilisateurs peuvent inviter des utilisateurs à visiter tous les secteurs qui acceptent les visites dans ClearID.
- **Créer automatiquement un identifiant à code QR pour les visiteurs :** Si la case est cochée, ClearID crée automatiquement un identifiant code QR pour les visiteurs à la création d'une demande de visite. Les visiteurs peuvent utiliser le code QR inclus dans l'e-mail de confirmation du visiteur pour accéder à des entrées de parking, tourniquets ou installations clôturées spécifiques. Le code QR peut également être utilisé lors de l'inscription auprès des équipes de sécurité, de l'accueil ou sur une borne Genetec ClearID[MC] Self-Service Kiosk.
- **Afficher le code d'inscription dans le champ nom du visiteur (tâche Gestion des visiteurs dans Security Desk) :**

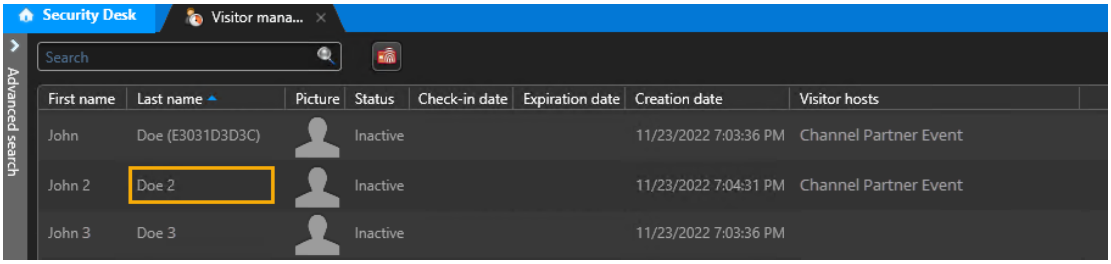
- Si la case est cochée, le champ du nom de famille affiche le nom de famille du visiteur et la valeur du code QR. Cette option est sélectionnée par défaut.

  La case doit être cochée pour qu'un scanner de codes QR puisse scanner et retrouver un visiteur préinscrit dans Security Desk.



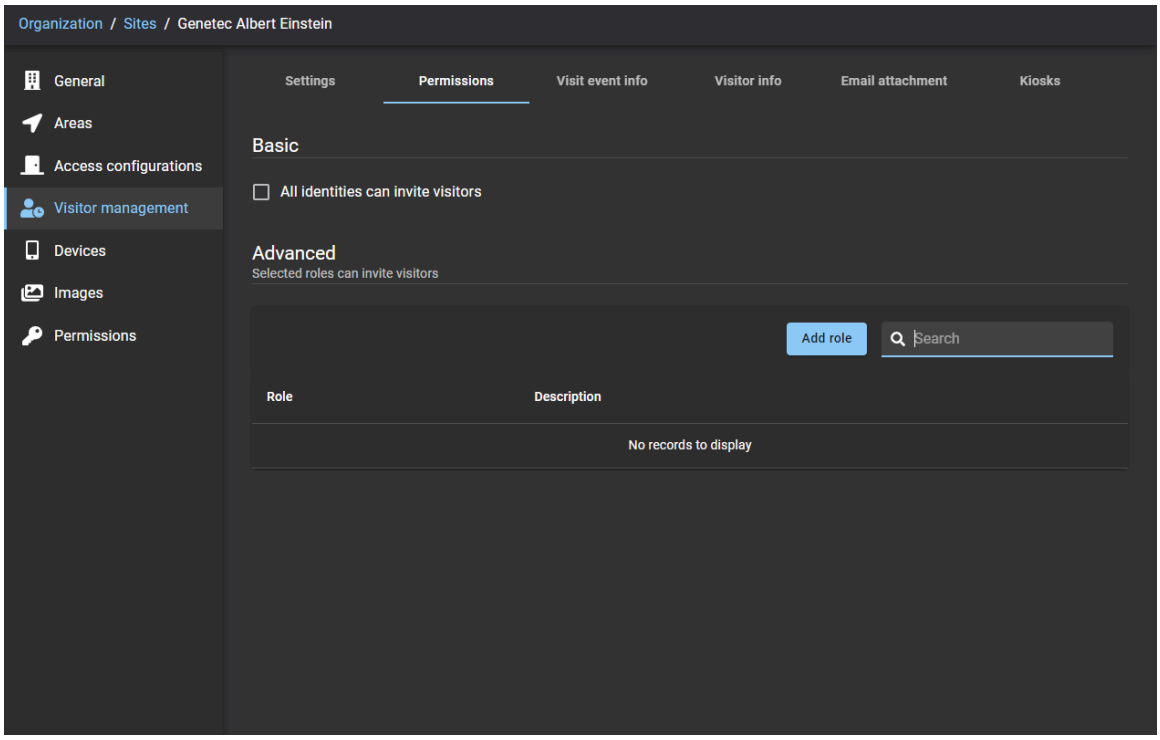
  CONSEIL : Vous pouvez utiliser le scanner de codes QR Zebra pour saisir le code QR dans le champ **Nom** à votre place. Dans la tâche *Gestion des visiteurs* de Security Desk, cliquez dans le champ **Rechercher**, scannez le code QR, et appuyez sur **Entrée**.

- Si la case est décochée, le champ du nom de famille affiche uniquement le nom de famille du visiteur.



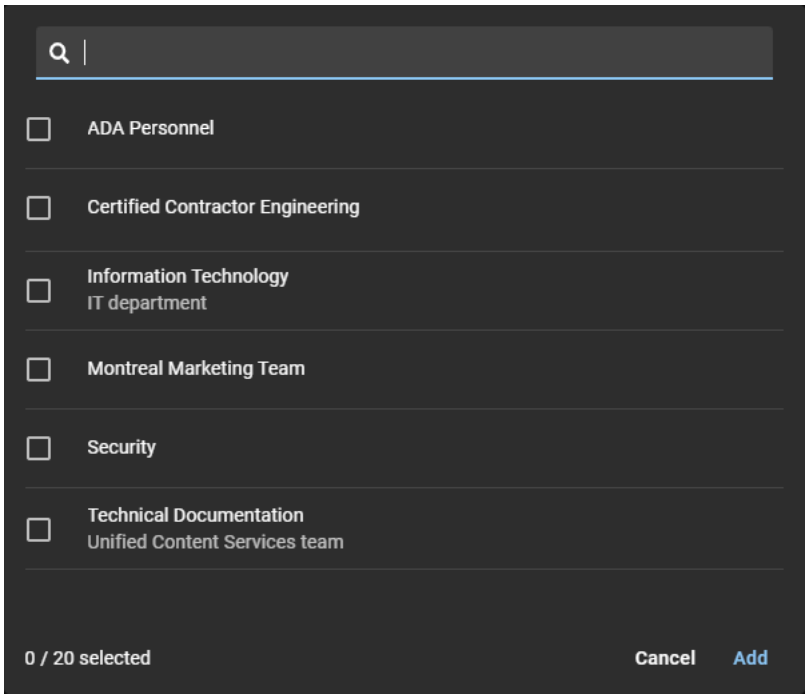
REMARQUE : Lorsque l'option du code d'enregistrement est modifiée, seuls les visiteurs créés après le changement sont modifiés, les visiteurs créés précédemment restent inchangés.

5 (Facultatif) Cliquez sur l'onglet **Autorisations**.



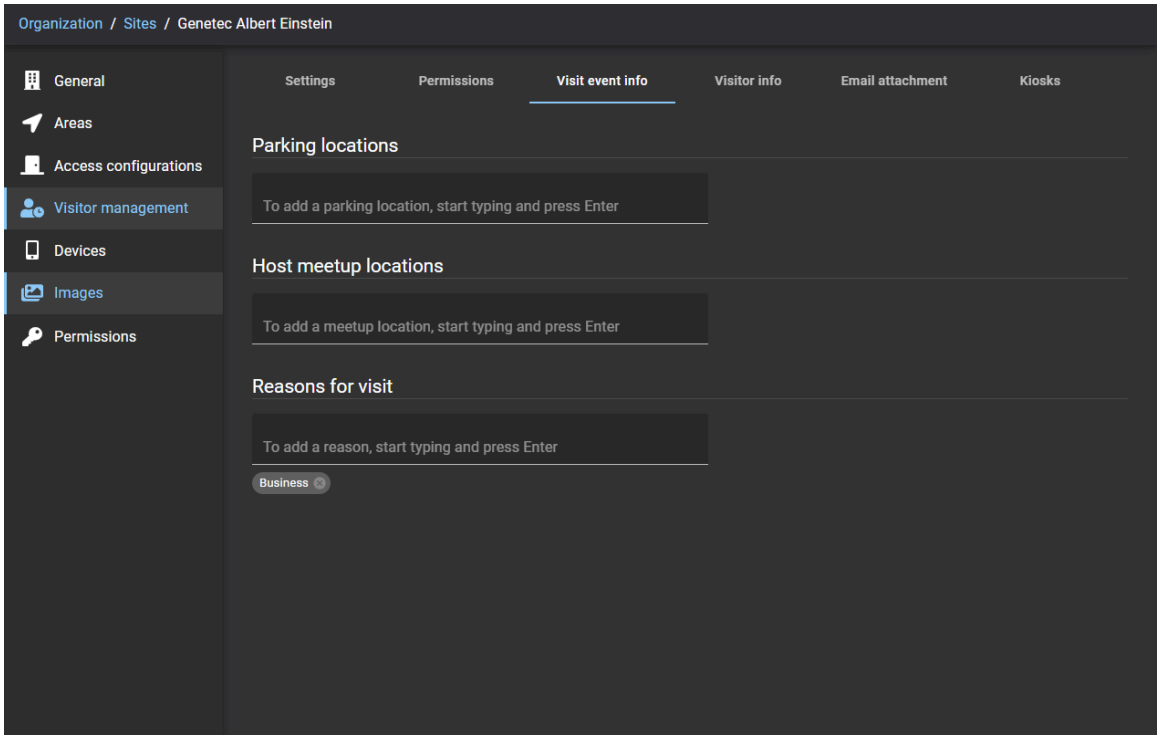
Procédez de l'une des manières suivantes :

- Dans la section *Paramètres de base*, cochez la case **Toutes les identités peuvent inviter des visiteurs** si vous souhaitez que toutes les identités puissent inviter des visiteurs sur ce site.
- Dans la section *Avancé*, Cliquez sur **Ajouter un rôle** si vous souhaitez utiliser les rôles pour gérer les personnes autorisées à inviter des visiteurs sur ce site. Vous pouvez rechercher et sélectionner les identités dont vous avez besoin et cliquer sur **Ajouter**.



CONSEIL : Si vous ajoutez de nouvelles autorisations de rôle, invitez les membres à se déconnecter et se reconnecter pour charger les nouvelles autorisations d'invitation de visiteurs immédiatement.

6 (Facultatif) Cliquez sur l'onglet **Infos sur l'événement de visite** et configurez les options nécessaires :



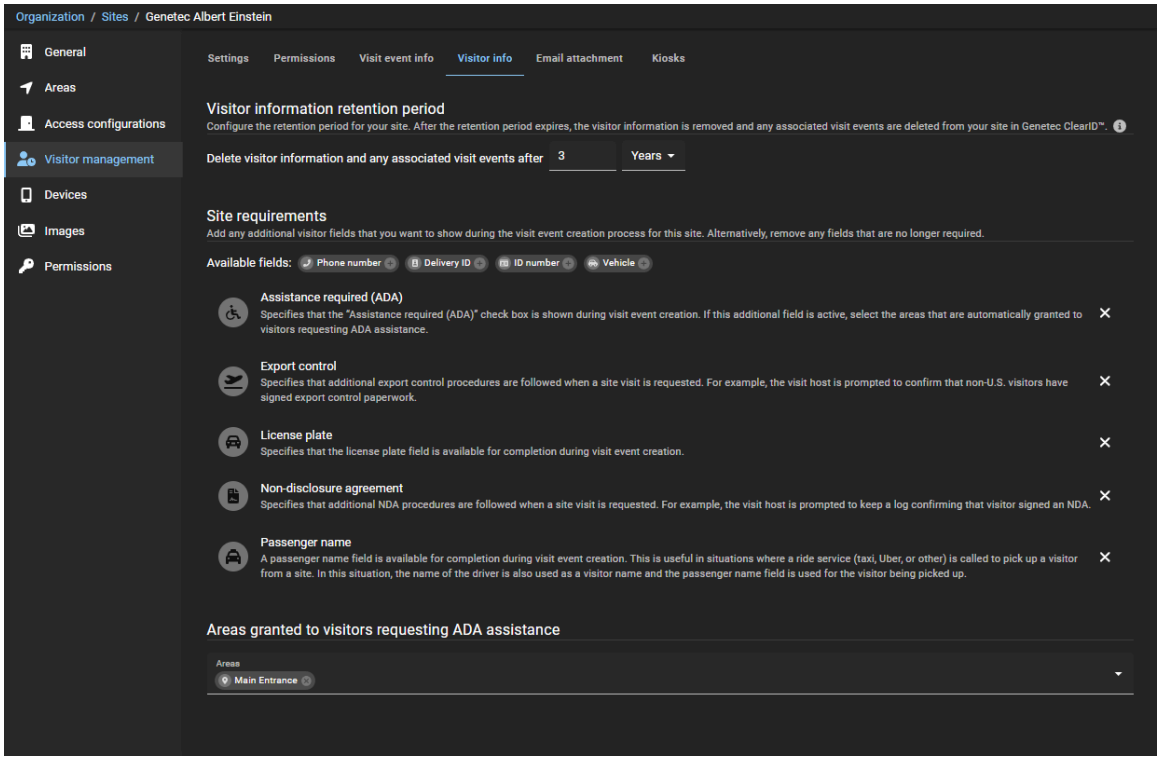
a) Dans la section *Emplacements de stationnement*, ajoutez des emplacements de stationnement si nécessaire.

b) Dans la section *Emplacements de rencontre des hôtes*, ajoutez des lieux de rencontre si nécessaire.

c) Dans la section *Motif de la visite*, ajoutez les raisons typiques des visites sur votre site.

Par exemple, réunion client, réunion partenaire, entretien d'embauche, livraison, ramassage taxi, ramassage Uber, ramassage ascenseur, etc.

7 (Facultatif) Cliquez sur l'onglet **Infos sur le visiteur** et configurez les options nécessaires :

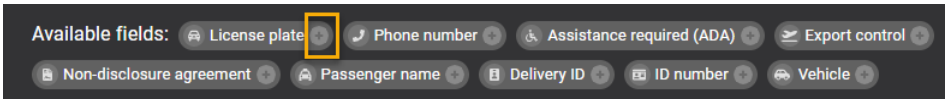


a) Dans la section *Période de rétention des données de visiteurs*, sélectionnez une période de rétention en jours, mois ou années.

La période de rétention par défaut et de 1 an, et la valeur maximale est de 3 ans.

REMARQUE : La période de rétention est configurable par site afin d'assurer la conformité avec les réglementations régissant les données de votre région.

b) Dans la section *Configuration requise pour le site Champs disponibles*, cliquez sur pour ajouter les champs que vous souhaitez intégrer au processus de création d'événements de visite pour votre site.



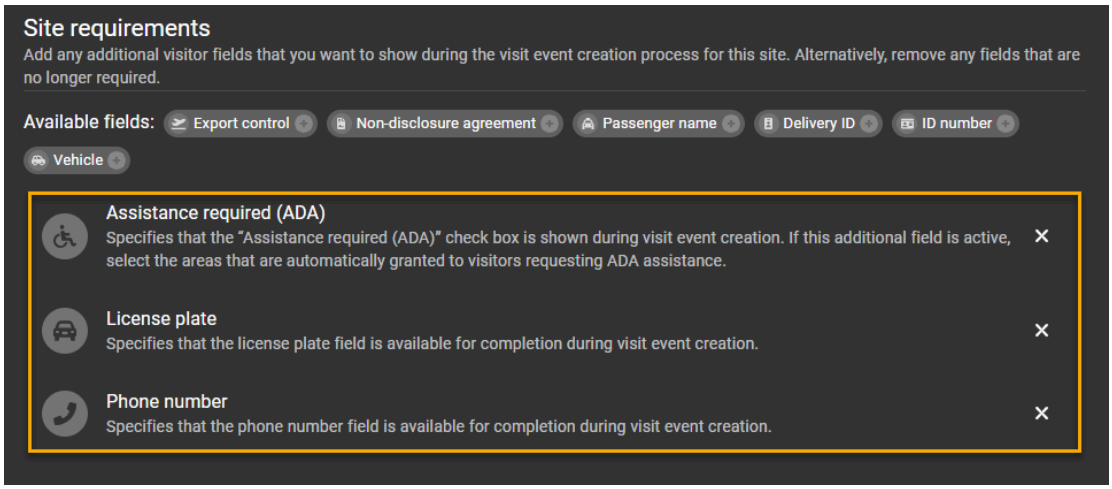
- **Plaque d'immatriculation :** Si cette case est cochée, un champ Plaque d'immatriculation est affiché lorsqu'une visite du site est demandée.
- **Numéro de téléphone :** Si cette case est cochée, un champ Numéro de téléphone est affiché lorsqu'une visite du site est demandée.
- **Assistance requise (ADA) :** Si cette case est cochée, une section *Secteurs accordés aux visiteurs demandant une assistance ADA* s'affiche.

  REMARQUE : Cette option d'assistance est utilisée pour se conformer à l'Americans with Disabilities Act (ADA).
- **Contrôle des exportations requis :** Si cette case est cochée, des procédures de contrôle des exportations supplémentaires sont suivies lorsqu'une visite du site est demandée. Par exemple, l'hôte de la visite est invité à confirmer que les visiteurs non américains ont signé les documents de contrôle des exportations.
- **Accord de non-divulgation :** Si cette case est cochée, des procédures NDA supplémentaires sont suivies lorsqu'une visite du site est demandée. Par exemple, l'hôte de visite est invité à tenir un journal confirmant que le visiteur a signé un accord de confidentialité.
- **Nom du passager :** Lorsque cette option est sélectionnée, un champ Nom du passager est fourni lors d'une demande de visite de site. Ce champ Nom du passager est par exemple utile lorsqu'un service de transport (taxi, Uber ou autre) est sollicité pour récupérer un visiteur sur un site. Dans ce

cas, le nom du conducteur est également consigné en tant que nom de visiteur et le champ Nom du passager est destiné au visiteur utilisant le service de transport.

- **ID de dépôt :** Lorsque cette option est sélectionnée, un champ ID de dépôt est fourni lors d'une demande de visite de site.
- **Numéro d'ID :** Si cette case est cochée, un champ Numéro d'ID est affiché lorsqu'une visite du site est demandée.
- **Véhicule :** Lorsque cette option est sélectionnée, un champ d'informations supplémentaire sur le véhicule est fourni lors d'une demande de visite de site.

REMARQUE : Les champs ajoutés sont affichés dans la section *Champs disponibles* plus loin dans la section.



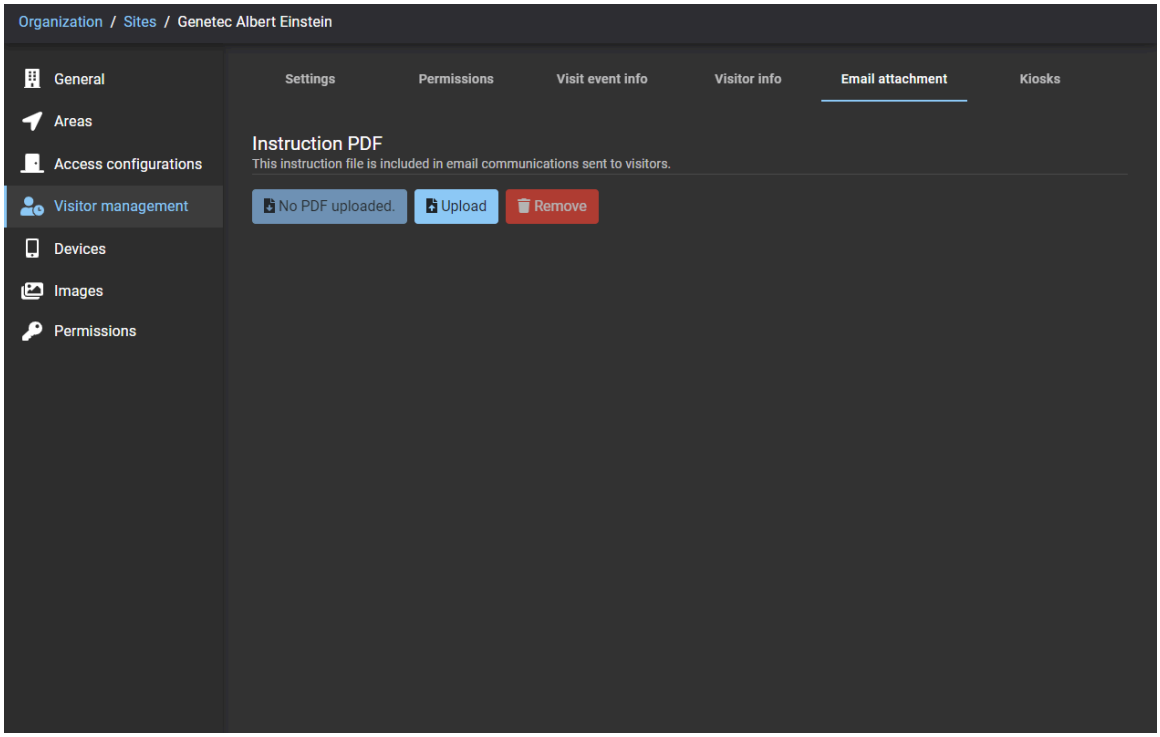
c) (Facultatif) Si vous avez ajouté **Assistance nécessaire (ADA)** aux exigences de votre site, allez dans la section *Secteurs autorisés aux visiteurs demandant une assistance ADA*, ajoutez les secteurs qui doivent automatiquement être autorisés pour ces utilisateurs.

REMARQUE : Lorsqu'un visiteur qui requiert une assistance d'accessibilité est invité sur le site par un employé, il est automatiquement ajouté à la liste des secteurs ADA.

Par exemple, s'il existe une porte spéciale pour l'accès en fauteuil roulant, les personnes responsables du site ou des installations ajoutent cette porte d'accès en fauteuil roulant à un secteur spécifique, qu'ils ajoutent ensuite à la liste des secteurs accordés aux visiteurs demandant une assistance ADA. Si un visiteur s'inscrit en activant ADA, ClearID lui accordera à lui seul l'accès à cette porte.

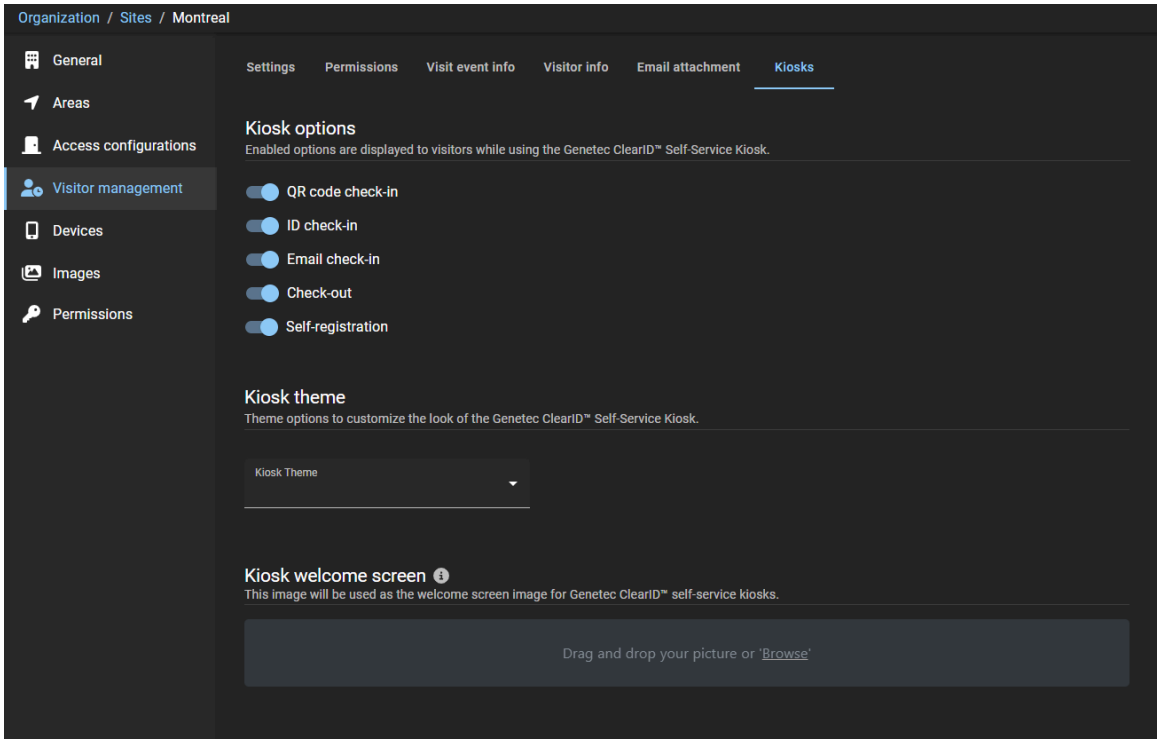
d) (Facultatif) Cliquez sur ✕ pour supprimer les champs de visiteurs qui ne sont plus nécessaires.

8 Cliquez sur l'onglet **Pièce jointe d'e-mail** et configurez les options nécessaires :



- **PDF d'instructions :** Ce fichier d'instructions vous permet d'inclure automatiquement un fichier PDF d'instructions de visite dans les communications par e-mail avec les visiteurs. Par exemple, les détails de l'emplacement, le plan du site, les itinéraires d'accès, etc. Quel que soit le nom du fichier chargé, le fichier d'instructions téléchargeable est enregistré en tant que *VisitInstructionsFile.pdf*.
  - **Aucun PDF téléchargé. :** Indique qu'aucun PDF d'instructions n'a encore été téléchargé.
  - **VisitInstructionsFile.pdf :** Cliquez pour télécharger une copie du fichier *VisitInstructionsFile.pdf*.
    REMARQUE : Ce bouton est uniquement visible et actif après le téléchargement d'un PDF d'instructions.
  - **Charger :** Cliquez pour télécharger un fichier PDF d'instructions.
    BONNE PRATIQUE : Si votre fichier d'instructions est un document Word, cliquez sur **Enregistrer au format Adobe PDF** avant de le charger pour vous assurer que les visiteurs ne peuvent pas modifier la procédure.
  - **Supprimer :** Cliquez sur cette option pour supprimer un fichier PDF d'instructions de visite des communications électroniques avec les visiteurs.

9 Dans l'onglet **Bornes**, personnalisez les options de configuration.

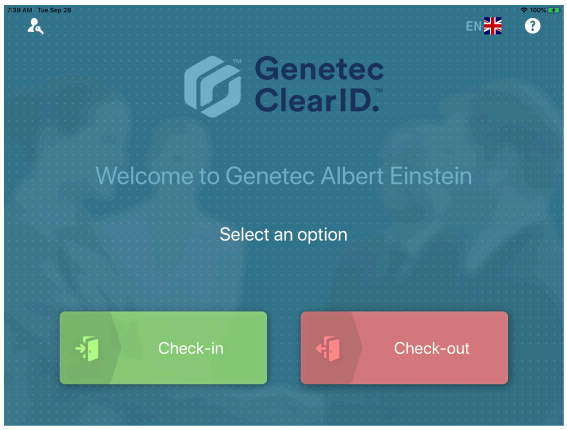


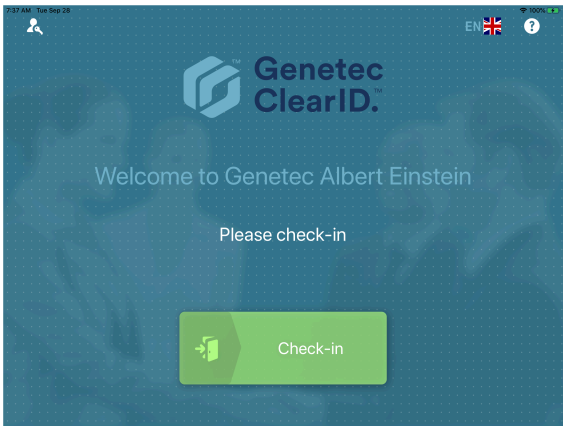
10 (Facultatif) Personnalisez les **Options de la borne**.

Ces options permettent de personnaliser les choix affichés pour les visiteurs dans ClearID Self-Service Kiosk durant le processus d'inscription ou de radiation.

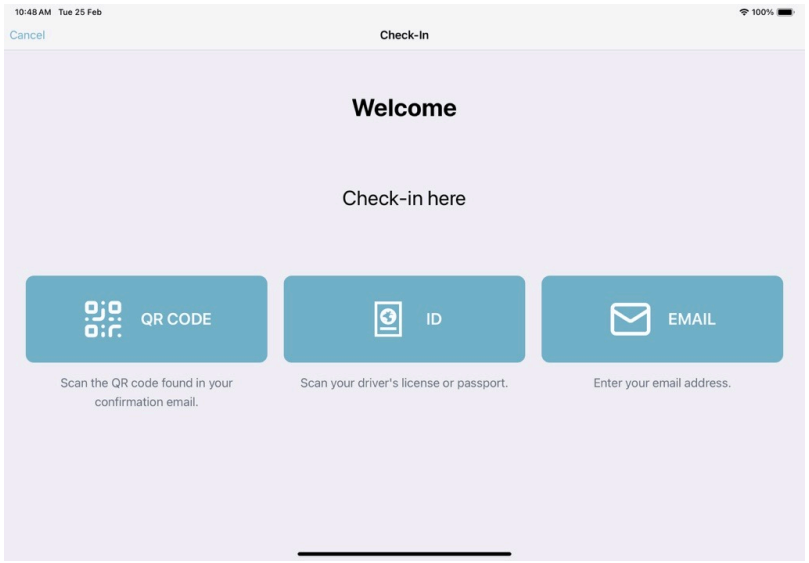
REMARQUE : L'option d'auto-inscription n'est affichée que si toutes les autres options d'inscription ne sont pas applicables.

L'exemple suivant montre l'écran d'inscription ou de radiation personnalisé pour deux scénarios différents.

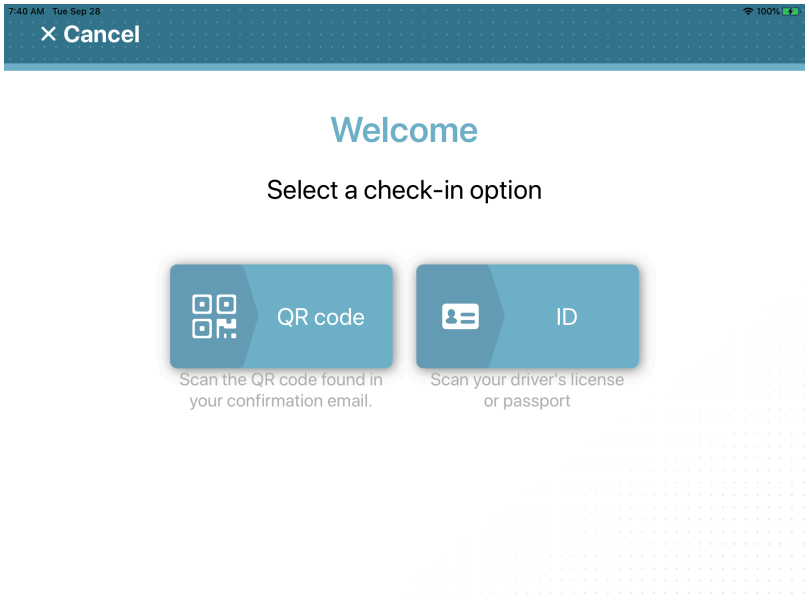




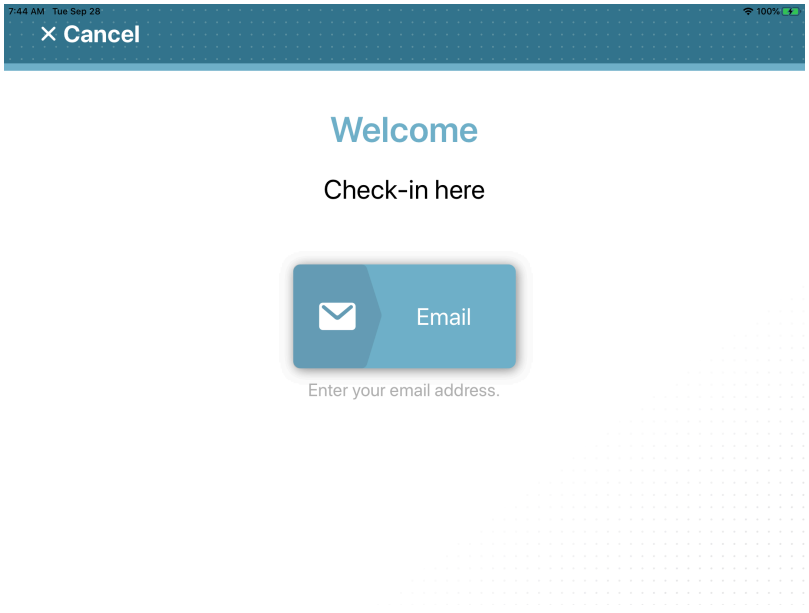
L'exemple suivant montre les **Options de borne** personnalisées avec les options d'inscription par **Code QR**, par **ID** et par **E-mail** activées.



L'exemple suivant montre les **Options de borne** personnalisées avec les options d'inscription par **Code QR** et par **ID** activées.



L’exemple suivant montre les **Options de borne** personnalisées seulement avec l'option d'inscription par **E-mail** activée.

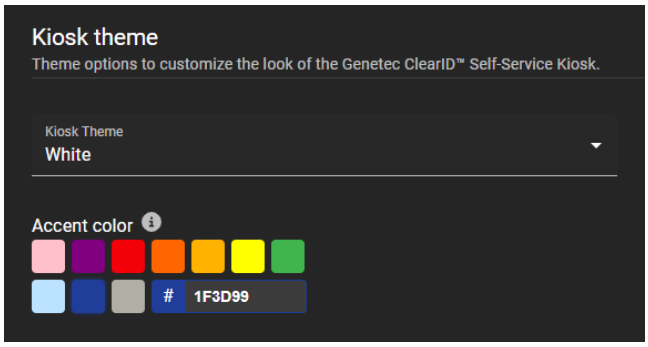


11 (Facultatif) Personnalisez le **Thème de la borne**.

a) Dans la section *Thème de la borne*, sélectionnez un thème parmi les suivants :

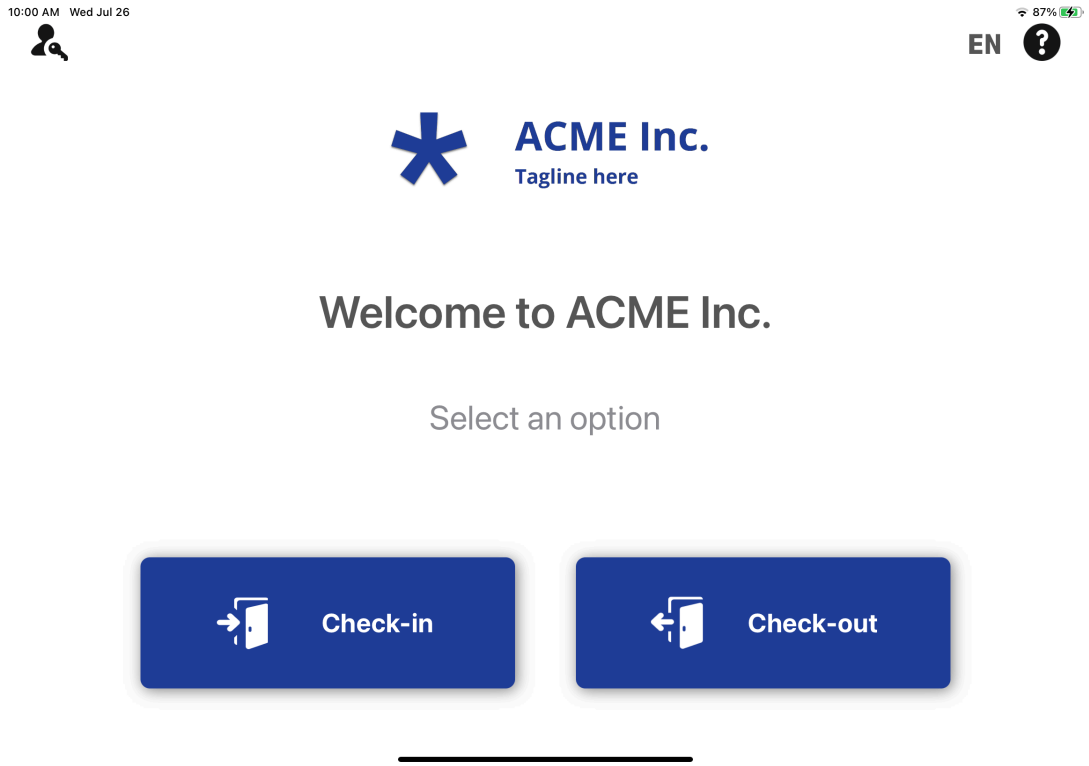
- **ClearID :** Le thème ClearID (code couleur HEX 35768D) n'a pas de couleur d'accentuation.
- **Blanc :** Le thème blanc propose des options supplémentaires pour choisir une couleur d'accentuation. Par exemple, pour suivre la charte graphique de votre organisation.

b) Si vous sélectionnez le thème de borne **Blanc**, sélectionnez une couleur d'accentuation.

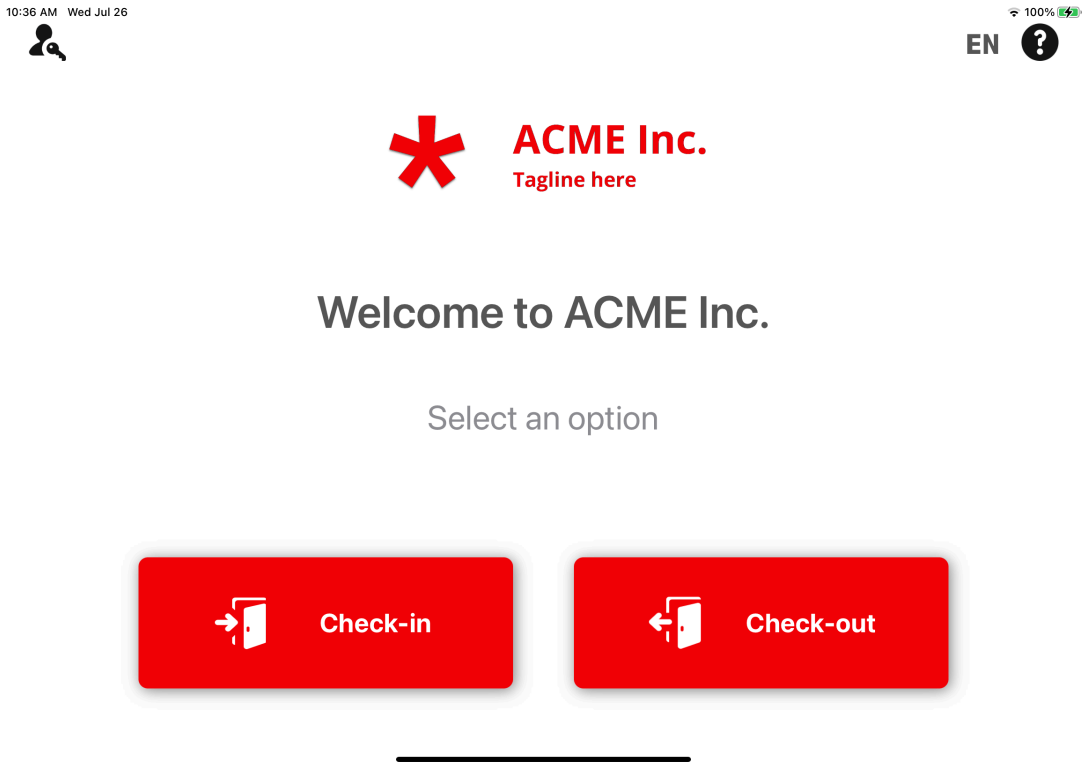


La couleur d'accentuation est appliquée aux boutons affichés dans ClearID Self-Service Kiosk.

L'exemple suivant montre le thème blanc avec la couleur d'accentuation bleue qui correspond au bleu de la charte de l'entreprise utilisée dans l'exemple.



L'exemple suivant montre le thème blanc avec la couleur d'accentuation rouge qui correspond au rouge de la charte de l'entreprise utilisée dans l'exemple.

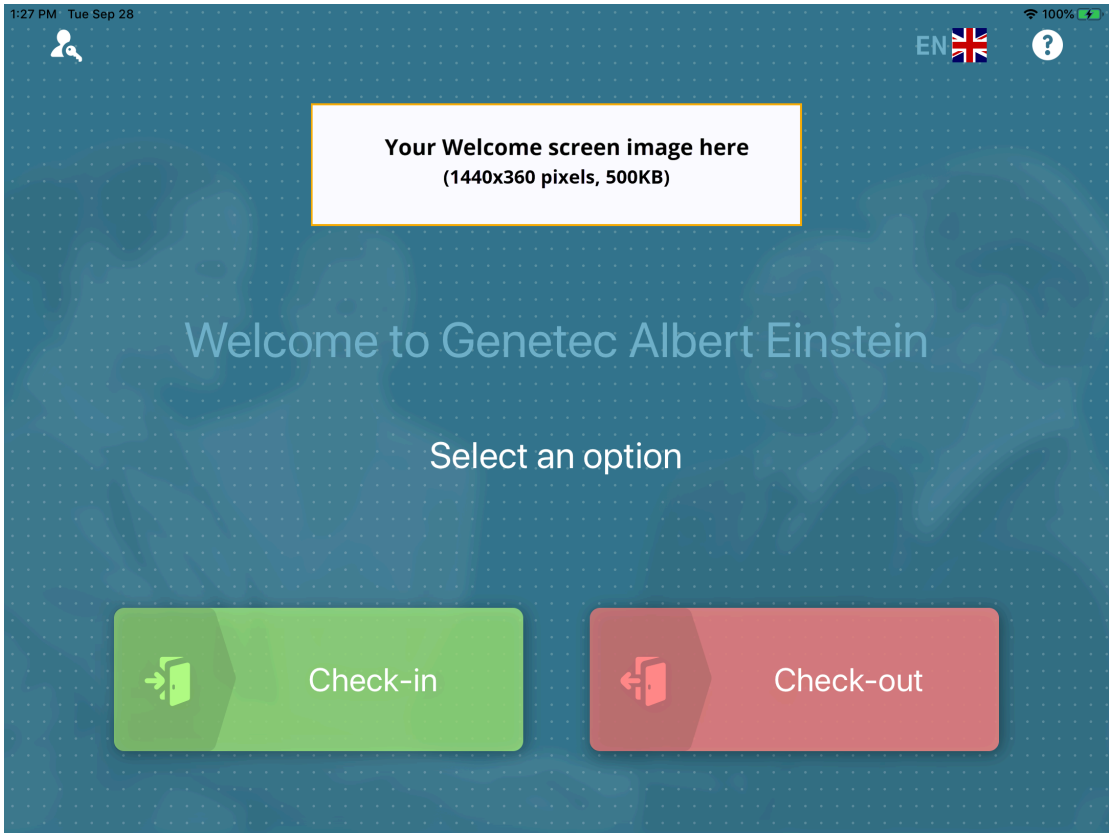

10:36 AM Wed Jul 26
100%
EN
ACME Inc.
Tagline here
Welcome to ACME Inc.
Select an option
Check-in
Check-out

12 (Facultatif) Personnalisez l'**Écran de bienvenue de la borne**.

a) Dans la section *Écran de bienvenue de la borne*, faites un glisser-déposer de votre image ou parcourez vos fichiers pour sélectionner une image d'**Écran de bienvenue de la borne**.

Cette image est utilisée pour le *nom de la société* ou le *logo* de l'écran de bienvenue de la borne.

Voici un exemple d'écran de bienvenue avec un logo personnalisé.



13 Cliquez sur **Enregistrer**.

REMARQUE : Les modifications des options sont synchronisées avec la borne toutes les 60 secondes.

La gestion des visiteurs est activée pour le site.

Lorsque vous avez terminé

Soumettre une demande d'accès ou de visite pour ce site.

Rubriques connexes

Présentation d'ADA

Fichier d'instructions pour les visiteurs (fichier PDF d'exemple)

À propos des processus, page 12

Inviter des visiteurs, page 373

Inscription sur une borne en libre-service, page 579

Activer les identifiants code QR pour les visiteurs, page 401

Afficher les sites où un utilisateur peut inviter des visiteurs

Un administrateur de comptes peut vouloir consulter la liste des sites où un utilisateur est autorisé à inviter des visiteurs, à des fins de vérification ou de mise à jour des accès.

Avant de commencer

- Configurez vos réglages de gestion des visiteurs.
- Ajoutez les membres au rôle.

À savoir

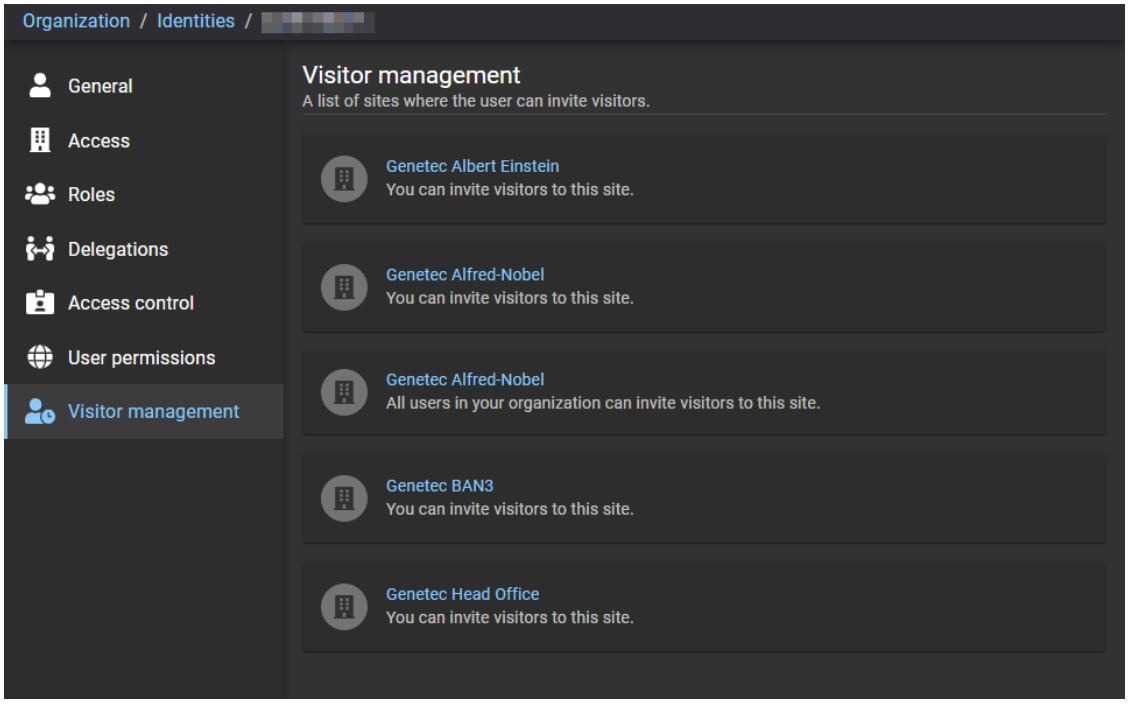
- Seuls les administrateurs de comptes peuvent afficher la liste des sites où un utilisateur peut inviter des visiteurs, ou accorder l'autorisation aux utilisateurs d'inviter des visiteurs à l'aide de rôles.
- Par défaut, les utilisateurs bénéficient automatiquement des autorisations *Inviter des visiteurs* pour leur site d'origine.

Procédure

1 Sur la page *d'accueil*, cliquez sur **Organisation** > **Identités**.

2 Recherchez ou sélectionnez un utilisateur.

3 Cliquez sur **Gestion des visiteurs** pour afficher la liste des sites où un utilisateur peut inviter des visiteurs.



Rubriques connexes

Accorder l'accès au portail Web, page 146

Modifier les sites

Une fois vos sites ajoutés, vous pouvez modifier les paramètres de chaque site individuellement. Un *Administrateur de compte* ou un *Propriétaire de site* peut modifier les *propriétaires de sites*, et modifier les options de gestion des visiteurs pour le site.

Avant de commencer

Créez vos sites.

À savoir

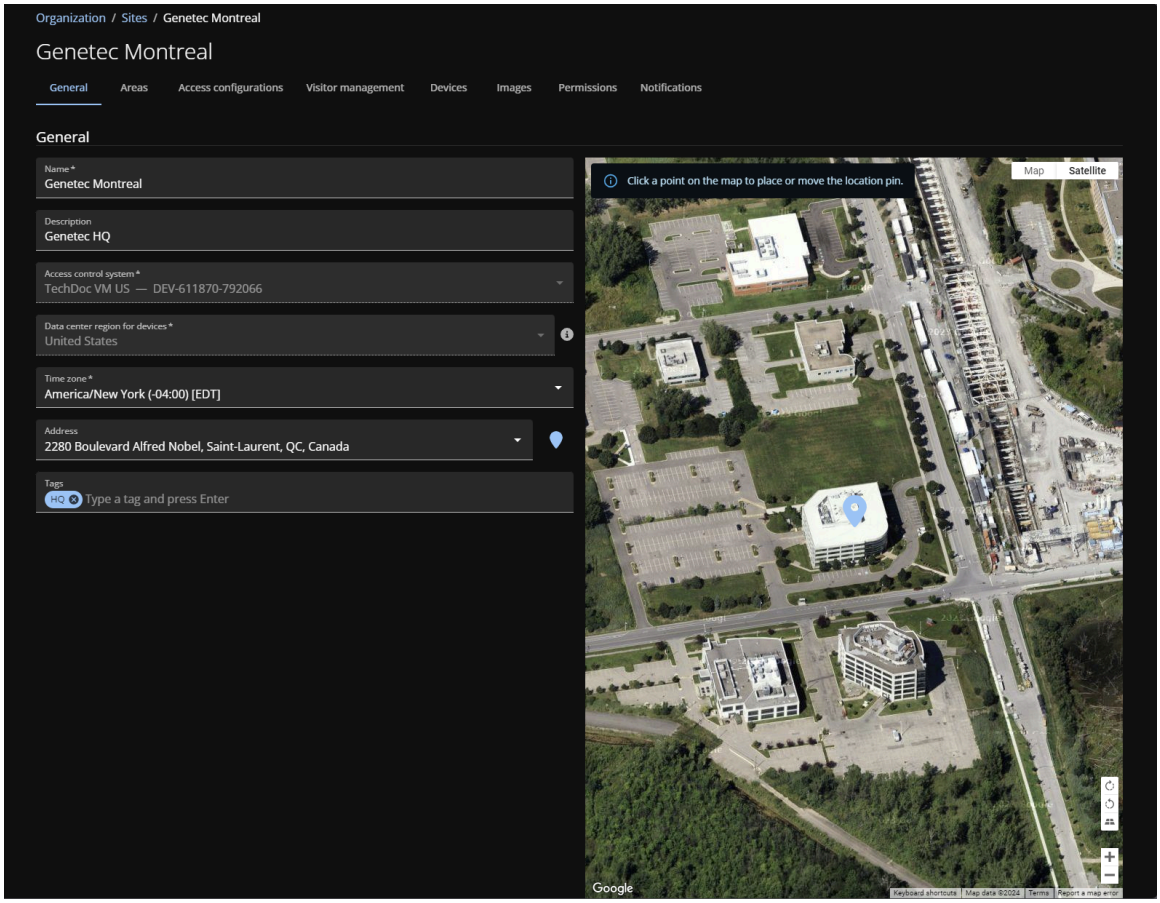
Pour modifier des sites dans Genetec ClearID[MC], vous devez être un *Administrateur de compte* ou un *Propriétaire de site*.

- Un *site* est associé à un système de contrôle d'accès Security Center.
- Plusieurs sites peuvent être associés à un même système de contrôle d'accès Security Center.

Procédure

1 Cliquez sur **Organisation** > **Sites**.

2 Recherchez un site à l'aide du champ de recherche ou sélectionnez un site dans la liste **Site**.



3 Sur la page *Général*, modifiez les champs selon vos besoins.

4 Sur la page *Notifications*, modifiez les champs selon vos besoins.

5 Cliquez sur **Enregistrer**.

Les paramètres de votre site ont été modifiés.

Rubriques connexes

Création de sites, page 252

Définir la durée maximale d'accès à un site

Pour appliquer une limite aux identités ayant un accès temporaire, vous pouvez fixer une durée d'accès au site. Lorsque la durée maximale est atteinte, l'accès prend fin.

À savoir

Si l'option de durée maximale d'accès à un site est activée dans votre compte, cette durée maximale est activée par défaut.

- Pour définir la durée maximale d'accès à un site dans Genetec ClearID[MC], vous devez être un propriétaire du site.
- Ce délai d'accès ne s'applique qu'aux identités individuelles ou aux accès accordés manuellement.
- Ce délai d'accès ne s'applique pas aux accès des rôles.

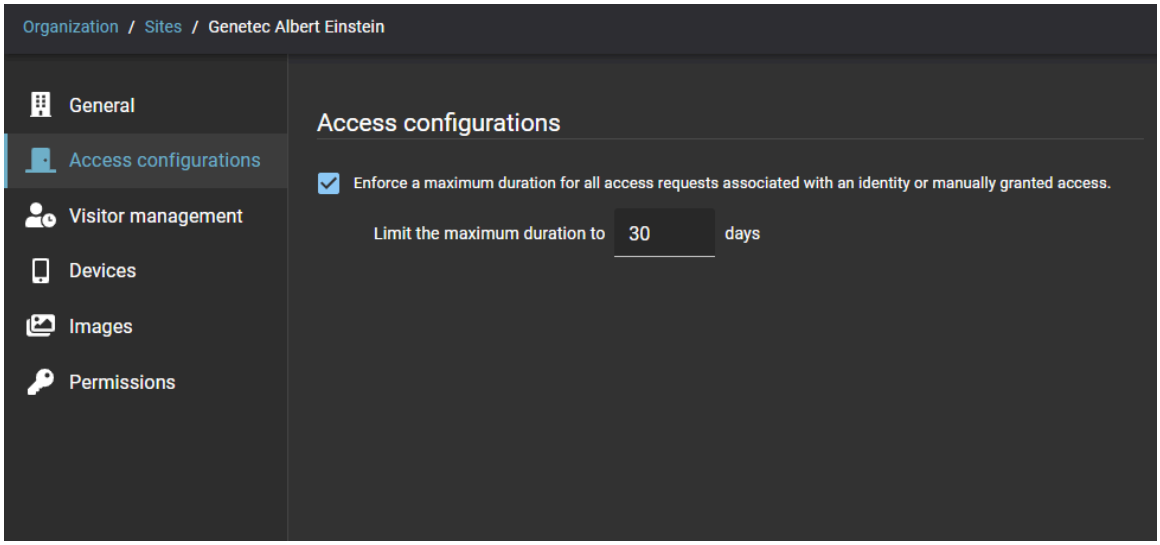
CONSEIL : Utilisez des groupes de rôles si des personnes doivent disposer d'un accès permanent à un site.

Procédure

1 Cliquez sur **Organisation** > **Sites**.

2 Recherchez et sélectionnez un site.

3 Cliquez sur **Configurations d'accès**.



a) Cochez la case **Appliquer une durée maximale pour toutes les demandes d'accès liées à une identité ou un accès accordé manuellement**.

b) Dans le champ **Limiter la durée maximale à**, entrez la durée maximale en jours.

Vous pouvez saisir une valeur en jours de 1 à 365. La valeur par défaut est de 30 jours.

Rubriques connexes

Ajouter des rôles, page 472
Ajouter des membres aux rôles, page 484
Demander un accès, page 156

Configurer les documents de demande d'accès pour les sites

Pour les sites soumis à des mesures ou des exigences de sécurité supplémentaires, les *propriétaires de sites* peuvent obliger les employés à charger des justificatifs tels que des copies de permis de conduire ou de certifications lorsqu'ils demandent l'accès à des secteurs.

Avant de commencer

Familiarisez-vous avec les workflows de demande d'accès.

À savoir

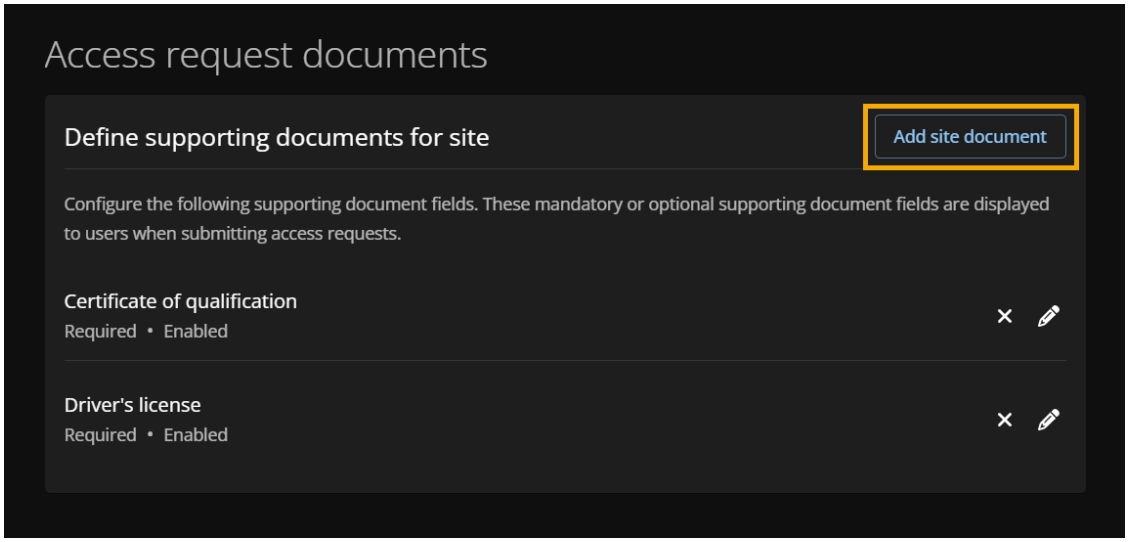
- Vous devez être un *propriétaire du site* pour configurer des justificatifs obligatoires ou facultatifs pour les demandes d'accès au niveau du site.
- Vous pouvez configurer jusqu'à 20 types de justificatifs par site.

IMPORTANT : Tous les secteurs héritent des justificatifs configurés au niveau du site. Le cas échéant, les propriétaires de site peuvent supprimer les configurations de justificatifs au niveau du site d'un secteur en accédant aux paramètres de demande d'accès à un secteur.

Procédure

1 Sur le portail web Genetec ClearID[MC], cliquez sur **Organisation** > **Site** > **Configurations d'accès**.

2 Sous *Définir des justificatifs pour le site*, cliquez sur **Ajouter un document de site**.



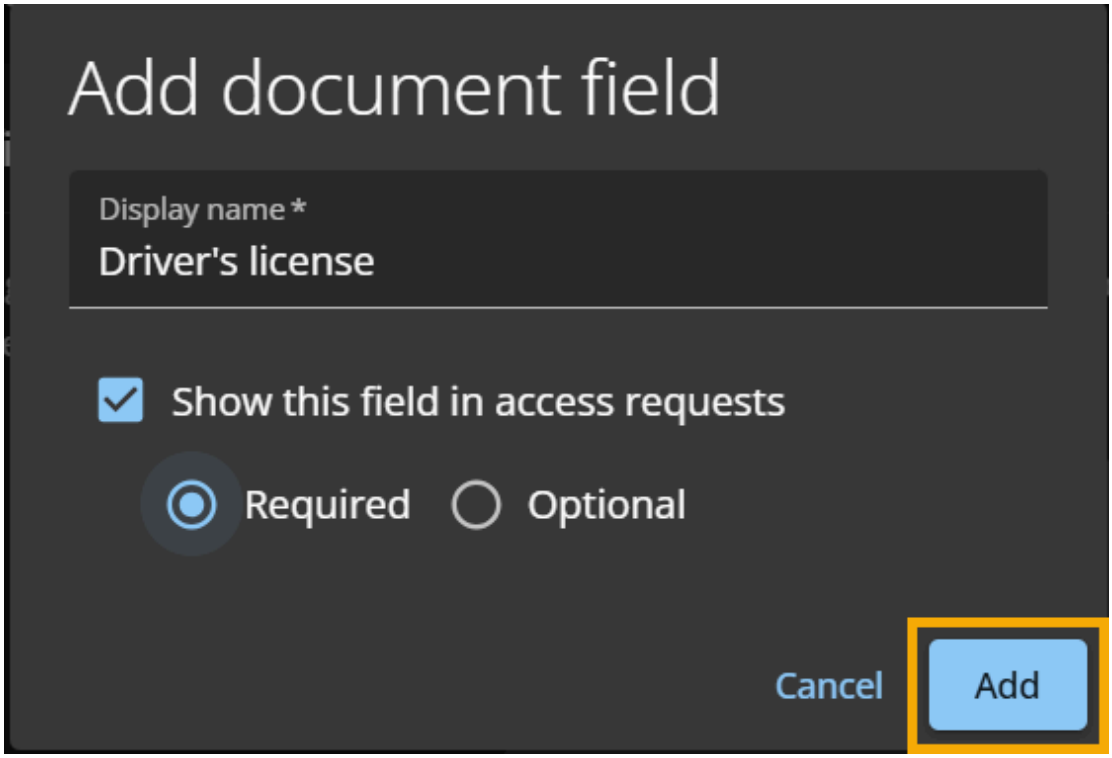
a) Dans le champ *Nom d'affichage*, saisissez un nom pour le type de document.

b) Sélectionnez **Afficher ce champ dans les demandes d'accès** pour afficher le champ de document dans les demandes d'accès au site.

CONSEIL : Lorsque cette case est décochée, le type de document reste disponible en mode brouillon.

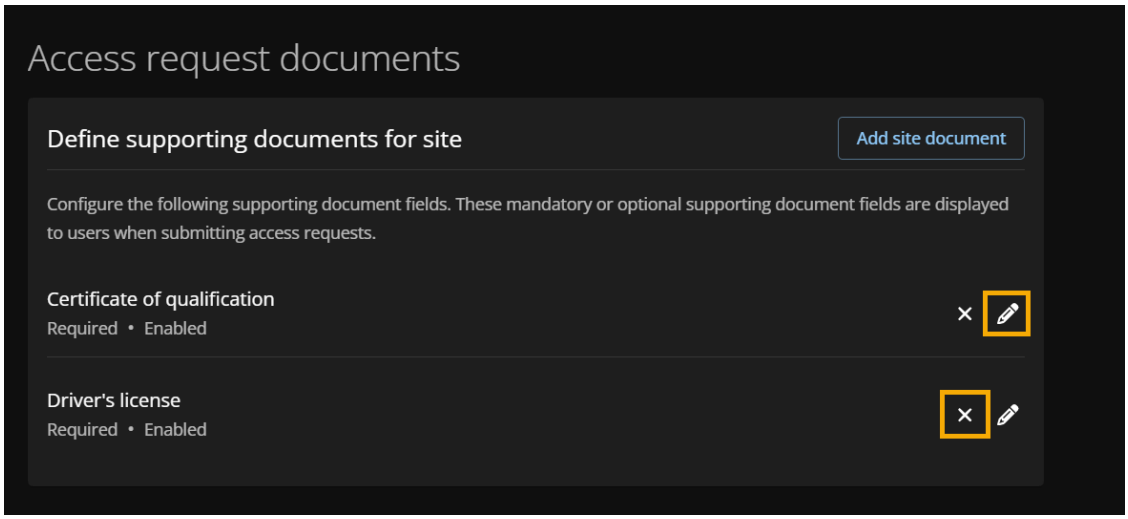
c) Indiquez si le chargement du document est obligatoire lors de la soumission d'une demande d'accès en cliquant sur le bouton radio **Obligatoire** ou **Facultatif**.

REMARQUE : Vous pouvez configurer une combinaison de types de documents obligatoires et facultatifs pour qu'ils apparaissent dans une seule demande d'accès.



3 Cliquez sur **Ajouter**.

4 (Facultatif) Vous pouvez modifier ou supprimer chaque type de document :



a) Cliquez sur pour modifier la configuration d'un justificatif.

b) Cliquez sur pour supprimer un justificatif configuré.

Personnaliser les notifications par e-mail pour un site

Pour communiquer des exigences particulières aux destinataires des e-mails, les *administrateurs de comptes* et les *propriétaires de sites* peuvent personnaliser le texte qui figure dans l'en-tête et le pied de page des e-mails de notification envoyés par Genetec ClearID[MC].

À savoir

Vous pouvez personnaliser le texte d'en-tête et de pied de page pour deux types d'e-mails de notification :

- Notifications d'accès accordé
- Notifications de confirmation de visite

Procédure

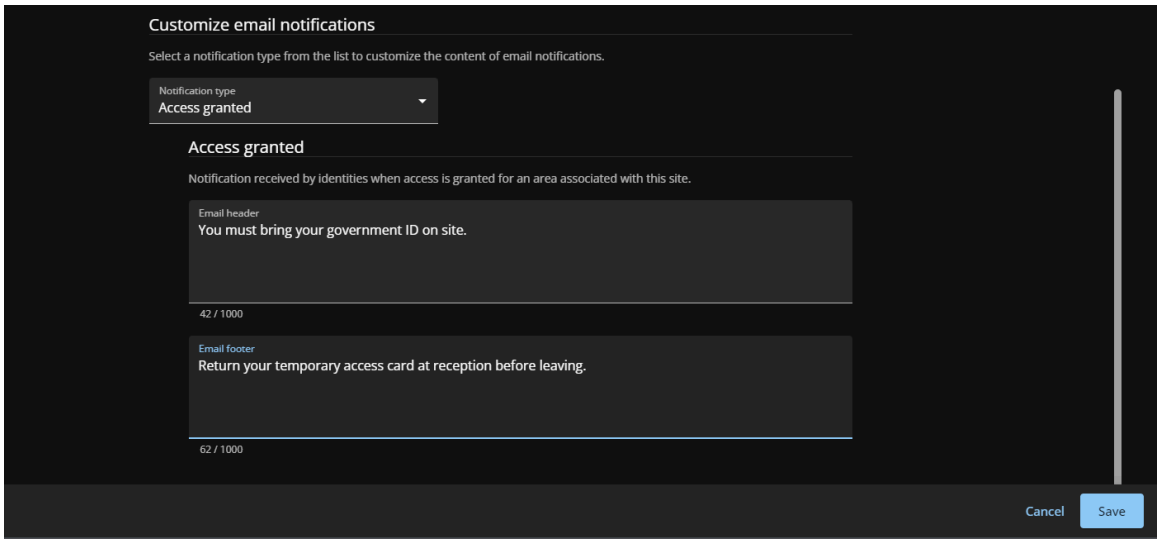
1 Cliquez sur **Organisation** > **Sites** > **Notifications**.

2 Dans la liste **Type de notification** de la section *Personnaliser les notifications par e-mail*, sélectionnez le type d'e-mail que vous souhaitez personnaliser.

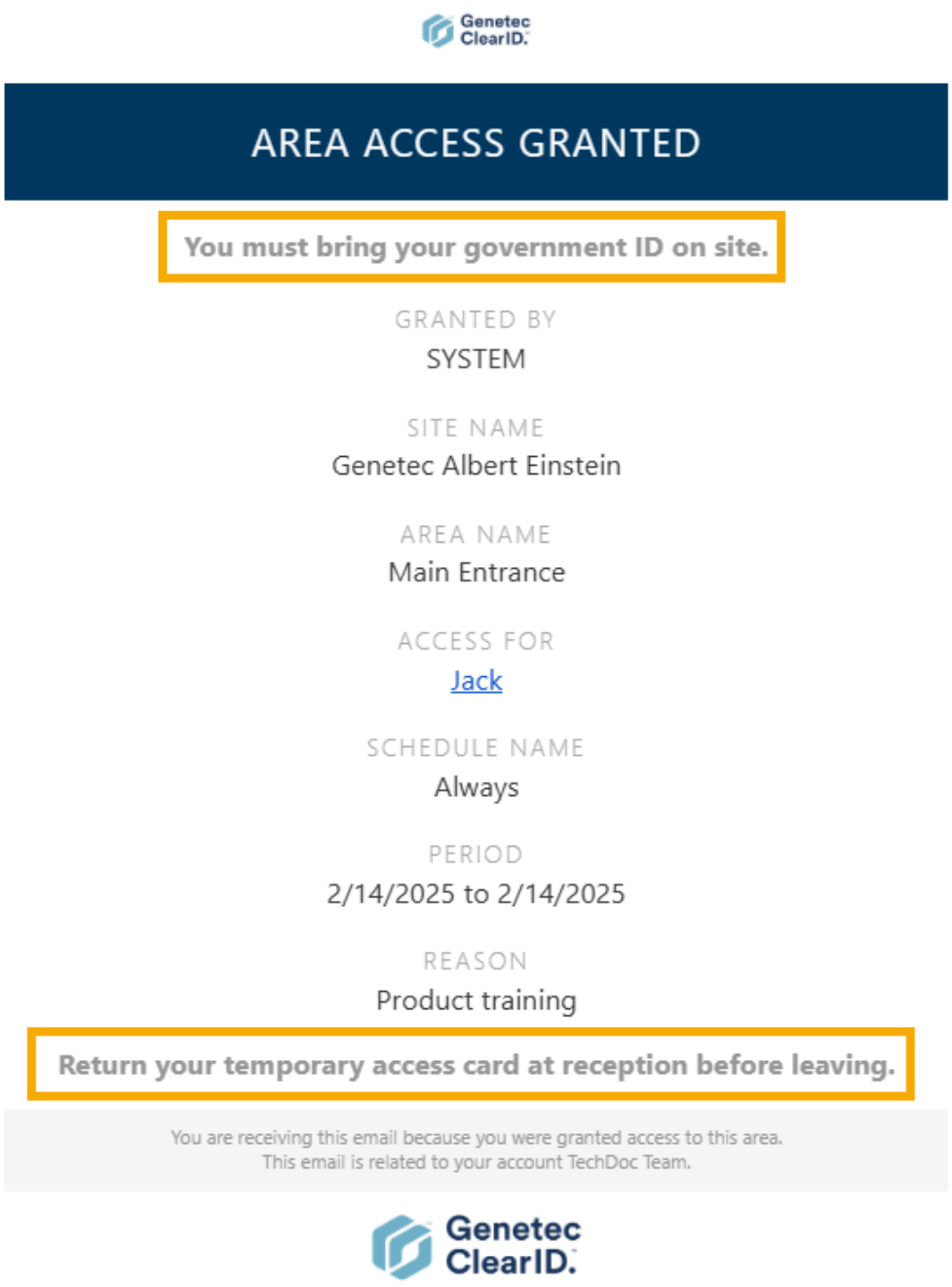
   a) Tapez votre texte dans le champ **En-tête d'e-mail**. Vous pouvez par exemple utiliser les champs texte personnalisés pour indiquer le matériel ou les documents exigés de la part des visiteurs, ou les étapes à suivre avant d'accéder à un secteur.

   b) Tapez votre texte dans le champ **Pied de page d'e-mail**.

   REMARQUE : Le texte dans l'en-tête et le pied de page des e-mails de notification est limité à 1 000 caractères.



3 Cliquez sur **Enregistrer**.
Les notifications par e-mail envoyées par ClearID utilisent votre texte personnalisé dans l'en-tête et le pied de page.



Personnaliser l’apparence des notifications par e-mail

En tant qu’*administrateur de compte*, vous pouvez personnaliser les couleurs des e-mails de notification Genetec ClearID[MC] pour qu’elles respectent la charte graphique de votre entreprise.

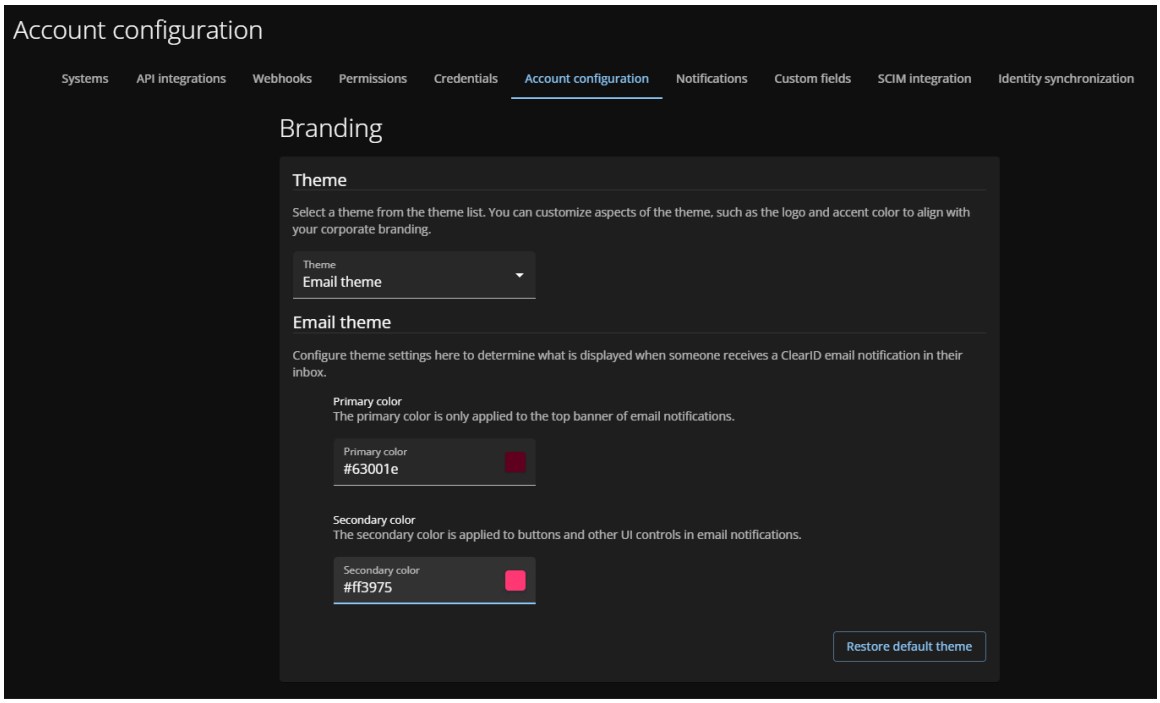
À savoir

Vous devez être *administrateur de compte* pour personnaliser l’aspect des notifications par e-mail.

Procédure

1 Sur le portail web ClearID, cliquez sur **Administration** > **Configuration du compte**.

2 Dans la section *Apparence*, sélectionnez **Thème de l’e-mail** dans la liste **Thème**.



3 Dans la section *Thème de l’e-mail*, configurez les couleurs des notifications par e-mail :

a) Dans le champ **Couleur principale**, utilisez le sélecteur de couleur pour choisir la couleur de la bannière supérieure des notifications par e-mail.

b) Dans le champ **Couleur secondaire**, utilisez le sélecteur de couleur pour choisir la couleur des boutons et des autres éléments d'interface des notifications par e-mail.

CONSEIL : Vous pouvez rétablir les couleurs par défaut du thème en cliquant sur le bouton **Restaurer le thème par défaut**.

4 Cliquez sur **Enregistrer**.

L’habillage personnalisé est appliqué à la bannière supérieure, aux boutons et aux éléments d'interface des notifications envoyées par e-mail par ClearID.

VISIT NAME

Channel Partner Event

See visit details

REQUESTER

HOSTS

SITE

Genetec Albert Einstein

Rue Albert Einstein, Saint-Laurent, QC, Canada

AREAS

Main Entrance

PERIOD

2/14/2025 5:00 PM to 2/14/2025 7:00 PM

APPROVED BY

Automatically approved by policy

You are receiving this email because you were added as a host or requester for this visit. If you want to change the event information, contact the requester.

Manage your email notification preferences in ClearID.

This email is related to your account TechDoc Team.

Genetec ClearID.

©2025 Genetec Inc. All rights reserved. | Privacy Policy | Terms of Service

À propos des examens d'accès

Un examen d’accès est le processus qui consiste à vérifier que l’accès à un secteur, un rôle ou une identité est toujours nécessaire et valable. Pour assurer le respect des règles de sécurité et la préparation aux audits, vous pouvez programmer l’exécution automatique de vos examens d'accès.

Généralement, le personnel de sécurité exporte manuellement une liste d'accès et l’envoie aux propriétaires de secteurs tous les semestres ou tous les trimestres.

Dans Genetec ClearID[MC], ces examens d'accès peuvent être programmés (automatisés) ou lancés manuellement. Il incombe à un responsable ou propriétaire de site de configurer la fréquence des examens d'accès, ou de lancer les examens manuellement afin d'assurer qu’ils soient effectués dans les temps.

- **Propriétaires de sites :** Les examens d'accès sont affichés dans le **Rapport d’examen d'accès**.
- **Approbateurs de secteurs ou responsables de rôles :** les examens d’accès aux secteurs sont affichés dans **Mes tâches** et les e-mails de notification.
- **Superviseurs :** Les examens d’accès d’identité sont affichées dans **Mes tâches** et les e-mails de notification.

REMARQUE : Seuls les propriétaires de site peuvent accéder aux **rapports d’examen d’accès**. Les approbateurs de secteur peuvent uniquement accéder aux secteurs pour lesquels ils sont approbateurs. Les superviseurs peuvent uniquement accéder aux examens pour leurs subordonnés directs.

Vous ne pouvez pas planifier un examen pour un site qui n’a pas de secteurs. Si un rôle ou un groupe est associé à un secteur ou une salle, le rôle ou le groupe est automatiquement intégré à l’examen du secteur. Tous les examens en état **Terminé** sont conservés à des fins d’audit et de suivi.

Examens d'accès planifiés

Vous pouvez planifier les examens d’accès d’un site afin qu’ils soient effectués tous les ans, tous les mois, toutes les semaines ou maintenant en fonction de vos besoins.

- Un examen d’accès du site pour un secteur de *Salle de serveurs* peut être planifié **Tous les ans**. Par exemple, à intervalles trimestriels, le premier jour du mois à 08:00.
- Un examen d’accès du site pour un secteur de *Centre de données* peut être planifié **Tous les mois**. Par exemple, le premier jour de chaque mois à 08:00.

Examens d'accès manuels

En cas de besoin, pour assurer le respect de règles de sécurité et en amont d’un audit, vous pouvez lancer un examen d’accès manuellement à l’aide de l’horaire **Maintenant**. Les examens d’accès manuels sont généralement utilisés pour tester les examens dans le but de préparer un examen annuel ou planifié, afin de vérifier que tous les participants sont correctement définis, ou pour forcer un examen à la suite d'un incident.

E-mails de notification d'examen accès

Les e-mails de notification d'examen d’accès sont envoyés aux approbateurs pertinents pour leur indiquer qu'un examen d'accès de secteur ou de rôle est en attente. Les propriétaires de sites ne reçoivent pas de notifications par e-mail.

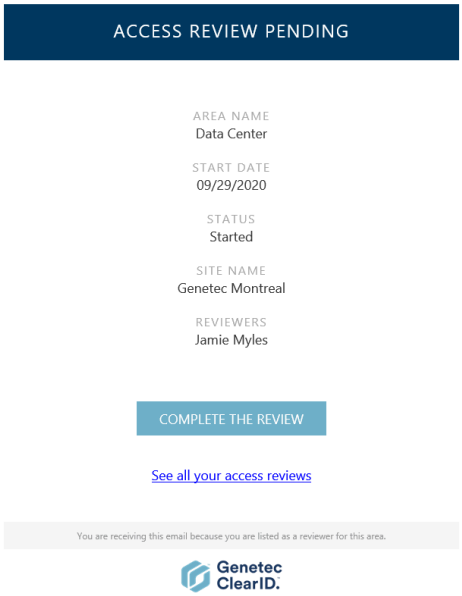


Illustration 3 : E-mail de notification d'examen d’accès en attente

- Lorsque vous cliquez sur le lien **TERMINER L’EXAMEN**, l’examen d'accès détaillé dans l’e-mail est affiché pour examen.
- Lorsqu'un approbateur de secteur ou un responsable de rôle clique sur l'hyperlien **Afficher toutes les analyses d'accès**, la page **Mes analyses d'accès** est affichée. Cette vue n’affiche que les examens d'accès qui concernent l’approbateur.

Des e-mails de rappel sont envoyés tous les 7 jours. Les e-mails de notification d'examen d’accès sont envoyés par *noreply@clearid.io*. Consultez votre dossier de courriers indésirables si vous ne recevez pas les notifications.

L’état des examens d’accès incomplets est automatiquement mis à jour sur l’état **Expiré** lorsque l’examen d’accès incomplet est remplacé par un examen planifié plus récent qui porte le même nom ou lorsque l’option **Appliquer une expiration pour les examens d’accès** est activée et que la période d’activation est dépassée.

Tous les examens en état **Terminé** sont conservés à des fins d’audit et de suivi. Vous ne pouvez pas modifier un examen d'accès terminé.

Rubriques connexes

Note sur la fonction d’examen d’accès (2 pages)

Configuration de l’expiration automatique pour les examens d’accès

Pour vous assurer que les examinateurs n’examinent que les informations d'accès actuelles, vous pouvez spécifier une période d'expiration pour les examens d'accès. Si vous ne définissez pas d'expiration, les examinateurs pourraient consulter les informations obsolètes.

Avant de commencer

En savoir plus sur les examens d'accès.

À savoir

Seul un administrateur de compte peut configurer les paramètres d'expiration pour les examens d'accès.

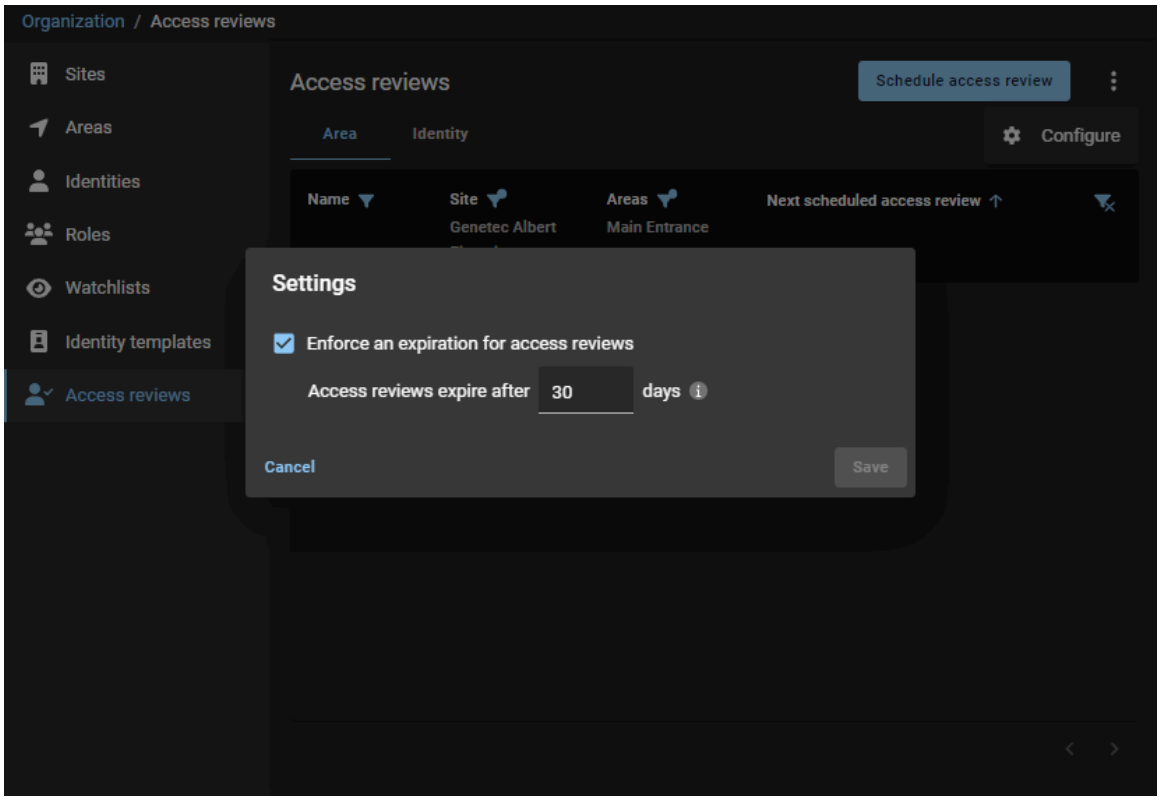
BONNE PRATIQUE : Le paramètre d'expiration des examens d'accès est activé par défaut et la période d'expiration par défaut est définie sur 30 jours.

- La période d’expiration définie pour les examens d’accès s’applique à tous les examens d’accès du système.
- Le nouveau paramètre d'expiration ne s’applique qu’aux examens d'accès créés après l’activation ou la modification du paramètre.
- Lorsque les examens d'accès expirent, leur état est réglé sur Expiré.
  - Les examens d'accès affichés dans **Mes tâches** sont alors définis sur Terminé avec le statut Expiré.

Procédure

1 Sur la page d’accueil, cliquez sur **Organisation** > **Examens d’accès**.

2 Cliquez sur ⋮, puis cliquez sur **Configurer**.



3 Dans la boîte de dialogue *Paramètres*, sélectionnez ou entrez la période d'expiration requise pour votre organisation.

CONSEIL : Choisissez un intervalle d'expiration qui correspond aux exigences d'examen d'accès de votre entreprise. Gardez également à l'esprit toutes les exigences légales ou d'audit qui pourraient s'appliquer.

4 (Facultatif) Si votre organisation ne souhaite pas appliquer d'expiration pour les examens d'accès, décochez la case **Appliquer une expiration pour les examens d'accès**.

5 Cliquez sur **Enregistrer** pour confirmer vos modifications.

Lorsque vous avez terminé

Configurez vos examens d'accès.

Configurer les examens d'accès à un secteur

Pour assurer le respect des règles de sécurité et la préparation aux audits, vous pouvez planifier les examens d'accès de secteur afin qu'ils aient lieu à intervalles réguliers. Vous pouvez également démarrer un examen d'accès de secteur manuellement en cas de besoin.

Avant de commencer

- Vérifiez que des secteurs ont été définis pour le site.
- Vérifiez que le site ne fait pas déjà partie d'un autre examen.

À savoir

- Seul un propriétaire de site peut configurer les examens d'accès de secteur.

BONNE PRATIQUE : Programmez vos examens d'accès du site afin qu'ils soient déclenchés automatiquement le jour, la semaine ou le moins précédant un audit ou un contrôle de sécurité, afin d'assurer votre conformité et votre préparation aux audits.

Procédure

- Sur le portail Web Genetec ClearID[MC], procédez de la manière suivante :
  - Planifier vos examens d'accès de secteur

Vos examens d'accès de secteur sont à présent configurés.

Lorsque vous avez terminé

Pour terminer vos examens d'accès de secteur le moment voulu, procédez de la manière suivante :

- Terminer un examen d'accès de secteur (propriétaire de site)
- Terminer un examen d'accès de secteur (propriétaire de secteur)

Rubriques connexes

Examiner les accès à un secteur, page 364
Note sur la fonction d'examen d'accès (2 pages)

Programmer les examens d'accès

Pour assurer le respect des règles de sécurité et la préparation aux audits, vous pouvez planifier les examens d'accès de secteur afin qu'ils aient lieu à intervalles réguliers.

Avant de commencer

- Vérifiez que des secteurs ont été définis pour le site.
- Vérifiez que le site ne fait pas déjà partie d'un autre examen.

À savoir

- Seul un propriétaire de site peut planifier les examens d'accès de secteur.
- Les propriétaires de sites peuvent définir un calendrier d'examen pour un ou plusieurs secteurs d'un site.

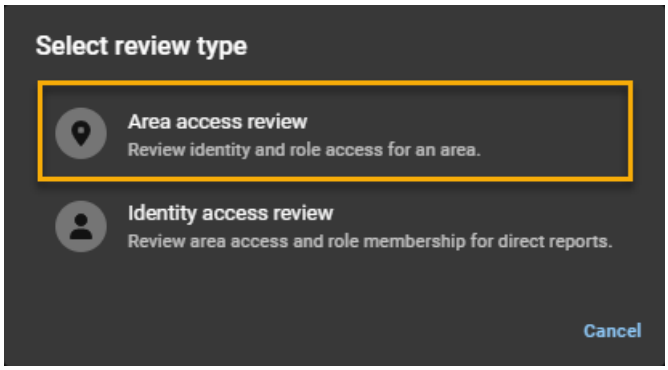
BONNE PRATIQUE : Programmez vos examens d'accès du site afin qu'ils soient déclenchés automatiquement le jour, la semaine ou le moins précédant un audit ou un contrôle de sécurité, afin d'assurer votre conformité et votre préparation aux audits.

Procédure

1 Sur la page d'accueil, cliquez sur **Organisation** > **Examens d'accès**.

2 Cliquez sur **Planifier un examen d'accès**.

3 Dans la boîte de dialogue **Sélectionner le type d'examen**, sélectionnez **Examen d'accès de secteur**.



4 Dans la boîte de dialogue *Horaire d'examen d'accès de site*, sélectionnez les options nécessaires.

a) Saisissez un Nom pour votre examen d'accès de secteur.

b) Sélectionnez la fréquence pour **Déclencher les examens de sites**, puis configurez les options.

REMARQUE : Les options affichées varient en fonction de la fréquence de **déclenchement des examens de site** que vous sélectionnez.

- **Tous les ans :** Spécifie un examen d'accès de site qui a lieu tous les ans.
- **Tous les mois :** Spécifie un examen d'accès de site qui a lieu tous les mois.
- **Toutes les semaines :** Spécifie un examen d'accès de site qui a lieu toutes les semaines.
- **Maintenant :** Spécifie un examen d'accès de site qui a lieu immédiatement.

Par exemple, un examen d'accès peut être lancé manuellement à l'aide de l'horaire *Maintenant*. Les examens d'accès manuels sont généralement utilisés pour tester les examens avant un examen

annuel ou planifié, afin de vérifier que tous les participants sont correctement définis, ou pour forcer un examen à la suite d'un incident.

c) Si vous avez sélectionné **Tous les ans**, sélectionnez le jour et le mois ou les mois auxquels vous souhaitez que l'examen d'accès de site soit planifié.

d) Si vous avez sélectionné **Tous les mois**, sélectionnez le jour auquel vous souhaitez que l'examen d'accès de site soit planifié.

e) Si vous avez sélectionné **Toutes les semaines**, sélectionnez le ou les jours auxquels vous souhaitez que l'examen d'accès de site soit planifié.

f) Sélectionnez l'heure à laquelle vous souhaitez que l'examen d'accès de site soit planifié.

REMARQUE : Les heures affichées dans les options de la boîte de dialogue *Horaires d'examen d'accès de site*, ainsi que tous les horaires d'examen planifiés, utilisent le fuseau horaire du site.

g) Recherchez ou sélectionnez le site que vous voulez inclure dans l'examen d'accès de site.

h) Recherchez ou sélectionnez les secteurs que vous voulez inclure dans l'examen d'accès de site.

i) (Facultatif) Dans le champ **Notes**, vous pouvez ajouter des informations supplémentaires si nécessaire.

Le champ **Notes** permet de saisir des informations plus détaillées sur l'examen d'accès de site. Il est généralement utilisé lorsque le site effectue une analyse de la sécurité. Par exemple, un examen IS0 27001 ou un rapport d'audit SOC 1 ou SOC 2.

Exemple: L'exemple suivant montre un examen d'accès de site pour un secteur *salle de serveurs* planifié pour avoir lieu **Tous les ans** à intervalles trimestriels, le premier du mois à 8 heures.

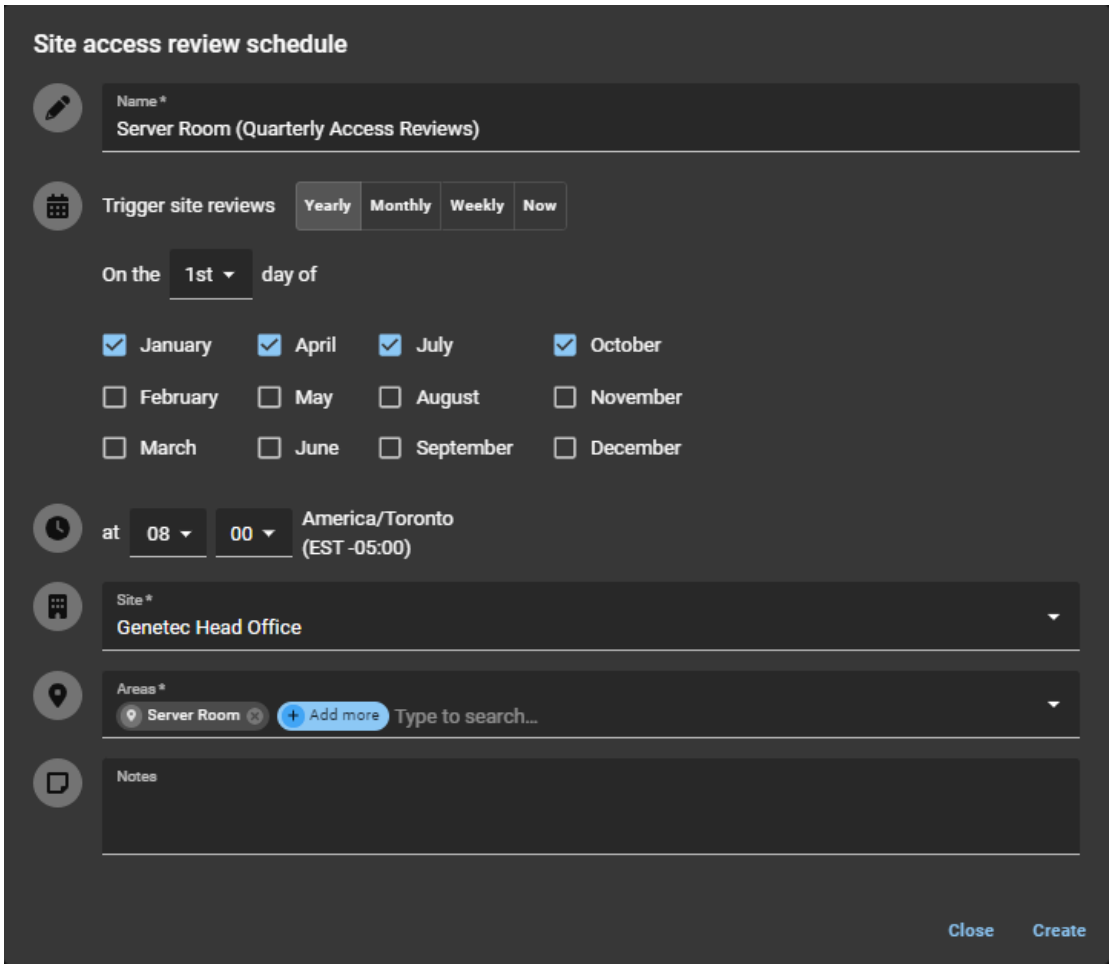


Illustration 4 : Salle de serveurs (examens d'accès trimestriels)

Exemple: L'exemple suivant montre un examen d'accès de site pour un secteur *Centre de données* planifié **Tous les mois**, le premier du mois à 8 heures.

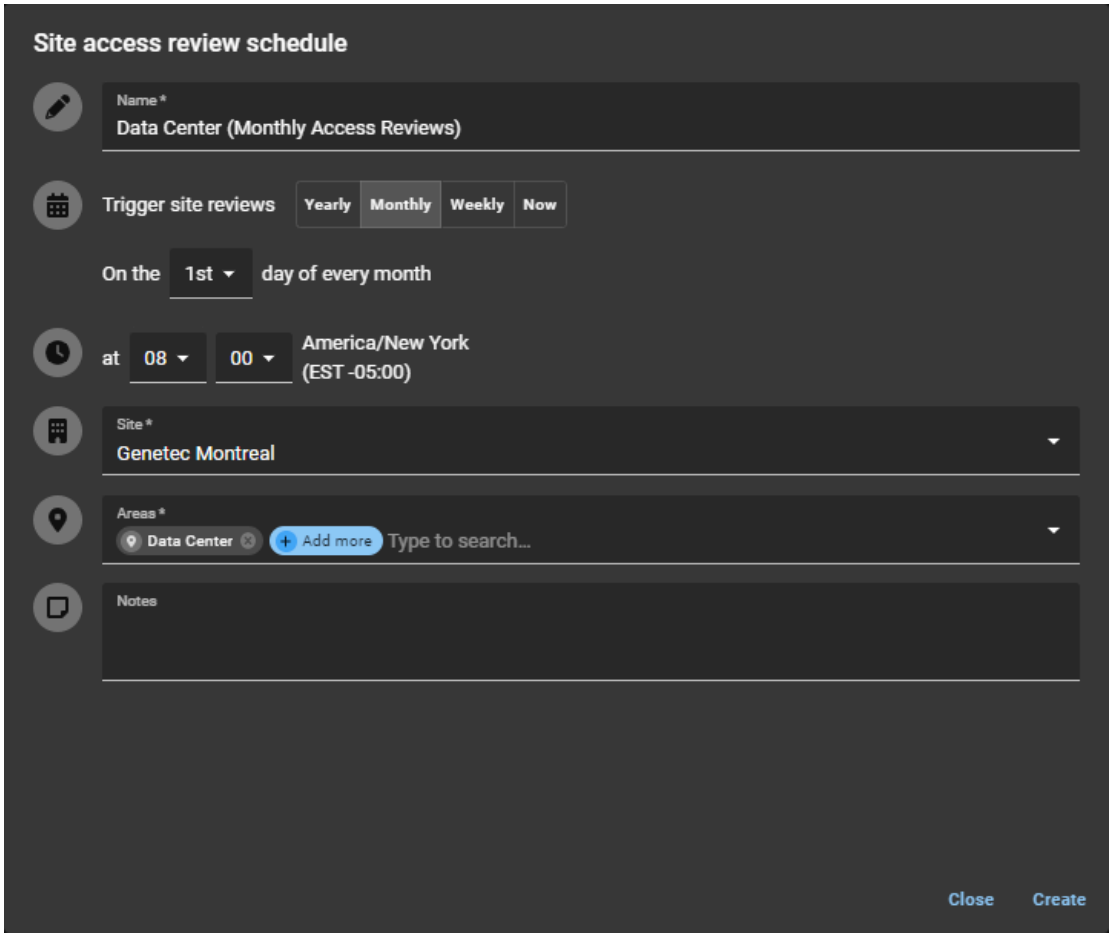


Illustration 5 : Centre de données (examens d'accès mensuels)

Exemple: L'exemple suivant montre un examen d'accès de site pour un secteur *centre de données* et *salle de serveurs* planifié pour **Maintenant**.

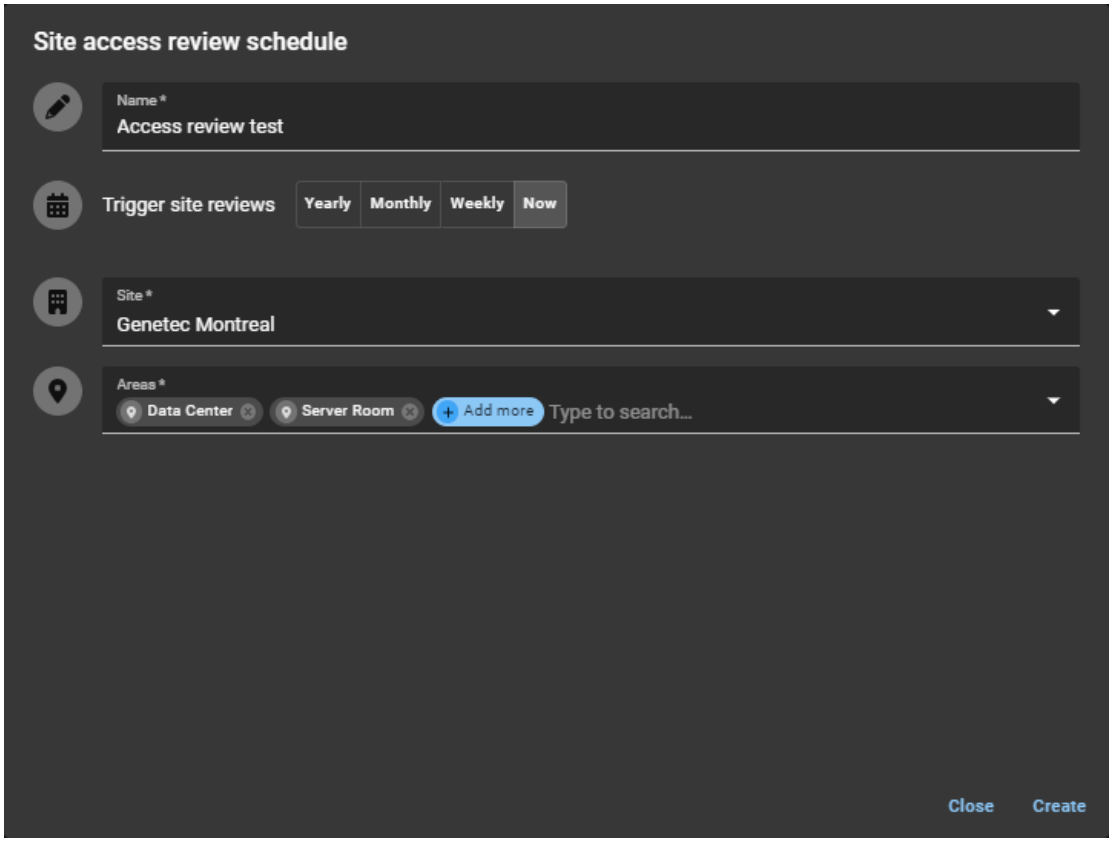
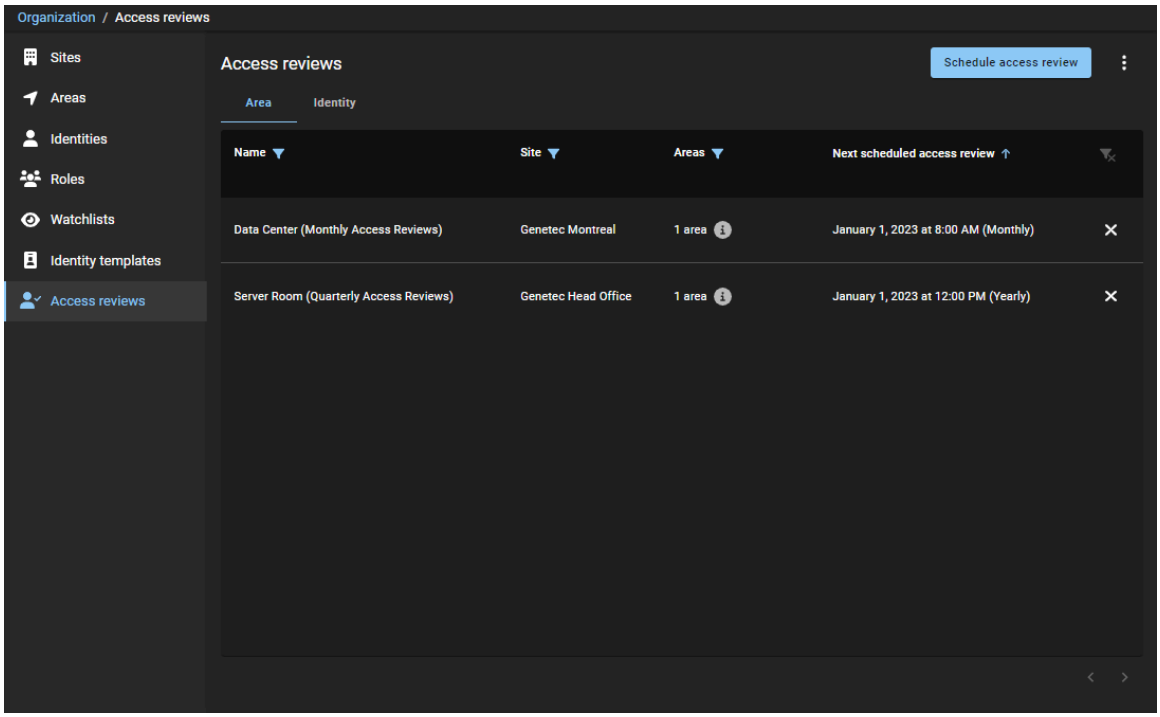


Illustration 6 : Centre de données et salle de serveurs (examen d'accès manuel prévu maintenant)

REMARQUE : Les examens d'accès configurés avec un horaire **Maintenant** ne sont pas affichés sur la page *Examens d'accès* planifiés. Ils sont affichés immédiatement dans la vue **Mes tâches** des examinateurs concernés.

5 Cliquez sur **Créer**.
Les examens d'accès planifiés sont affichés sur la page *Examens d'accès*.



6 (Facultatif) Cliquez sur un examen d'accès de secteur dans la liste pour afficher les détails de la planification.
   a) Cliquez sur **Accéder au rapport d'examen d'accès** pour afficher tous les examens d'accès.

Les examens d'accès de secteur sont à présent planifiés pour votre site.

Lorsque vous avez terminé

Pour terminer vos examens d'accès le moment voulu, procédez de la manière suivante :

- Terminer un examen d’accès de secteur ou de rôle (propriétaire de site)
- Terminer un examen d’accès de secteur ou de rôle (propriétaire de secteur)

Configurer les examens d'accès d'identité

Pour assurer le respect des règles de sécurité et la préparation aux audits, vous pouvez planifier les examens d'accès d’identité afin qu'ils aient lieu à intervalles réguliers.

Avant de commencer

- Vérifiez que le superviseur a défini des identités de subordonnés directs.

À savoir

- Seul un administrateur de compte peut configurer les examens d'accès d’identité.

BONNE PRATIQUE : Planifiez vos examens d'accès d'identité afin qu’ils soient déclenchés automatiquement avant un audit ou un contrôle de sécurité, afin d'assurer votre conformité et votre préparation aux audits.

Procédure

- Sur le portail Web Genetec ClearID^{MC}, procédez de la manière suivante :
  - Planifier vos examens d'accès d'identité

Vos examens d'accès sont à présent configurés.

Lorsque vous avez terminé

Terminer un examen d’accès d’identité (superviseur)

Programmer les examens d'accès d'identité

Pour assurer le respect des règles de sécurité et la préparation aux audits, vous pouvez planifier les examens d'accès d’identité afin qu'ils aient lieu à intervalles réguliers. Ces examens d'accès d’identité sont effectués en fonction d'une liste de rôles sélectionnés.

Avant de commencer

- Vérifiez que les rôles à examiner ont déjà été définis.
- Vérifiez que toutes les identités requises ont été associées aux rôles corrects.

À savoir

- Seul un administrateur de compte peut planifier les examens d'accès d’identité.
- Pour les examens d'accès d'identité, seules les planifications **Tous les ans** sont prises en charge.
- Vous pouvez planifier jusqu'à cinq examens d'accès d'identité à la fois et chaque examen peut inclure un maximum de 20 rôles.

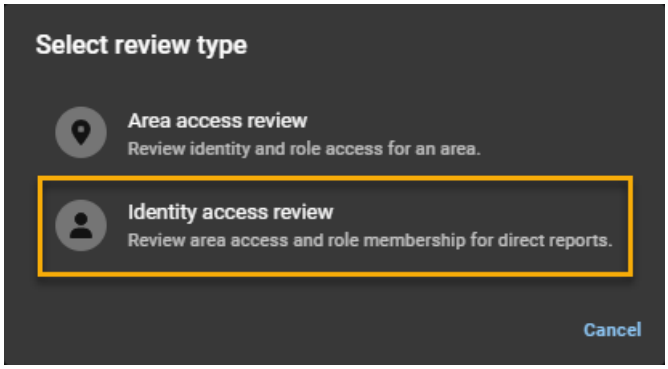
BONNE PRATIQUE : Planifiez vos examens d'accès d'identité afin qu’ils soient déclenchés automatiquement avant un audit ou un contrôle de sécurité, afin d'assurer votre conformité et votre préparation aux audits.

Procédure

1 Sur la page d’accueil, cliquez sur **Organisation** > **Examens d’accès**.

2 Cliquez sur **Planifier un examen d'accès**.

3 Dans la boîte de dialogue **Sélectionner le type d'examen**, sélectionnez **Examen d'accès d'identité**.



4 Dans la boîte de dialogue *Planification d'examen d'accès d'identité*, sélectionnez les options nécessaires.

a) Saisissez un Nom pour votre examen d'accès d'identité.

Par exemple, vous pouvez saisir `Examen d'accès des sous-traitants` pour les électriciens ou `Examen d'accès d'identité du centre de données` pour vos subordonnés directs qui ont besoin d'accéder à un centre de données.

b) Sélectionnez les options **Déclencher des examens d'identité** dont vous avez besoin.

- Sélectionnez le jour et le mois auxquels vous souhaitez que l'examen d'accès d'identité soit planifié.
- Sélectionnez l'heure à laquelle vous souhaitez que l'examen d'accès d'identité soit planifié.

REMARQUE : Les heures affichées dans les options de la boîte de dialogue *Horaires d'examen d'accès des identités*, ainsi que tous les horaires d'examen planifiés, utilisent le fuseau UTC.

c) Sélectionnez les **Rôles** que vous voulez inclure dans l'examen d'accès d'identité.

Des examens d'accès d'identité seront générés pour toutes les identités de ce rôle (état actif et inactif). Les identités inactives sont clairement identifiées dans l'examen.

d) (Facultatif) Si vous avez sélectionné **Tous les ans**, vous pouvez ajouter des informations supplémentaires si nécessaire, dans le champ **Notes**.

Le champ **Notes** permet de saisir des informations plus détaillées sur l'examen d'accès d'identité. Il est généralement utilisé lorsqu'un superviseur effectue un examen de la sécurité. Par exemple, un examen IS0 27001 ou un rapport d'audit SOC 1 ou SOC 2.

Exemple: L'exemple suivant montre un examen d'accès d'identité pour le rôle *Sous-traitants électriciens* planifié **Tous les ans**, le premier janvier à midi.

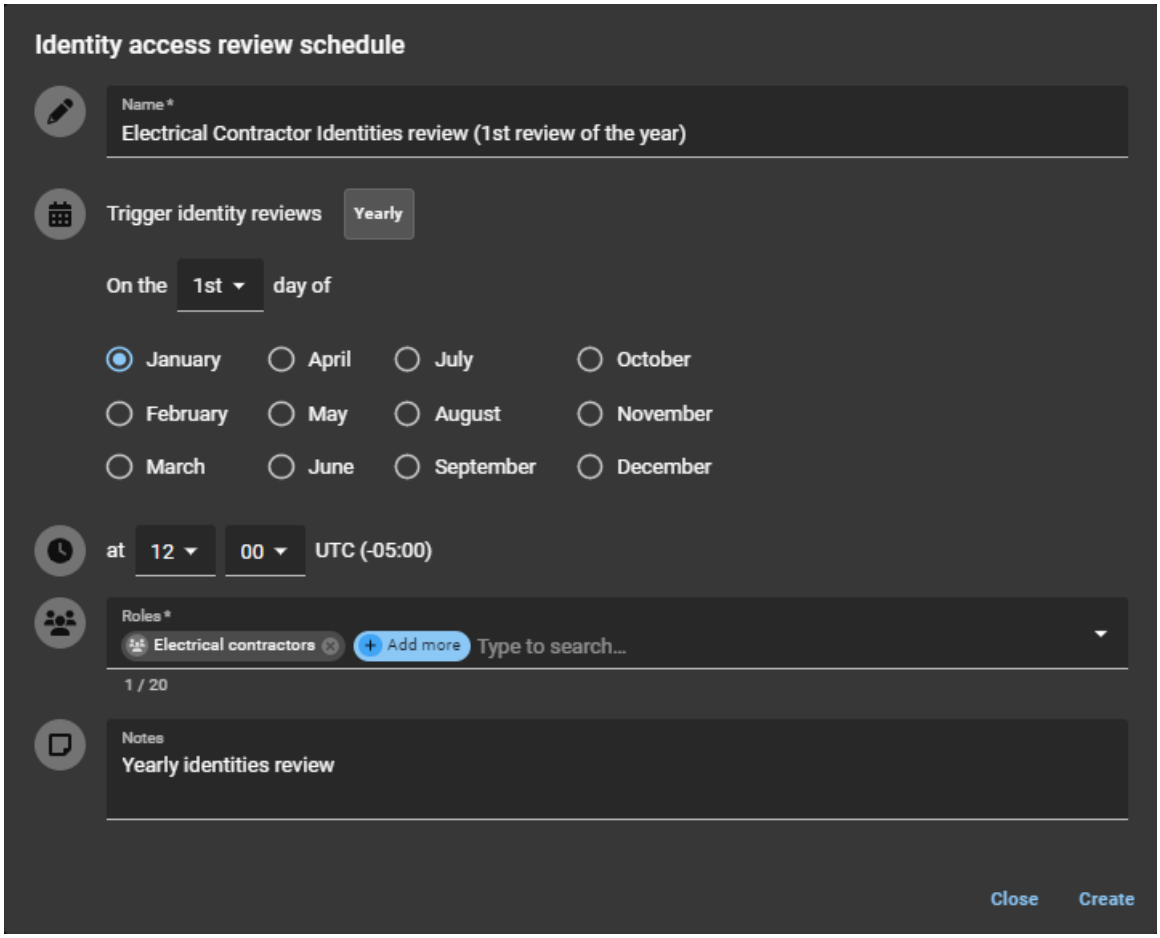


Illustration 7 : Examen de l'accès d'identité (examens de l'accès annuels)

5 Cliquez sur **Créer**.

6 (Facultatif) Cliquez sur un examen d'accès d’identité dans la liste pour afficher les détails de la planification.
   a) Cliquez sur **Accéder au rapport d'examen d'accès** pour afficher tous les examens d'accès.

Vos examens d'accès d’identité sont à présent planifiés.

Lorsque vous avez terminé

Pour terminer vos examens d'accès le moment voulu, procédez de la manière suivante :

- Terminer un examen d’accès d’identité (superviseur)

Modifier les examens d'accès

Une fois vos examens d’accès de secteur ou d’identité configurés et planifiés, vous pouvez les modifier ou les supprimer si nécessaire.

Avant de commencer

- Programmer les examens d'accès, page 287
- Programmer les examens d'accès d'identité, page 293

À savoir

- Seul un propriétaire de site peut modifier les examens d'accès de secteur.
- Seul un administrateur de compte peut modifier les examens d'accès d’identité.

Procédure

1. Si vous devez apporter des modifications ou supprimer la planification d’un examen d’accès d’identité, cliquez sur **Organisation** > **Examens d'accès**.
2. Pour modifier un examen d'accès de secteur, cliquez sur l'onglet **Secteur**.
3. Pour modifier la planification d’un examen d’accès d’identité, cliquez sur l’onglet **Identité**.
4. Cliquez sur un examen dans la liste et apportez les modifications nécessaires, puis cliquez sur **Enregistrer**.
5. (Facultatif) Pour supprimer un examen d’accès, cliquez sur à côté de l’examen que vous souhaitez supprimer, puis cliquez sur **Supprimer** pour confirmer la suppression.

À propos du rapport d’examen d'accès

Dans Genetec ClearID[MC], un rapport d’examens d’accès renvoie une liste d’examens d'accès. Le rapport contient des informations sur les examens d’accès de secteurs, de rôles ou d’identités, ainsi que l’état d’examen actuel (non démarré, démarré, en cours, terminé ou expiré).

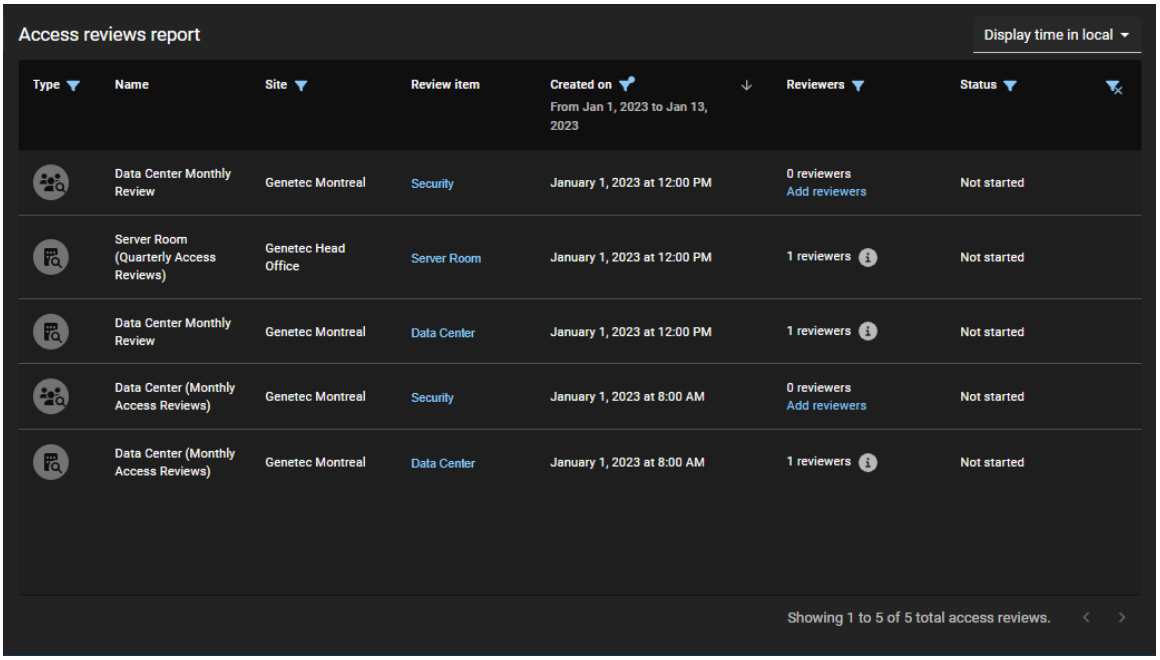


Illustration 8 : Rapport d’examen d'accès

Le rapport d’examen d’accès est utilisé pour les éléments suivants :

- Propriétaires de sites : Pour vérifier l’état des examens d’accès au site pour les secteurs ou les rôles.
- Superviseurs : Pour vérifier l’état des examens d’accès aux identités (pour leurs subordonnés directs).
- Audits : Pour fournir des informations aux auditeurs.

Vous pouvez utiliser les filtres de colonnes pour affiner le résultat de la recherche par type d’examen, site, date de création, évaluateurs et état.

Par exemple, vous pouvez filtrer le rapport pour afficher les examens terminés, puis sélectionner un examen et choisir **Imprimer** (version papier) ou**Imprimer** > **Destination** > **Enregistrer au format PDF** (version électronique). La version papier ou électronique peut ensuite être transmise aux contrôleurs ou à d'autres membres de votre organisation.

Qui peut voir quoi ?

- Les approbateurs de secteurs ou les responsables de rôles voient uniquement les filtres pertinents pour les examens de secteurs ou de rôles.
- Les superviseurs voient uniquement leurs subordonnés directs.
- Les administrateurs voient tout.

Rubriques connexes

Vérifier l’état des examens d'accès, page 299

Vérifier l’état des examens d'accès

Il incombe au propriétaire ou responsable de site de vérifier l'état des examens d'accès pour assurer le respect des normes de sécurité de l’organisation ou en amont d'un audit, et de s'assurer que les processus d’examens sont effectués dans les temps. Un superviseur peut également vérifier l'état des examens d’accès d'identité pour leurs subordonnés directs.

Avant de commencer

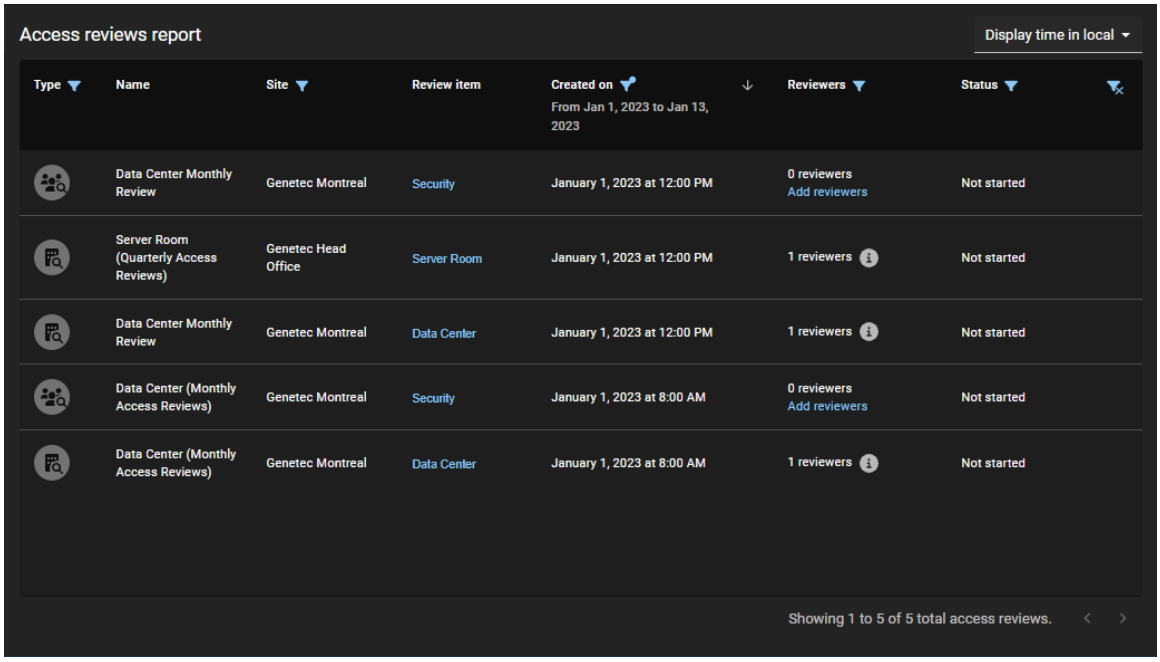
Configurez vos examens d'accès.

À savoir

- Seul un propriétaire de site peut voir l’intégralité du **Rapport d’examen d'accès** pour vérifier l’état ou la progression d'un examen d'accès de secteur ou de rôle pour son site.
- Un approbateur de secteur ou un responsable de rôle voit uniquement ses propres examens dans la version **Mes analyses d'accès** du rapport.
- Les propriétaires de sites qui ne sont pas propriétaires ou approbateurs de secteurs ou propriétaires ou responsables de rôles ne verront pas d’examens d'accès dans **Tableau de bord** > **Mes tâches**.
- Filtres : Lorsqu'aucun type, site ou examinateur n'est sélectionné, tous les résultats sont affichés dans le rapport.

Procédure

1 Sur le *Tableau de bord*, cliquez sur **Rapports** > **Analyse d’accès**.

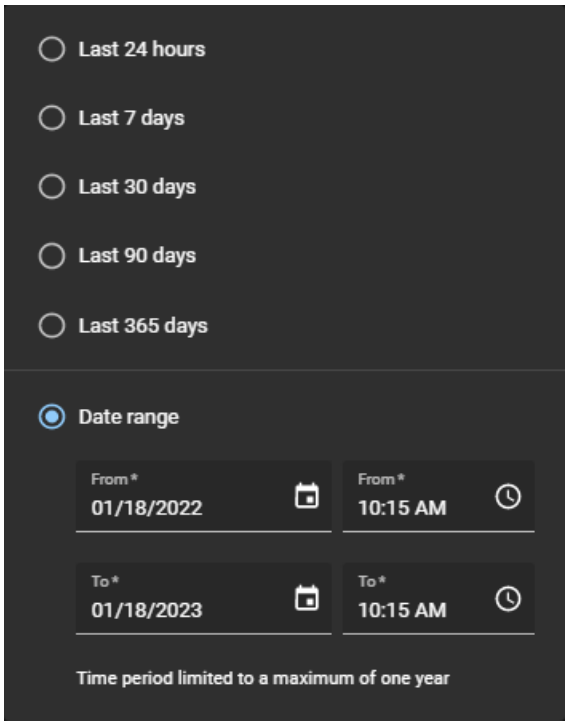


CONSEIL : Si un examen a `0 examinateur` dans la colonne **Examinateurs**, vous pouvez cliquer sur le lien **Ajouter des examinateurs** pour en ajouter. Cette situation survient généralement lorsqu’aucun propriétaire ou approbateur n'a été défini.

2 Sur la page *Rapport d'analyse d'accès*, sélectionnez l'heure d'affichage dont vous avez besoin parmi les options suivantes :

- **Heure d'affichage locale :** Affichez les heures de rapport en utilisant l'heure système locale de l'ordinateur de l'utilisateur connecté.
- **Heure d'affichage UTC :** Affichez les heures de rapport en utilisant le temps universel coordonné (UTC).

3 Dans la colonne **Créé le**, sélectionnez l'une des options ou cliquez sur **Plage de dates** et précisez une plage de dates et d'heures pour afficher une liste des analyses d'accès.



4 (Facultatif) Si la liste est longue, configurez des filtres de colonnes de rapport supplémentaires pour affiner les résultats du rapport selon les besoins.

a) Dans la colonne **Type**, sélectionnez un ou plusieurs types d'avis comme demandé :

- **Examen d'accès à un secteur :** Affiche les analyses d'accès aux secteurs.
- **Examen d'accès à un rôle :** Affiche les analyses d'accès aux rôles.
- **Analyse d'accès d'identité :** Affiche les examens d'accès d'identité.

b) Dans la colonne **Site**, entrez une chaîne de recherche ou sélectionnez un ou plusieurs sites dans la liste.

c) Dans la colonne **Évaluateurs**, saisissez le nom ou l'adresse e-mail d'un évaluateur d'accès pour afficher les analyses auxquels il est associé.

d) Dans la colonne **Statut**, sélectionnez les options de statut que vous souhaitez afficher lors de la vérification de l'analyse d'accès.

REMARQUE : L'état des examens d'accès incomplets est automatiquement mis à jour sur l'état **Expiré** lorsque l'examen d'accès incomplet est remplacé par un examen planifié plus récent qui porte le même nom ou lorsque l'option **Appliquer une expiration pour les examens d'accès** est activée et que la période d'activation est dépassée.

e) (Facultatif) Cliquez sur pour réinitialiser les filtres.

5 Dans la colonne **Élément d'analyse** , cliquez sur un lien hypertexte pour vérifier les détails de l'analyse d'accès ou pour terminer l'analyse.

6 (Facultatif) Vous pouvez voir la liste des évaluateurs en cliquant sur l'icône d'information ( ) à côté des **évaluateurs**.

7 (Facultatif) Si vous avez sélectionné une analyse d'accès à un secteur, cliquez sur les hyperliens dans la colonne **Élément d'analyse** pour afficher des informations supplémentaires sur l'analyse d'accès.

8 (Facultatif) Si vous avez sélectionné une analyse d'accès, cliquez sur **Continuer l'analyse** pour terminer l'analyse d'accès maintenant.

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles.

Lorsque vous avez terminé

Pour terminer vos examens d'accès le moment voulu, procédez de la manière suivante :

- Terminer un examen d'accès de secteur (propriétaire de site)
- Terminer un examen d'accès de secteur (propriétaire de secteur)
- Terminer un examen d'accès d'identité (superviseur)

Rubriques connexes

À propos du rapport d'examen d'accès, page 298

Terminer un examen d'accès à un secteur (propriétaire de site)

Pour assurer le respect des normes de sécurité ou vous préparer à un audit, vous pouvez effectuer des examens d'accès pour savoir qui a accès à un secteur ou un rôle. Ces examens périodiques sont effectués par un propriétaire de site.

Avant de commencer

Configurez les examens d'accès pour votre site.

À savoir

- Vous ne pouvez pas modifier un examen d'accès terminé.
- Tous les examens en état **Terminé** sont conservés à des fins d'audit et de suivi.

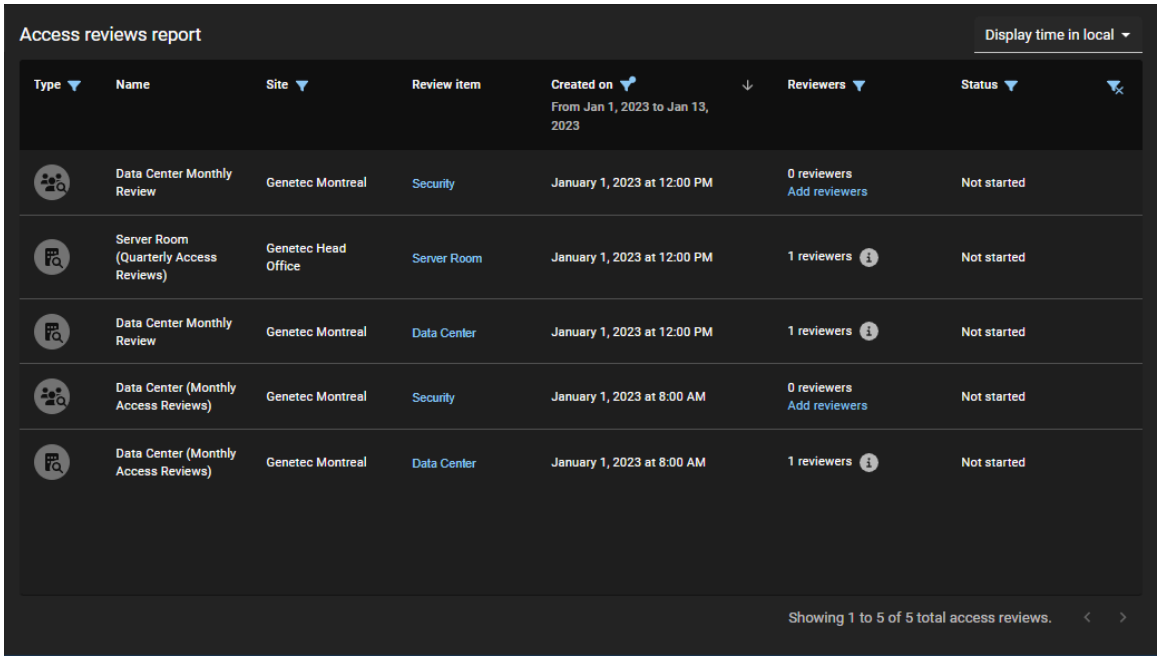
Procédure

Pour terminer un examen d'accès de secteur :

1 Sur la page d'*accueil*, cliquez sur **Rapports** > **Examens d'accès**.

2 (Facultatif) Configurez les filtres de la colonne rapport selon les besoins.

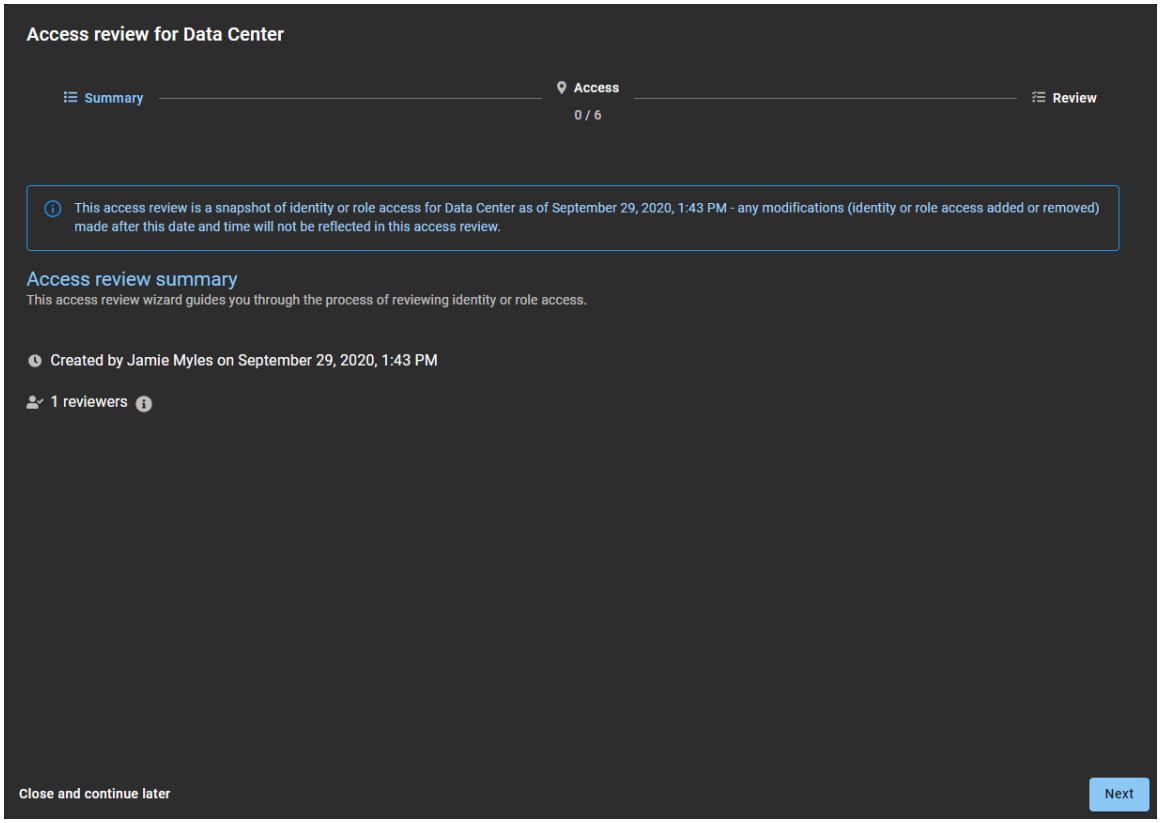
3 Dans la section *Rapport d'examen d'accès*, sélectionnez l'examen d'accès de secteur qui vous intéresse.



a) Cliquez sur un lien hypertexte de secteur dans la colonne **Élément d'examen** pour démarrer l'examen d'accès.

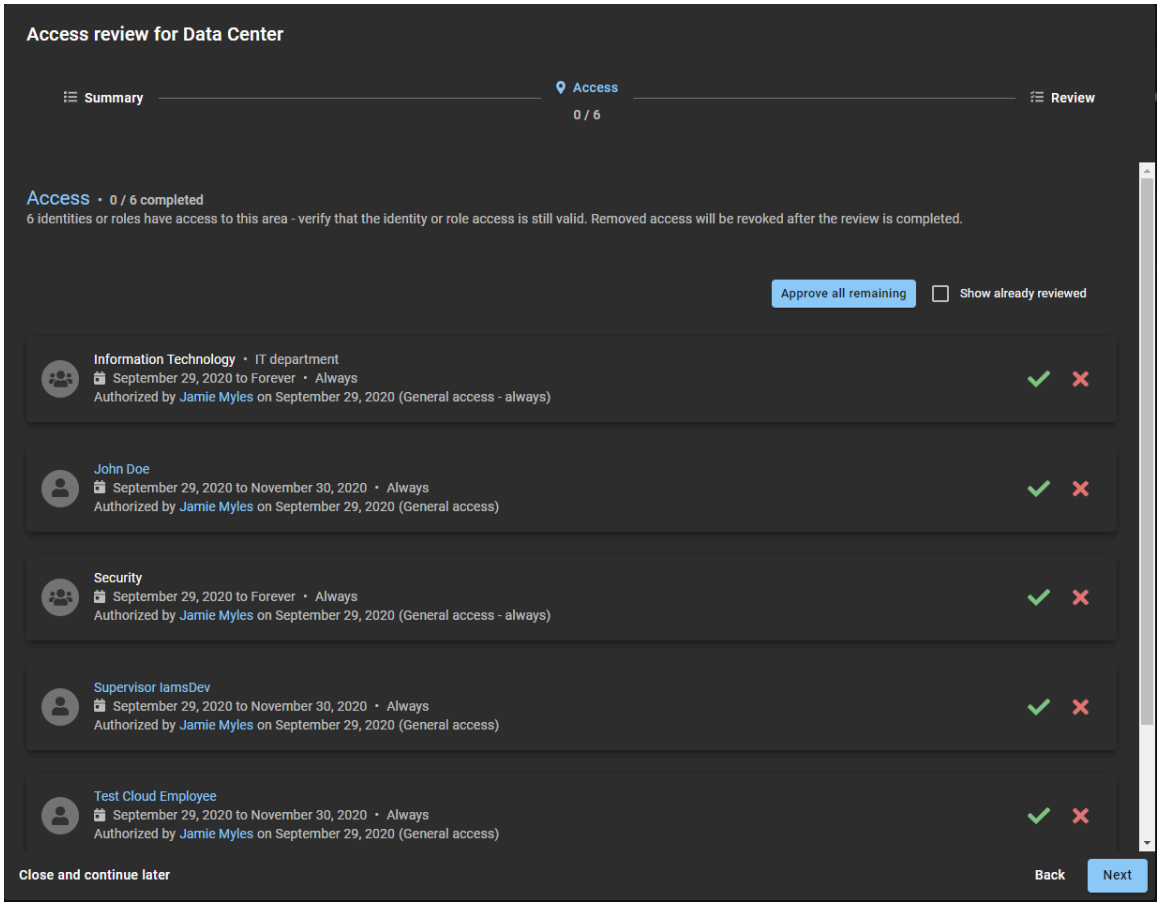
b) Cliquez sur **Continuer l'examen**.

4 Examinez les détails dans la section **Résumé** de l’examen d'accès de secteur.



a) Cliquez sur pour afficher les détails de l’examinateur.
b) (Facultatif) Cliquez sur **Fermer et continuer plus tard** pour remettre l’examen à plus tard.
c) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d’examen d’accès.

5 Examinez les informations dans la section **Accès** de l'examen d'accès.



a) Cliquez sur **Conserver l'accès** ( ) pour confirmer que l'accès est toujours valable.

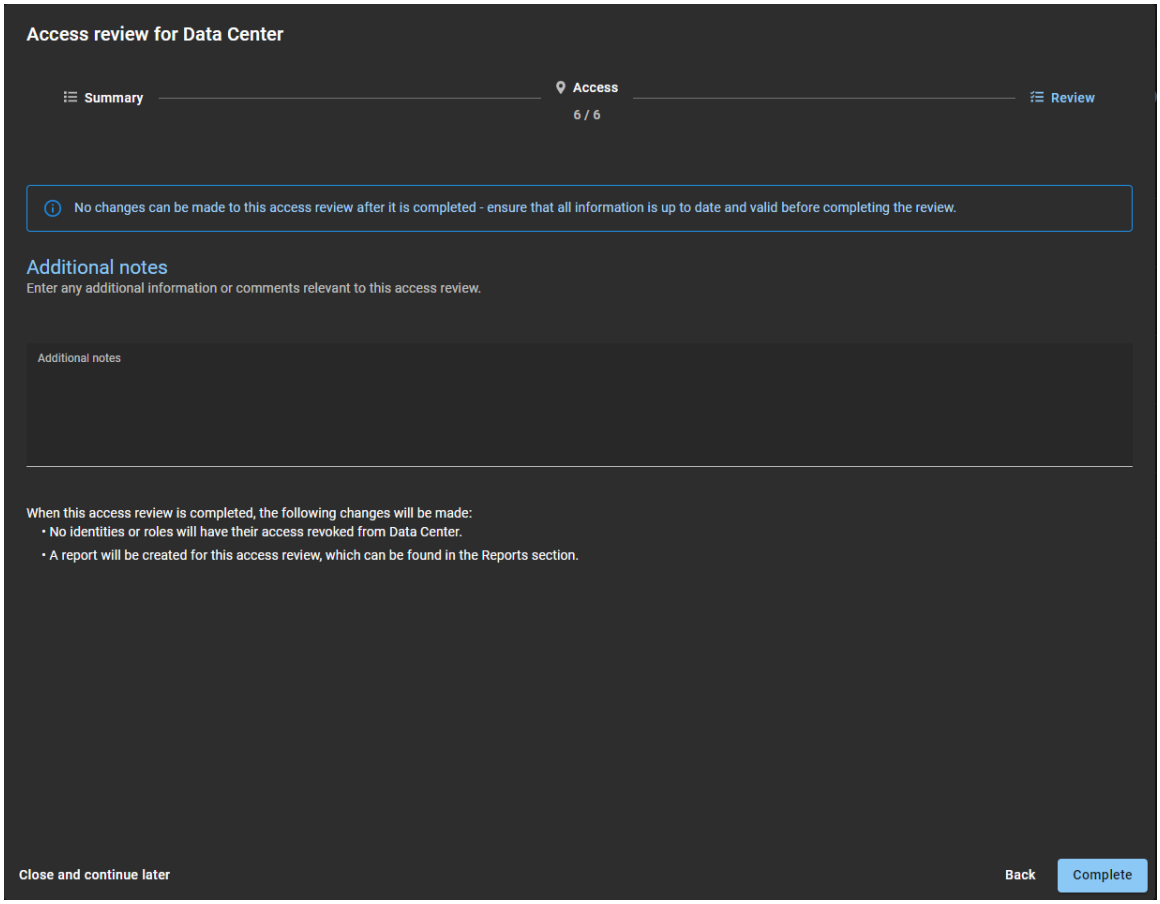
CONSEIL : Utilisez **Approuver tous les autres** pour accélérer le processus d'approbation lorsque la liste est longue, puis supprimez tout accès qui n'est plus nécessaire.

b) Cliquez sur **Supprimer l'accès** ( ) pour supprimer un accès qui n'est plus nécessaire.

c) (Facultatif) Sélectionnez **Afficher les accès déjà examinés** pour revenir en arrière et apporter des modifications.

d) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d'examen d'accès.

6 Vérifiez l'exactitude des informations dans la section *Examen* de l'examen d'accès.



a) Le cas échéant, ajoutez vos commentaires dans la section **Notes complémentaires**.

b) Avant de cliquer sur **Terminer**, vérifiez le résumé des modifications juste après la section **Notes complémentaires**.

Ce résumé affiche les modifications qui seront apportées aux identités ou aux rôles lorsque vous cliquerez sur **Terminer**.

c) (Facultatif) Si des informations vous semblent erronées, cliquez sur **Précédent** pour revenir aux sections précédentes et corriger les erreurs.

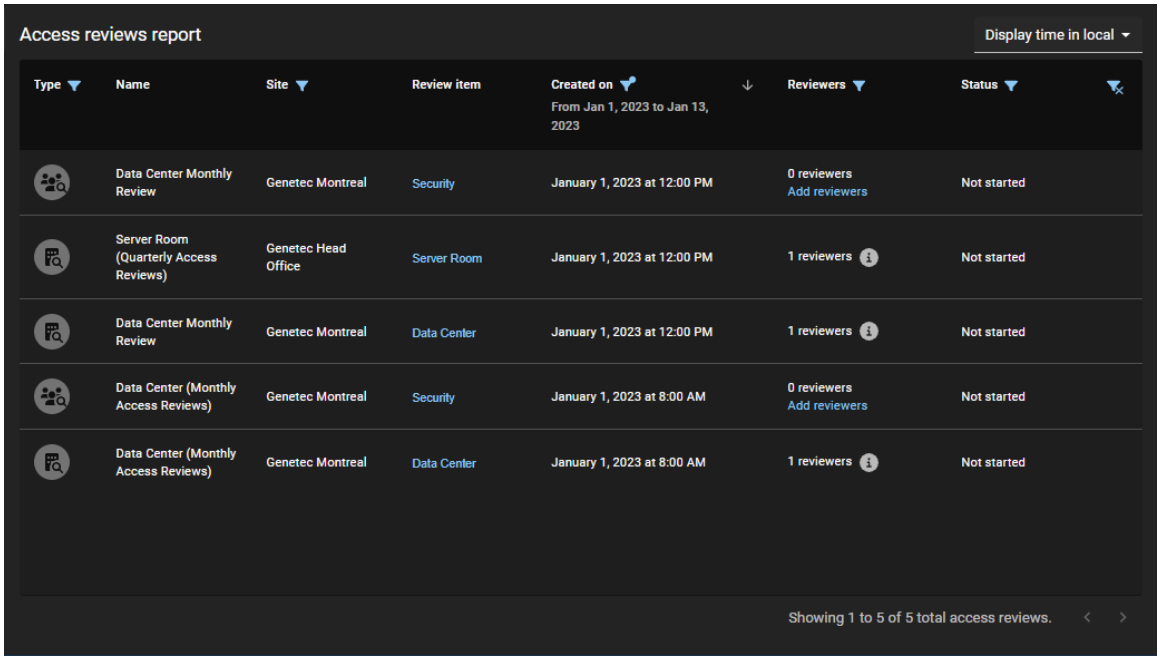
d) Si les informations dans la section **Examen** vous semblent exactes, cliquez sur **Terminer**.

Pour terminer un examen d'accès de rôle :

1 Sur la page d'*accueil*, cliquez sur **Rapports** > **Examens d'accès**.

2 (Facultatif) Configurez les filtres de la colonne rapport selon les besoins.

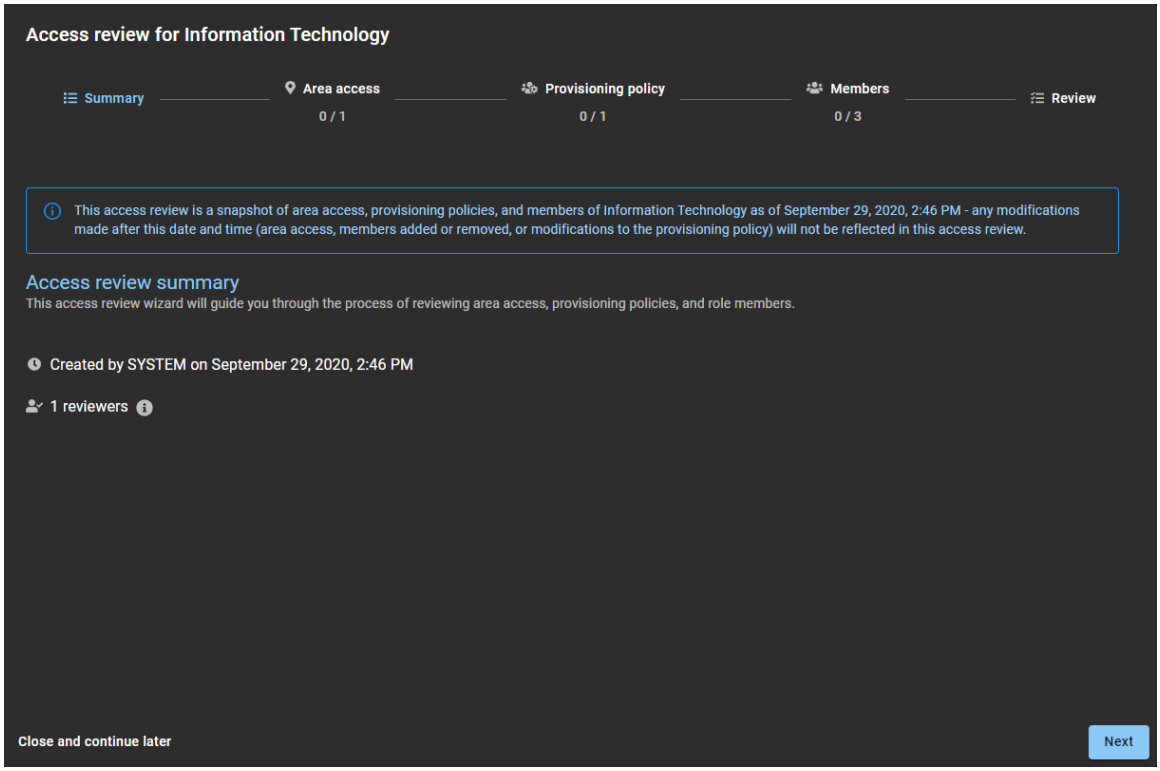
3 Dans la section *Rapport d'examen d'accès*, sélectionnez l'examen d'accès de rôle qui vous intéresse.



a) Cliquez sur un lien hypertexte de rôle dans la colonne **Élément d'examen** pour démarrer l'examen d'accès.

b) Cliquez sur **Continuer l'examen**.

4 Examinez les détails dans la section **Résumé** de l'examen d'accès de rôle.

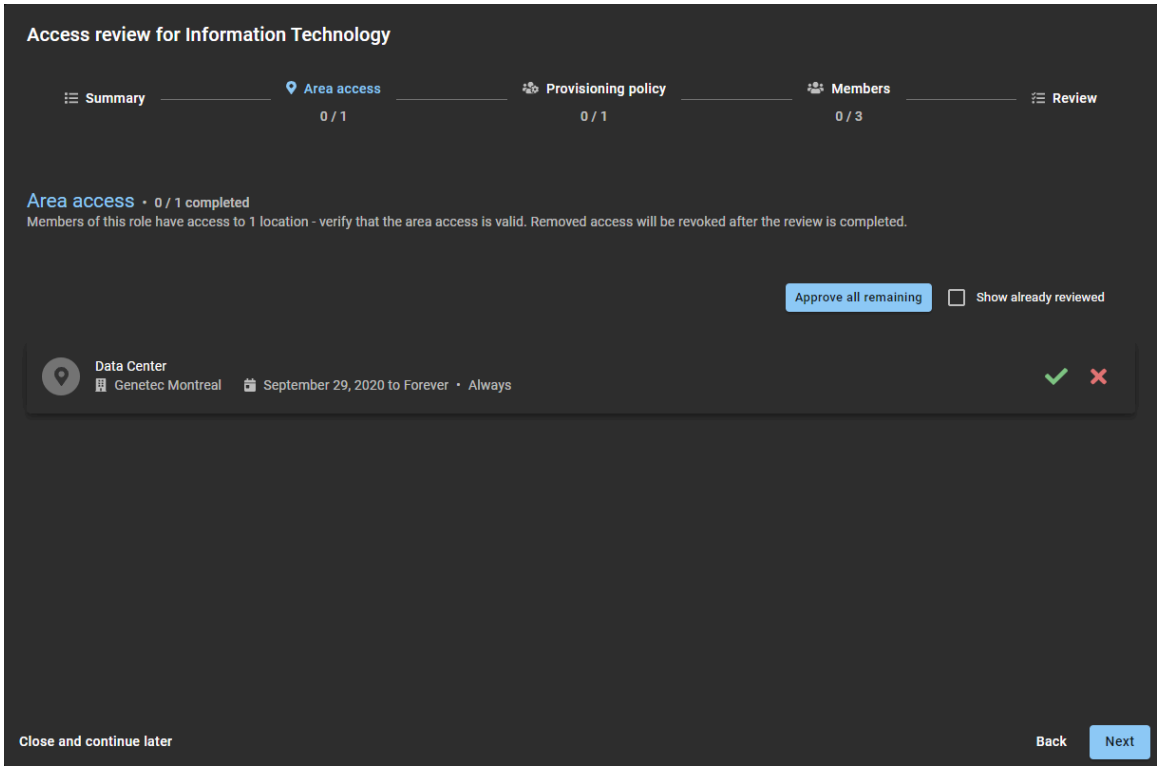


a) Cliquez sur pour afficher les détails de l'examinateur.

b) (Facultatif) Cliquez sur **Fermer et continuer plus tard** pour remettre l'examen à plus tard.

c) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d'examen d'accès.

5 Examinez les informations dans la section **Accès au secteur** de l’examen d'accès.



a) Cliquez sur **Conserver l'accès** ( ) pour confirmer que l'accès est toujours valable.

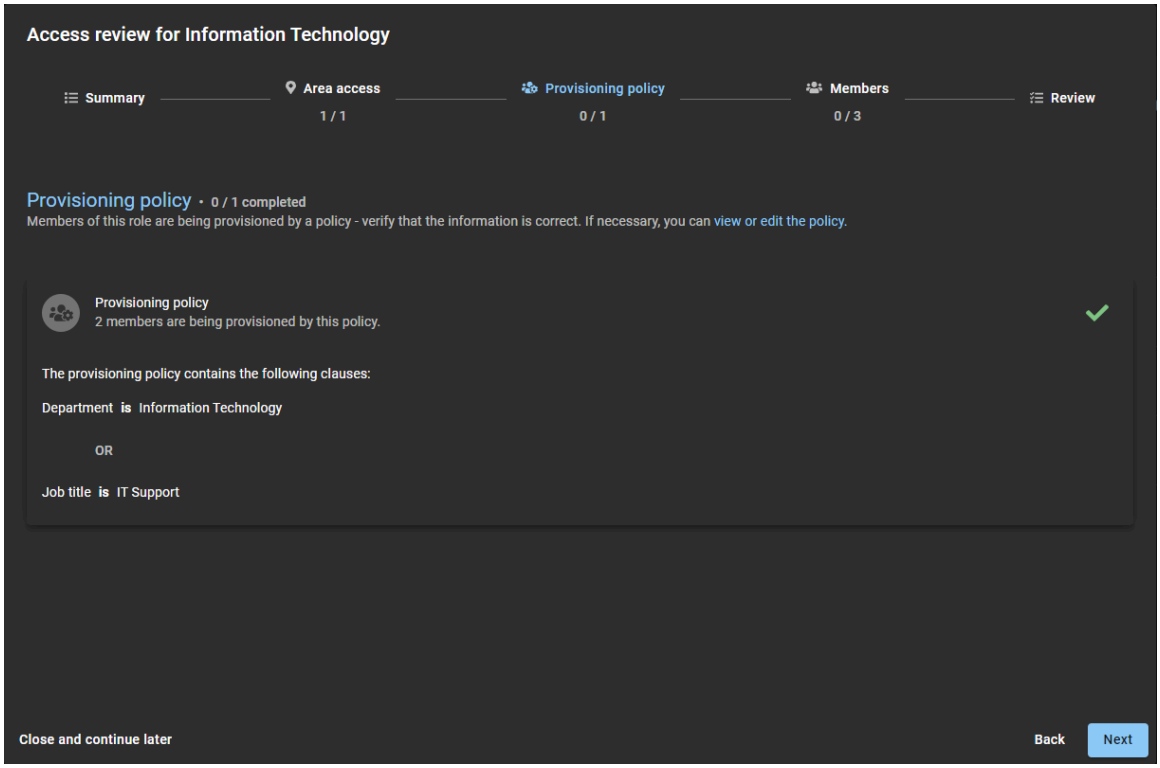
CONSEIL : Utilisez **Approuver tous les autres** pour accélérer le processus d'approbation lorsque la liste est longue, puis supprimez tout accès qui n'est plus nécessaire.

b) Cliquez sur **Supprimer l'accès** ( ) pour supprimer un accès qui n’est plus nécessaire.

c) (Facultatif) Sélectionnez **Afficher les accès déjà examinés** pour revenir en arrière et apporter des modifications.

d) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d’examen d’accès.

6 Vérifiez que les stratégies dans la section **Stratégie de provisionnement** de l'examen d'accès de rôle sont toujours valables.

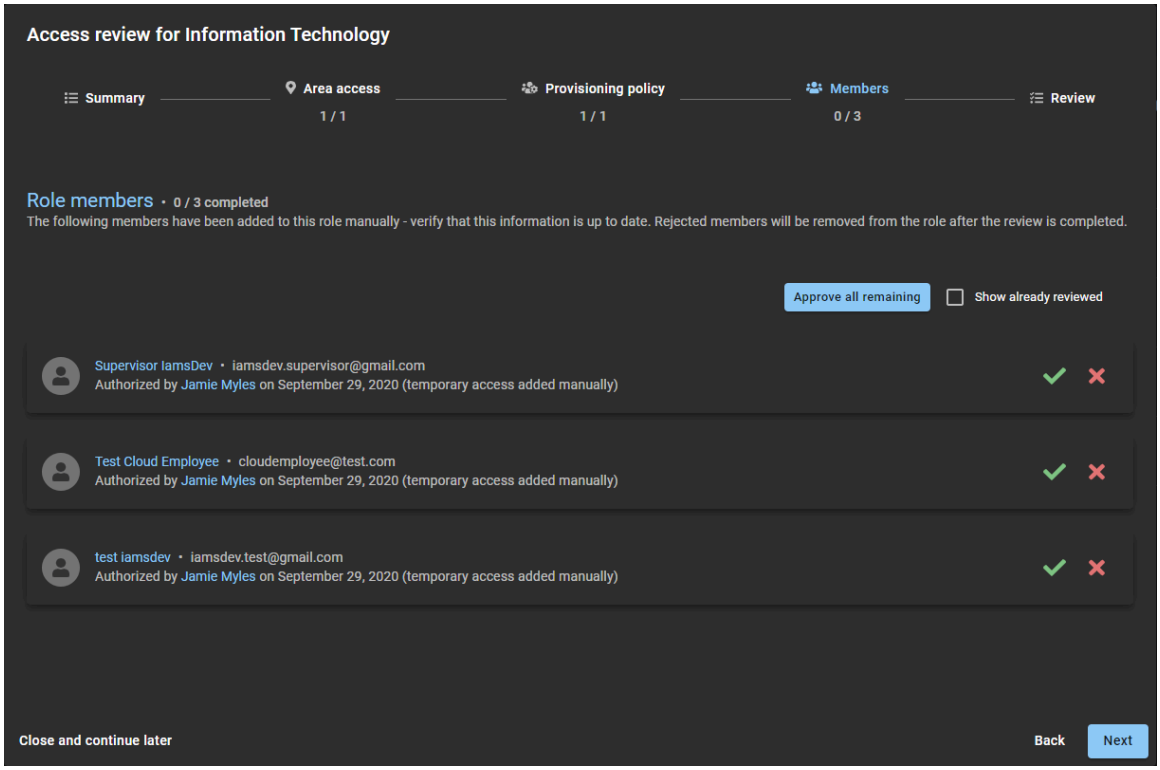


a) (Facultatif) Cliquez sur **Voir ou modifier la stratégie** pour ouvrir la page *Stratégie de provisionnement* afin d'afficher ou modifier la stratégie.

b) Cliquez sur **Approuver la stratégie** ( ) pour confirmer qu'elle est toujours valable.

c) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d'examen d'accès.

7 Vérifiez que les membres sont toujours valables dans la section **Membres** de l'examen d'accès de rôle.



a) Cliquez sur **Conserver l'accès** ( ) pour confirmer que l'accès est toujours valable.

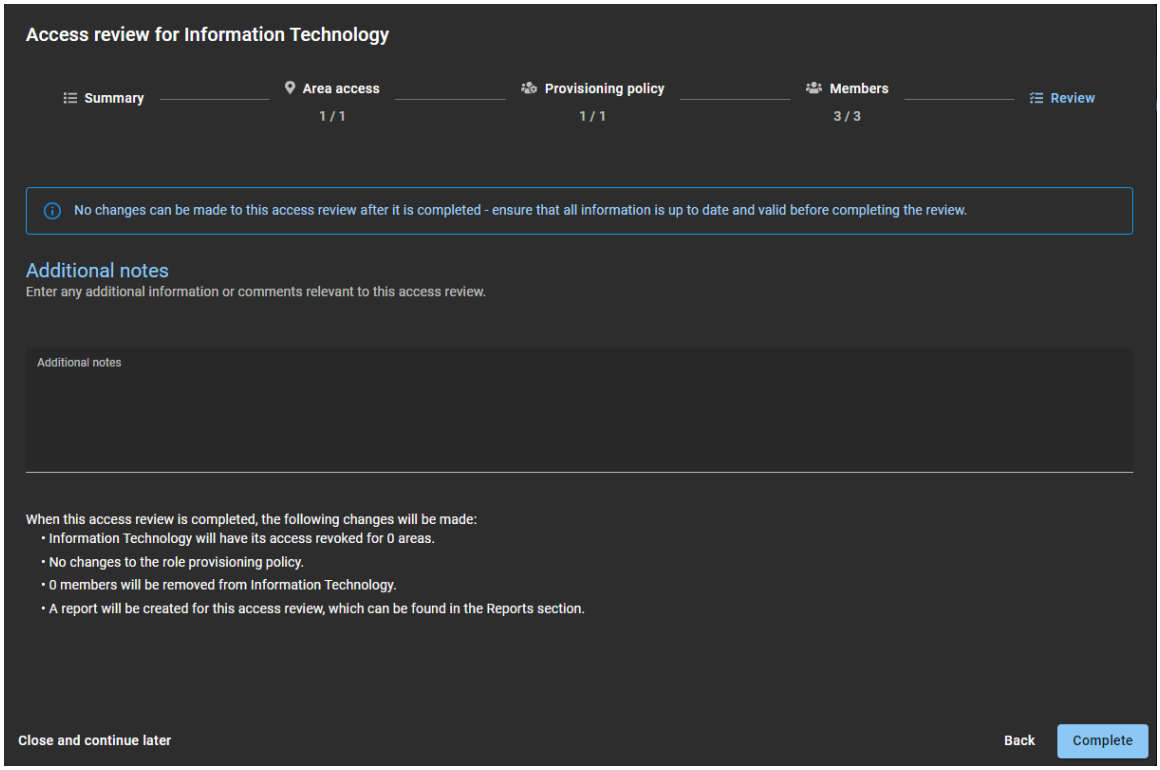
CONSEIL : Utilisez **Approuver tous les autres** pour accélérer le processus d'approbation lorsque la liste est longue, puis supprimez tout accès qui n'est plus nécessaire.

b) Cliquez sur **Supprimer l'accès** ( ) pour supprimer un accès qui n'est plus nécessaire.

c) (Facultatif) Sélectionnez **Afficher les accès déjà examinés** pour revenir en arrière et apporter des modifications.

d) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d'examen d'accès.

8 Vérifiez l'exactitude des informations dans la section **Examen** de l'examen d'accès de rôle.



a) Le cas échéant, ajoutez vos commentaires dans la section **Notes complémentaires**.
b) Avant de cliquer sur **Terminer**, vérifiez le résumé des modifications juste après la section **Notes complémentaires**.
c) (Facultatif) Si des informations vous semblent erronées, cliquez sur **Précédent** pour revenir aux sections précédentes et corriger les erreurs.
d) Si les informations dans la section **Examen** vous semblent exactes, cliquez sur **Terminer**.

Lorsque vous avez terminé

Générez un rapport d'examen d'accès.

Rubriques connexes

Examiner les accès à un secteur, page 364
Note sur la fonction d'examen d'accès (2 pages)

Terminer un examen d'accès (approbateur de secteur ou responsable de rôle)

Pour assurer le respect des normes de sécurité ou vous préparer à un audit, vous pouvez effectuer des examens d'accès pour savoir qui a accès à un secteur ou un rôle. Ces examens périodiques sont réalisés par un approbateur de secteur ou un responsable de rôle.

Avant de commencer

Recherchez une notification *Examens d'accès en attente* dans votre boîte aux lettres ou sur la page *Mes tâches*.

À savoir

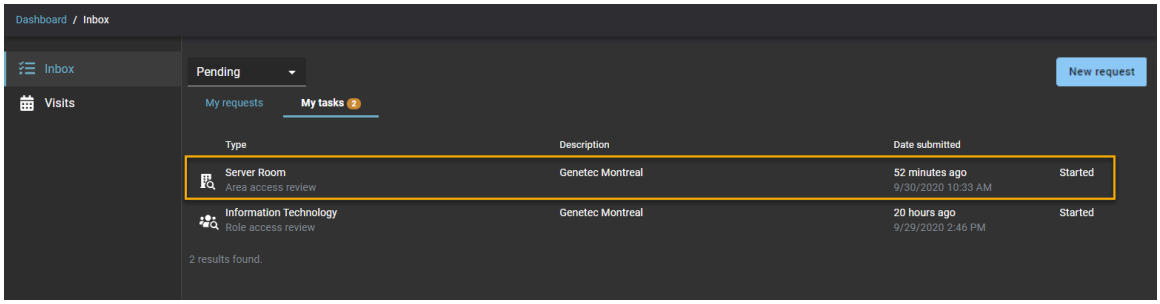
- Les approbateurs de secteur ou les responsables de rôle peuvent réaliser un examen d'accès depuis la page **Mes tâches** du **Tableau de bord** ou depuis un e-mail de notification.
- Vous ne pouvez pas modifier un examen d'accès terminé.
- Tous les examens en état **Terminé** sont conservés à des fins d’audit et de suivi.
-

Procédure

Pour terminer un examen d'accès de secteur depuis la page Tableau de bord :

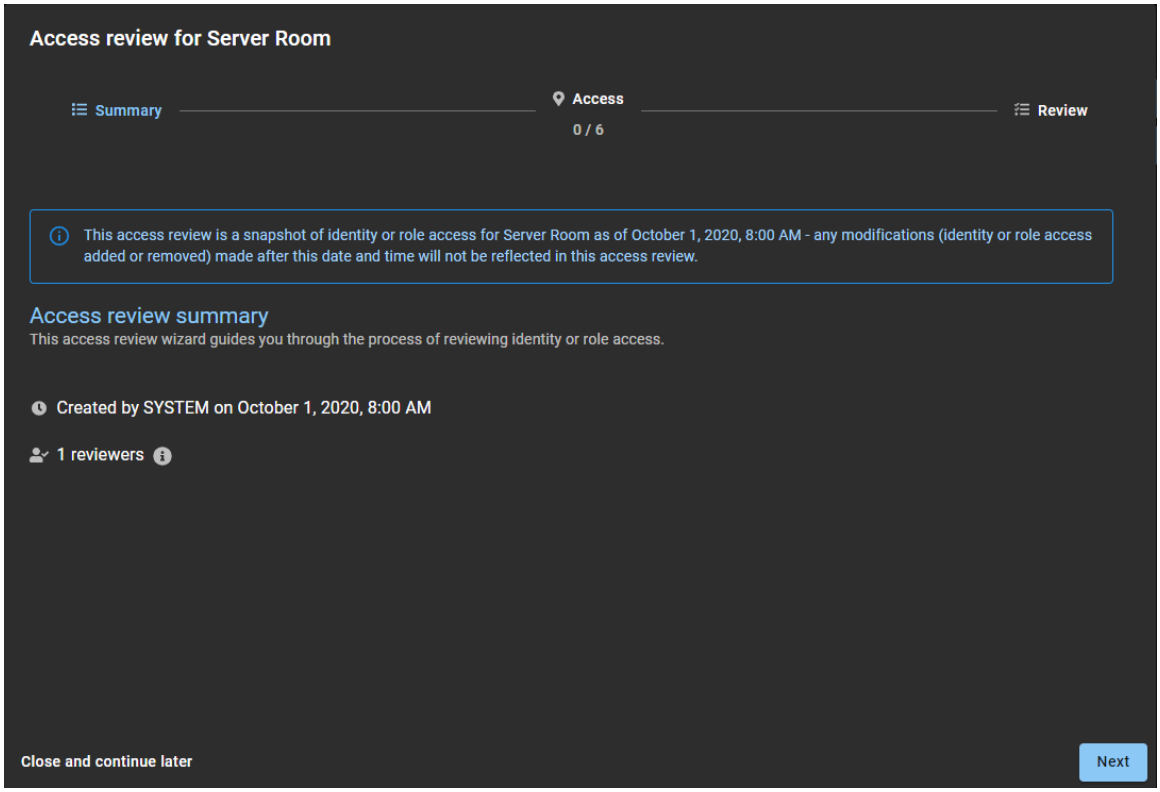
1 Cliquez sur **Tableau de bord** > **Mes tâches**.

2 Dans la liste **Mes tâches**, cliquez sur le secteur concerné.



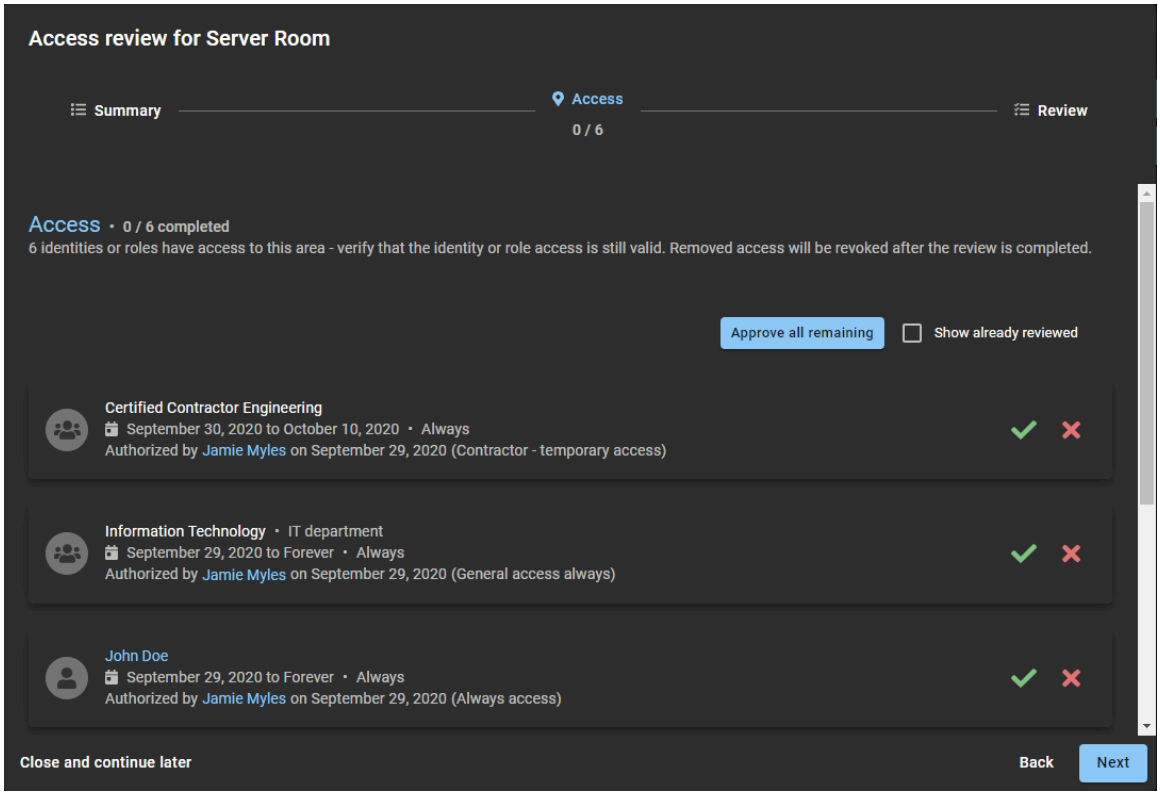
3 Cliquez sur **Continuer l’examen**.

4 Examinez les détails dans la section **Résumé** de l’examen d'accès de secteur.



a) Cliquez sur pour afficher les détails de l’examinateur.
b) (Facultatif) Cliquez sur **Fermer et continuer plus tard** pour remettre l’examen à plus tard.
c) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d’examen d’accès.

5 Examinez les informations dans la section **Accès** de l'examen d'accès.



a) Cliquez sur **Conserver l'accès** ( ) pour confirmer que l'accès est toujours valable.

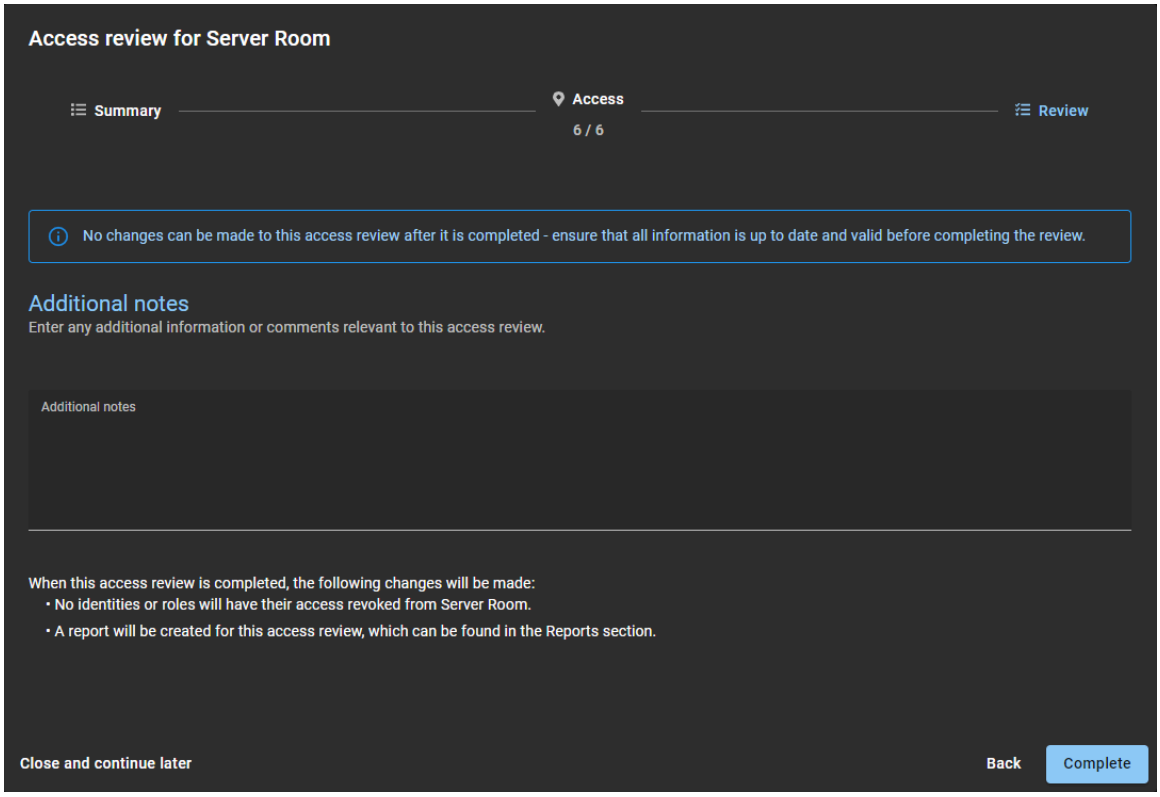
CONSEIL : Utilisez **Approuver tous les autres** pour accélérer le processus d'approbation lorsque la liste est longue, puis supprimez tout accès qui n'est plus nécessaire.

b) Cliquez sur **Supprimer l'accès** ( ) pour supprimer un accès qui n'est plus nécessaire.

c) (Facultatif) Sélectionnez **Afficher les accès déjà examinés** pour revenir en arrière et apporter des modifications.

d) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d'examen d'accès.

6 Vérifiez l'exactitude des informations dans la section *Examen* de l'examen d'accès.



a) Le cas échéant, ajoutez vos commentaires dans la section **Notes complémentaires**.

b) Avant de cliquer sur **Terminer**, vérifiez le résumé des modifications juste après la section **Notes complémentaires**.

Ce résumé affiche les modifications qui seront apportées aux identités ou aux rôles lorsque vous cliquerez sur **Terminer**.

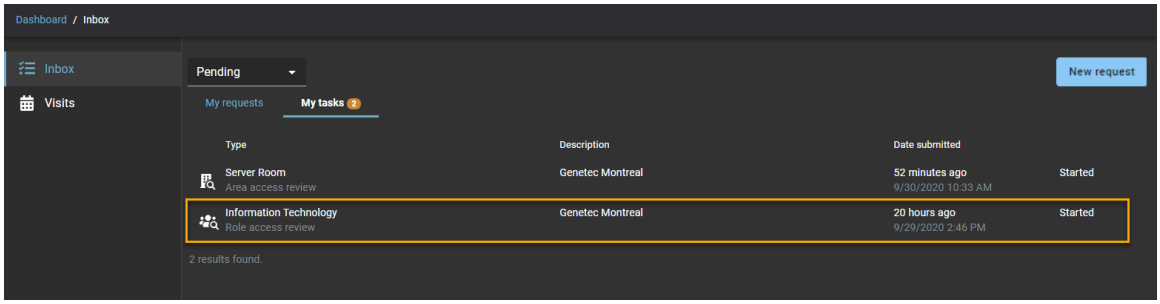
c) (Facultatif) Si des informations vous semblent erronées, cliquez sur **Précédent** pour revenir aux sections précédentes et corriger les erreurs.

d) Si les informations dans la section **Examen** vous semblent exactes, cliquez sur **Terminer**.

Pour terminer un examen d'accès de rôle depuis la page Tableau de bord :

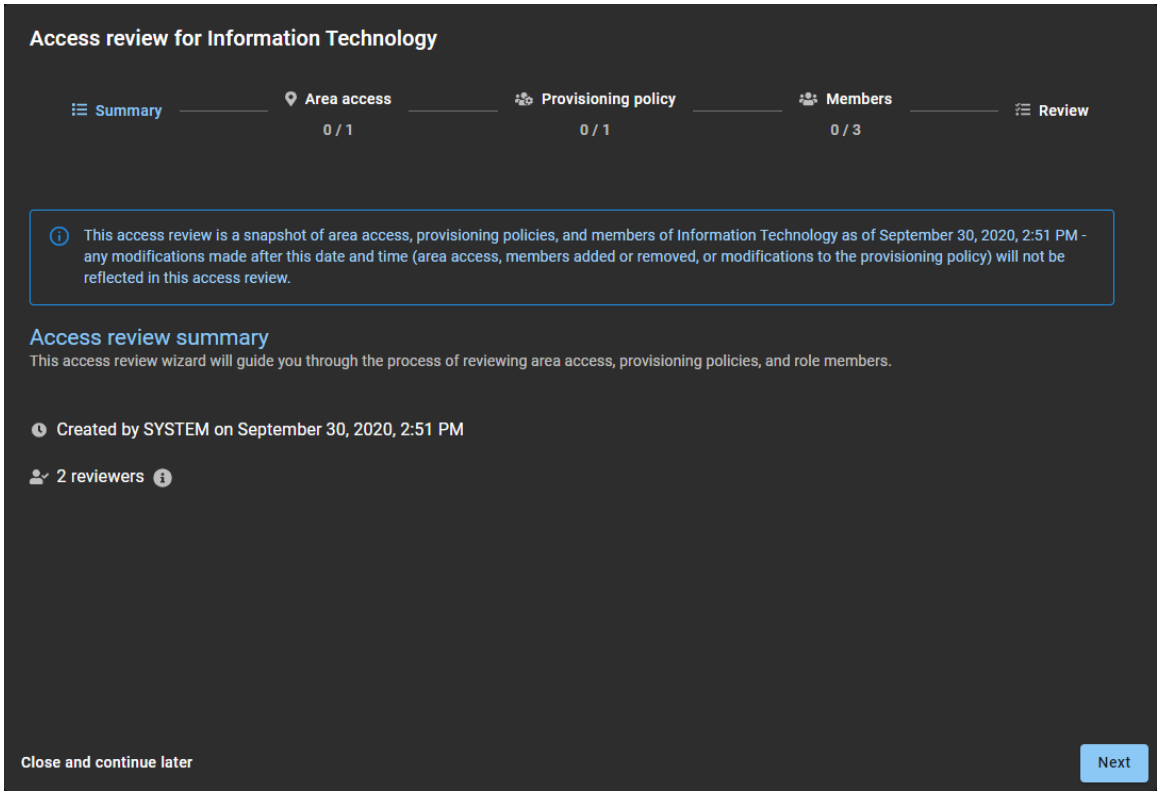
1 Cliquez sur **Tableau de bord** > **Mes tâches**.

2 Dans la liste **Mes tâches**, cliquez sur le rôle concerné.



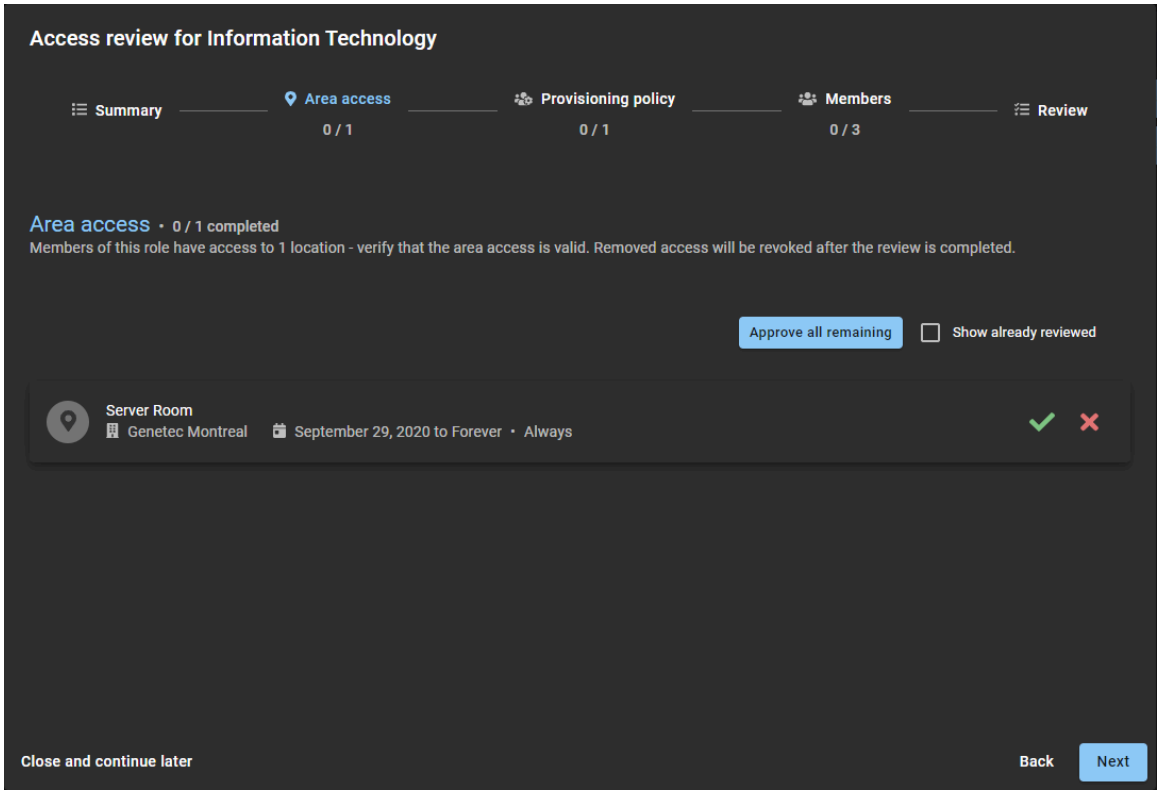
3 Cliquez sur **Continuer l'examen**.

4 Examinez les détails dans la section **Résumé** de l’examen d'accès de rôle.



a) Cliquez sur pour afficher les détails de l’examinateur.
b) (Facultatif) Cliquez sur **Fermer et continuer plus tard** pour remettre l’examen à plus tard.
c) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d’examen d’accès.

5 Examinez les informations dans la section **Accès au secteur** de l'examen d'accès.



a) Cliquez sur **Conserver l'accès** ( ) pour confirmer que l'accès est toujours valable.

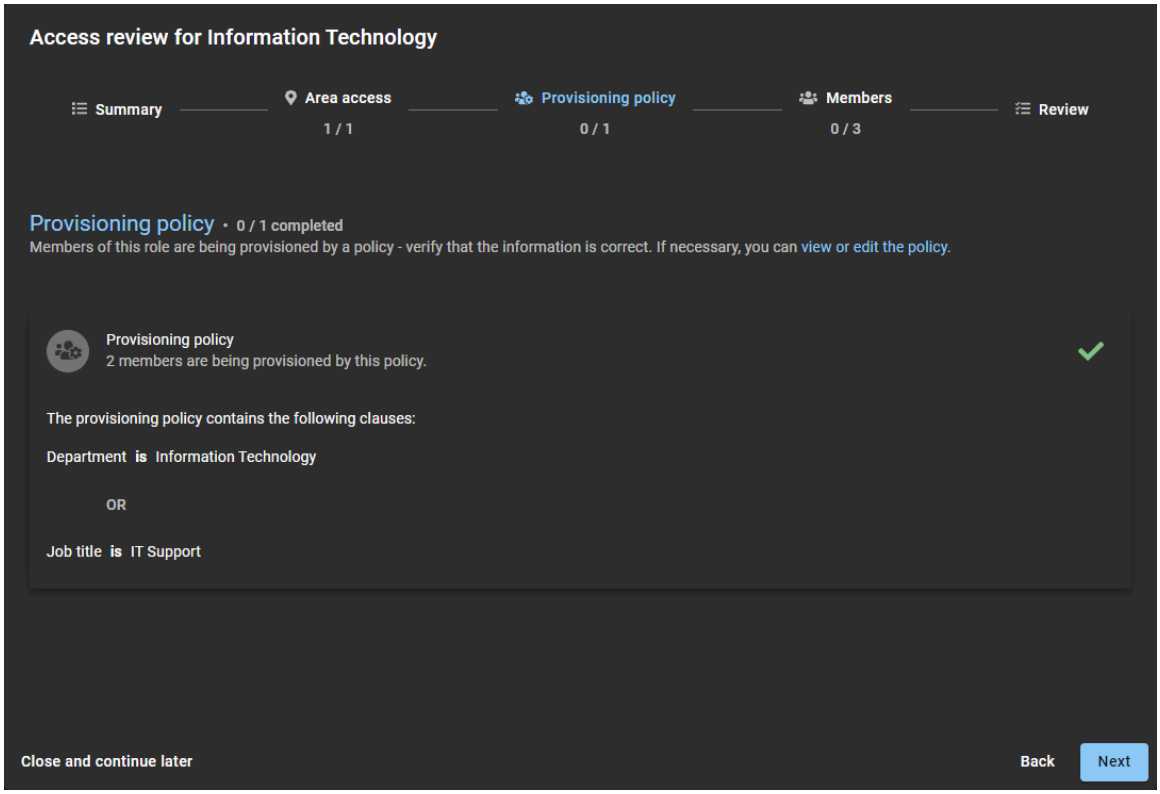
CONSEIL : Utilisez **Approuver tous les autres** pour accélérer le processus d'approbation lorsque la liste est longue, puis supprimez tout accès qui n'est plus nécessaire.

b) Cliquez sur **Supprimer l'accès** ( ) pour supprimer un accès qui n'est plus nécessaire.

c) (Facultatif) Sélectionnez **Afficher les accès déjà examinés** pour revenir en arrière et apporter des modifications.

d) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d'examen d'accès.

6 Vérifiez que les stratégies dans la section **Stratégie de provisionnement** de l'examen d'accès de rôle sont toujours valables.

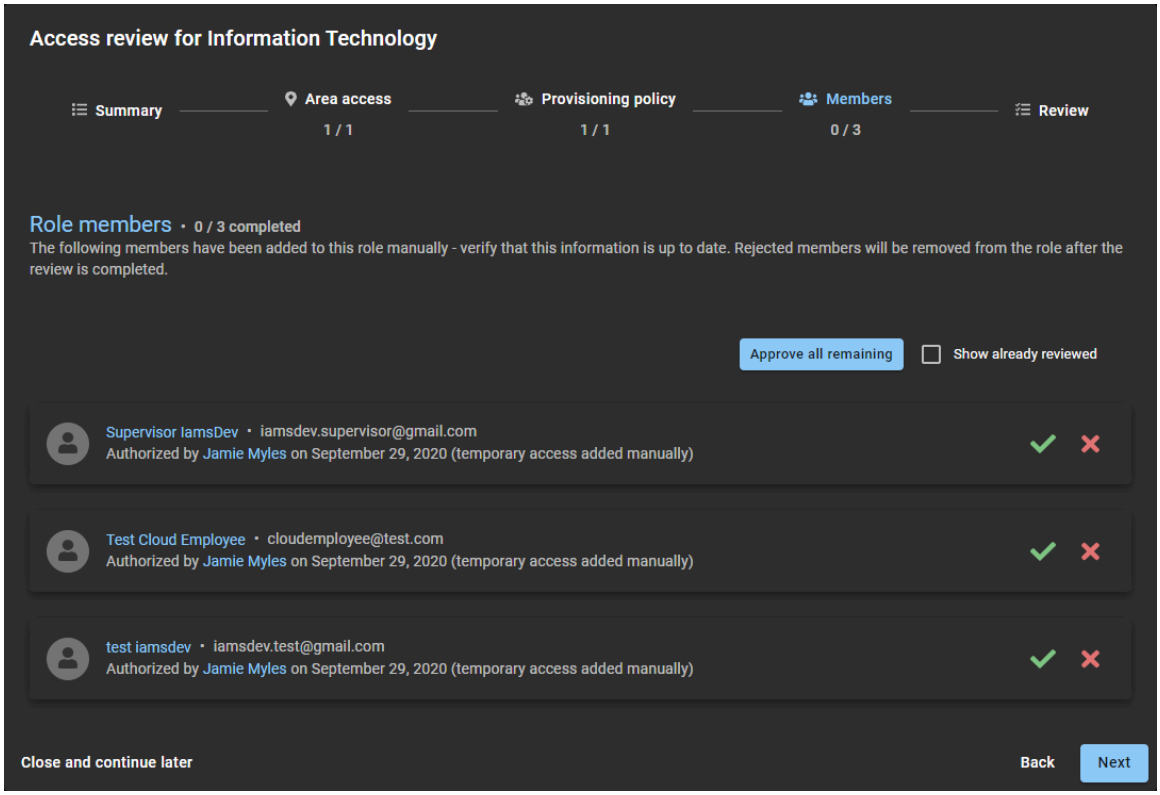


a) (Facultatif) Cliquez sur **Voir ou modifier la stratégie** pour ouvrir la page *Stratégie de provisionnement* afin d'afficher ou modifier la stratégie.

b) Cliquez sur **Approuver la stratégie** (✔) pour confirmer qu'elle est toujours valable.

c) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d'examen d'accès.

7 Vérifiez que les membres sont toujours valables dans la section **Membres** de l'examen d'accès de rôle.



a) Cliquez sur **Conserver l'accès** ( ) pour confirmer que l'accès est toujours valable.

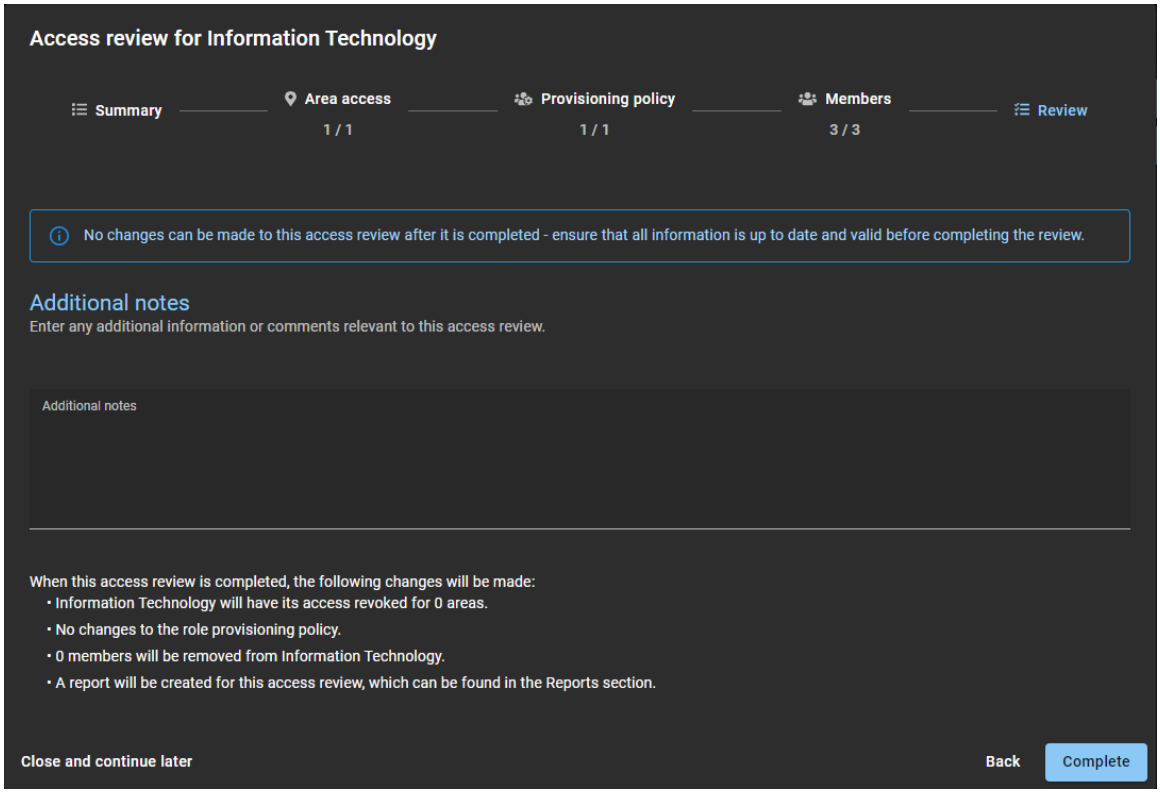
CONSEIL : Utilisez **Approuver tous les autres** pour accélérer le processus d'approbation lorsque la liste est longue, puis supprimez tout accès qui n'est plus nécessaire.

b) Cliquez sur **Supprimer l'accès** ( ) pour supprimer un accès qui n'est plus nécessaire.

c) (Facultatif) Sélectionnez **Afficher les accès déjà examinés** pour revenir en arrière et apporter des modifications.

d) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d'examen d'accès.

8 Vérifiez l'exactitude des informations dans la section **Examen** de l’examen d'accès de rôle.



a) Le cas échéant, ajoutez vos commentaires dans la section **Notes complémentaires**.
b) Avant de cliquer sur **Terminer**, vérifiez le résumé des modifications juste après la section **Notes complémentaires**.
c) (Facultatif) Si des informations vous semblent erronées, cliquez sur **Précédent** pour revenir aux sections précédentes et corriger les erreurs.
d) Si les informations dans la section **Examen** vous semblent exactes, cliquez sur **Terminer**.

Lorsque vous avez terminé

Générer un résumé d’examen d'accès, page 326

Rubriques connexes

Note sur la fonction d’examen d’accès (2 pages)

Terminer un examen d’accès d’identité (superviseur)

Afin de garantir la conformité en matière de sécurité ou la préparation aux audits, vous pouvez effectuer des examens d'accès d'identité afin de vérifier l'accès aux secteurs et rôles par vos subordonnés directs. Ces examens périodiques sont effectués par un superviseur.

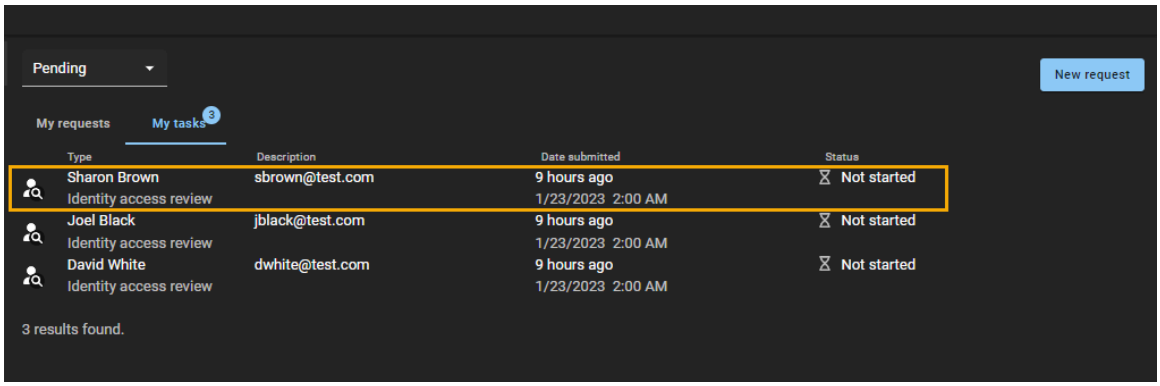
À savoir

- Les superviseurs peuvent réaliser un examen d'accès d’identité depuis la page **Mes tâches** du **Tableau de bord** ou depuis un e-mail de notification.
- Vous ne pouvez pas modifier un examen d'accès terminé.
- Tous les examens en état **Terminé** sont conservés à des fins d’audit et de suivi.

Procédure

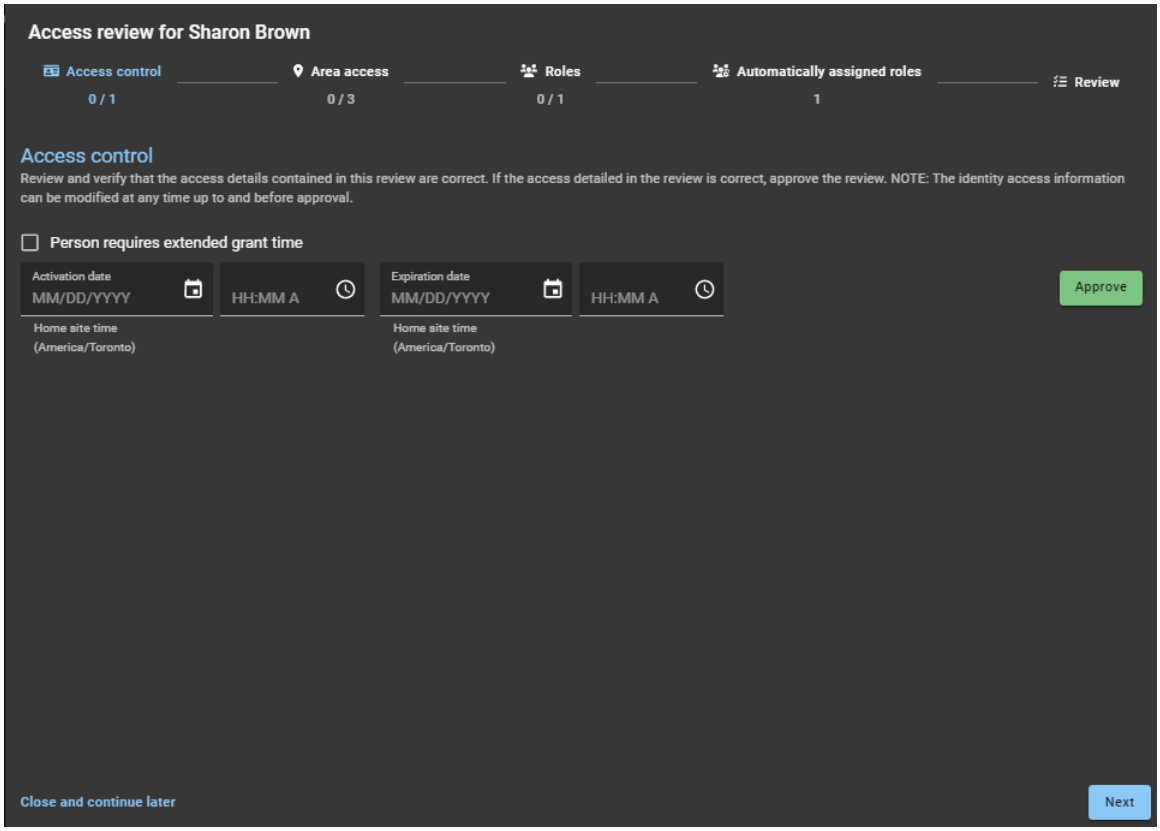
1 Cliquez sur **Tableau de bord** > **Mes tâches**.

2 Dans la liste **Mes tâches**, cliquez sur l’examen d’accès d'identité dont vous avez besoin.



3 Cliquez sur **Continuer l’examen**.

4 Dans la section *Contrôle d'accès*, examinez le contrôle d'accès.



a) (Facultatif) Si vous souhaitez prolonger le délai de déverrouillage des portes (après avoir accordé l'accès) pour les titulaires de cartes dont la propriété « Délai d'accès prolongé » est activée, cochez la case **Personne ayant besoin d'un délai d'accès prolongé**.

b) (Facultatif) Entrez ou sélectionnez une **Date d'activation** `MM/JJ/AAAA` et une heure `HH:MM.AM` pour le titulaire de cartes.

   Si les champs d'activation sont vides, la date et l'heure actuelles par défaut sont utilisées.

c) (Facultatif) Entrez ou sélectionnez une **Date d'expiration** `MM/JJ/AAAA` et une heure `HH:MM.AM` pour le titulaire de cartes.

   Lorsque les champs d'expiration sont vides, le titulaire de cartes n'expire jamais.

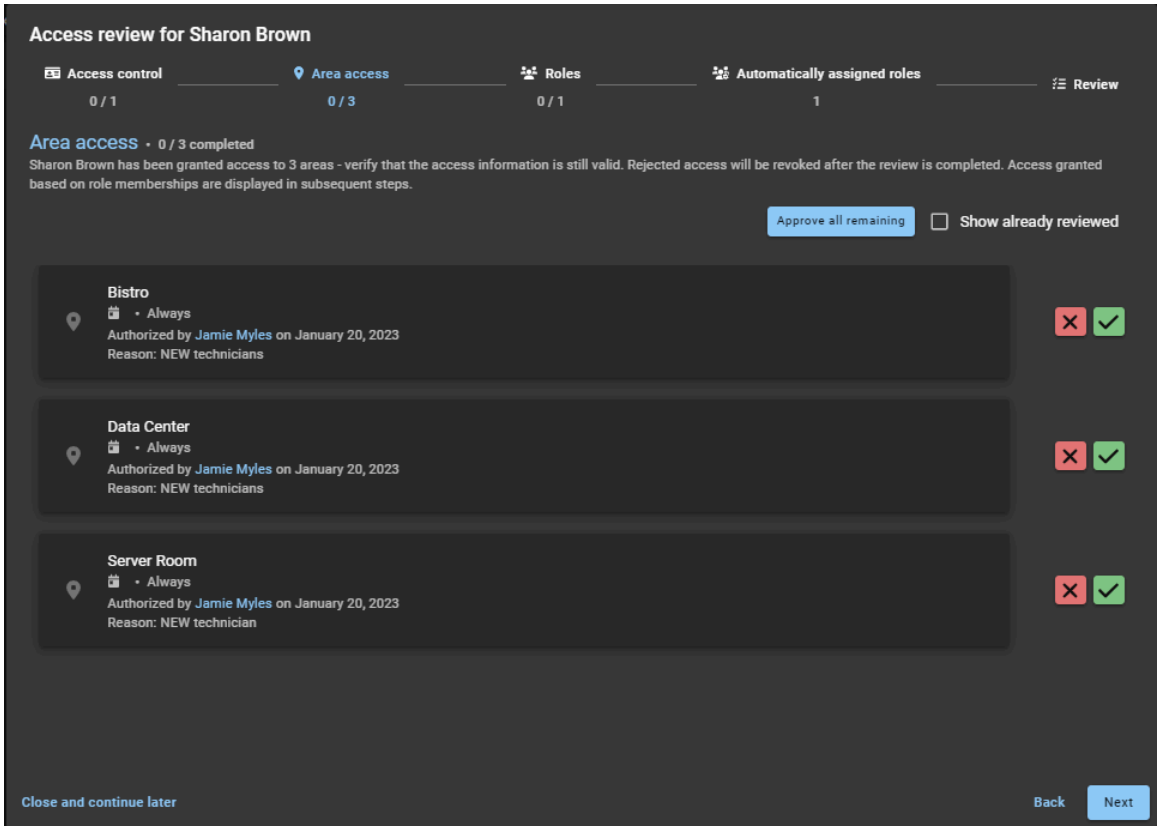
d) Cliquez sur **Approuver** pour approuver les paramètres de contrôle d'accès.

   REMARQUE : Après avoir spécifié une **Date d'activation** ou une **Date d'expiration**, vous devez inclure une heure. En cas d'absence d'heure, le bouton **Approuver** est désactivé.

e) (Facultatif) Si vous changez d'avis sur les paramètres, vous pouvez répéter les étapes précédentes pour apporter d'autres modifications, puis cliquer à nouveau sur **Approuver**.

f) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d'examen d'accès.

5 Dans la section *Accès au secteur*, examinez l'accès au secteur.



a) Cliquez sur **Conserver l'accès** ( ) pour confirmer que l'accès est toujours valable.

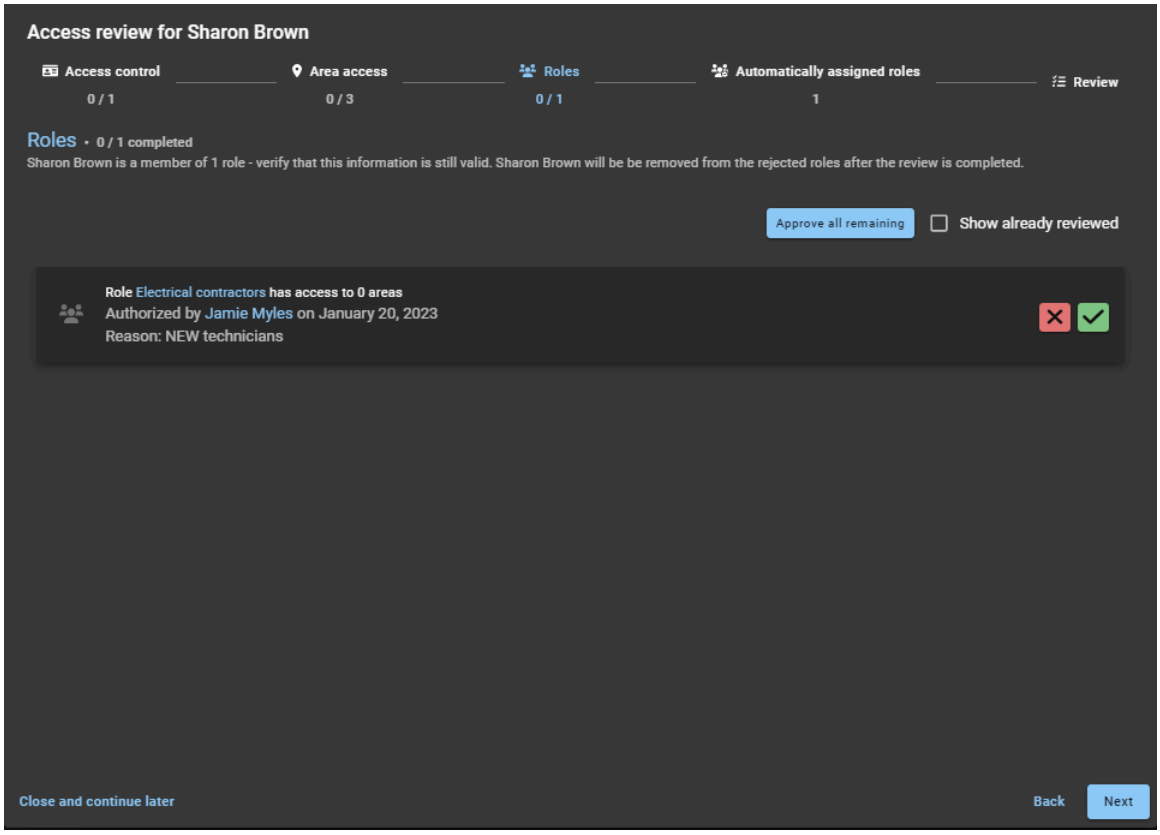
CONSEIL : Utilisez **Approuver tous les autres** pour accélérer le processus d'approbation lorsque la liste est longue, puis supprimez tout accès qui n'est plus nécessaire.

b) Cliquez sur **Supprimer l'accès** ( ) pour supprimer un accès qui n'est plus nécessaire.

c) (Facultatif) Sélectionnez **Afficher les accès déjà examinés** pour revenir en arrière et apporter des modifications.

d) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d'examen d'accès.

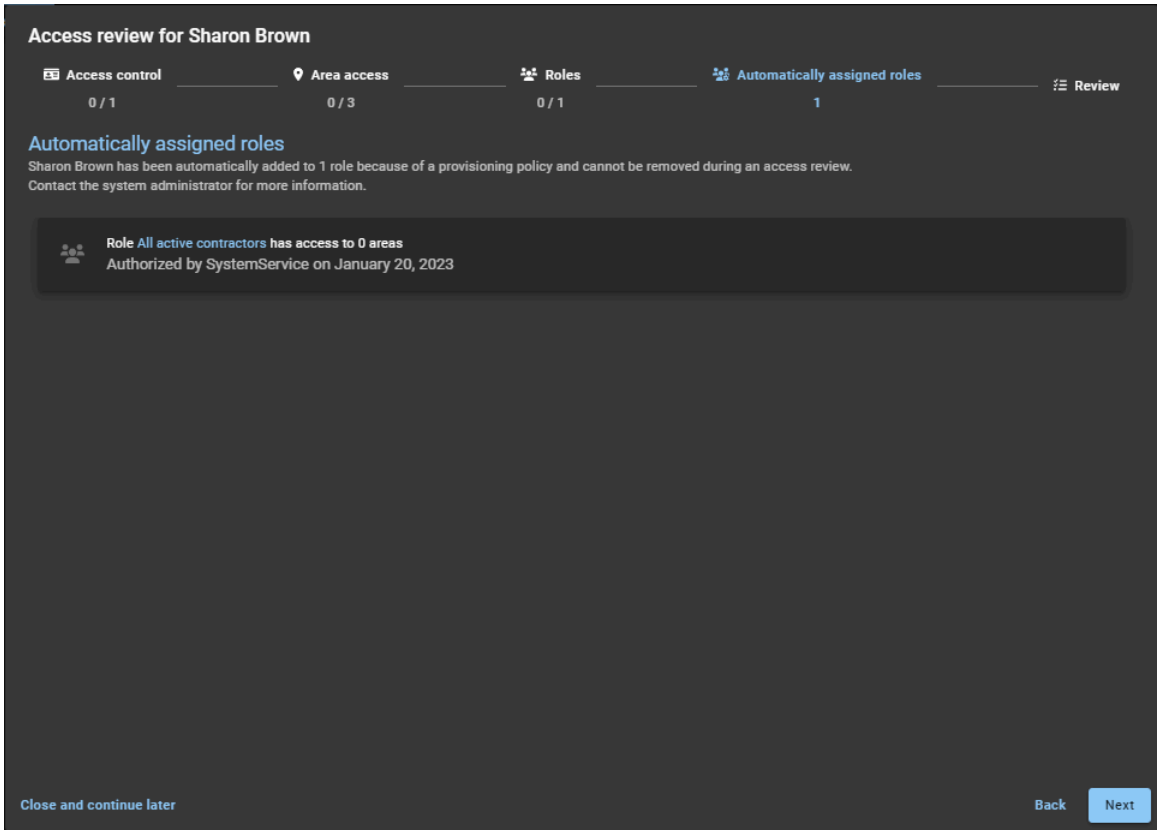
6 Dans la section *Rôles*, examinez les rôles.



a) Vérifiez les informations sur le rôle et choisissez de **Conserver l'accès** ou de **Supprimer l'accès** selon les besoins.

b) Cliquez sur **Suivant** pour passer à la section suivante de l'assistant d'examen d'accès.

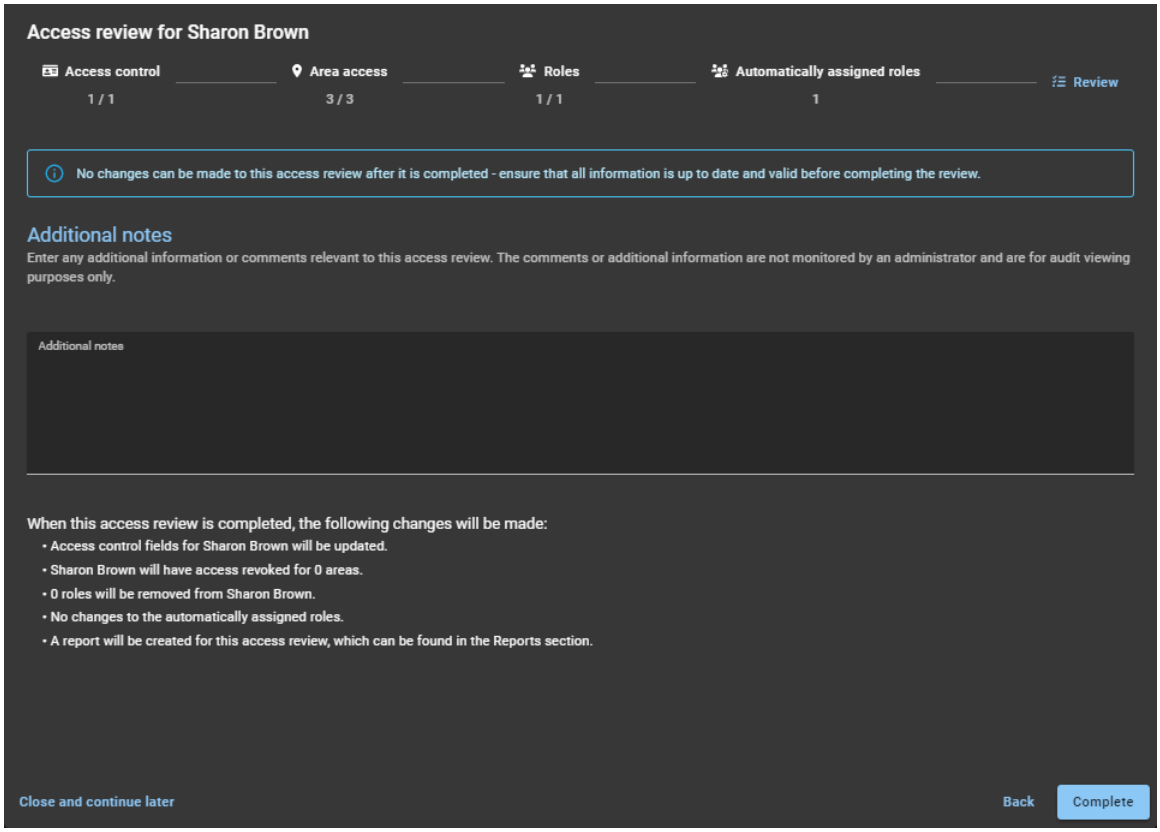
7 Dans la section *Rôles attribués automatiquement*, examinez les rôles attribués automatiquement.



Les informations relatives aux Rôles attribués automatiquement ici constituent un contexte utile pour qu'un superviseur puisse les examiner afin d'en vérifier l'exactitude et la compréhension. Elles comprennent d'autres accès que les subordonnés directs peuvent avoir en plus de leur accès au secteur attribué manuellement.

REMARQUE : Les superviseurs ne peuvent modifier aucune de ces informations car les rôles ont été automatiquement attribués en fonction de la configuration effectuée par un administrateur de compte. Si les informations relatives aux rôles attribués automatiquement ne sont plus applicables, contactez l'administrateur du compte.

8 Dans la section *Examen*, vérifiez que les informations relatives à l'examen sont exactes.



a) Le cas échéant, ajoutez vos commentaires dans la section **Notes complémentaires**.
b) Avant de cliquer sur **Terminer**, vérifiez le résumé des modifications juste après la section **Notes complémentaires**.
c) (Facultatif) Si des informations vous semblent erronées, cliquez sur **Précédent** pour revenir aux sections précédentes et corriger les erreurs.
d) Si les informations dans la section **Examen** vous semblent exactes, cliquez sur **Terminer**.

9 Répétez cette procédure pour chaque identité répertoriée dans la boîte de réception de votre tableau de bord **Mes tâches**.

Lorsque vous avez terminé

Générer un résumé d'examen d'accès, page 326

Générer un résumé d’examen d'accès

Vous pouvez générer un résumé d’examen d'accès pour tout examen d'accès terminé, afin de l’envoyer à un auditeur ou à d'autres membres de votre organisation.

Avant de commencer

Terminez vos examens d'accès.

À savoir

Vous ne pouvez générer un résumé d’examen d'accès que pour un seul examen d'accès terminé.

Procédure

1 Sur la page d'*accueil*, cliquez sur **Rapports** > **Examens d'accès**.

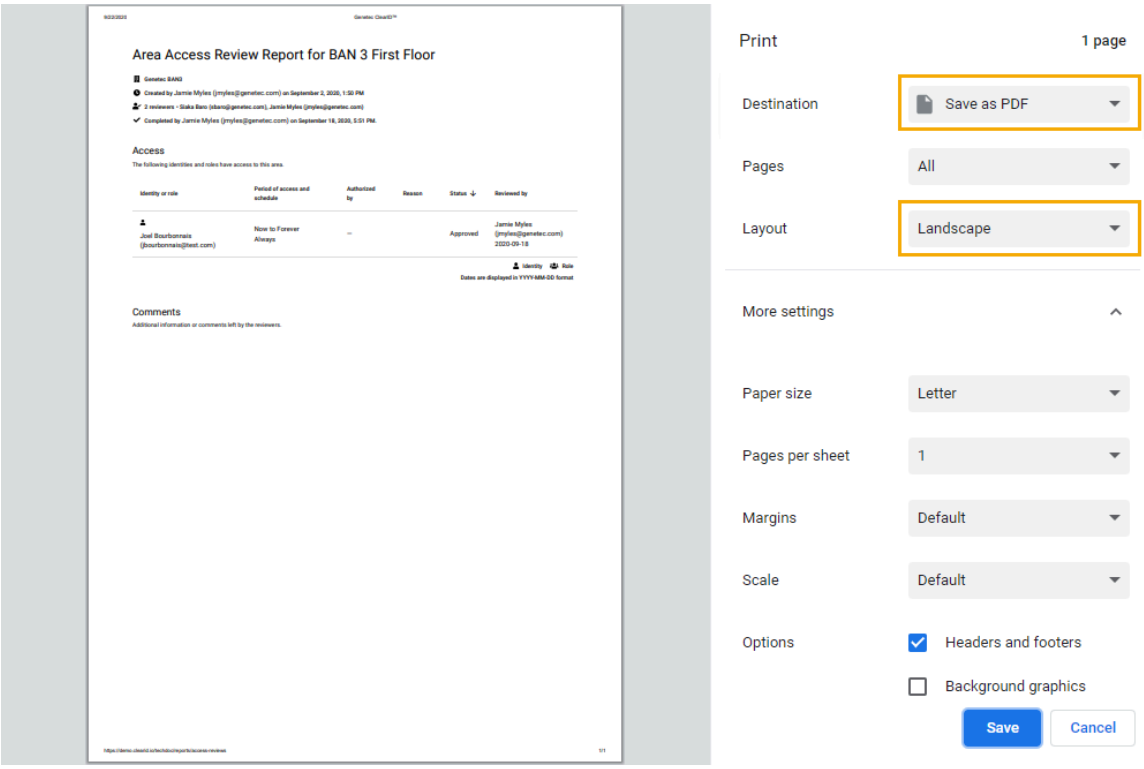
2 Configurez les filtres de la colonne rapport pour limiter les résultats de rapport selon ce dont vous avez besoin.
   a) Cliquez sur le filtre **État** et sélectionnez **Terminé**.
   b) Dans la colonne **Élément d’examen**, cliquez sur l'élément d'examen correspondant à l'*examen d'accès terminé* dont vous avez besoin.

3 Cliquez sur **Imprimer**.
   REMARQUE : L’option de mise en page **Portrait** et la case à cocher **Graphique d'arrière-plan** ne sont pas prises en charge.

4 Dans la section *Imprimer*, sélectionnez une option dans la liste **Destination**.

Les rapports sont généralement envoyés vers une imprimante pour obtenir une sortie papier, ou enregistrés au format PDF pour pouvoir les transmettre aux contrôleurs ou les partager par e-mail. D'autres options de destination sont également disponibles.

BONNE PRATIQUE : Dans la liste **Mise en page**, sélectionnez **Paysage** pour un affichage optimal.



IMPORTANT : Les options affichées dans la boite de dialogue *Imprimer* dépendent de votre navigateur, de votre ordinateur et des périphériques connectés et de la configuration de votre organisation.

5 (Facultatif) Dans la section **Plus de paramètres**, sélectionnez l'option **En-têtes et pieds de page** si vous souhaitez inclure la **Date** et le **Nom de fichier** du rapport dans l'en-tête.

6 Si vous avez sélectionné une imprimante, cliquez sur **Imprimer** et suivez les instructions à l'écran.

7 Si vous avez sélectionné **Enregistrer au format PDF**, cliquez sur **Enregistrer** et suivez les instructions à l'écran.

CONSEIL : Utilisez un nom de fichier qui vous aidera à retrouver les rapports d'examen d'accès lors d'un audit ou d'un suivi. Intégrez toutes les informations utiles, comme le secteur, le rôle ou le groupe et la date. Par exemple, *Centre de données - Examen d'accès Juillet 2020*, *Salle serveur - Examen d'accès Août 2020* ou encore *Service informatique - Examen d'accès Septembre 2020*. Le nom de fichier par défaut est *<Area or Role name> - Examen d'accès AAAA-MM-JJ.pdf*.

Votre rapport est désormais imprimé ou enregistré au format PDF pour une consultation ultérieure.

Lorsque vous avez terminé

Vous pouvez à présent envoyer le rapport d'examen d'accès à un contrôleur ou à d'autres membres de votre organisation.

À propos du rapport de demandes d'accès

Dans Genetec ClearID[MC], un rapport de demandes d’accès renvoie une liste de demandes d'accès à un site particulier. Le rapport inclut des informations sur la date de la demande d'accès, le secteur demandé, l'état, le demandeur, le destinataire de la demande et la période d'accès.

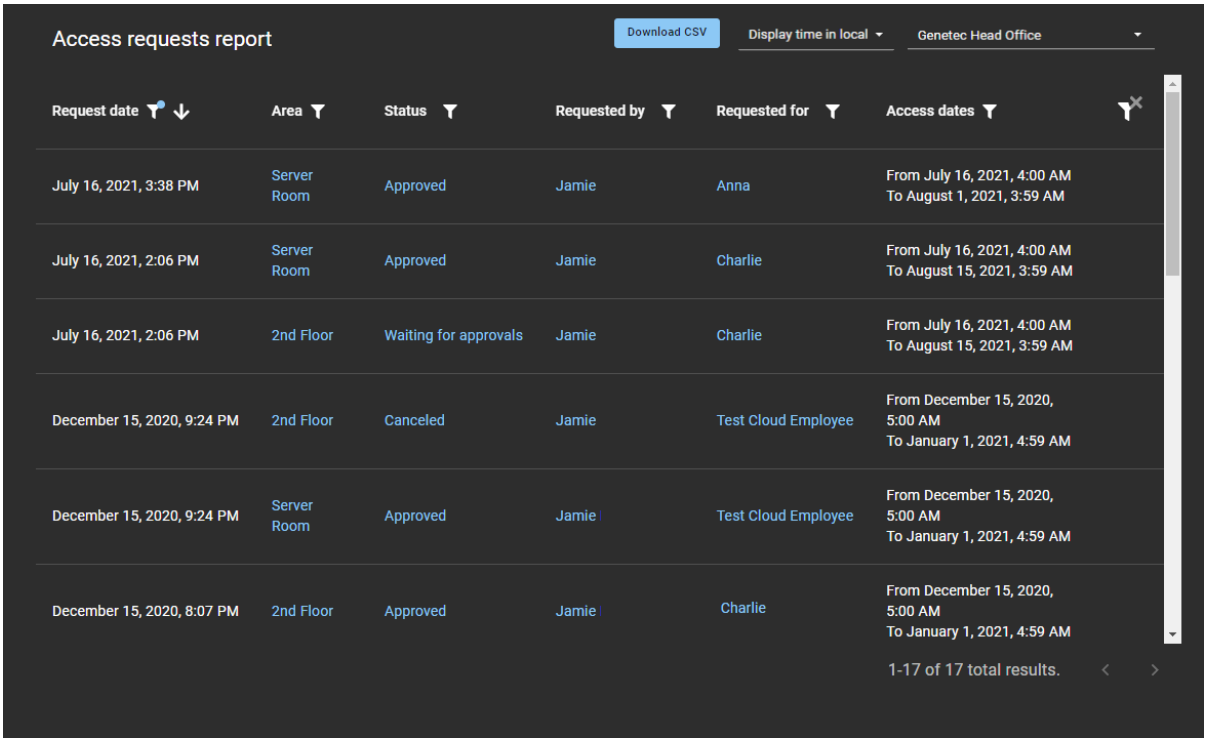


Illustration 9 : Rapport Demandes d’accès

Le rapport de demandes d'accès est utilisé par les *propriétaires de secteurs* et les *propriétaires de sites* pour vérifier l'état de l'ensemble des demandes d'accès d'un site spécifique et de tous les secteurs associés. Le rapport peut également être utilisé pour fournir des informations de demande d'accès aux contrôleurs.

Les filtres peuvent servir à affiner le résultat du rapport par date de la demande, secteur, état, demandeur, destinataire et période d'accès.

Rubriques connexes

Vérifier l’état des demandes d'accès, page 329

Vérifier l’état des demandes d'accès

En tant que *propriétaires de zone* et *propriétaires de site* , vous pouvez vérifier l'état des demandes d'accès au niveau du site pour les zones associées à un site spécifique. À l’aide du rapport de demande d’accès, vous pouvez vous assurer que l’organisation est conforme aux normes de sécurité, prête pour l’audit et que les demandes sont traitées en temps opportun.

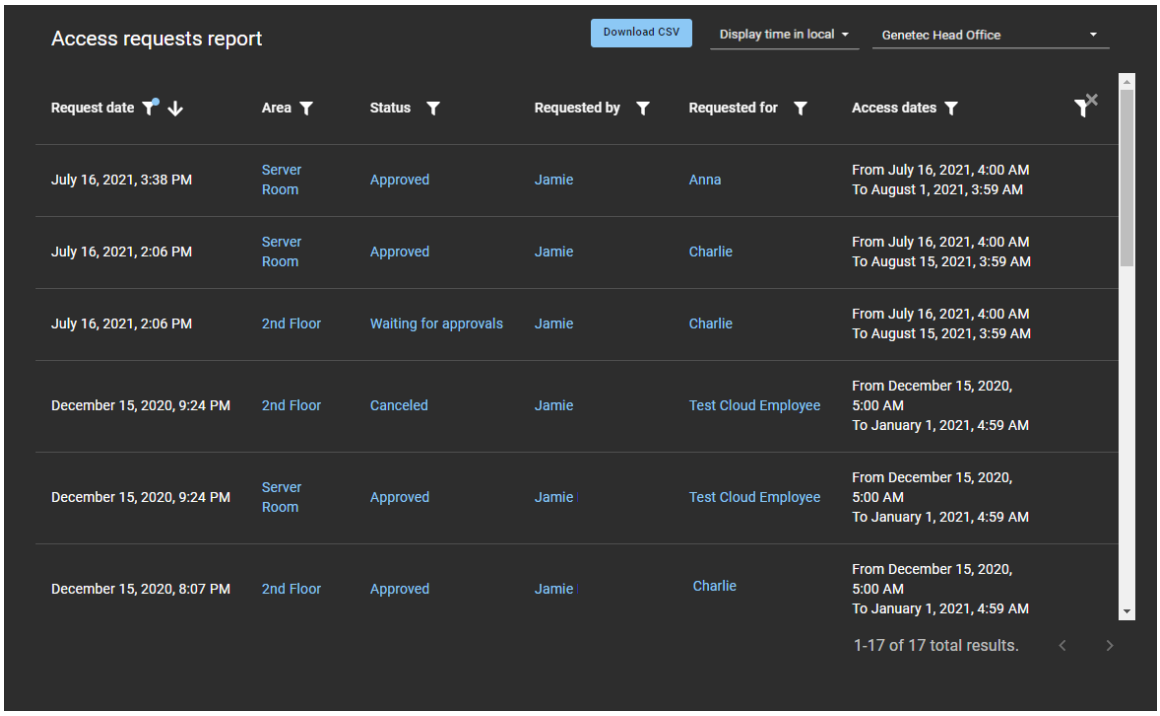
Avant de commencer

Vous devez être propriétaire d'une *zone ou propriétaire* d'un *site* pour afficher le **rapport sur les demandes d'accès** et vérifier l'état ou la progression des demandes d'accès.

Procédure

1 Depuis le *tableau*de bord, cliquez sur **Rapports** > **Demandes d’accès** .

CONSEIL : Vous pouvez filtrer les résultats pour répondre à différentes exigences. Par exemple, pour rechercher les demandes en retard, vous pouvez filtrer sur En **attente d'approbations** dans la colonne **Statut** .



2 Dans la page *Rapport des demandes d’accès* , sélectionnez le format d’heure d’affichage requis. Choisissez l'une des options suivantes :

- **Heure d'affichage locale :** Affichez les heures de rapport en utilisant l'heure système de l'ordinateur de l'utilisateur connecté.
- **Heure d'affichage UTC :** Affichez les heures de rapport en utilisant le temps universel coordonné (UTC).
- **Heure d'affichage dans le fuseau horaire du site :** Afficher les heures des rapports en utilisant le fuseau horaire du site.

3 Dans la liste des **sites** , sélectionnez le site pour lequel vous souhaitez examiner les demandes d’accès.

4 Dans la colonne **Date de la demande**, **sélectionnez l'une des options ou cliquez sur Plage** de dates et spécifiez une période pour afficher une liste des révisions d'accès.
   a) Si vous sélectionnez **Plage de dates**, utilisez le calendrier pour indiquer la plage de dates désirée.
      REMARQUE : Le délai de demande de date est limité à un maximum d'un an.
   b) (Facultatif) Pour trier les résultats du rapport par **date de demande** dans l'ordre croissant ( ) ou décroissant ( ), cliquez sur .

5 Dans la colonne**Secteur**, cliquez sur l'icône pour filtrer les résultats par nom de secteur.
   a) Recherchez un secteur ou cochez une ou plusieurs **cases** pour filtrer les résultats en fonction des secteurs qui vous intéressent.
   b) Cliquez sur l'hyperlien **Nom du secteur** pour afficher et vérifier les détails du secteur.
      CONSEIL : Pour révoquer une demande d'accès, cliquez sur le lien hypertexte **Nom de la zone** dans le rapport, puis cliquez sur **Accès** et cliquez sur à côté d'un utilisateur.

6 Dans la colonne **État** , cliquez sur l'icône pour filtrer les résultats par état.
   a) Cochez une ou plusieurs **cases** pour filtrer le résultat en fonction des états souhaités (Envoyé, En attente d'approbation, Refusé, Approuvé, Annulé ou Terminé).
   b) (Facultatif) Cliquez sur l'hyperlien **État** pour afficher la demande d'accès.
      REMARQUE : Si vous êtes un approbateur, vous pouvez **Approuver** ou **Refuser** la demande d'accès en attente lors de l'affichage de la demande.

7 Dans la colonne **Demandé par** , cliquez sur l'icône pour filtrer les résultats par demandeur d'accès.
   a) Entrez un nom d'utilisateur ou une adresse e-mail dans le champ de recherche.
   b) (Facultatif) Cliquez sur le lien **Demandeur** pour afficher des informations synthétiques sur celui-ci.

8 Dans la colonne **Demandé pour**,cliquez sur l'icône pour filtrer les résultats par destinataire d'accès.
   a) Sélectionnez l'une des options suivantes :
      - **Tous :** Affiche l'ensemble des demandes d'accès des identités et des rôles.
      - **Une identité :** Sélectionnez **Une identité**, puis entrez une identité dans le champ de recherche si vous souhaitez filtrer les demandes d'accès d'une identité spécifique.
      - **Un rôle :** Sélectionnez **Un rôle**, puis entrez un rôle dans le champ de recherche si vous souhaitez filtrer les demandes d'accès d'un rôle spécifique.
   b) (Facultatif) Cliquez sur l'hyperlien **Demandé pour** pour afficher des détails résumés sur le destinataire.

9 Dans la colonne **Période d'accès**, cliquez sur l'icône pour filtrer les résultats en fonction d'une plage de dates.

10 Cliquez sur **Télécharger CSV** pour télécharger une copie du rapport des demandes d'accès au format CSV. Le rapport peut ensuite être utilisé à des fins d'audit, pour conserver un exemplaire physique, pour le joindre à une demande d'audit, pour une analyse hors ligne ou encore pour traiter ou consolider les données dans un tableur pour d'autres publics.
   a) Suivez les instructions dans votre navigateur pour télécharger le fichier exporté.
      Le fichier est exporté sous la forme d'un fichier *.CSV* dans le dossier de téléchargement par défaut de votre navigateur. Par défaut, le fichier exporté est créé d'après le nom de votre site. Par exemple, AccessRequest_*yoursitename*_*fromdate*_to_*todate*.csv (*AccessRequest_Genetec_Montreal_2024-09-14.csv*).
      REMARQUE : Les colonnes et les entrées dans le fichier CSV peuvent varier en fonction des filtres sélectionnés au moment de télécharger le rapport.

11 (Facultatif) Cliquez sur pour réinitialiser les filtres.

Vous avez maintenant vérifié l'état de toutes les demandes d'accès au niveau du site pour toutes les zones associées à un site spécifié.

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles.

Lorsque vous avez terminé

Approuvez ou refusez les demandes d'accès, selon les besoins :

- Approuver les demandes d’accès à un secteur, page 366
- Refuser les demandes d’accès à un secteur, page 368

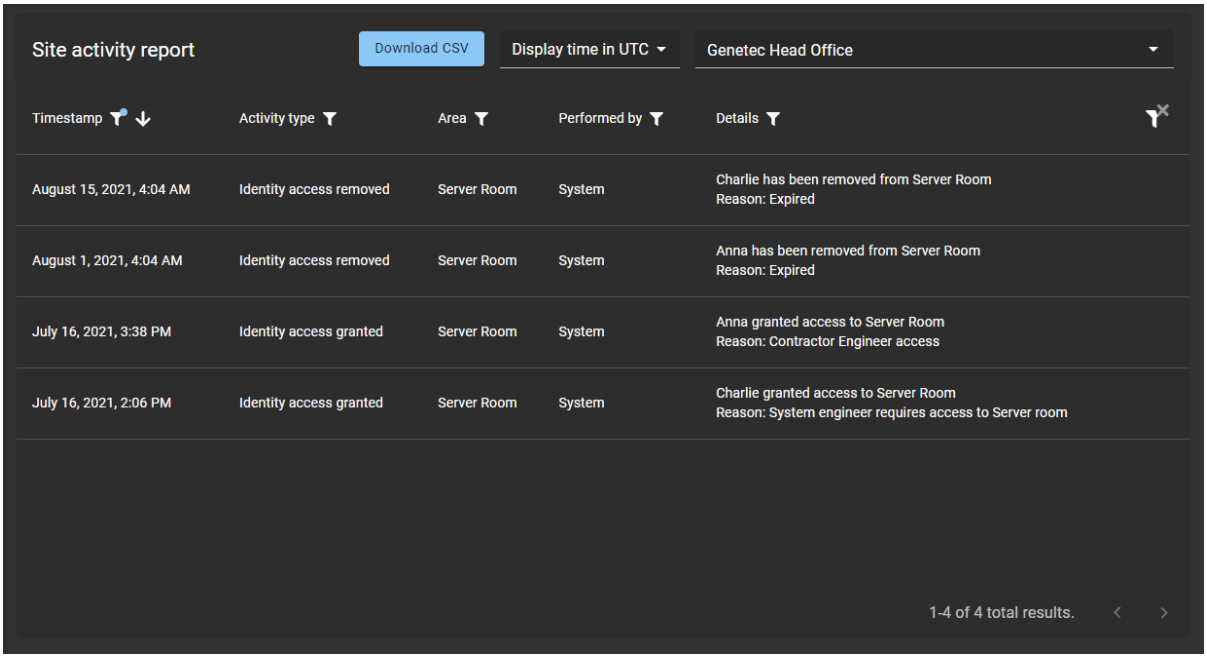
Rubriques connexes

À propos du rapport de demandes d'accès, page 328
Demander un accès, page 156

À propos du rapport d'activité de site

Dans Genetec ClearID[MC], le rapport d'activité de site est un historique des activités ou des événements associés à un site particulier. Le rapport contient des informations d'horodatage, de type d'activité, de secteur, sur les personnes ayant effectué l'activité, ainsi qu'une section détails qui contient des informations de motif.

Rapport d'activité du site



Le rapport d'activité du site est utilisé par les *propriétaires de site* pour vérifier les événements de l'historique de configuration au niveau d'un site. Le rapport peut également être utilisé pour fournir des informations sur les activités du site aux contrôleurs.

Des filtres peuvent être utilisés pour affiner le résultat de la recherche par horodatage, type d'activité, secteur, effectué par et détails.

Rubriques connexes

Afficher un rapport d'activité de site, page 333

Afficher un rapport d'activité de site

Vous pouvez afficher un rapport d'activité de site pour consulter l'historique des activités ou des événements d'un site particulier.

Avant de commencer

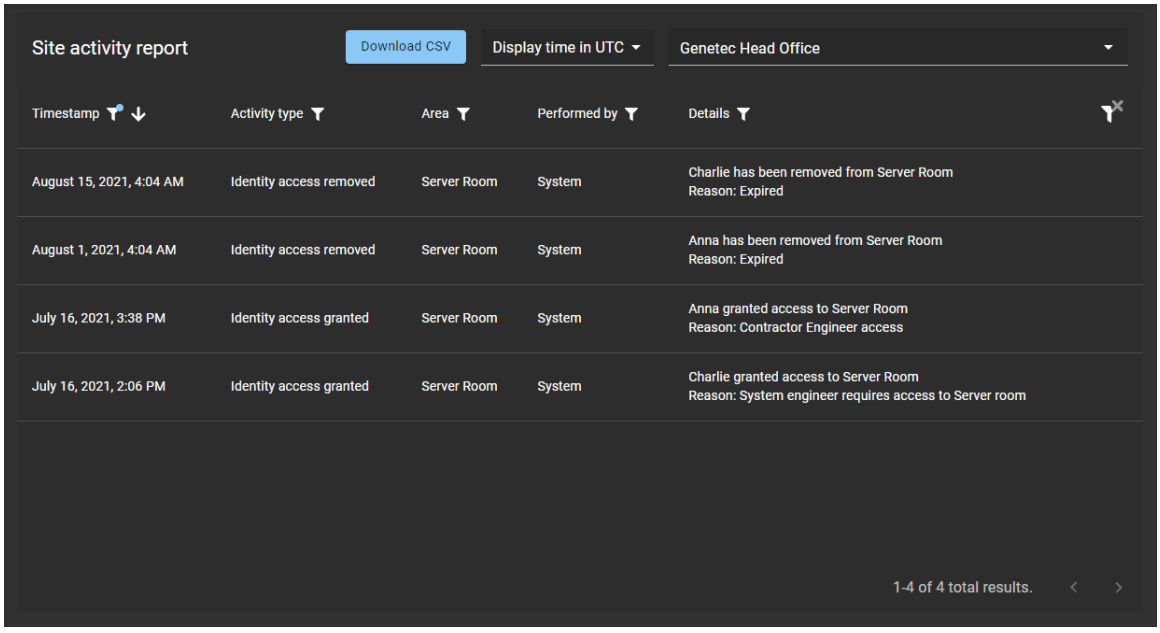
- Ajouter des gestionnaires de secteurs
- Ajouter des membres de rôle
- Demander l'accès

À savoir

Seul le propriétaire d'un site peut afficher un **rapport d'activité de site** pour consulter l'historique des activités ou des événements d'un site particulier.

Procédure

1 Sur la page d'accueil, cliquez sur **Rapports** > **Activité de site**.



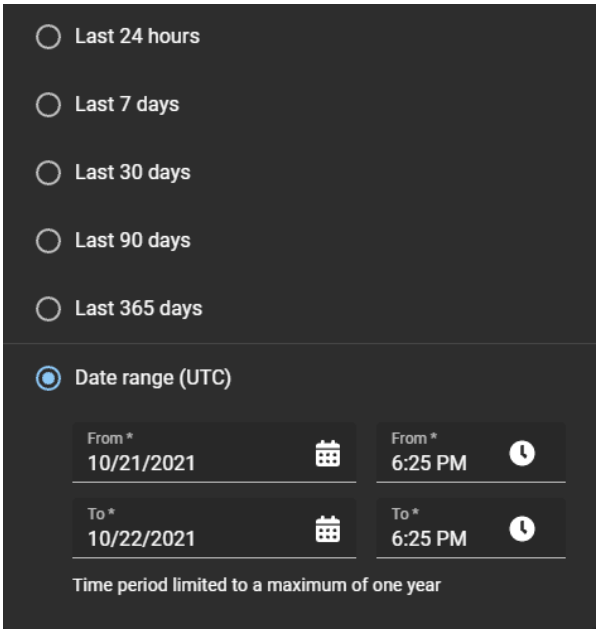
2 Sur la page *Rapport d'activité de site*, sélectionnez l'heure d'affichage dont vous avez besoin. Choisissez l'une des options suivantes :

- **Heure d'affichage locale :** Les heures d'affichage sont affichées via l'heure du système de l'ordinateur de l'utilisateur connecté.
- **Heure d'affichage UTC :** Les heures du rapport sont affichées au format UTC (temps universel coordonné).
- **Heure d'affichage dans le fuseau horaire du site :** Les heures du rapport sont affichées en fonction du fuseau horaire du site.

3 Dans la liste de **sites**, sélectionnez le site dont vous avez besoin.

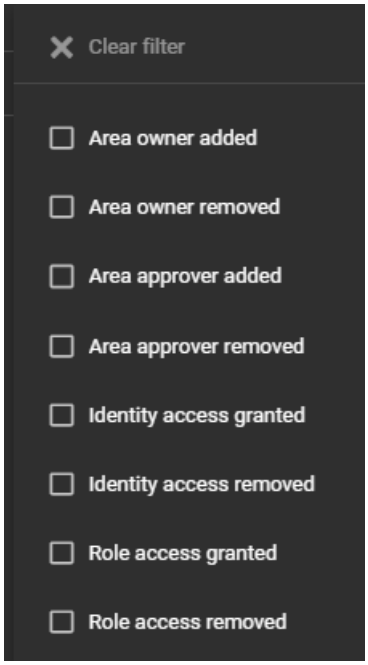
4 Dans la colonne **Horodatage**, cliquez sur pour filtrer le résultat par date.

a) Sélectionnez une plage de dates prédéfinie parmi les choix disponibles, ou spécifiez une plage particulière à l'aide du sélecteur de plage de dates.

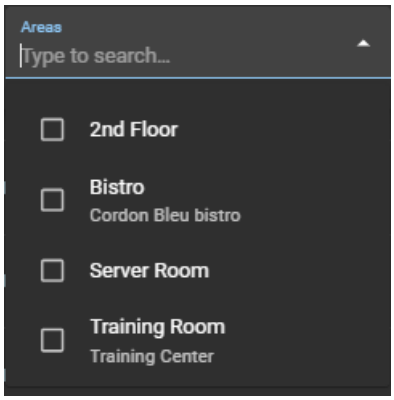


b) (Facultatif) Utilisez les icônes de tri (et) pour afficher le résultat en ordre croissant ou décroissant.

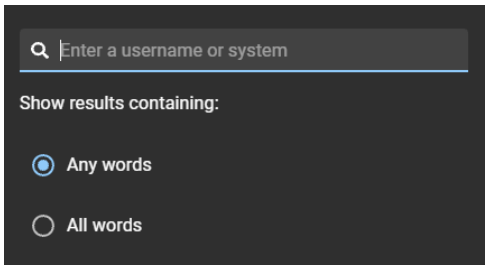
5 Dans la colonne **Type d'activité** , cliquez sur pour filtrer le résultat par type d'activité.



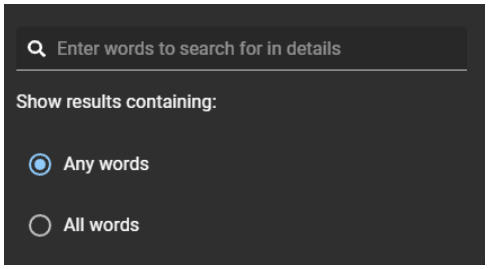
6 Dans la colonne **Secteur**, cliquez sur pour filtrer le résultat par secteur.



7 Dans la colonne **Effectué par**, cliquez sur pour ouvrir une boîte de dialogue de recherche et filtrer les résultats sur la personne ayant effectué une activité. Il peut s'agir de tâches effectuées par un utilisateur particulier ou de tâches effectuées automatiquement par le système.



8 Dans la colonne **Détails**, cliquez sur pour ouvrir une boîte de dialogue qui permet de rechercher dans les détails ou les motifs à l'aide de critères de recherche.



9 Cliquez sur **Télécharger un fichier CSV** pour télécharger une copie du rapport d'activité de site au format CSV. Le rapport peut ensuite être utilisé à des fins d'audit, pour conserver un exemplaire physique, pour le joindre à une demande d'audit, pour une analyse hors ligne ou encore pour traiter ou consolider les données dans un tableur pour d'autres publics.

a) Suivez les instructions dans votre navigateur pour télécharger le fichier exporté.

Le fichier est exporté sous la forme d'un fichier *.CSV* dans le dossier de téléchargement par défaut de votre navigateur. Par défaut, le fichier exporté est créé d'après le nom de votre site. Par exemple, *nomdevotresite*_from_*datededébut*_to_*datedefin*_SiteActivityReport.csv (*Siège_de_Genetec_from_2020-10-22_to_2021-10-22_SiteActivityReport.csv*).

REMARQUE : Les colonnes et les entrées dans le fichier CSV peuvent varier en fonction des filtres sélectionnés au moment de télécharger le rapport.

10 (Facultatif) Cliquez sur pour réinitialiser les filtres.

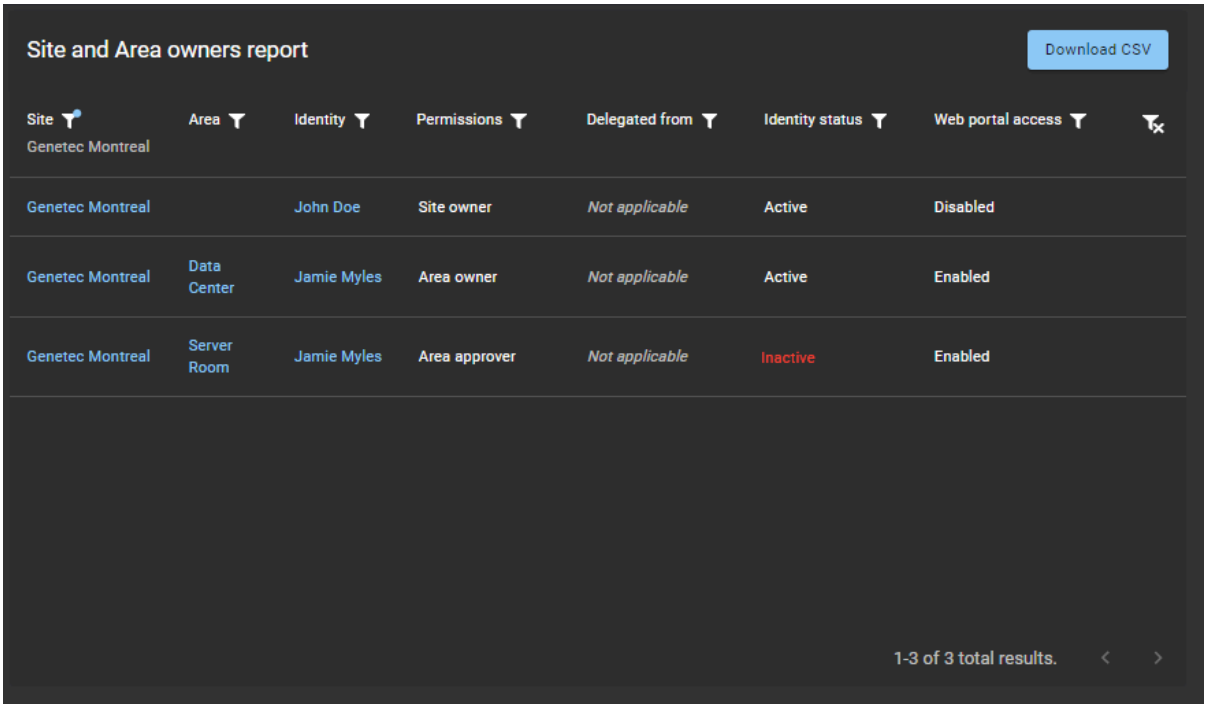
Rubriques connexes

À propos du rapport d'activité de site, page 332

À propos du rapport Propriétaires de sites et de secteurs

Dans Genetec ClearID[MC], le rapport Propriétaires de sites et de secteurs est une liste qui fournit une vue d'ensemble de toutes les identités et de leurs autorisations. Seules les identités qui sont des propriétaires de sites, approbateurs de secteurs, propriétaires de secteurs ou responsables de listes de surveillance sont affichées dans ce rapport. Le rapport contient des informations sur les sites, secteurs, identités, autorisations, délégations, l'état des identités et les accès au portail web.

Rapport Propriétaires de sites et de secteurs.



Le rapport Propriétaires de sites et de secteurs permet aux administrateurs de comptes d'obtenir une vue d'ensemble de toutes les identités et leurs autorisations. Lorsque le rapport est utilisé par un propriétaire de site, seules les informations sur ses propres sites sont affichées.

Des filtres peuvent être utilisés pour affiner le résultat de la recherche par site, secteur, identité, autorisations, délégué par, état d'identité et accès au portail Web.

Rubriques connexes

Afficher le rapport Propriétaires de sites et de secteurs, page 337

Afficher le rapport Propriétaires de sites et de secteurs

Vous pouvez utiliser le rapport Propriétaires de sites et de secteurs pour obtenir une vue d'ensemble des identités et de leurs autorisations.

Avant de commencer

Vérifiez que vous avez affecté des identités aux éléments suivants :

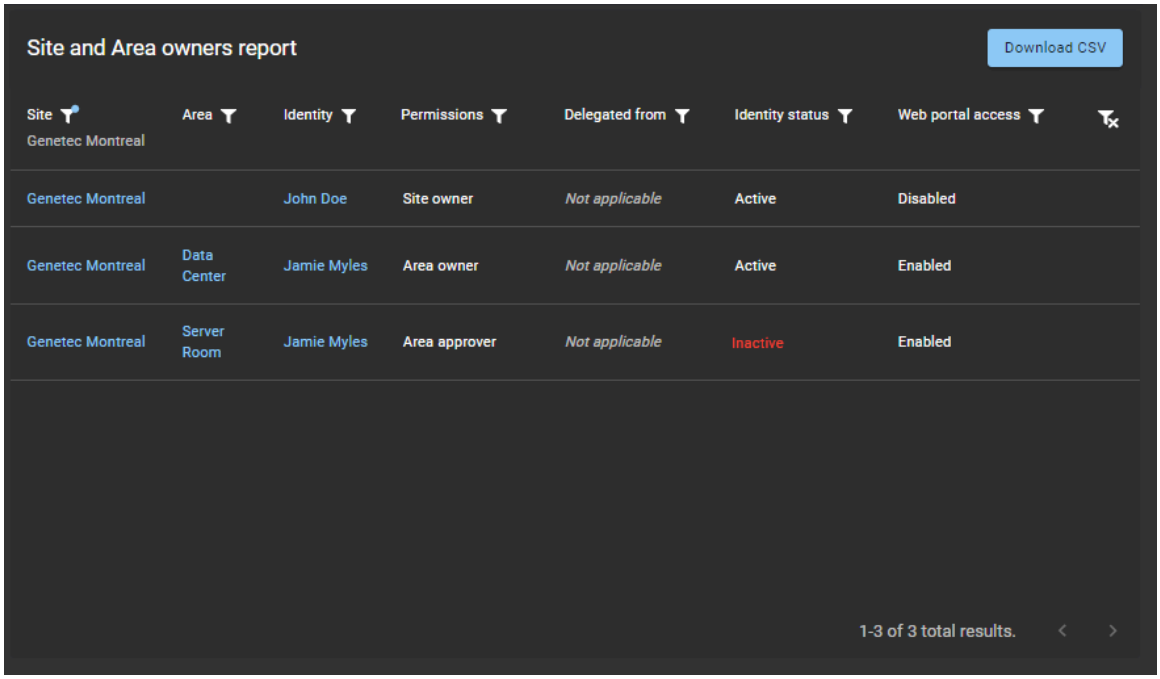
- Propriétaires de sites
- Propriétaires et approbateurs de secteurs
- Gestionnaires de listes de surveillance

À savoir

Seul un administrateur de comptes ou un propriétaire de site peut afficher un rapport **Propriétaires de sites et de secteurs** pour consulter toutes les identités et leurs autorisations. Lorsque le rapport est utilisé par un propriétaire de site, seules les informations sur ses propres sites sont affichées.

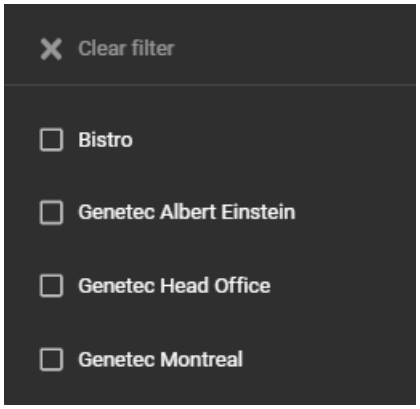
Procédure

1 Sur la page d'accueil, cliquez sur **Rapports** > **Rapport Propriétaires de sites et de secteurs**.

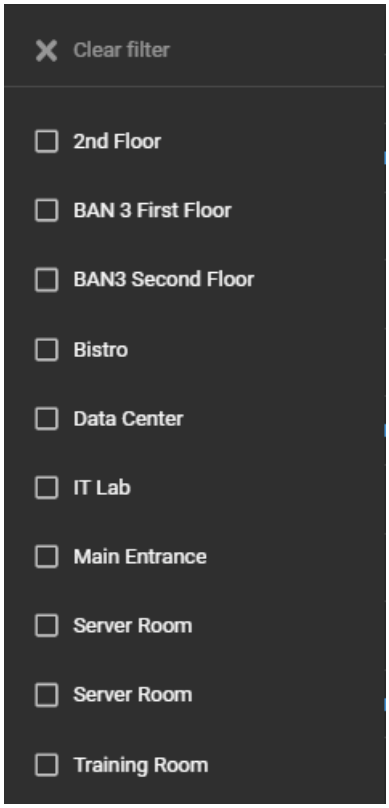


2 Sur la page *Rapport Propriétaires de sites et de secteurs*, sélectionnez les filtres de votre choix.

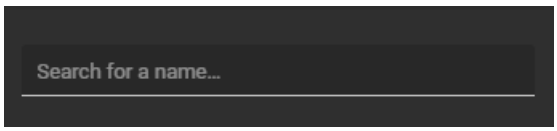
a) Dans la colonne **Site**, cliquez sur pour filtrer le résultat par site.



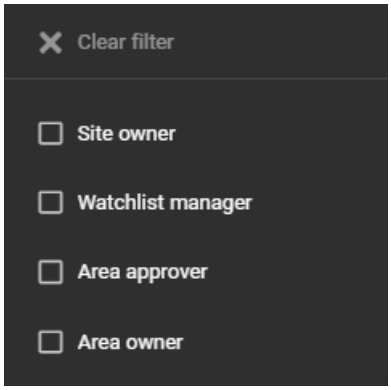
b) Dans la colonne **Secteur**, cliquez sur pour filtrer le résultat par secteur.



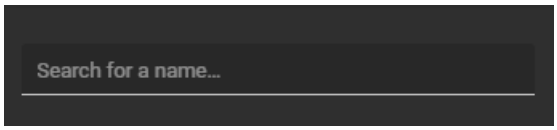
c) Dans la colonne **Identité**, cliquez sur pour ouvrir une boîte de dialogue de recherche et filtrer le résultat par une identité.



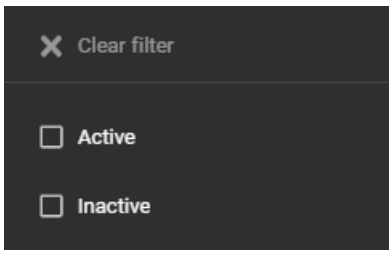
d) Dans la colonne **Autorisations**, cliquez sur pour filtrer le résultat par type d'autorisation.



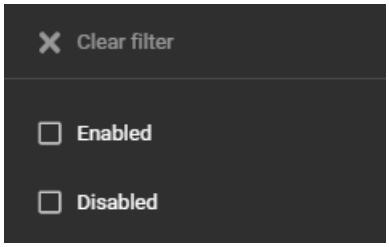
e) Dans la colonne **Délégué par**, cliquez sur pour ouvrir une boîte de dialogue de recherche et filtrer le résultat par une personne ayant délégué des tâches.



f) Dans la colonne **État d'identité**, cliquez sur l'icône pour filtrer les résultats par état d'identité.



g) Dans la colonne **Accès au portail Web**, cliquez sur pour filtrer le résultat par accès au portail Web.



3 Cliquez sur **Télécharger un fichier CSV** pour télécharger une copie du rapport des propriétaires de sites et de secteurs au format CSV. Ce format peut être utilisé à des fins d'audit, pour conserver un exemplaire physique, pour le joindre à une demande d'audit, pour une analyse hors ligne ou encore pour traiter ou consolider les données dans un tableur pour d'autres publics.

a) Suivez les instructions dans votre navigateur pour télécharger le fichier exporté.

Le fichier est exporté sous la forme d'un fichier *.CSV* dans le dossier de téléchargement par défaut de votre navigateur. Par défaut, le fichier exporté est créé d'après le nom du rapport et la date de téléchargement. Par exemple, *SiteAreaOwners_2022-02-14.csv*.

REMARQUE : Les colonnes et les entrées dans le fichier CSV peuvent varier en fonction des filtres sélectionnés au moment de télécharger le rapport.

4 (Facultatif) Cliquez sur pour réinitialiser les filtres.

Rubriques connexes

À propos du rapport Propriétaires de sites et de secteurs, page 336

8

Gérer les secteurs

Découvrez comment gérer les secteurs.

Cette section aborde les sujets suivants:

- " À propos des secteurs ", page 342
- " Créer des secteurs ", page 343
- " Ajouter des responsables de secteurs ", page 353
- " Ajouter des horaires à un secteur ", page 354
- " Configurer les documents de demande d'accès pour les secteurs ", page 356
- " Accorder l'accès à un secteur ", page 359
- " Examiner les accès à un secteur ", page 364
- " Approuver les demandes d’accès à un secteur ", page 366
- " Refuser les demandes d’accès à un secteur ", page 368

À propos des secteurs

Dans Genetec ClearID[MC], un secteur est une entité logique qui définit la relation entre les propriétaires de secteurs et les portes Synergis[MC]. Les secteurs sont gérés par le propriétaire du secteur.

Les portes ne sont pas gérées dans Genetec ClearID[MC] mais dans Security Center :

- La gestion des portes dans ClearID n'est pas envisageable en raison de la distance du matériel.
- Les portes doivent être configurées correctement dans Security Center et associées au matériel physique qui gère la porte.
- Une fois que des secteurs ont été créés dans ClearID et synchronisés avec Security Center, les portes peuvent être ajoutées à ces secteurs dans Security Center.

  REMARQUE : Les portes déplacées vers des secteurs héritent des règles d'accès du secteur correspondant.
- La configuration des portes est effectuée dans Security Center indépendamment des secteurs. Une fois que les *portes* et les *secteurs* ont été créés dans Security Center, les portes doivent être ajoutées aux secteurs.

Rubriques connexes

Ajouter des portes à un secteur, page 346

Créer des secteurs

Dans Genetec ClearID[MC], un secteur est une entité logique qui définit la relation entre les propriétaires de secteurs et les portes Synergis[MC]. Les secteurs sont gérés par le propriétaire du secteur.

Avant de commencer

- Créez vos sites.

À savoir

- Seuls les administrateurs de compte ou les *propriétaires de sites* peuvent créer des secteurs dans Genetec ClearID[MC].
- Dans Genetec ClearID[MC] un propriétaire de secteur est une identité qui a un pouvoir sur un secteur. Le propriétaire peut définir la stratégie liée à un secteur et affecter des approbateurs de secteur.
- Un *secteur* est lié ou associé à un système Security Center.

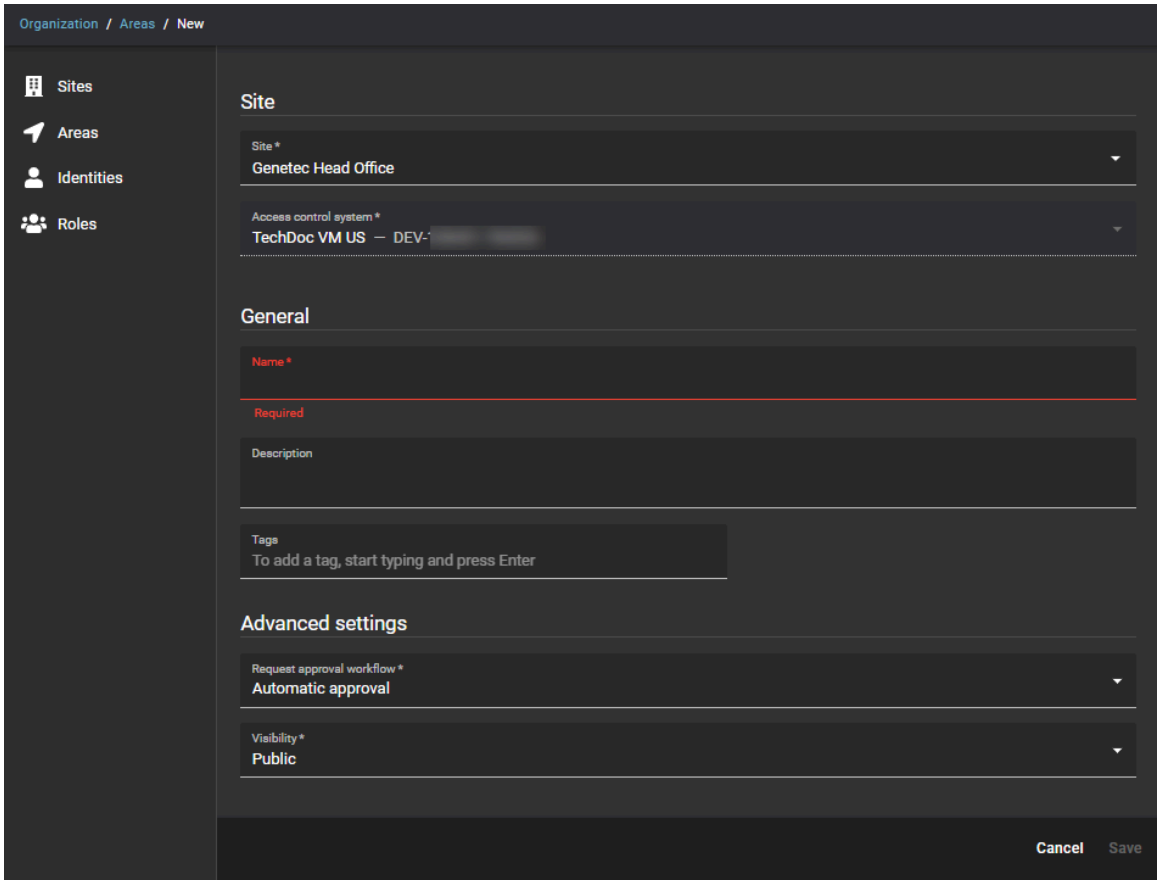
Procédure

1 Cliquez sur **Organisation** > **Secteurs**.

2 Cliquez sur **Créer un secteur**.

REMARQUE : Les champs obligatoires sont mis en évidence dans l'interface utilisateur avec un astérisque (*).

3 Dans la section *Site*, remplissez les champs :



- **Site :** Dans la liste **Site**, sélectionnez le site auquel vous souhaitez associer votre secteur.
- **Système de contrôle d'accès :** Ce champ est prérempli en fonction du site précédemment sélectionné. Ce système de contrôle d'accès sert à répercuter les modifications apportées à ClearID dans Security Center.

  REMARQUE : Si un message d'avertissement s'affiche à la place des informations ACS connexes, cliquez sur le lien pour revenir à la configuration du site et saisir les informations ACS connexes.

a) Dans la section *Paramètres généraux*, remplissez les champs :

- **Nom :** Saisissez un nom pour le secteur.
- **Description :** Entrez une description qui indique l'emplacement géographique ou physique du bâtiment ou du secteur.
- **Balises :** Saisissez d'autres mots clés ou catégories de termes de recherche qui pourraient être utilisés pour trouver le secteur.

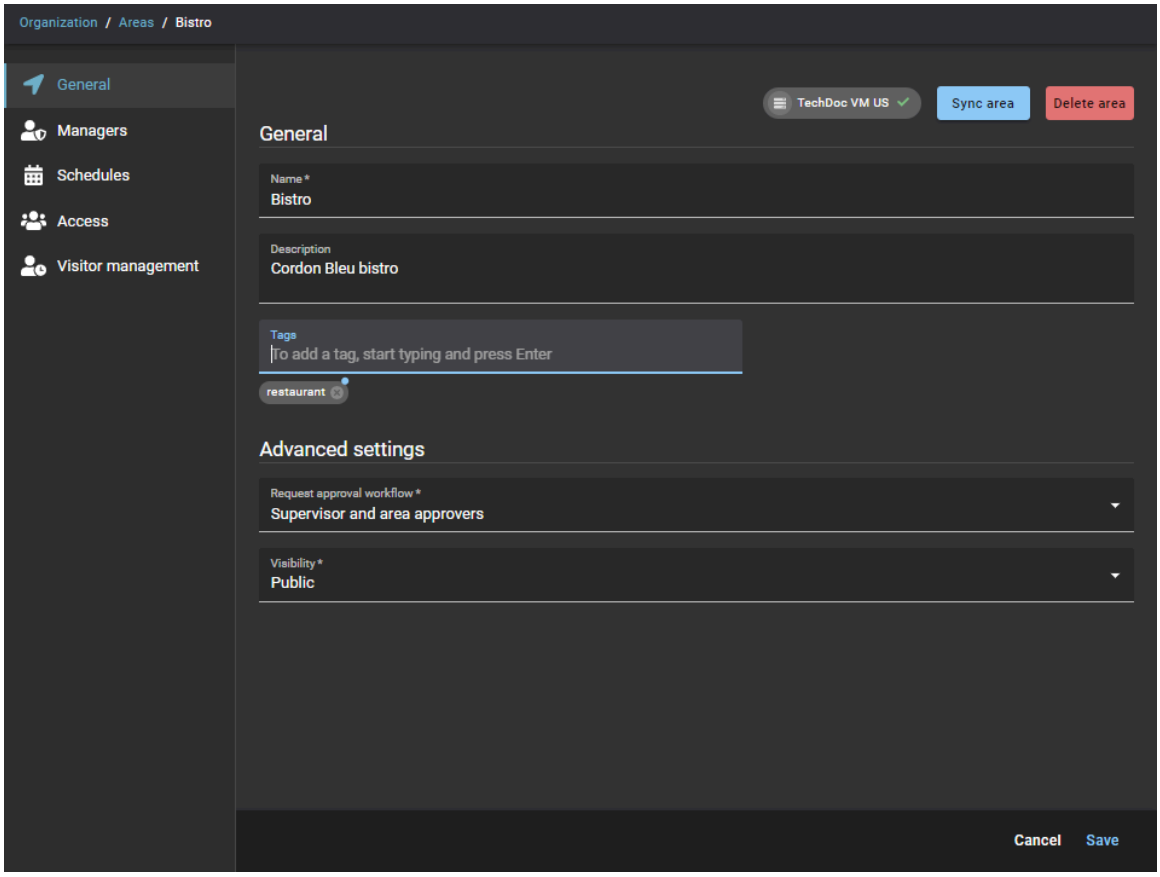
b) Dans la section *Options avancées*, sélectionnez les options nécessaires.

- **Processus d'approbation de demande :** Choisissez l'option de processus d'approbation dont vous avez besoin :
  - **Approbation automatique :** Les demandes de secteur sont automatiquement approuvées via une politique basée sur les rôles.
  - **Approbateurs de secteur :** Les demandes de secteur sont approuvées manuellement par les approbateurs de secteur autorisés.
  - **Superviseur et approbateurs de secteur :** Les demandes de secteur sont approuvées manuellement par le superviseur et les approbateurs de secteur.
  - **Superviseurs :** Les demandes de secteur sont approuvées manuellement par les superviseurs.
- **Visibilité :** Choisissez l'option de visibilité dont vous avez besoin :

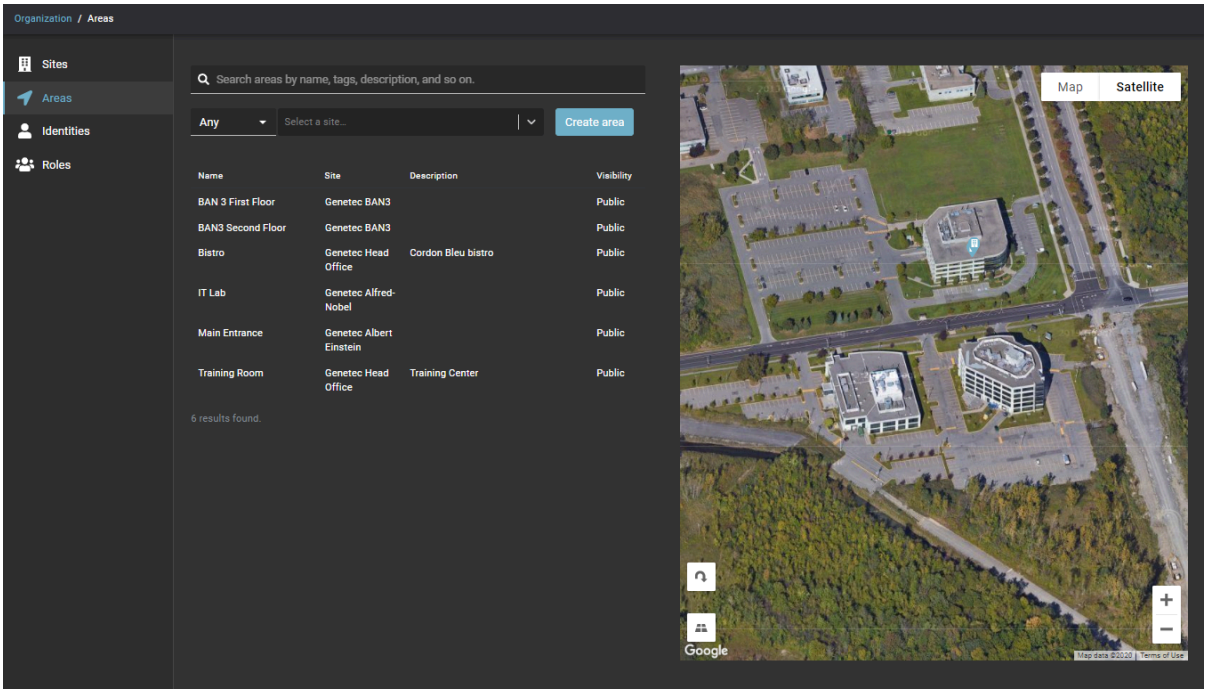
- **Public :** Le secteur est visible par tous et des demandes d'accès peuvent être créées pour le secteur. Ce sont les paramètres par défaut.
- **Privé :** Le secteur est privé et doit être masqué, et les demandes d'accès ne sont pas prises en charge pour le secteur.

4 Cliquez sur **Enregistrer**.

Lorsque le secteur est enregistré, des commandes sont automatiquement envoyées au module externe pour créer un secteur dans Security Center.



Votre secteur a été créé dans ClearID.



Lorsque vous avez terminé

Ajoutez des responsables de secteurs.

Ajouter des portes à un secteur

Avant d'envoyer de demandes d'accès ou d'inviter des visiteurs, vous devez ajouter les portes de vos secteurs aux secteurs associés qui ont été créés automatiquement dans Security Center par Genetec ClearID[MC].

Avant de commencer

Créez vos secteurs.

À savoir

- Seuls les utilisateurs Config Tool dotés du privilège *Afficher les propriétés de portes* peuvent ajouter des portes dans Security Center qui sont associées à des secteurs dans ClearID.
- Lorsqu'un secteur est créé dans ClearID, le secteur est créé automatiquement dans Security Center.
- Les portes doivent ensuite être ajoutées aux secteurs qui ont été créés automatiquement dans Security Center.

Les portes appartenant à un secteur peuvent être configurées comme portes *Captives* ou de *Périmètre* :

- Les portes de périmètre servent à entrer et à sortir du secteur, et permettent ainsi de contrôler les accès.
- Les portes captives sont utilisées dans un secteur.

Configurez correctement les *côtés de porte* pour le bon fonctionnement des options *Comptage d'individus* et *antiretour*. Les côtés *Entrée* et *Sortie* d'une porte sont définis par rapport au secteur que vous configurez.

Procédure

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Vue secteur*.

2 Sélectionnez un secteur et cliquez sur l'onglet **Propriétés**.

3 Dans la section *Portes*, cliquez sur **Ajouter un élément** (), puis sélectionnez les portes que vous souhaitez associer à votre secteur.

4 Pour toutes les portes de la section *Portes*, configurez le type de porte :

- Si la porte permet de pénétrer ou quitter le secteur, réglez le curseur sur **Périmètre**.
- Si la porte est située à l'intérieur du secteur, réglez le curseur sur **Captive**.

  REMARQUE : Lorsqu'un secteur plus petit est imbriqué dans un secteur plus grand, il est inutile d'ajouter les portes de périmètre du secteur enfant en tant que portes captives du secteur parent. Le système organise automatiquement les secteurs imbriqués lors du calcul du nombre d'individus et de l'application des règles d'antiretour.
- Pour échanger les côtés d'une porte, sélectionnez la porte et cliquez sur **Permuter les côtés de porte**.

5 Cliquez sur **Appliquer**.

Vos portes ont à présent été ajoutées aux secteurs Security Center qui sont associés aux secteurs ClearID.

Lorsque vous avez terminé

Vous pouvez désormais envoyer des demandes d'accès ou inviter des visiteurs dans ClearID.

Rubriques connexes

À propos des secteurs, page 342

Activer la gestion des visiteurs pour un secteur

Avant que les visiteurs puissent demander une visite d'un secteur, vous devez configurer les paramètres de gestion des visiteurs pour votre secteur.

Avant de commencer

Créez vos secteurs.

À savoir

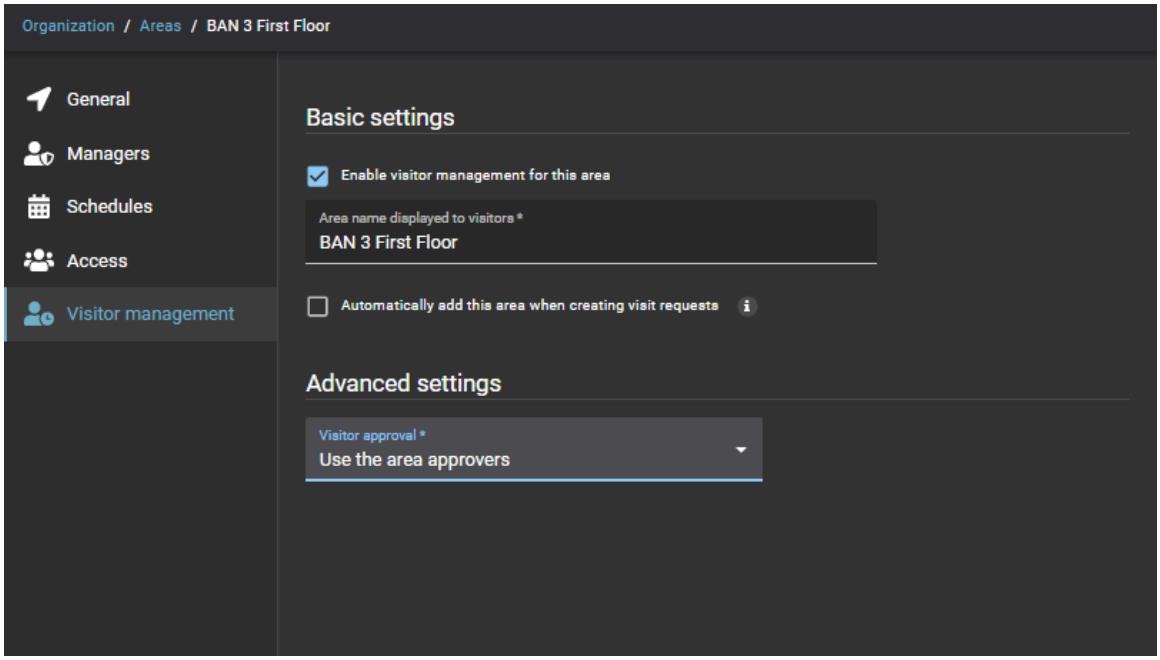
- La gestion des visiteurs pour les secteurs est désactivée par défaut.
- Seuls les *propriétaires de secteurs* ou les *propriétaires de sites* peuvent activer la gestion des visiteurs pour un secteur dans Genetec ClearID^{MC}.
- Les options affichées lors de la création d'une demande de visite varient en fonction des utilisateurs demandant l'accès et des paramètres que vous configurez ici.

Procédure

1 Cliquez sur **Organisation** > **Secteurs**.

2 Dans l'onglet **Secteurs**, sélectionnez un secteur dans la liste.

3 Sous l'onglet **Gestion des visiteurs**, configurez les options suivantes :



- **Réglages de base :** Sélectionnez l'option **Activer la gestion des visiteurs pour ce secteur** pour activer la gestion des visiteurs pour ce secteur.
- **Nom du secteur affiché pour les visiteurs :** Saisissez le nom du secteur que vous souhaitez afficher dans les notifications par e-mail envoyées aux visiteurs.
- **Ajouter automatiquement ce secteur lors de la création de demandes de visite :** Si vous sélectionnez cette option, tous les invités de votre demande de visite se verront automatiquement accorder l'accès au secteur demandé.
- **Options avancées :** Si vous souhaitez définir l'accès des invités dans votre demande de visite, indiquez les approbateurs requis :
- **Approbation de visiteur :** Choisissez les approbateurs pour l'accès des visiteurs parmi les options suivantes :
  - **Approuver automatiquement les visiteurs :** Approuvez automatiquement les demandes d'accès à ce secteur.
  - **Utiliser les approbateurs de secteur :** Seuls les approbateurs de secteur peuvent approuver ou refuser les demandes d'accès à ce secteur.
  - **Définir les approbateurs de visite :** Seules les personnes figurant dans la liste **Approbateurs de visite** peuvent approuver ou refuser les demandes d'accès à ce secteur.

4 Cliquez sur **Enregistrer**.

La gestion des visiteurs est activée pour le secteur.

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles.

Lorsque vous avez terminé

Des demandes d'accès ou de visite peuvent désormais être envoyées pour ce secteur.

Rubriques connexes

À propos des processus, page 12

À propos des secteurs imbriqués

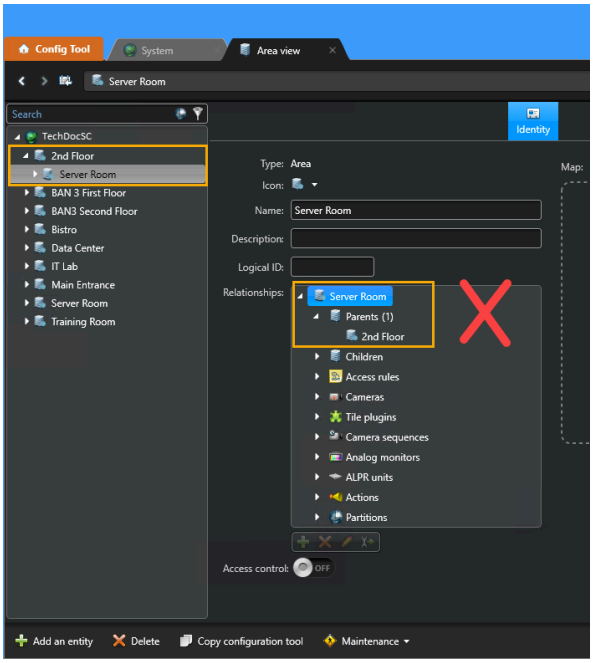
Dans Security Center, les secteurs imbriqués peuvent servir à créer des regroupements logiques afin de pouvoir accorder l'accès automatiquement à des secteurs associés lorsqu'un accès est demandé à l'un des secteurs imbriqués dans ClearID[MC]

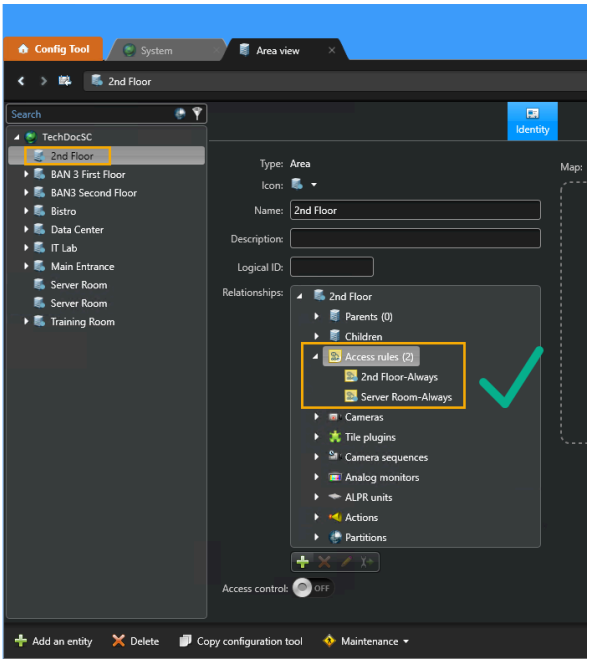
Les secteurs imbriqués sont utiles pour les organisations disposant d'un grand nombre de secteurs restreints, de regroupements logiques ou de dépendances de secteur. Par exemple, lorsque l'accès à des secteurs sécurisés nécessite de passer par d'autres secteurs :

- **Exemple 1 :** la demande d'accès à une salle de serveurs peut automatiquement accorder l'accès à l'étage où se trouve la salle de serveurs.
- **Exemple 2 :** une demande d'accès à un secteur restreint peut autoriser automatiquement l'accès à l'étage où se trouve le secteur restreint, mais également au bâtiment dans lequel se trouvent l'étage et le secteur restreint.

REMARQUE : Dans Config Tool, l'imbrication de secteurs à l'aide des options **Parents** et **Enfants** de la section *Relations* de la vue **Secteur** ne permet pas d'hériter les accès.

BONNE PRATIQUE : Imbriquez les secteurs à l'aide des options **Règles d'accès** de la section *Relations* de la vue **Secteur** pour hériter de l'accès requis. Vous pouvez créer des secteurs imbriqués afin d'ajouter des relations de règles d'accès pour un maximum de trois secteurs associés logiquement. Il n'est pas recommandé d'imbriquer plus de trois secteurs.





L'ajout de plusieurs règles d'accès à un secteur crée l'association de groupes logiques pour les secteurs imbriqués. Cette association de relations permet d'assurer que les secteurs accordent automatiquement l'accès aux autres secteurs associés lorsque l'accès est demandé à l'un des secteurs imbriqués. Par défaut, ClearID crée automatiquement des règles d'accès pour chaque horaire ajouté à un secteur.

IMPORTANT : Si les horaires de l'un des secteurs imbriqués changent, les relations de secteur (règles d'accès) doivent être à nouveau configurées.

Rubriques connexes

Accorder automatiquement l'accès aux secteurs, page 350

Accorder automatiquement l'accès aux secteurs

Pour accorder automatiquement l'accès à des secteurs qui forment un groupe logique, vous pouvez créer des secteurs imbriqués pour Genetec ClearID[MC] dans Security Center.

Avant de commencer

- Créez les secteurs dont vous avez besoin.
- En savoir plus sur les secteurs imbriqués.
- Planifiez le regroupement logique de vos secteurs avant de configurer vos secteurs imbriqués pour accorder ou hériter automatiquement des accès.

À savoir

Seul un administrateur Security Center ou un intégrateur système peut configurer ou associer les secteurs imbriqués.

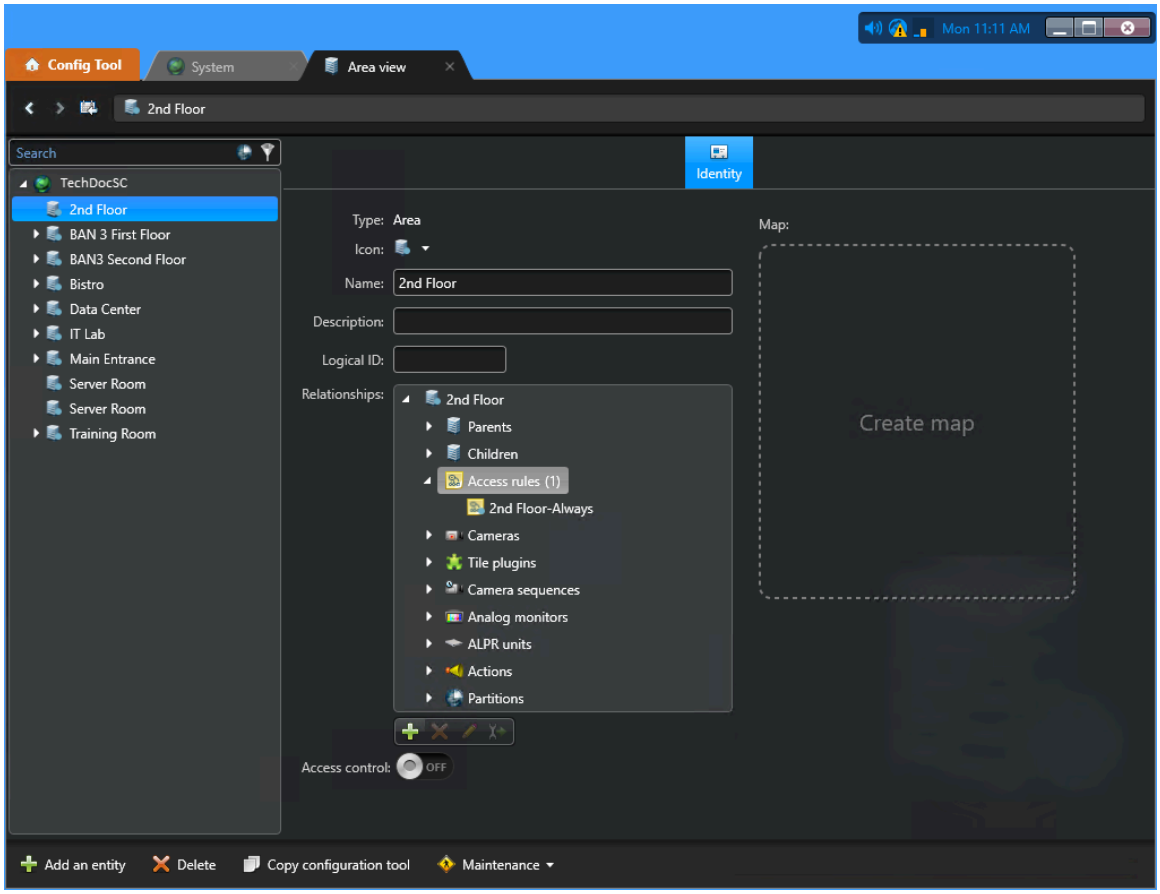
Si les horaires de l'un des secteurs imbriqués changent, les relations de secteur (règles d'accès) doivent être à nouveau configurées.

BONNE PRATIQUE : Imbriquez les secteurs à l'aide des options **Règles d'accès** de la section *Relations* de la vue **Secteur** pour hériter de l'accès requis. Vous pouvez créer des secteurs imbriqués afin d'ajouter des relations de règles d'accès pour un maximum de trois secteurs associés logiquement. Il n'est pas recommandé d'imbriquer plus de trois secteurs.

Procédure

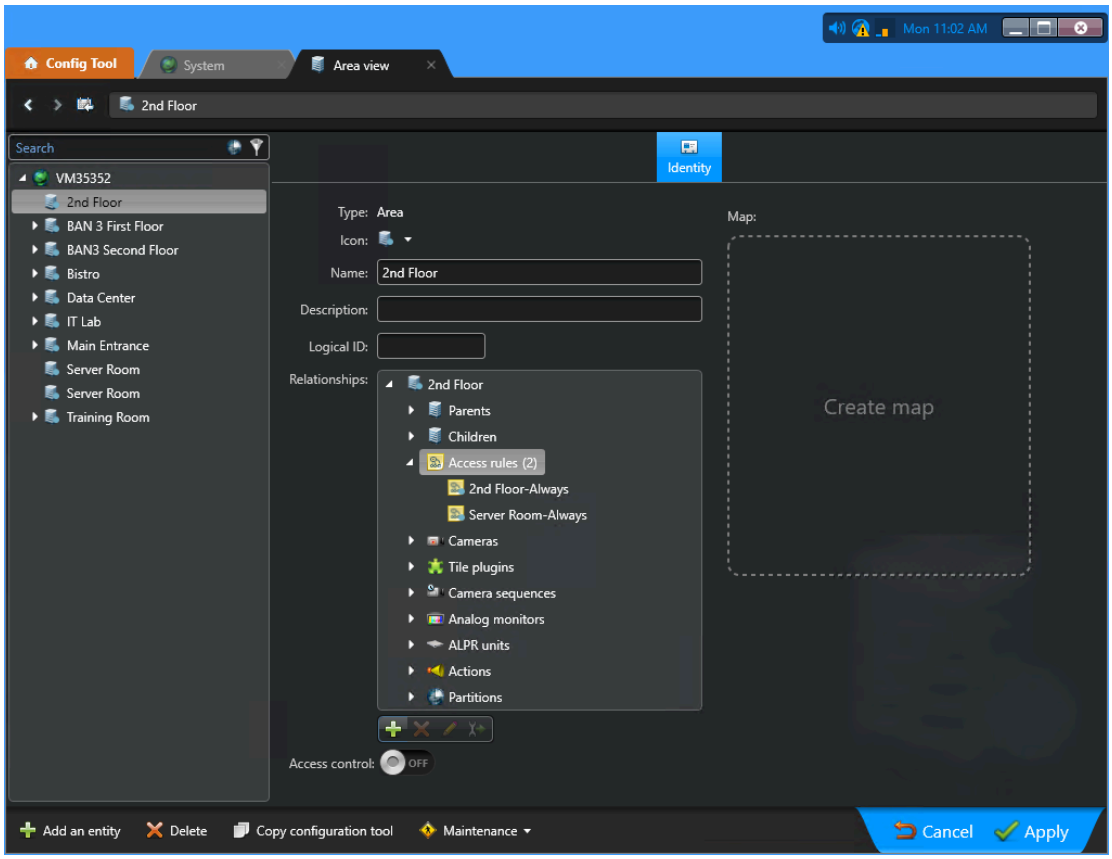
1 Sur la page d’accueil de Config Tool, ouvrez la tâche *Vue secteur*.

2 Dans la **vue Secteur**, cliquez sur un secteur dans le volet de navigation de gauche.



3 Dans la section **Relations** de l'onglet **Identité**, cliquez deux fois sur **Règles d'accès**.

a) Cliquez sur **Insérer un élément** ( ), puis recherchez et sélectionnez les *règles d'accès* qui contiennent les horaires requis pour les *secteurs* que vous souhaitez associer au secteur sélectionné à l'étape 2, page 351.



CONSEIL : Vous pouvez également cliquer sur **Type d'entité** et cocher la case **Règle d'accès**, puis cliquer sur **Rechercher** pour afficher uniquement les règles d'accès dans la liste d'entités.

b) (Facultatif) Répétez la procédure pour d'autres secteurs.

4 Cliquez sur **Appliquer**.

Lorsqu'une demande d'accès est reçue pour un secteur qui appartient à un groupe de secteurs, l'accès est accordé automatiquement en fonction des relations configurées pour les secteurs. Dans l'exemple précédent, toute personne ayant accès à la salle des serveurs a également automatiquement accès au 2e étage.

Ajouter des responsables de secteurs

Les responsables de secteurs sont composés de deux rôles distincts : les propriétaires de secteurs et les approbateurs de secteurs. Avant de pouvoir définir des stratégies pour un secteur, affecter des approbateurs de secteur ou approuver ou refuser les demandes d'accès à un secteur, vous devez ajouter vos responsables de secteurs.

Avant de commencer

Créez vos secteurs.

À savoir

- Seuls les *propriétaires de secteurs* ou les *propriétaires de sites* peuvent ajouter des responsables de secteurs dans Genetec ClearID[MC].
- Dans Genetec ClearID[MC] un propriétaire de secteur est une identité qui a un pouvoir sur un secteur. Le propriétaire peut définir la stratégie liée à un secteur et affecter des approbateurs de secteur.
- Dans Genetec ClearID[MC] un approbateur de secteur est une identité qui a un pouvoir d'approbation sur un secteur. L'approbateur peut approuver ou refuser les demandes d'accès à un secteur. Il est également responsable de l'approbation des examens d'accès de secteurs.

Procédure

1 Cliquez sur **Organisation** > **Secteurs**.

2 Dans l'onglet **Secteurs**, sélectionnez un secteur dans la liste.

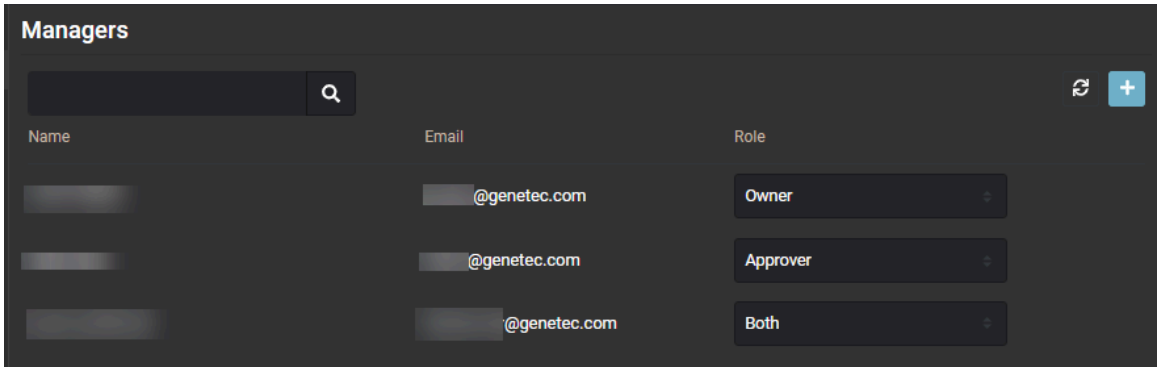
3 Cliquez sur **Responsables** pour ajouter des responsables de secteurs.

4 Utilisez le champ Rechercher ou cliquez sur **Ajouter** ( ) pour ajouter des responsables de secteurs.

5 Sélectionnez le ou les utilisateurs requis, puis cliquez sur **Confirmer**.

6 Sélectionnez le type de **Rôle** pour les utilisateurs que vous avez ajouté :

- Propriétaire
- Approbateur
- Les deux



7 Cliquez sur **Enregistrer**.

Les personnes sélectionnées sont ajoutées au secteur en tant que propriétaire, approbateur ou les deux.

Lorsque vous avez terminé

Ajouter des horaires à un secteur , page 354.

Ajouter des horaires à un secteur

Avant de permettre aux utilisateurs d'accéder à un secteur, vous devez ajouter des horaires à vos secteurs.

Avant de commencer

Définissez des horaires dans Security Center. Pour en savoir plus, voir Créer un horaire.

À savoir

- Seuls les *propriétaires de secteurs* peuvent ajouter des horaires aux secteurs dans Genetec ClearID[MC].
- Un horaire est une entité qui définit des contraintes horaires qui peuvent être appliquées à de nombreuses situations au sein du système. Chaque contrainte horaire est décrite par une plage de dates (quotidien, hebdomadaire, mensuel, annuel ou à dates spécifiques) et par une plage horaire (toute la journée, plage fixe, journée ou nuit).
- Les horaires disponibles dépendent des horaires définis dans le système de contrôle d'accès Security Center sélectionné lorsque vous créez votre secteur.
- Exemples d'horaires : toujours, jours de la semaine, week-end, 09:00-17:00, etc.
- Lorsqu'un horaire est ajouté à un secteur, une *règle d'accès* est automatiquement créée dans Security Center. La règle d'accès *secteur-horaire* spécifie l'horaire associé au secteur. ClearID ajoute et supprime automatiquement l'accès d'un *titulaire de cartes* ou d'un *groupe de titulaires de cartes* concerné par la règle d'accès en fonction de l'horaire spécifié dans ClearID.

Procédure

1 Cliquez sur **Organisation** > **Secteurs**.

2 Dans l'onglet **Secteurs**, sélectionnez un secteur dans la liste.

3 Cliquez sur **Horaires**.

4 Cliquez sur **Ajouter un horaire** pour configurer l'horaire de votre secteur.

a) Saisissez un terme de recherche et cliquez sur **Rechercher** ( ).

b) Sélectionnez un horaire dans la liste et cliquez sur **Confirmer**.

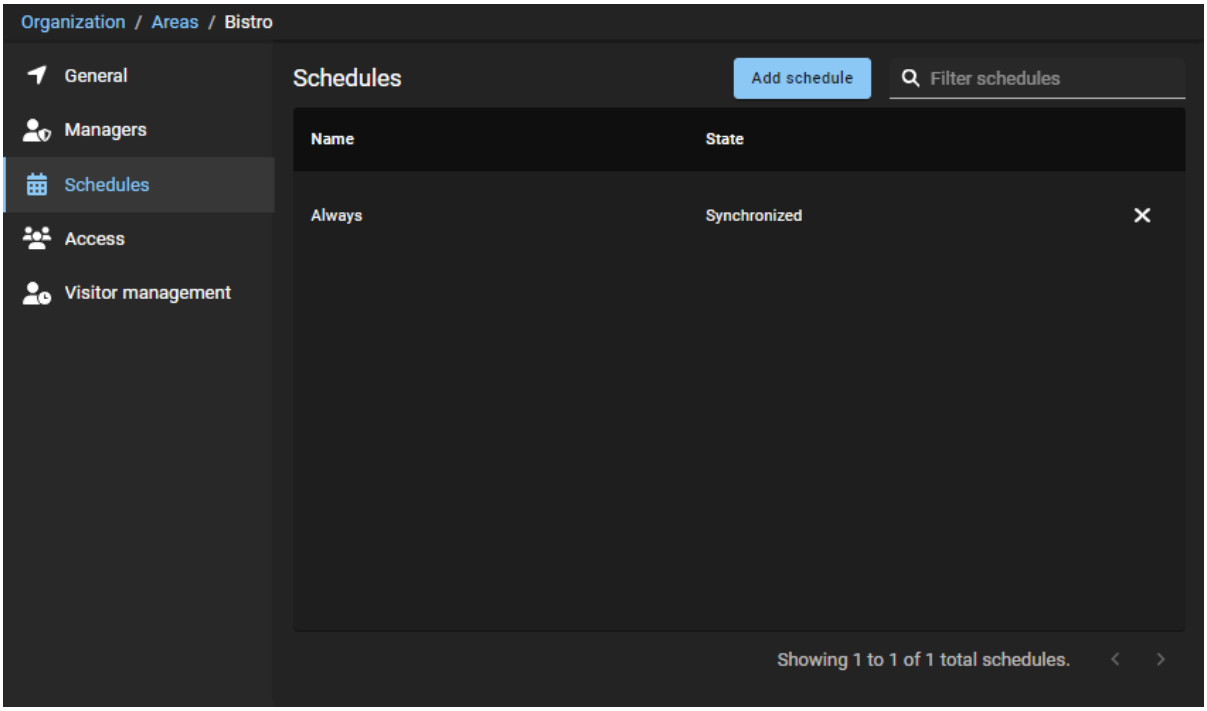
Cette liste affiche uniquement les horaires qui ne figurent pas déjà dans la liste **Horaires**.

c) (Facultatif) Répétez les étapes précédentes pour ajouter des horaires supplémentaires.

5 (Facultatif) Cliquez sur **Supprimer** ( ) pour supprimer tous les horaires qui ne sont plus requis.

6 Cliquez sur **Enregistrer**.

Vos horaires ont été ajoutés au secteur.



Lorsque vous avez terminé

Accordez l'accès à votre secteur.

Configurer les documents de demande d'accès pour les secteurs

Pour les secteurs soumis à des mesures ou des exigences de sécurité supplémentaires, les *propriétaires de sites* et les *propriétaires de secteurs* peut obliger les employés à charger des justificatifs tels que des copies de permis de conduire ou de certifications lorsqu'ils demandent l'accès à des secteurs.

Avant de commencer

Familiarisez-vous avec les workflows de demande d'accès.

À savoir

- En tant que *propriétaire du site*, vous pouvez gérer les justificatifs pour les demandes d'accès au niveau du site.
- Les propriétaires de sites ou de secteurs peuvent configurer d'autres conditions de justificatifs au niveau du secteur.
- Vous pouvez configurer jusqu'à 20 types de justificatifs par secteur.

Procédure

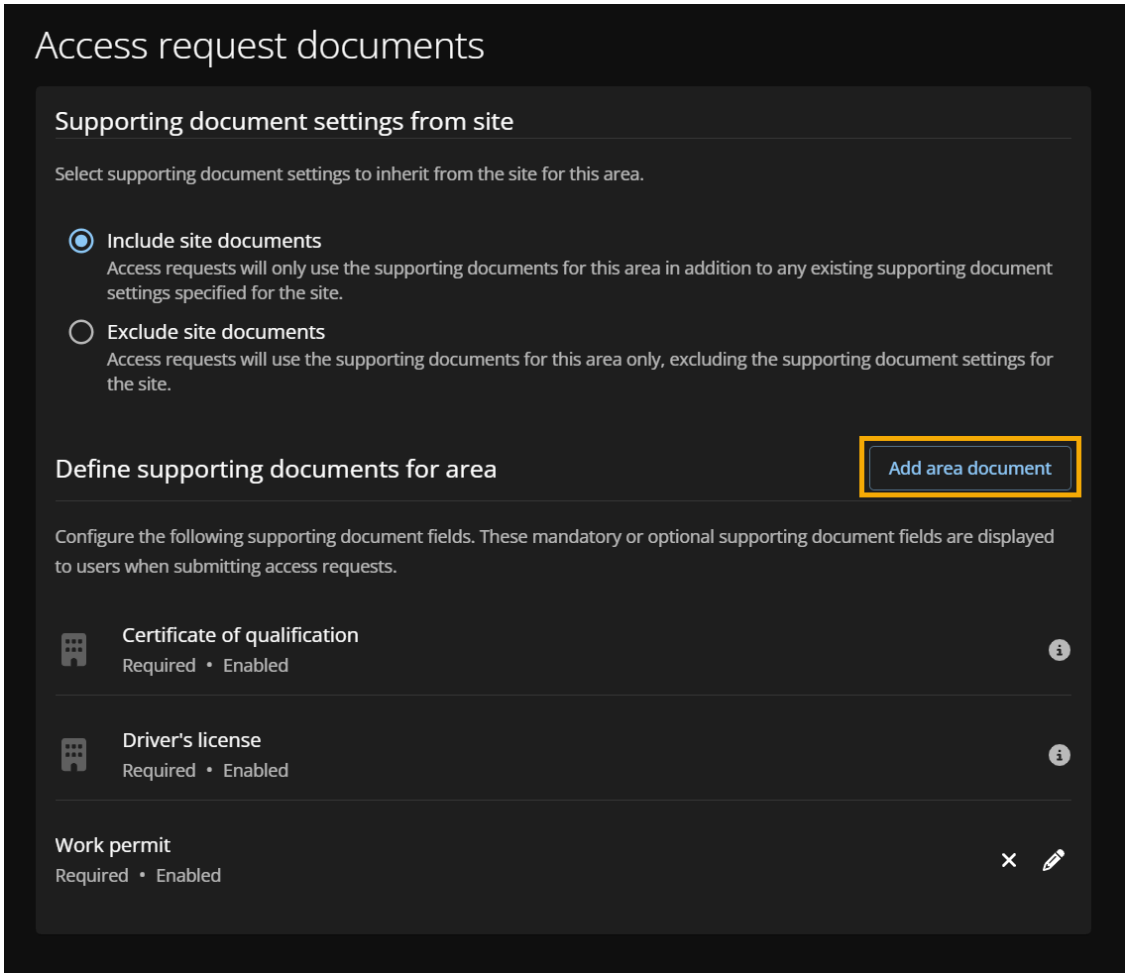
1 Dans le portail web Genetec ClearID^{MC}, cliquez sur **Organisation** > **Site** > **Secteur** > **Réglages de demande d'accès**.

2 (*Propriétaire du site*) Sous *Paramètres de justificatifs du site*, cochez le bouton radio pour choisir si le secteur spécifique hérite ou non des conditions de justificatif configurées au niveau du site :

- **Inclure les documents du site :** Les demandes d'accès utilisent les justificatifs pour le secteur en plus des paramètres de justificatifs indiqués pour le site.
- **Exclure les documents du site :** Les demandes d'accès n'utilisent que les justificatifs pour le secteur, à l'exception des paramètres de justificatif pour le site.

REMARQUE : Inclure les documents du site est sélectionné par défaut pour les secteurs. Les *propriétaires de sites* peuvent modifier ces paramètres.

3 Sous *Définir des justificatifs pour le secteur*, cliquez sur **Ajouter un document de secteur**.



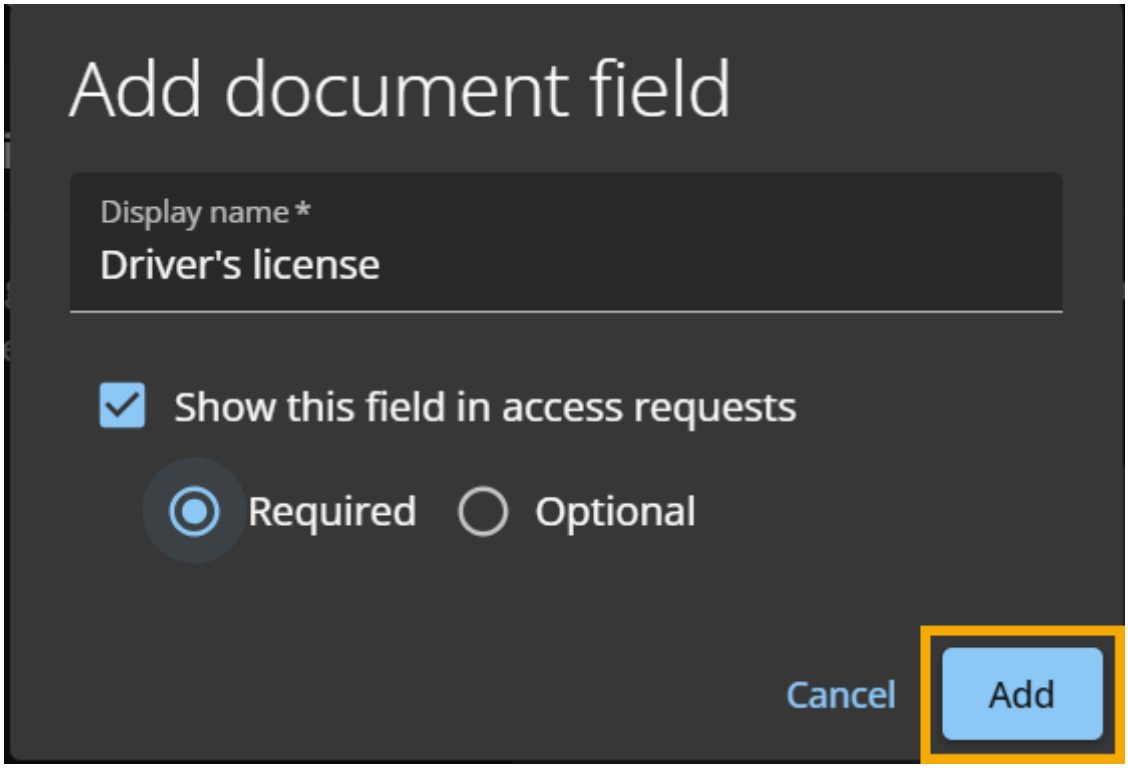
a) Dans le champ *Nom d'affichage*, saisissez un nom pour le type de document.

b) Sélectionnez **Afficher ce champ dans les demandes d'accès** pour afficher le champ de document dans les demandes d'accès.

CONSEIL : Lorsque cette case est décochée, le type de document reste disponible en mode brouillon.

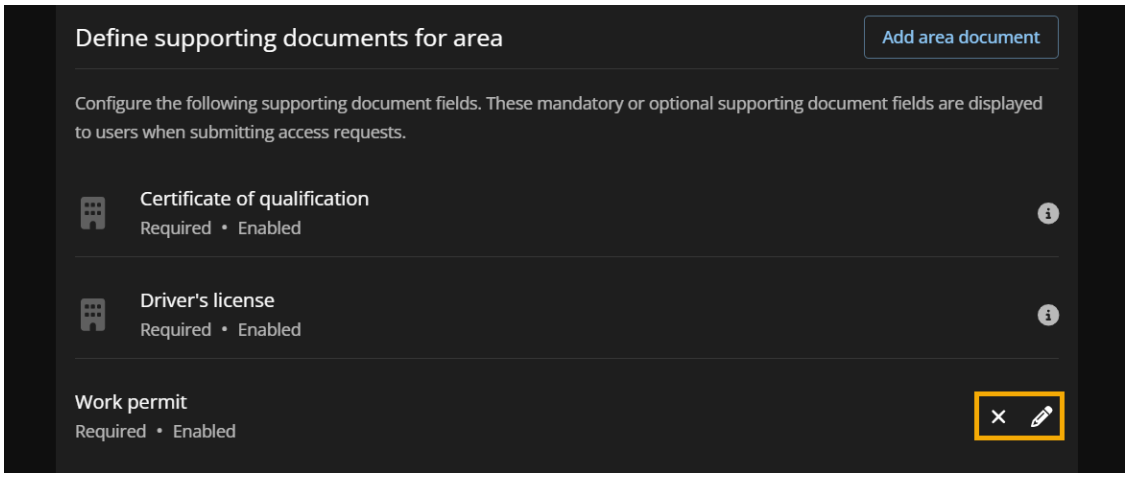
c) Indiquez si le chargement du document est obligatoire lors de la soumission d'une demande d'accès en cliquant sur le bouton radio **Obligatoire** ou **Facultatif**.

REMARQUE : Vous pouvez configurer une combinaison de types de documents obligatoires et facultatifs pour qu'ils apparaissent dans une seule demande d'accès.



4 Cliquez sur **Ajouter**.

5 (Facultatif) Les icônes vous permettent de modifier ou de supprimer chaque type de document :



a) Cliquez sur pour modifier la configuration d'un justificatif.

b) Cliquez sur pour supprimer un justificatif configuré.

Accorder l'accès à un secteur

Pour accorder l'accès à un secteur, vous devez ajouter des identités ou des rôles à un secteur et planifier un accès par individu ou par rôle.

Avant de commencer

Ajoutez des horaires à vos secteurs.

À savoir

- Seuls les *propriétaires de secteur*, les *approbateurs de secteur* et les superviseurs peuvent accorder l'accès au secteur.
- La page *Accès* affiche l'ensemble des identités, rôles ou visiteurs qui ont actuellement accès au secteur.

Procédure

1 Cliquez sur **Organisation** > **Secteurs**.

2 Dans l'onglet **Secteurs**, sélectionnez un secteur dans la liste.

3 Cliquez sur **Accès**.

4 Sélectionnez un filtre parmi les suivants :

- **Tous :**
  - Si toutes les icônes de filtre de type de demande d'accès sont disponibles ( ), tous les types de demande d'accès sont affichés.
  - Si toutes les icônes de filtre de type de demande d'accès sont indisponibles (), tous les types de demande d'accès sont masqués.
- **Accès d'identité ( ) :** Afficher ou masquer les accès d'identité.
- **Accès de rôle ( ) :** Afficher ou masquer les accès de rôle.
- **Demandes de visite ( ) :** Afficher ou masquer les demandes de visite.

5 Cliquez sur **Ajouter un accès**.

a) Dans la boîte de dialogue *Accorder l'accès au secteur*, sélectionnez **Identités** ou **Rôles**.

6 Si vous sélectionnez **Identités**, renseignez les champs :

a) Saisissez un nom d'identité et cliquez sur **Rechercher** ( ).

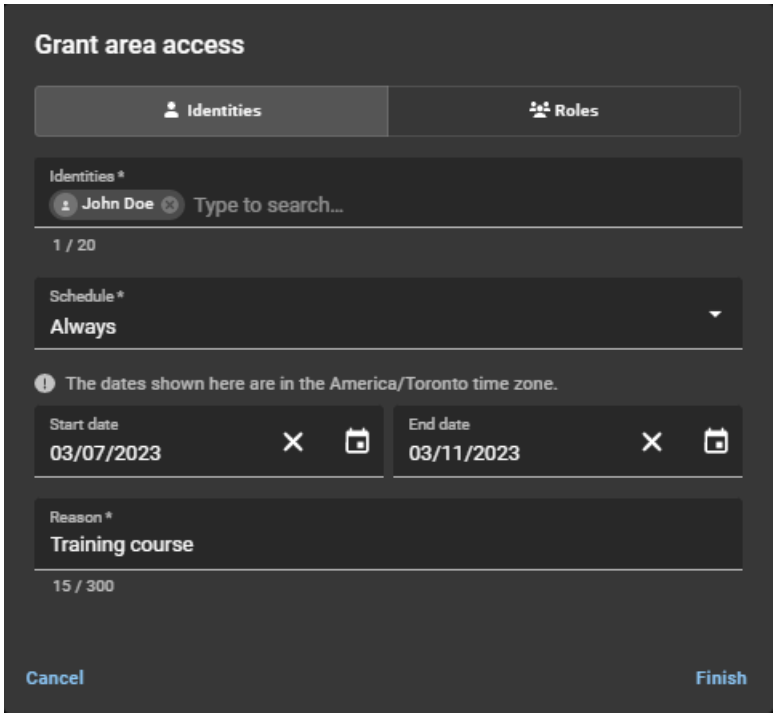
b) Sélectionnez le nom de l'identité dans la liste **Identités**.

c) Recherchez ou sélectionnez l'*horaire* désiré dans la liste **Horaire**.

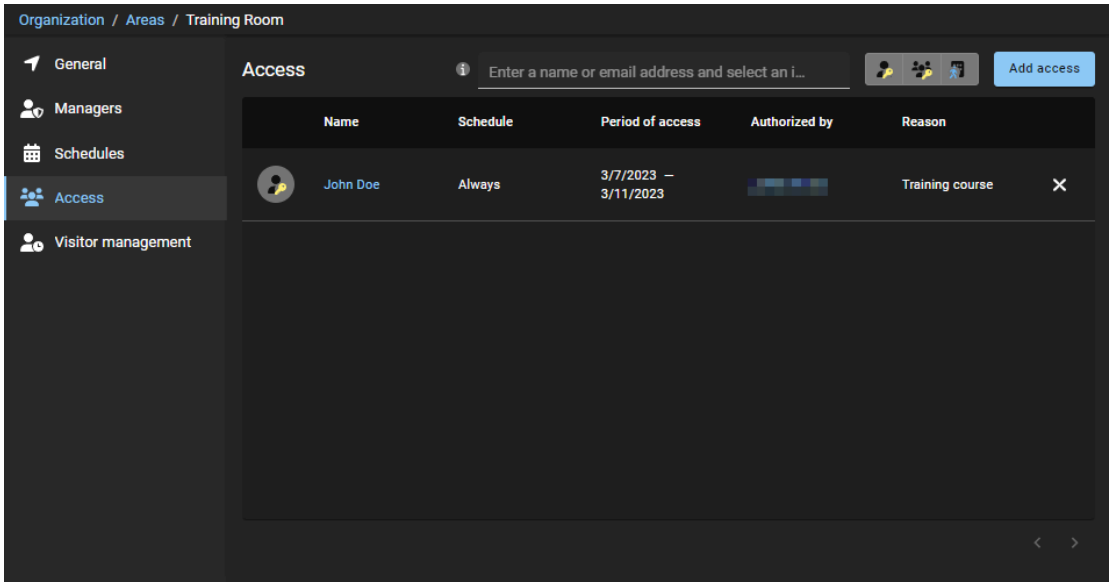
Exemples d'horaires : toujours, jours de la semaine, week-end, 09:00-17:00, etc.

d) Configurez la période durant laquelle vous souhaitez autoriser l'accès.

- **Date de début :** Lancer un sélecteur de calendrier pour choisir la date à laquelle l'accès doit commencer. La valeur par défaut est Maintenant.
- **Date de fin :** Lancer un sélecteur de calendrier pour choisir la date à laquelle l'accès doit expirer. La valeur par défaut est Indéfini.
- **Motif :** (Facultatif) Indiquez un motif pour la période d'accès demandée. Par exemple, accès nécessaire pour la conférence des partenaires commerciaux, accès nécessaire des employés pour un projet sur plusieurs semaines, etc.



e) Cliquez sur **Terminer**.



f) (Facultatif) Cliquez sur **Supprimer** ( ) pour révoquer tous les accès qui ne sont plus requis.

7 Si vous sélectionnez **Rôles**, renseignez les champs :

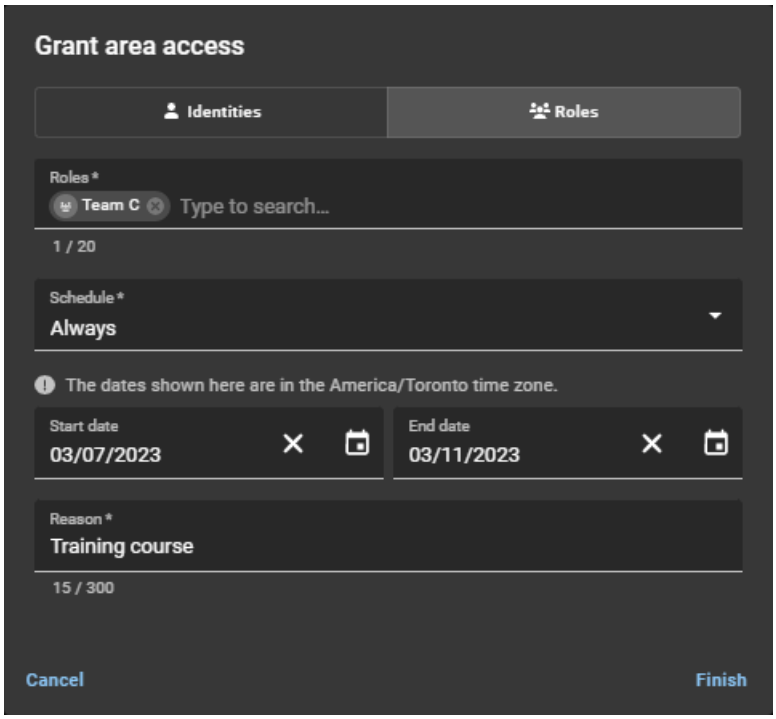
a) Saisissez un nom de rôle et cliquez sur **Rechercher** ( ).

b) Sélectionnez le nom du rôle dans la liste **Rôles**.

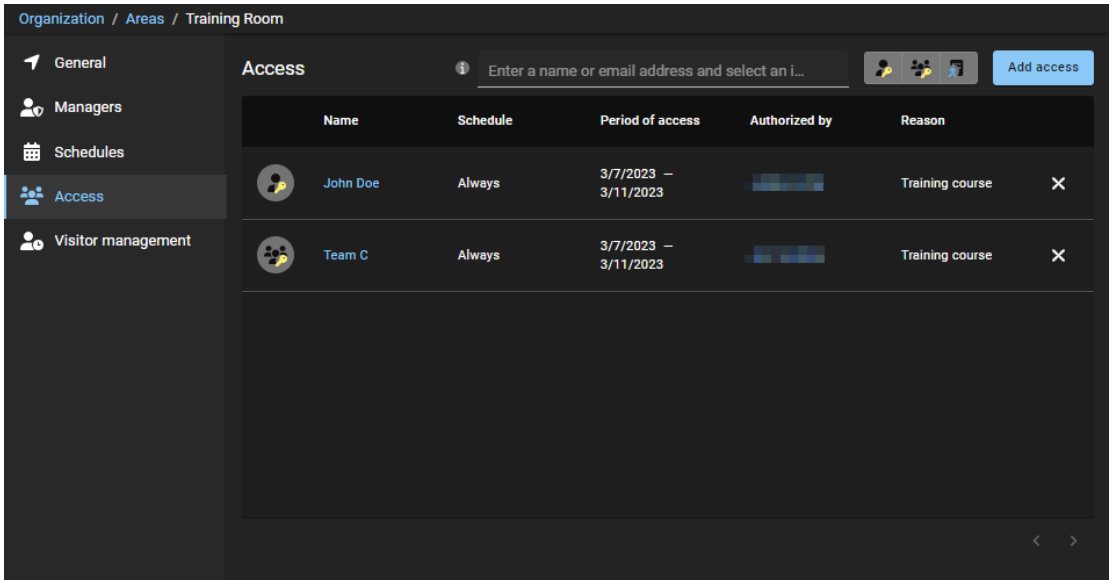
c) Recherchez ou sélectionnez l'*horaire* désiré dans la liste **Horaire**.

d) Configurez la période durant laquelle vous souhaitez autoriser l'accès.

- **Date de début :** Lancer un sélecteur de calendrier pour choisir la date à laquelle l'accès doit commencer. La valeur par défaut est Maintenant.
- **Date de fin :** Lancer un sélecteur de calendrier pour choisir la date à laquelle l'accès doit expirer. La valeur par défaut est Indéfini.
- **Motif :** (Facultatif) Indiquez un motif pour la période d'accès demandée. Par exemple, accès nécessaire pour la conférence des partenaires commerciaux, accès nécessaire des employés pour un projet sur plusieurs semaines, etc.



e) Cliquez sur **Terminer**.



f) (Facultatif) Cliquez sur **Supprimer** ( ) pour révoquer tous les accès qui ne sont plus requis.

Vos demandes d'accès ont été accordées pour ce secteur.

Examiner les accès à un secteur

Pour effectuer un audit ou vérifier qui a accès à un secteur, une analyse doit être effectuée régulièrement par un propriétaire de secteur, un approbateur de secteur ou un propriétaire de site.

À savoir

Seuls les *propriétaires de secteur*, les *approbateurs de secteur* et les *propriétaires de site* peuvent examiner l'accès au secteur.

Cette procédure décrit comment vérifier qui a accès à un secteur spécifié, secteur par secteur.

Procédure

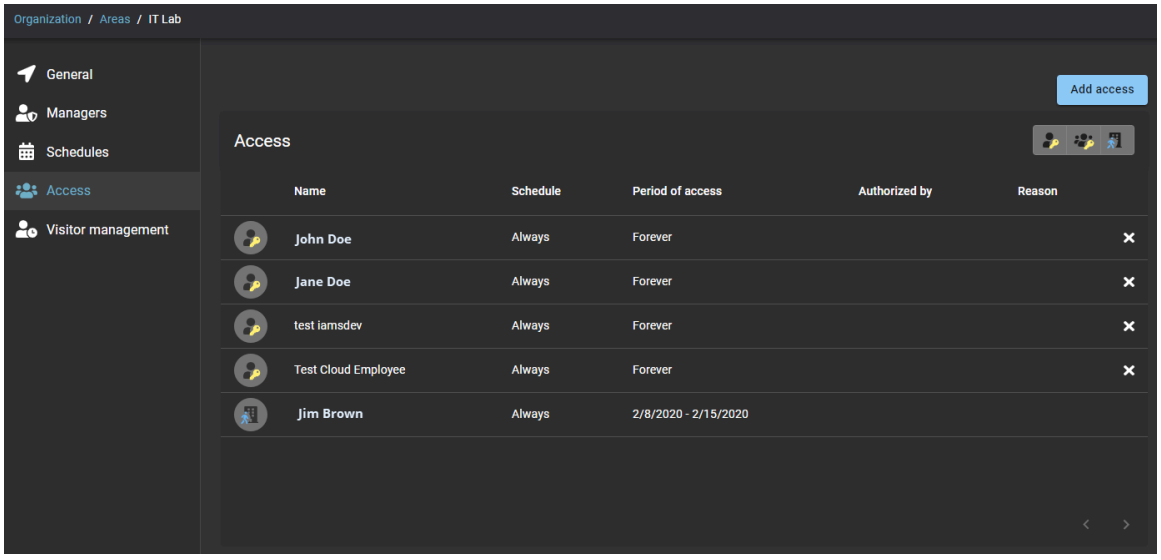
1 Cliquez sur **Organisation** > **Secteurs**.

2 Dans l'onglet **Secteurs**, sélectionnez un secteur dans la liste.

3 Cliquez sur **Accès**.

4 Sélectionnez un filtre de demande d'accès :

- **Tous :**
  - Si toutes les icônes de filtre de type de demande d'accès sont disponibles ( ), tous les types de demande d'accès sont affichés.
  - Si toutes les icônes de filtre de type de demande d'accès sont indisponibles ( ), tous les types de demande d'accès sont masqués.
- **Accès d'identité ( ) :** Afficher ou masquer les accès d'identité.
- **Accès de rôle ( ) :** Afficher ou masquer les accès de rôle.
- **Demandes de visite () :** Afficher ou masquer les demandes de visite.



5 Consultez la liste d'accès pour identifier les rôles, identités ou visiteurs qui peuvent être supprimés ou qui nécessitent un examen plus approfondi.

Lorsque vous avez terminé

Approuvez les demandes d'accès ou rejetez les demandes d'accès.

Rubriques connexes

Configurer les examens d'accès à un secteur, page 287
Terminer un examen d'accès à un secteur (propriétaire de site), page 302

Approuver les demandes d'accès à un secteur

Pour approuver les demandes d'accès à un secteur, un *Propriétaire de secteur*, un *Approbateur de secteur* ou un *Superviseur* doit examiner les approbations en attente. Il peut ensuite décider quelles demandes approuver.

Avant de commencer

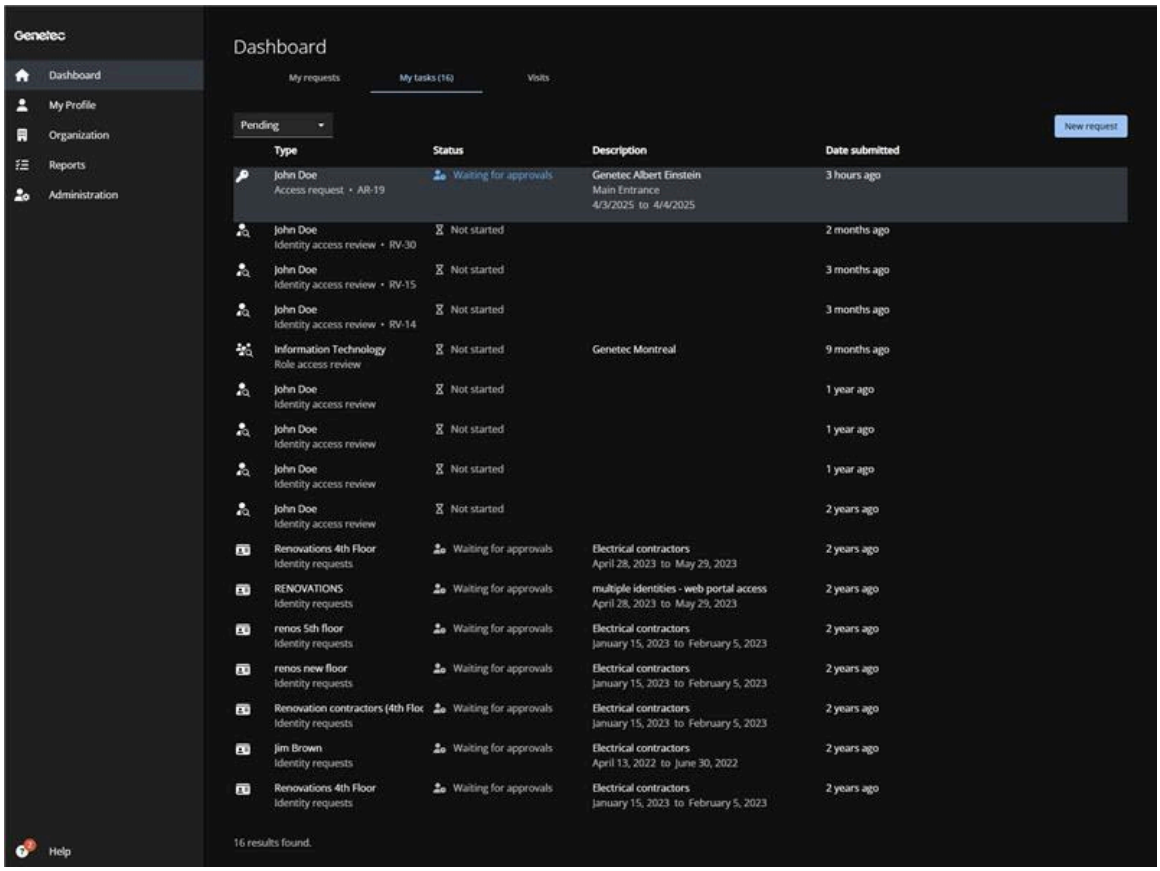
Vérifiez que des demandes d'accès aux secteurs ont déjà été envoyées.

À savoir

Seuls les *propriétaires de secteur*, les *approbateurs de secteur* et les superviseurs peuvent approuver les demandes d'accès à un secteur.

Procédure

1 Cliquez sur **Tableau de bord** > **Mes tâches**.

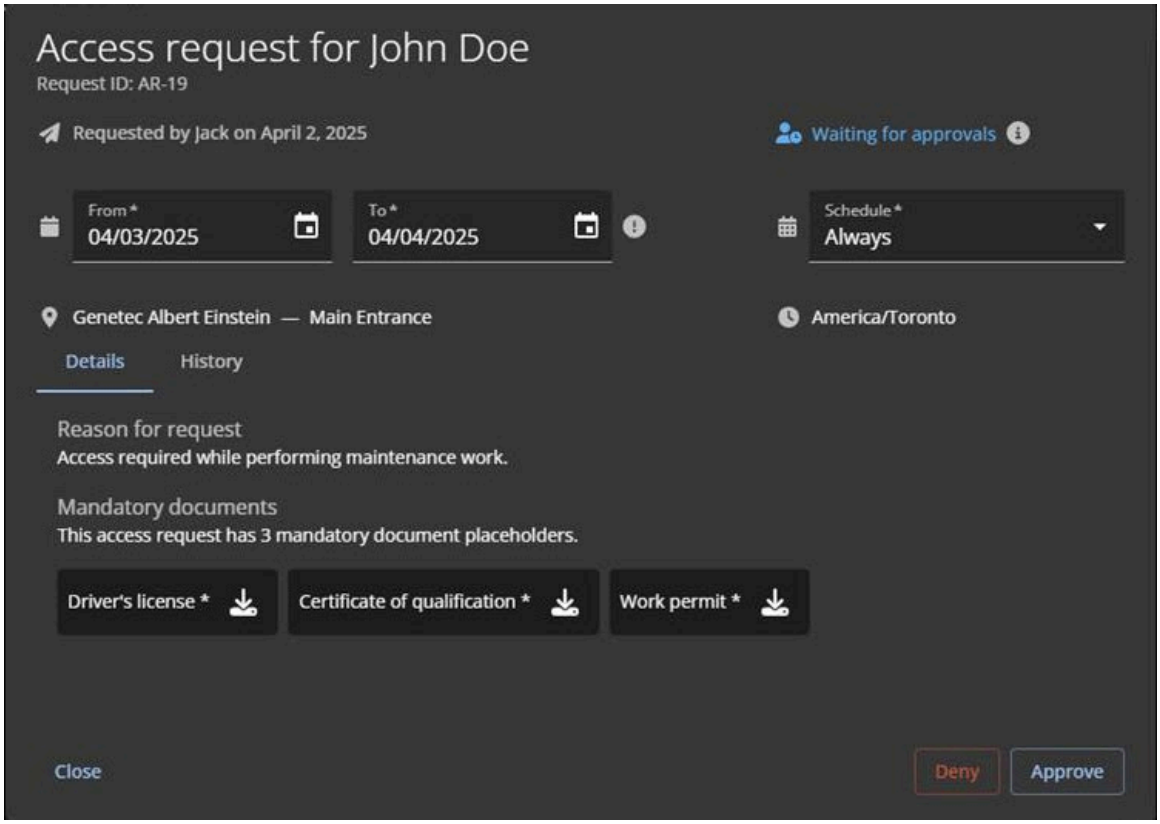


2 Dans la liste **État**, filtrez les tâches qui sont affichées :

- **État :** Sélectionnez un état parmi les suivants :

- **Tous :** Affiche toutes les tâches en attente ou terminées.
- **En attente :** Affiche les tâches en attente d'approbation.
- **Terminé :** Affiche les tâches terminées et leur état. Par exemple, approuvé, terminé, refusé ou annulé.

3 Cliquez sur une demande d'accès pour afficher des informations complémentaires sur celle-ci.



4 Passez en revue les détails de la demande et apportez les modifications nécessaires.

CONSEIL : Vous pouvez modifier la demande si vous remarquez une erreur ou un élément à modifier dans la demande. Par exemple, vous pouvez modifier les dates liées à la fermeture d'un bureau ou le calendrier d'accès pour qu'il soit plus adapté.

5 (Facultatif) Dans le champ **Historique**, saisissez un commentaire sur les modifications que vous apportez à la demande d'accès.

6 Cliquez sur **Approuver**.

7 (Facultatif) Dans le champ **Motif d'approbation**, saisissez un motif d'approbation d'accès.

8 Cliquez sur **Confirmer**.

Les demandes d'accès au secteur sont désormais approuvées. Les employés ou visiteurs peuvent accéder au secteur pendant les périodes spécifiées dans leur demande d'accès.

Refuser les demandes d’accès à un secteur

Pour refuser les demandes d'accès à un secteur, un *Propriétaire de secteur*, un *Approbateur de secteur* ou un *Superviseur* doit examiner les approbations en attente. Il peut ensuite décider quelles demandes refuser.

Avant de commencer

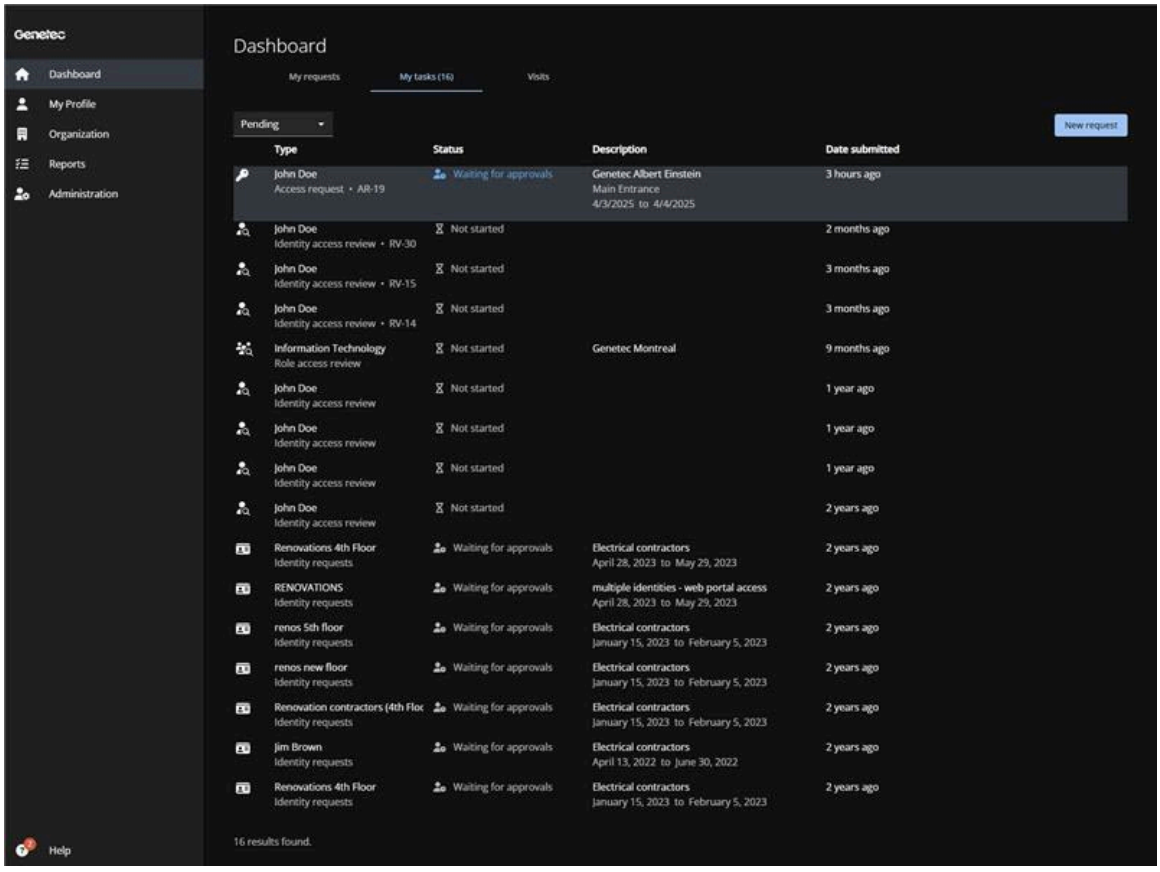
- Vérifiez que des demandes d'accès aux secteurs ont déjà été envoyées.
- Examinez les accès aux secteurs pour identifier ceux qui ne sont plus requis.

À savoir

Seuls les *propriétaires de secteur*, *les approbateurs de secteur* et les superviseurs peuvent rejeter les demandes d'accès à un secteur.

Procédure

1 Cliquez sur **Tableau de bord** > **Mes tâches**.

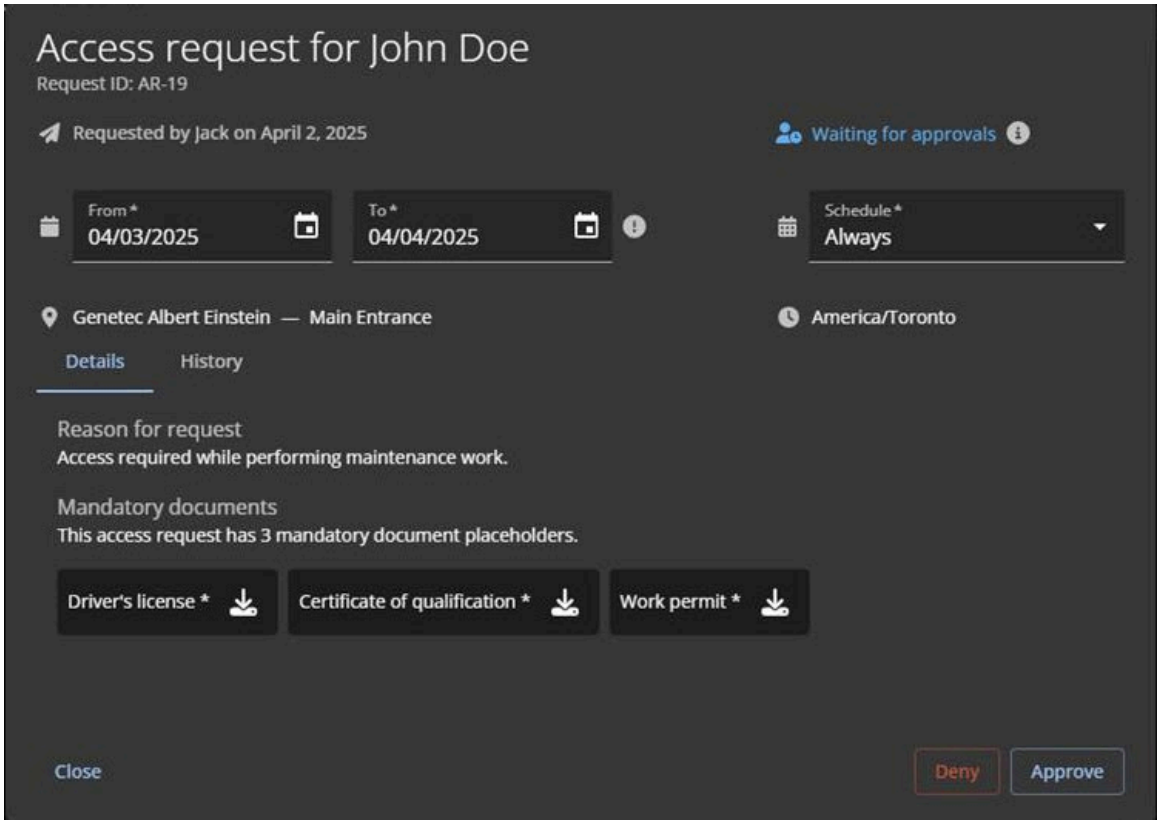


2 Dans la liste **État**, filtrez les tâches qui sont affichées :

- **État :** Sélectionnez un état parmi les suivants :

- **Tous :** Affiche toutes les tâches en attente ou terminées.
- **En attente :** Affiche les tâches en attente d'approbation.
- **Terminé :** Affiche les tâches terminées et leur état. Par exemple, approuvé, terminé, refusé ou annulé.

3 Cliquez sur une demande d'accès pour afficher des informations complémentaires sur celle-ci.



4 Examinez les détails de la demande.

5 (Facultatif) Dans le champ **Historique**, saisissez un commentaire sur les modifications que vous apportez à la demande d'accès.

6 Cliquez sur **Refuser**.

7 (Facultatif) Dans le champ **Raison du refus**, saisissez la raison pour laquelle la demande d'accès a été refusée.

REMARQUE : Si les documents de demande d'accès justificatifs sont incorrects ou non valables, vous pouvez notifier le demandeur en incluant ces informations dans le champ **Motif du refus**. Le demandeur devra ensuite soumettre à nouveau une demande d’accès accompagnée de pièces justificatives valides.

8 Cliquez sur **Confirmer**.

Les demandes d'accès à un secteur sont désormais rejetées. Les employés ou les visiteurs ne peuvent plus accéder au secteur.

9

Gestion des visiteurs

Découvrez comment gérer les demandes de visites et les demandes d'accès.

Cette section aborde les sujets suivants:

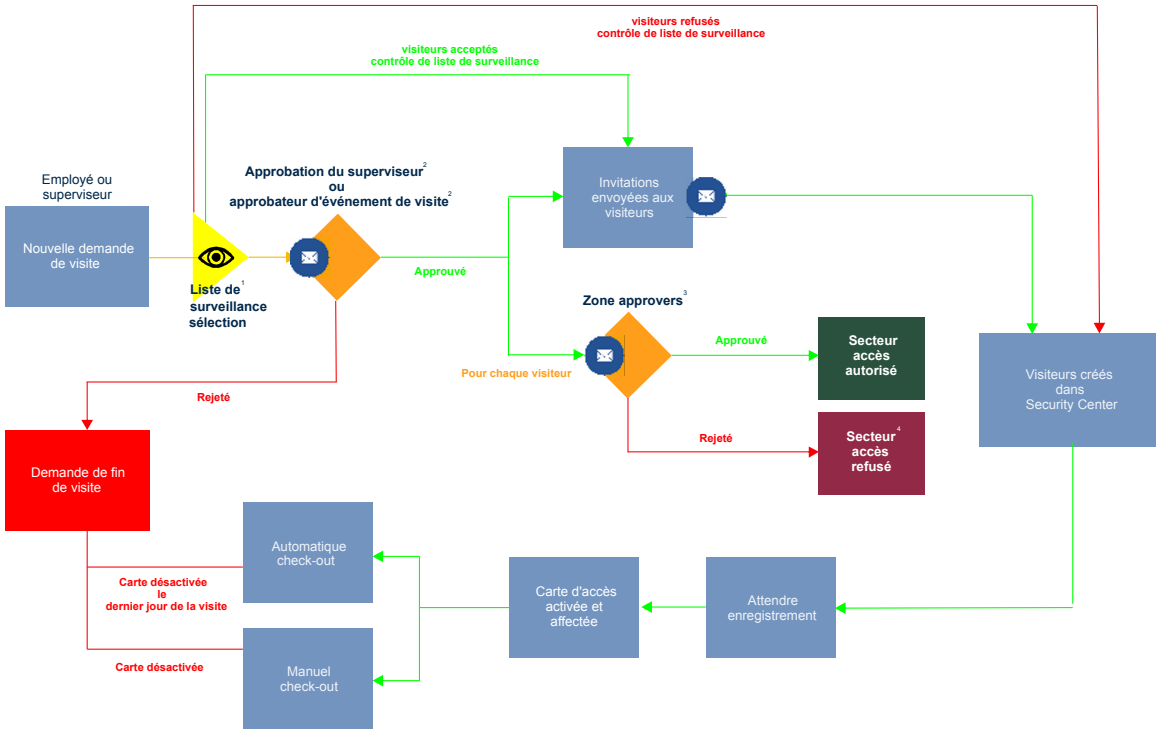
- " À propos du processus de demande de visite ", page 371
- " À propos du processus de liste de surveillance de demande de visite ", page 372
- " Inviter des visiteurs ", page 373
- " Examiner les événements de visite ", page 388
- " Copier un événement de visite ", page 390
- " Modifier les événements de visite ", page 391
- " Approuver les demandes de visite ", page 393
- " À propos des rapports de visiteurs ", page 395
- " Afficher un rapport de visiteurs ", page 396
- " Identifiants code QR pour les visiteurs ", page 398

À propos du processus de demande de visite

Un processus de demande de visite est une série d'activités effectuées par le système ou par des personnes habilitées au cours du cycle de vie d'une demande de visite. Les activités peuvent modifier l'état et les propriétés des demandes de visite, affecter d'autres entités du système, ou attendre que certaines conditions soient réunies.

Le processus permet d'automatiser les tâches liées aux demandes de visite, comme l'approbation ou le rejet des demandes d'accès, afin que les personnes chargées de l'examen et de l'approbation puissent se concentrer sur d'autres tâches.

Le diagramme suivant illustre le *processus de demande de visite* exécuté dans Genetec ClearID[MC] et Synergis[MC].



[1] (Facultatif) Pour en savoir plus, voir Processus de liste de surveillance de demande de visite.

[2] (Facultatif) L'approbation peut être activée ou désactivée pour chaque site.

[3] (Facultatif) L'approbation peut être activée ou désactivée pour chaque secteur.

[4] L'événement de visite et le visiteur ont été créés dans Security Center, mais l'accès au secteur a été refusé. Le visiteur peut potentiellement accéder aux secteurs interdits s'il est escorté par un hôte, cette décision revenant à l'organisation.

Rubriques connexes

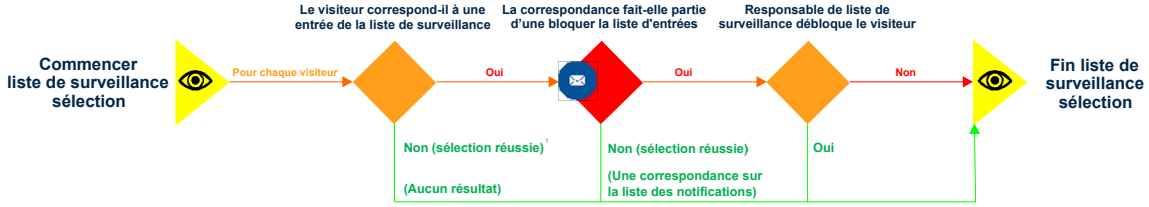
À propos des processus, page 12

À propos du processus de liste de surveillance de demande de visite

Un processus de liste de surveillance est une série d'activités effectuées par le système ou par des personnes habilitées au cours du cycle de vie d'une demande de visite si les listes de surveillance sont activées. Les activités peuvent modifier l'état et les propriétés des listes de surveillance, affecter d'autres entités du système, ou attendre que certaines conditions soient réunies.

Le processus permet d'automatiser la recherche de personnes ou d'entreprises d'intérêt parmi les visiteurs lors d'une inscription ou d'un enregistrement en libre-service, afin que les personnes chargées de l'examen et de l'approbation puissent se concentrer sur d'autres tâches.

Le schéma suivant illustre le déroulement du *processus de liste de surveillance* (si la fonction de liste de surveillance est activée pour votre compte) dans Genetec ClearID[MC] et dans Synergis[MC], parallèlement au processus de demande de visite.



[1] L'inscription des visiteurs n'est confirmée que lorsque les visiteurs contrôlés n'ont pas été trouvés dans des listes de blocage. Les visiteurs bloqués ne reçoivent pas d'e-mail de notification de visite.

Rubriques connexes

À propos des processus, page 12

Inviter des visiteurs

Pour inviter une ou plusieurs personnes à venir sur site ou à un événement, utilisez le portail en libre-service. L'utilisation d'un portail en libre-service avec des approbateurs de secteur spécifiés simplifie le processus d'approbation et évite d'interrompre une chaîne de personnes qui ne sont pas forcément les bons approbateurs.

Avant de commencer

1. Familiarisez-vous avec les processus.
2. Activez la gestion des visiteurs pour votre site.
3. Assurez-vous que vous disposez des autorisations requises pour inviter des visiteurs sur le site.

À savoir

Vous pouvez ajouter des visiteurs individuellement ou importer une liste étendue de visiteurs à l'aide d'un fichier CSV.

- Si vous avez moins de cinq visiteurs à inviter, ajoutez vos visiteurs individuellement.
- Si vous avez plus de cinq visiteurs à inviter, vous pouvez préparer un fichier CSV pour importer votre liste d'invités.
- Si votre site d'accueil d'identité est configuré, vous êtes automatiquement autorisé à inviter des visiteurs sur ce site uniquement si les options de gestion des visiteurs du site ont été configurées pour permettre aux utilisateurs d'inviter des visiteurs.
- Les options affichées lors de la création d'une invitation visiteur peuvent varier en fonction des paramètres du site et des paramètres configurés pour la gestion des visiteurs.

REMARQUE : Les champs obligatoires sont mis en évidence dans l'interface utilisateur avec un astérisque (*).

Procédure

1 Connectez-vous au portail en libre-service.

2 Procédez de l'une des manières suivantes :

- Cliquez sur **Tableau de bord** > **Mes demandes** > **Nouvelle demande** > **Inviter des visiteurs**.
- Cliquez sur **Tableau de bord** > **Visites** > **Nouvel événement de visite**.

3 Dans l'assistant *Nouvel événement de visite*, suivez les instructions pour l'une des situations suivantes :

- Invitez des visiteurs manuellement
- Invitez des visiteurs en important un fichier CSV

4 Cliquez sur **Terminer**.

Votre demande de visite a été soumise et attend les approbations requises.

Lorsque vous avez terminé

Confirmez si la demande a été approuvée ou rejetée :

- Recherchez un e-mail *Visite approuvée* dans votre boîte de réception.
- Consultez **Mes demandes** dans Genetec ClearID[MC].

Rubriques connexes

Activer la gestion des visiteurs pour un site, page 257
Note sur la fonction de gestion des visiteurs (2 pages)

Inviter des visiteurs manuellement

Si vous avez moins de cinq visiteurs à inviter à votre événement, vous pouvez les ajouter manuellement.

Avant de commencer

1. Familiarisez-vous avec les processus.
2. Activez la gestion des visiteurs pour votre site.
3. Assurez-vous que vous disposez des autorisations requises pour inviter des visiteurs sur le site.

À savoir

- Si vous avez configuré un site principal pour votre identité, vous êtes automatiquement autorisé à inviter des visiteurs sur ce site. L'accès n'est accordé automatiquement que si les options de gestion des visiteurs du site ont été configurées pour autoriser les gens à inviter des visiteurs.
- Les options affichées lors de l'invitation de visiteurs peuvent varier en fonction des paramètres du site et des réglages configurés pour la gestion des visiteurs.

REMARQUE : Les champs obligatoires sont mis en évidence dans l'interface utilisateur avec un astérisque (*).

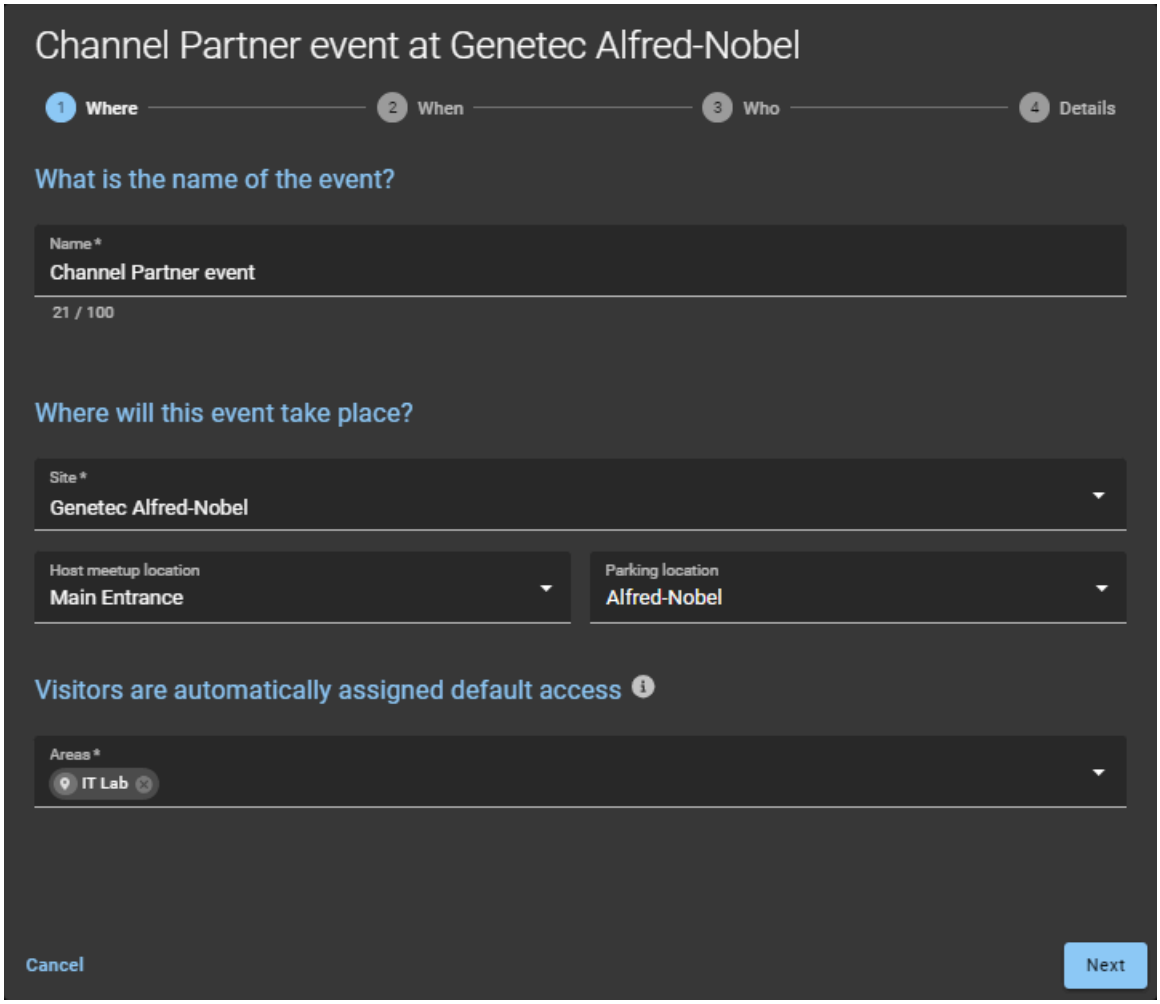
Procédure

1 Connectez-vous au portail en libre-service.

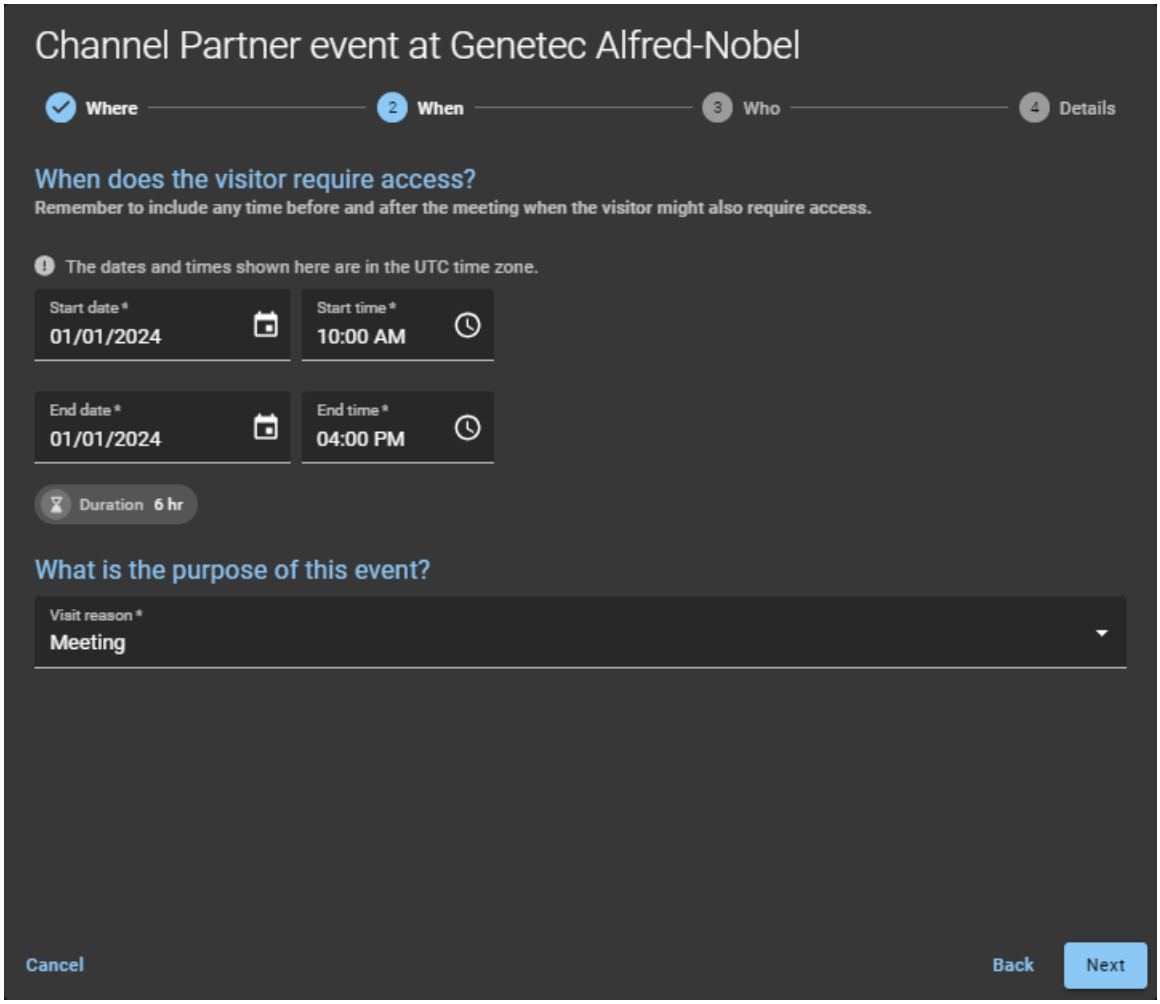
2 Procédez de l'une des manières suivantes :

- Cliquez sur **Tableau de bord** > **Mes demandes** > **Nouvelle demande** > **Inviter des visiteurs**.
- Cliquez sur **Tableau de bord** > **Visites** > **Nouvel événement de visite**.

3 Dans l'assistant *Nouvel événement de visite*, entrez ou sélectionnez *où* l'événement aura lieu.

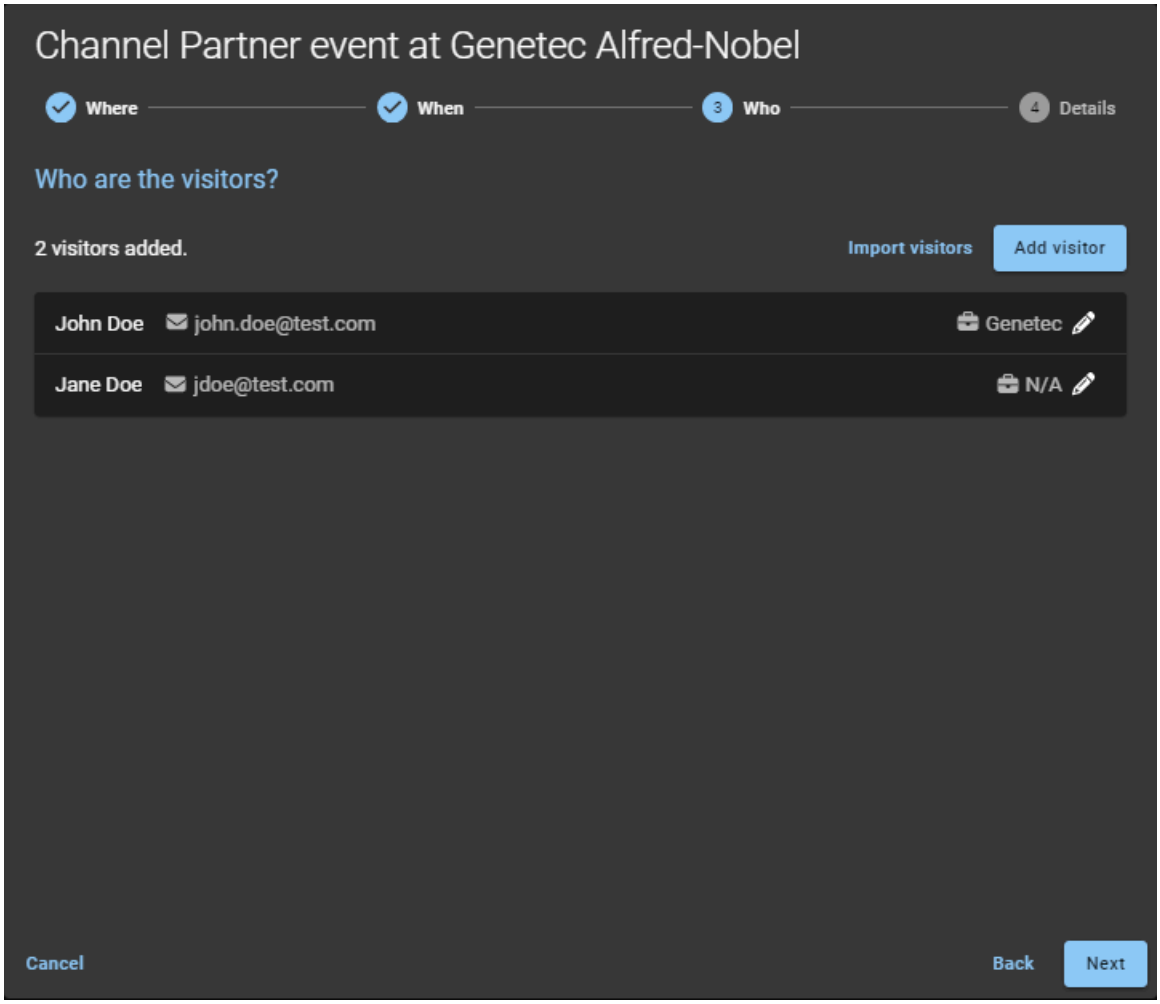


4 Entrez ou sélectionnez les informations spécifiant *quand* l'événement aura lieu, ainsi que son objectif.



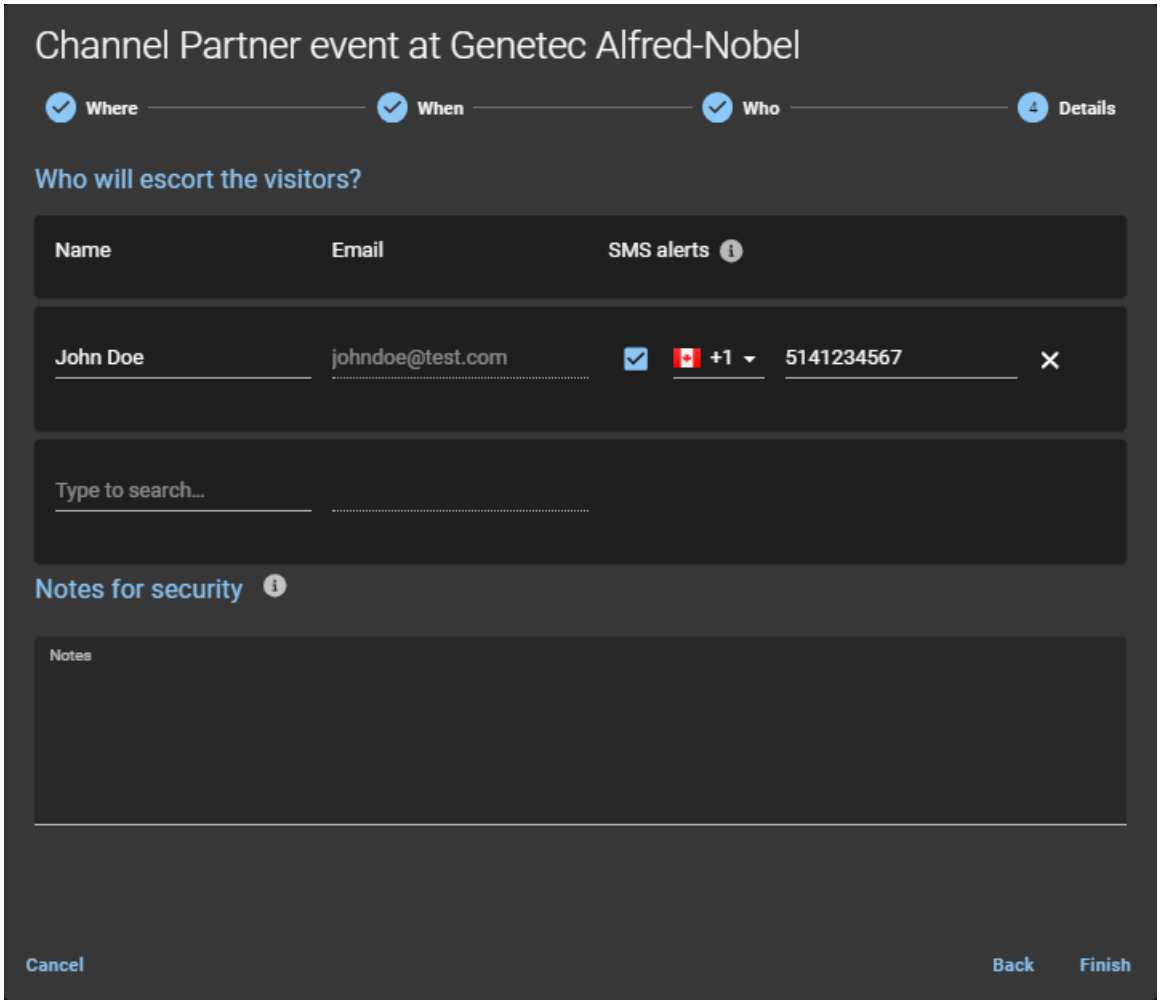
CONSEIL : Pensez à inclure le temps nécessaire avant et après l'événement durant lequel le visiteur peut avoir besoin d'un accès.

5 Entrez ou sélectionnez les informations spécifiant *qui* inviter à l'événement.



a) Cliquez sur **Ajouter un visiteur** et remplissez les champs.
b) Cliquez sur **Enregistrer**.
c) Répétez la procédure pour chaque visiteur supplémentaire.

6 Entrez les *informations* sur l'événement.



- **Nom :** Le nom de l'hôte de l'événement visiteur.
- **E-mail :** L'adresse e-mail pour l'hôte de l'événement visiteur.
- **SMS :** Saisissez un numéro de téléphone mobile pour envoyer des notifications d'alerte par SMS aux hôtes de visiteur lorsque le visiteur s'inscrit.
  - **REMARQUE :** Utilisez le champ de recherche pour ajouter des hôtes de visiteurs. Vous pouvez ajouter jusqu'à 10 hôtes de visiteur.
- **(Facultatif) Remarques concernant la sécurité :** Ajoutez des notes sur le visiteur, l'invitation de visite ou l'événement de visite.

7 Cliquez sur **Terminer**.

Votre demande de visite a été soumise et attend les approbations requises.

Lorsque vous avez terminé

Confirmez si la demande a été approuvée ou rejetée :

- Recherchez un e-mail *Visite approuvée* dans votre boîte de réception.
- Consultez **Mes demandes** dans ClearID.

Rubriques connexes

Alertes SMS, page 385
À propos des notifications par e-mail, page 186
Note sur la fonction de gestion des visiteurs (2 pages)

Inviter des visiteurs à l’aide de l’importation CSV

Si vous avez plus de cinq visiteurs à inviter à votre événement, vous pouvez importer un fichier CSV pour remplir votre liste d'invités.

Avant de commencer

1. Familiarisez-vous avec les processus.
2. Activez la gestion des visiteurs pour votre site.
3. Assurez-vous que vous disposez des autorisations requises pour inviter des visiteurs sur le site.

À savoir

- Si vous avez configuré un site principal pour votre identité, vous êtes automatiquement autorisé à inviter des visiteurs sur ce site. L'accès n’est accordé automatiquement que si les options de gestion des visiteurs du site ont été configurées pour autoriser les gens à inviter des visiteurs.
- Les options affichées lors de l’invitation de visiteurs peuvent varier en fonction des paramètres du site et des réglages configurés pour la gestion des visiteurs.

CONSEIL : Pour **Importer des visiteurs**, vous pouvez utiliser un fichier CSV exemple fourni par le système. Les colonnes dans le fichier CSV correspondent aux réglages de configuration du site. Vous pouvez ensuite compléter les détails du visiteur dans le fichier CSV et importer tous les visiteurs en un seul clic. Par exemple, importer 500 personnes pour une visite de site ou un événement client.

REMARQUE : Les champs obligatoires sont mis en évidence dans l'interface utilisateur avec un astérisque (*).

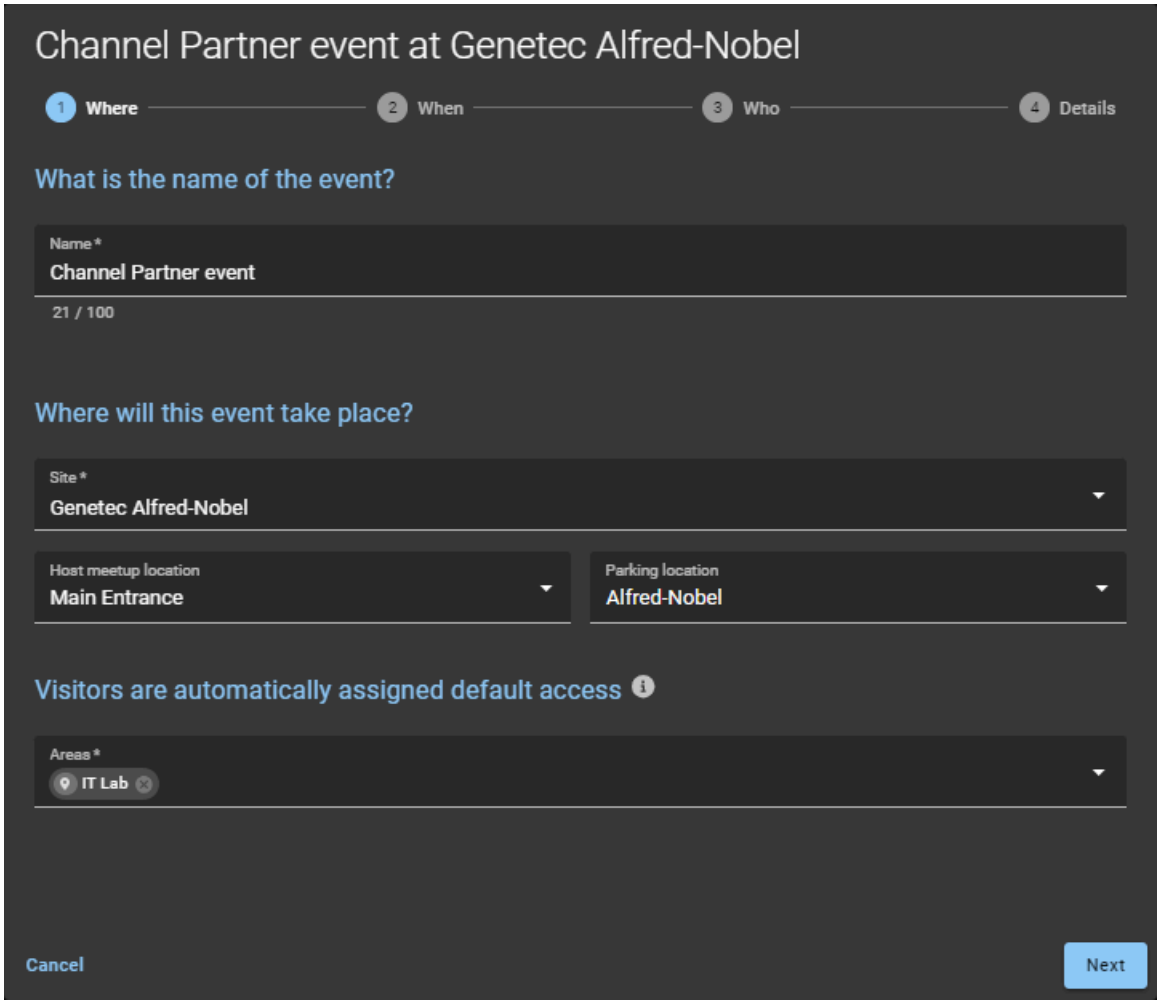
Procédure

1 Connectez-vous au portail en libre-service.

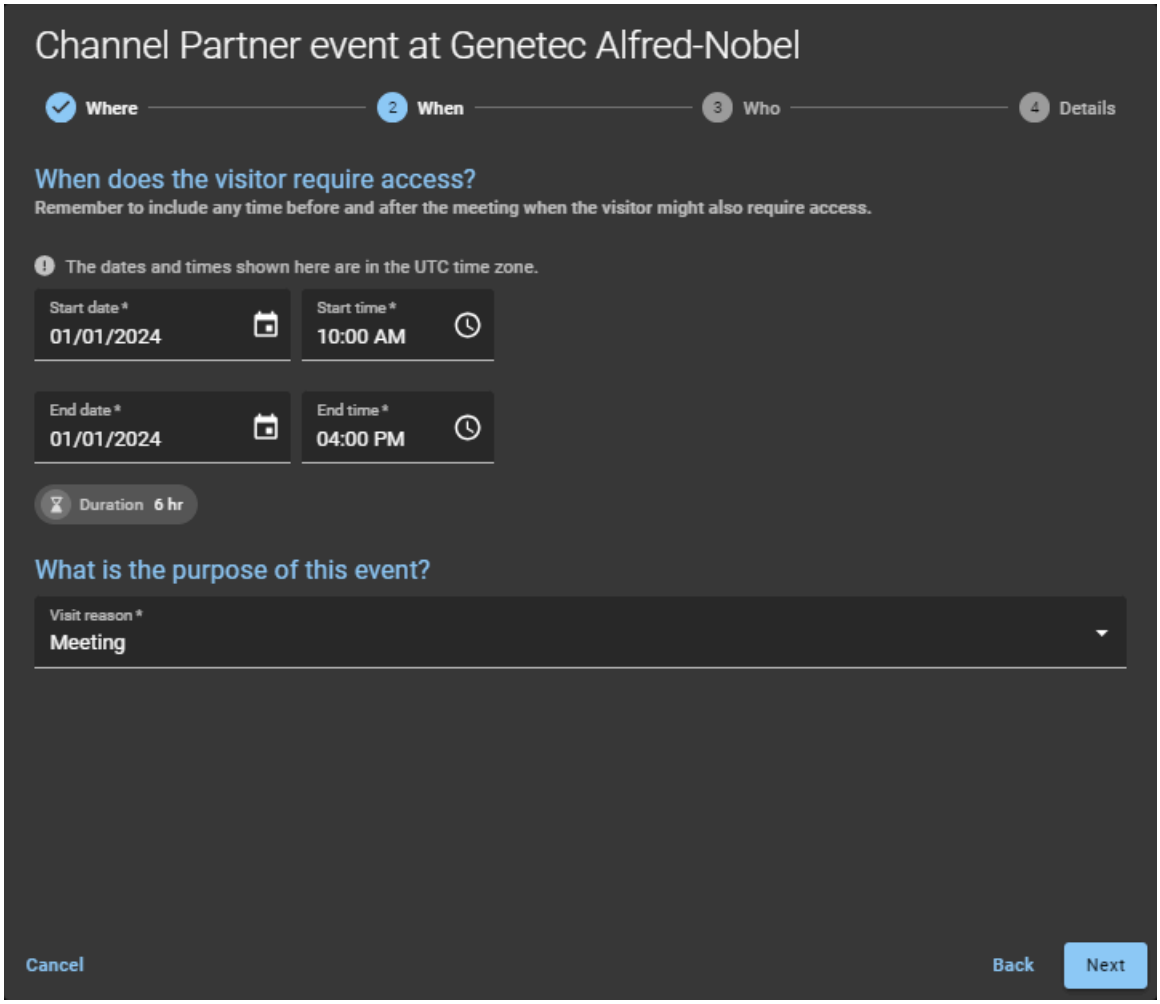
2 Procédez de l'une des manières suivantes :

- Cliquez sur **Tableau de bord** > **Mes demandes** > **Nouvelle demande** > **Inviter des visiteurs**.
- Cliquez sur **Tableau de bord** > **Visites** > **Nouvel événement de visite**.

3 Dans l'assistant *Nouvel événement de visite*, entrez ou sélectionnez *où* l'événement aura lieu.

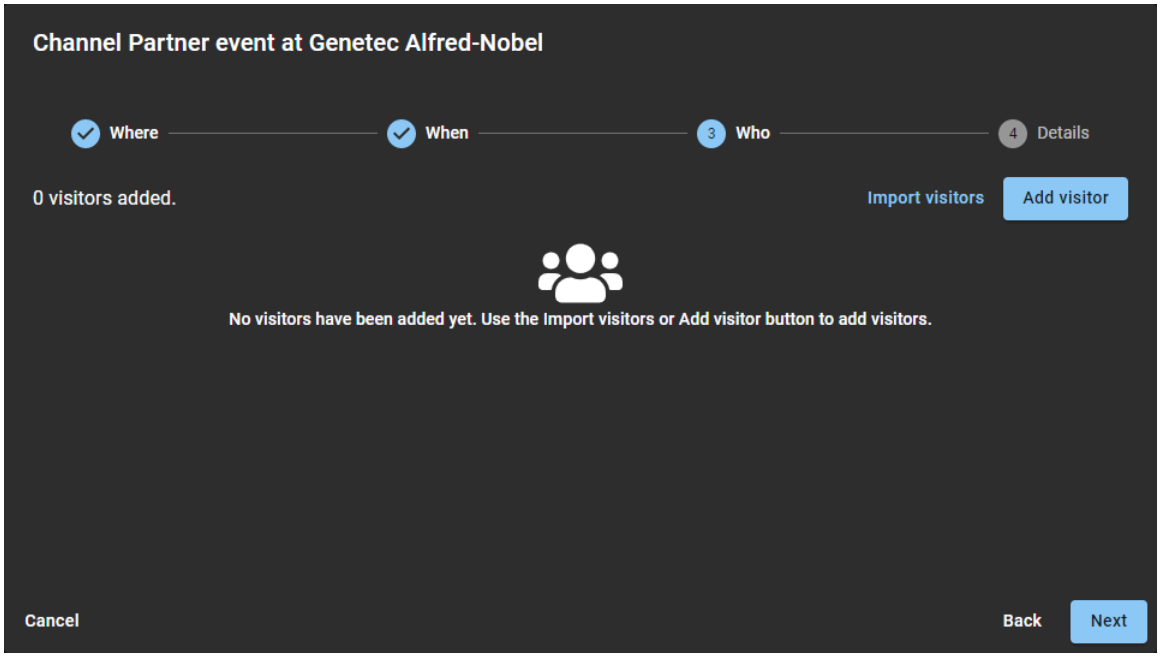


4 Entrez ou sélectionnez les informations spécifiant *quand* l'événement aura lieu, ainsi que son objectif.



CONSEIL : Pensez à inclure le temps nécessaire avant et après l'événement durant lequel le visiteur peut avoir besoin d'un accès.

5 Préparez-vous à importer les personnes que vous souhaitez inviter à l'événement (*qui*).

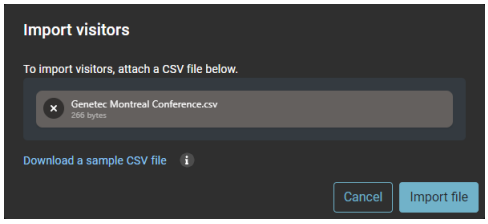


a) Dans la section *Qui participera à cet événement ?*, cliquez sur **Importer des visiteurs**, puis sélectionnez l'une des options suivantes :

- Utiliser un fichier CSV existant.
- Télécharger un exemple de fichier CSV.

6 Si vous avez choisi d'utiliser un fichier CSV existant, procédez comme suit :

a) Faites glisser et déposez un fichier CSV contenant les clients que vous souhaitez inviter ou cliquez sur **Parcourir** pour sélectionner le fichier dont vous avez besoin.



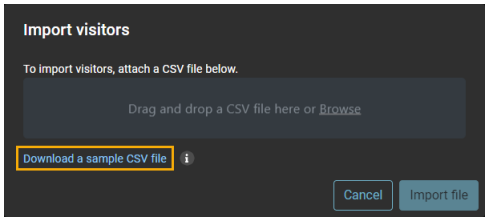
b) Cliquez sur **Importer un fichier** pour importer la liste des visiteurs.

c) Cliquez sur **Confirmer** pour terminer l'importation.

d) (Facultatif) Cliquez sur **Modifier** ( ) pour modifier les informations sur les visiteurs puis cliquez sur **Enregistrer** pour confirmer la mise à jour.

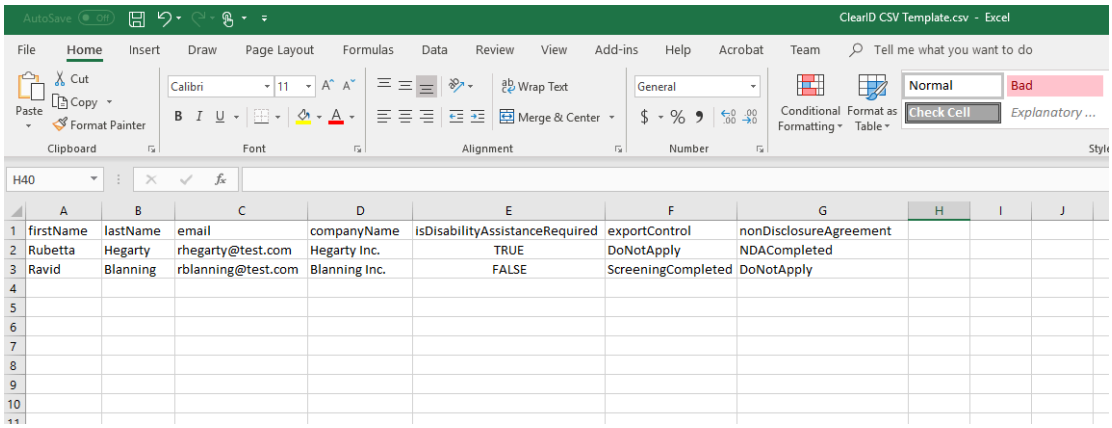
7 Si vous avez choisi **Télécharger un exemple de fichier CSV**, procédez comme suit :

a) Cliquez sur **Télécharger un modèle de fichier CSV**.



b) Sélectionnez et ouvrez le fichier CSV téléchargé.

c) Pour chaque visiteur, saisissez une ligne complète d'informations dans le modèle de fichier CSV.



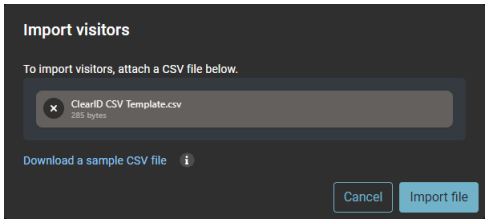
	A	B	C	D	E	F	G	H	I	J
1	firstName	lastName	email	companyName	isDisabilityAssistanceRequired	exportControl	nonDisclosureAgreement			
2	Rubetta	Hegarty	rhegarty@test.com	Hegarty Inc.	TRUE	DoNotApply	NDACompleted			
3	Ravid	Blanning	rblanning@test.com	Blanning Inc.	FALSE	ScreeningCompleted	DoNotApply			
4										
5										
6										
7										
8										
9										
10										

REMARQUE : Les colonnes du modèle CSV peuvent varier en fonction des paramètres de configuration de votre site.

d) Enregistrez la liste des visiteurs au format CSV.

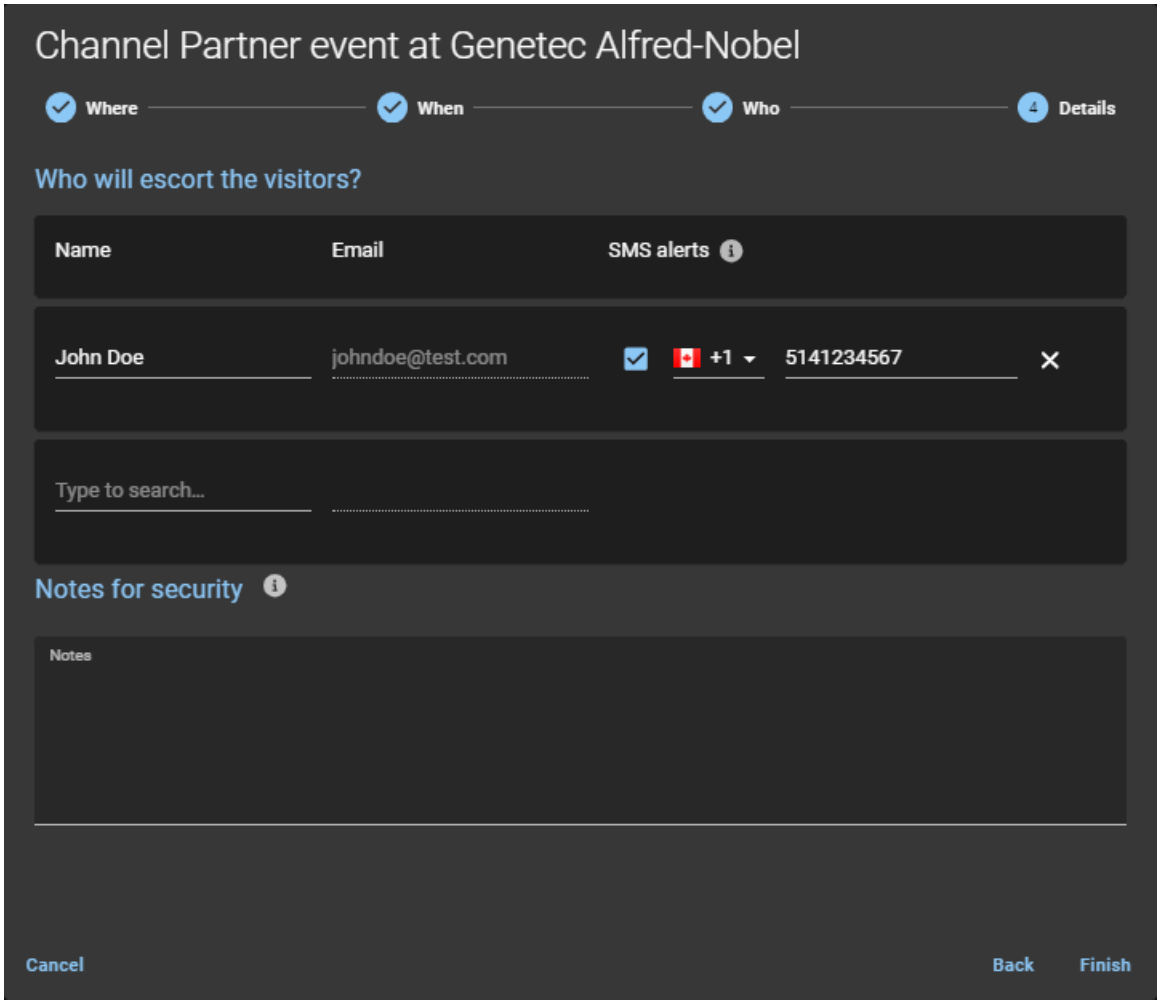
e) Revenez à la boîte de dialogue *Importer des visiteurs*, et faites un glisser-déposer ou cliquez sur **Parcourir** pour sélectionner le fichier que vous venez de créer.

f) Cliquez sur **Importer un fichier** pour importer la liste des visiteurs.



g) Cliquez sur **Confirmer** pour terminer l'importation.

8 Entrez les *informations* sur l'événement.



- **Nom :** Le nom de l'hôte de l'événement visiteur.
- **E-mail :** L'adresse e-mail pour l'hôte de l'événement visiteur.
- **SMS :** Saisissez un numéro de téléphone mobile pour envoyer des notifications d'alerte par SMS aux hôtes de visiteur lorsque le visiteur s'inscrit.
  - **REMARQUE :** Utilisez le champ de recherche pour ajouter des hôtes de visiteurs. Vous pouvez ajouter jusqu'à 10 hôtes de visiteur.
- **(Facultatif) Remarques concernant la sécurité :** Ajoutez des notes sur le visiteur, l'invitation de visite ou l'événement de visite.

9 Cliquez sur **Terminer**.

Votre demande de visite a été soumise et attend les approbations requises.

Lorsque vous avez terminé

Confirmez si la demande a été approuvée ou rejetée :

- Recherchez un e-mail *Visite approuvée* dans votre boîte de réception.
- Consultez **Mes demandes** dans ClearID.

Rubriques connexes

Alertes SMS, page 385
À propos des notifications par e-mail, page 186
Note sur la fonction de gestion des visiteurs (2 pages)

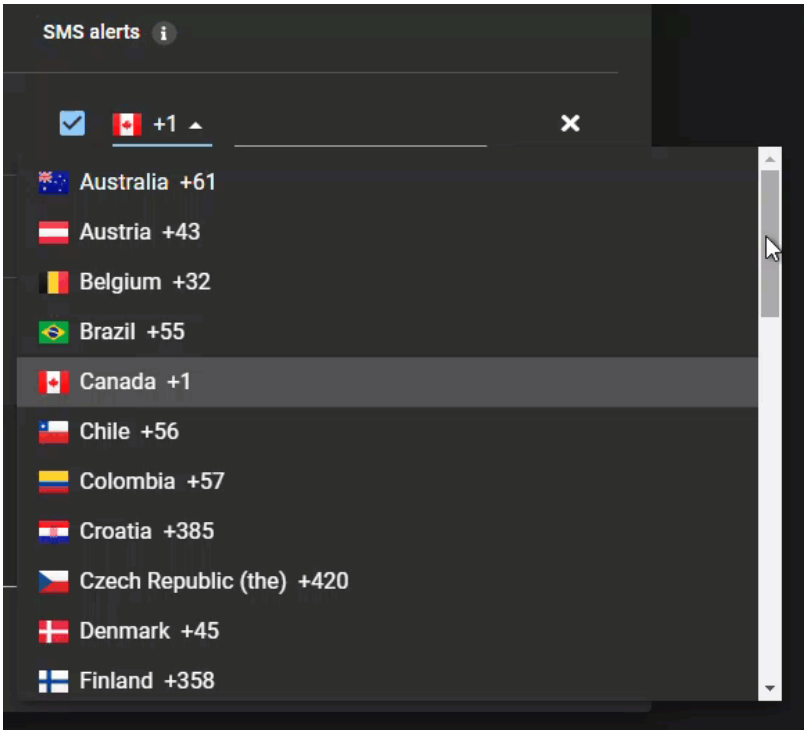
Alertes SMS

Dans Genetec ClearID[MC], les alertes SMS sont utilisées dans l'assistant d'événement de visite pour notifier les hôtes de visiteurs lorsque les visiteurs s'inscrivent.

Les alertes SMS pour l'enregistrement des visiteurs sont prises en charge pour les pays suivants :

Pays	Code postal
L'Autriche	+43
Australie	+61
Belgique	+32
Brésil	+55
Canada	+1
Chili	+56
Colombie	+57
Croatie	+385
République tchèque (la)	+420
Danemark	+45
Finlande	+358
France	+33
Allemagne	+49
Grèce	+30
Islande	+354
Inde	+91
Irlande	+353
Italie	+39
Japon	+81
Luxembourg	+352

Pays	Code postal
Malaisie	+60
Mexique	+52
Monaco	+377
Pays-Bas	+31
Norvège	+47
Pérou	+51
Philippines (les)	+63
Portugal	+351
Roumanie	+40
Singapour	+65
Espagne	+34
Suède	+46
Suisse	+41
Taïwan (Province de Chine)	+886
Thaïlande	+66
Royaume-Uni (Grande-Bretagne et Irlande du Nord) (le)	+44
États-Unis d'Amérique (les)	+1
Vietnam	+84



Rubriques connexes

Inviter des visiteurs manuellement, page 374
Inviter des visiteurs à l'aide de l'importation CSV, page 379

Examiner les événements de visite

Les propriétaires de secteur, le personnel de sécurité et l'accueil peuvent examiner les visites ou événements en cours ou à venir pour leur secteur. Des visites peuvent être demandées pour des employés d'autres sites, des prestataires de maintenance, des rendez-vous, des réunions, des entretiens, des clients, des conférences de partenaires commerciaux, etc.

À savoir

Seuls les *propriétaires de secteur*, l'équipe de sécurité ou les réceptionnistes peuvent examiner les visites.

Procédure

1 Cliquez sur **Tableau de bord** > **Visites**.

2 (Facultatif) Saisissez des critères de recherche.

Seuls les résultats de recherche pour les visites qui contiennent le mot saisi dans le nom de la visite sont affichés. Par exemple, si vous entrez `Formation`, seules les visites dont le nom contient le mot *Formation* sont affichées dans le résultat de la recherche.

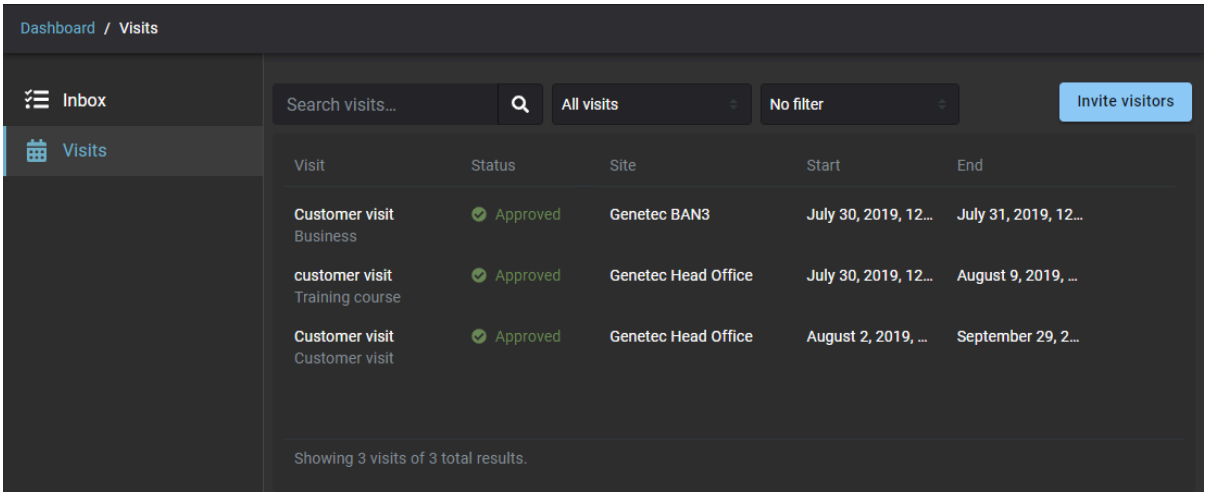
3 Sélectionnez les options dont vous avez besoin.

- **Visites actuelles et à venir :** Affiche les visites actuelles et à venir. Par défaut, 10 visites sont affichées et vous pouvez cliquer sur le bouton **Charger plus** pour afficher les 10 visites suivantes.
- **Visites passées :** Affiche les visites passées. Par défaut, les 10 visites précédentes sont affichées et vous pouvez cliquer sur le bouton **Charger plus** pour afficher les 10 visites antérieures. Vous pouvez rechercher toutes les visites passées au cours de la dernière année.
- **Toutes les visites :** Affiche toutes les visites. Par défaut, 10 visites sont affichées et vous pouvez cliquer sur le bouton **Charger plus** pour afficher les 10 visites suivantes.

4 (Facultatif) Sélectionnez un filtre dans la liste **Filtre** pour filtrer les résultats par état de demande de visite.

- Aucun filtre
- Approuvé
- Annulé
- Refusé
- Soumis
- En attente d'approbation

Les visites correspondant à vos sélections sont affichées.



Lorsque vous avez terminé

Copiez un événement de visite.

Copier un événement de visite

Vous pouvez copier un événement de visite pour réutiliser les informations de visites ou d'événements de visite récurrents qui impliquent un grand nombre de participants.

Avant de commencer

Consultez les événements de visite.

À savoir

- Tout utilisateur peut copier ses visites pour en créer une autre.
- Utilisez la fonction **Copier l'événement** lorsque vous avez des visites récurrentes ou une visite qui implique un grand nombre de participants. Par exemple, dans les situations suivantes :
  - Visites récurrentes
  - Réunion avec les mêmes participants ou presque qu'une réunion précédente
  - Visites mensuelles de clients
  - Conférence annuelle de partenaires commerciaux

Procédure

1 Cliquez sur **Tableau de bord** > **Visites**.

2 Cliquez sur l'événement de visite que vous souhaitez copier.

3 Cliquez sur **Copier l'événement**.

Une copie de l'événement de visite est créée.

4 Modifiez l'événement de visite selon vos besoins et cliquez sur **Enregistrer**.

Par exemple, modifier les détails de l'événement, modifier la date, ajouter ou supprimer des visiteurs, ajouter ou supprimer des hôtes ou modifier les notifications.

Le nouvel événement de visite est créé, et une notification par e-mail de *Visite créée* est envoyée à tous les hôtes et visiteurs.

Modifier les événements de visite

Vous voudrez parfois modifier un événement de visite, pour changer les informations ou ajouter ou supprimer des visiteurs ou des hôtes. La mise à jour des informations sur l'événement de visite permet d'informer les visiteurs en cas de changements affectant l'événement prévu.

Avant de commencer

Créez vos événements de visite dans Genetec ClearID[MC] en procédant de la manière suivante :

- Inviter des visiteurs manuellement, page 374
- Inviter des visiteurs à l'aide de l'importation CSV, page 379

À savoir

- Les événements ne peuvent que être modifiés avant le début de l'événement de visite.
- Toute modification est mise en avant dans le nouvel e-mail de notification envoyé aux destinataires concernés.
- Si l'approbation des visites est activée, toutes les modifications apportées à un événement de visite, autres que les modifications dans le champ **Motif**, génèrent des notifications qui sont envoyées aux approbateurs désignés afin qu'ils valident les modifications ou les ajouts.
- Le remplacement de l'adresse e-mail d'un visiteur ou d'un hôte par une autre adresse déclenche une notification d'annulation à l'ancienne adresse et une notification d'événement de visite à la nouvelle adresse.
- Si l'approbation des événements de visite est activée, la modification du nom d'un visiteur ou d'un hôte ne déclenche pas d'e-mail de notification pour les visiteurs, mais elle déclenche à nouveau le processus d'approbation.

Procédure

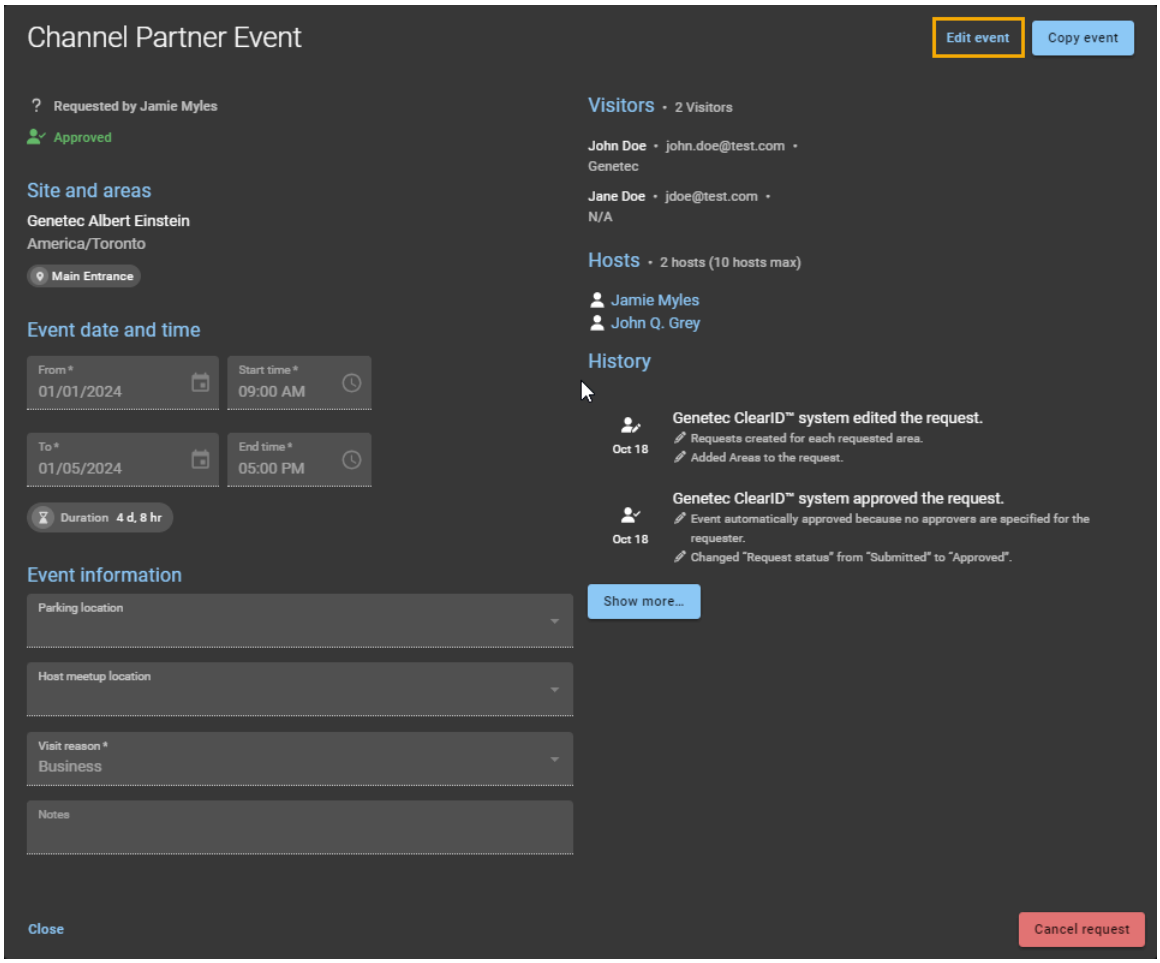
1 Cliquez sur **Tableau de bord** > **Visites**.

2 (Facultatif) Si la liste est longue, utilisez les menus déroulants et les filtres de colonne pour affiner le résultat.

- **Nom :** Entrez des critères de recherche pour rechercher l'événement de visite par nom.
- **État :** Entrez un ou plusieurs critères pour rechercher l'événement de visite par état de l'événement.
- **Site :** Commencez à taper pour trouver ou sélectionner un site dans la liste **Site**.
- **Date :** Dans la colonne **Date**, utilisez les boutons croissant () ou décroissant () pour modifier l'ordre des résultats.

3 Cliquez sur un événement de visite pour afficher les informations et vérifier qu'il s'agit bien de l'événement que vous souhaitez modifier.

4 Cliquez sur **Modifier l'événement**.



5 Modifiez les éléments de votre choix selon vos besoins :

a) Dans le champ **Nom**, modifiez le nom[1].

b) Dans la section *Date et heure de l'événement*, modifiez la date et l'heure de début et de fin[1].

c) Dans la section *Informations sur l'événement*, modifiez le lieu de stationnement, de rendez-vous avec l'hôte ou les remarques[1].

La modification du **Motif de la visite** pour un événement de visite ne déclenche pas de notification d'approbation, car le motif n'a pas d'incidence sur la présence ou non des visiteurs.

d) Dans la section *Visiteurs*, ajoutez, modifiez ou supprimez des visiteurs.

Toute modification apportée aux visiteurs déclenche un nouvel examen basé sur les critères de contrôle de la liste de surveillance.

e) Dans la section *Hôtes*, ajoutez, modifiez ou supprimez des hôtes.

REMARQUE : [1]La modification des champs **Nom**, **Date et heure de l'événement** et **Informations sur l'événement** ne redéclenche pas l'approbation (si l'approbation est activée).

6 Cliquez sur **Enregistrer** pour confirmer vos modifications.

Lorsque vous avez terminé

Examinez les infos sur l'événement de visite pour vérifier qu'il n'y a pas d'erreurs.

Approuver les demandes de visite

Pour modifier les demandes de visite, un *Approbateur d'événement de visite* doit examiner les approbations en attente, puis décider quelles demandes approuver.

Avant de commencer

Activez la gestion des visiteurs pour les sites.

À savoir

Lorsqu'une demande de visite est envoyée, les *approbateurs d'événement de visite* reçoivent une notification par e-mail.

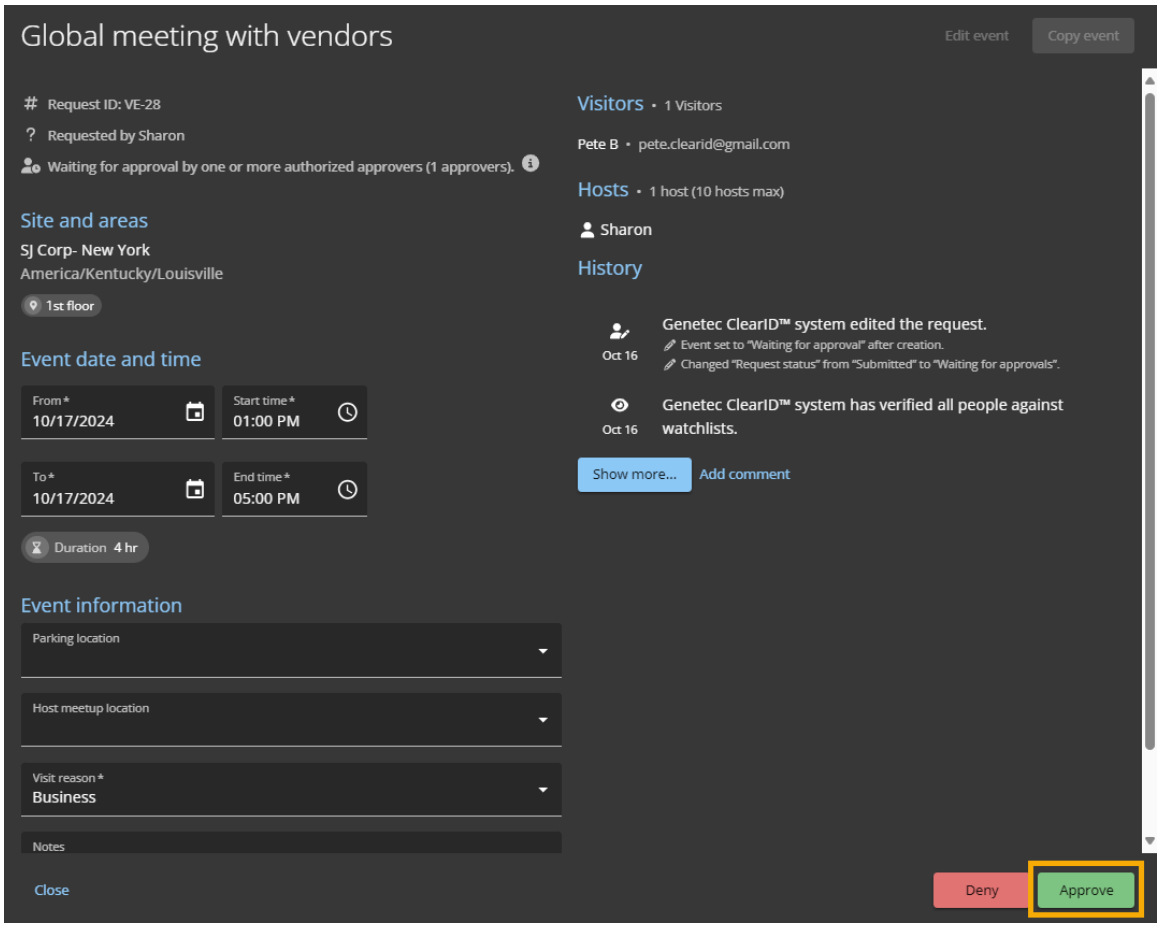
Procédure

1 Pour afficher les détails d'une demande avant de l'approuver ou de la refuser, cliquez sur **Approuver** dans l’e-mail de demande de visite.

Vous êtes redirigé vers le portail Genetec ClearID^{MC} où vous êtes invité à vous identifier.

2 Examinez les détails de la demande, et apportez toute modification nécessaire.

CONSEIL : Vous pouvez modifier la demande si vous remarquez une erreur ou un élément à modifier dans la demande. Par exemple, vous pouvez modifier les dates en fonction de dates de fermeture des bureaux, ou indiquer une zone de stationnement plus adaptée.



a) (Facultatif) Cliquez sur **Afficher plus...** pour voir l'historique des modifications apportées à la demande de visite.

b) (Facultatif) Cliquez sur **Ajouter un commentaire** pour ajouter des remarques à l'historique de la demande de visite. Vous pouvez par exemple indiquer pourquoi vous avez modifié la date et l'heure de la visite.

3 Cliquez sur **Approuver**.

a) (Facultatif) Dans le champ **Motif d'approbation**, indiquez pourquoi la visite a été approuvée.

b) Cliquez sur **Confirmer**.

CONSEIL : Pour afficher la liste de toutes les approbations en attente, allez dans **Tableau de bord** > **Mes tâches** et sélectionnez **En attente** dans la liste.

Un e-mail de confirmation est envoyé au visiteur l'informant des détails de la visite.

À propos des rapports de visiteurs

Dans Genetec ClearID[MC], un rapport de visiteurs est une liste de toutes les visites prévues ou en cours, ou des visites effectuées dans le passé sur un site particulier. Le rapport inclut des informations sur le nom du visiteur, le demandeur de l'événement, le nom de l'événement, l'arrivée prévue, l'inscription, la radiation et l'état de la liste de surveillance.

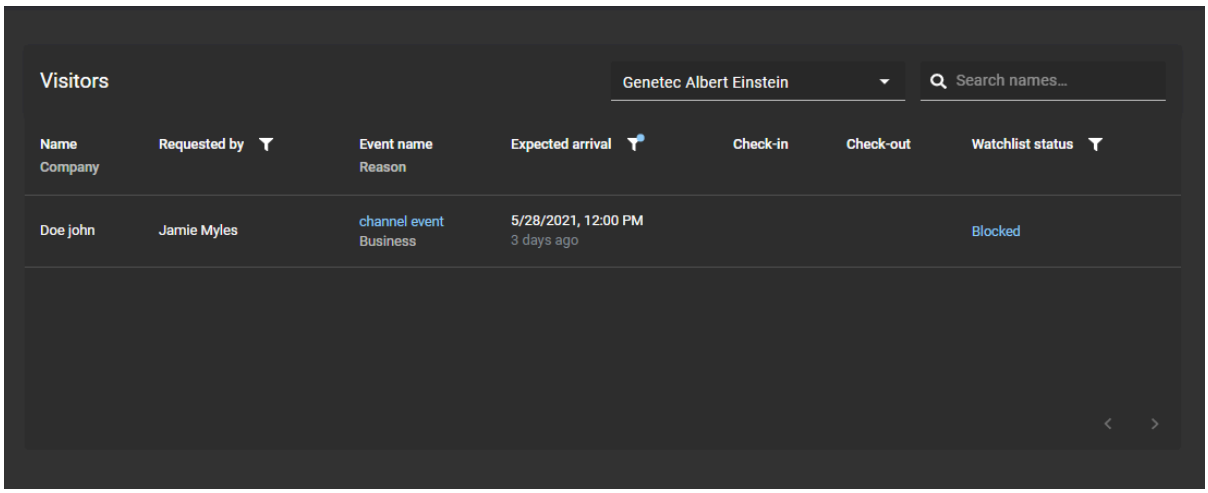


Illustration 10 : Rapport de visiteurs

Le rapport de visiteurs est utilisé par les *propriétaires de site* et les *responsables de liste de surveillance* pour vérifier les visites en cours ou à venir ou celles qui se sont produites dans le passé ainsi que pour fournir des informations aux contrôleurs.

Des filtres peuvent être utilisés pour affiner le résultat de la recherche par instigateur de la requête, arrivée prévue et état de la liste de surveillance.

Rubriques connexes

Afficher un rapport de visiteurs, page 396

Afficher un rapport de visiteurs

Vous pouvez afficher un rapport de visiteurs pour toute visite en cours ou prévue, ou pour les visites effectuées dans le passé. Le résultat du rapport est propre à un site, et peut être filtré par demandeur d'événement, arrivée prévue et état de la liste de surveillance.

Avant de commencer

Invitez vos visiteurs.

À savoir

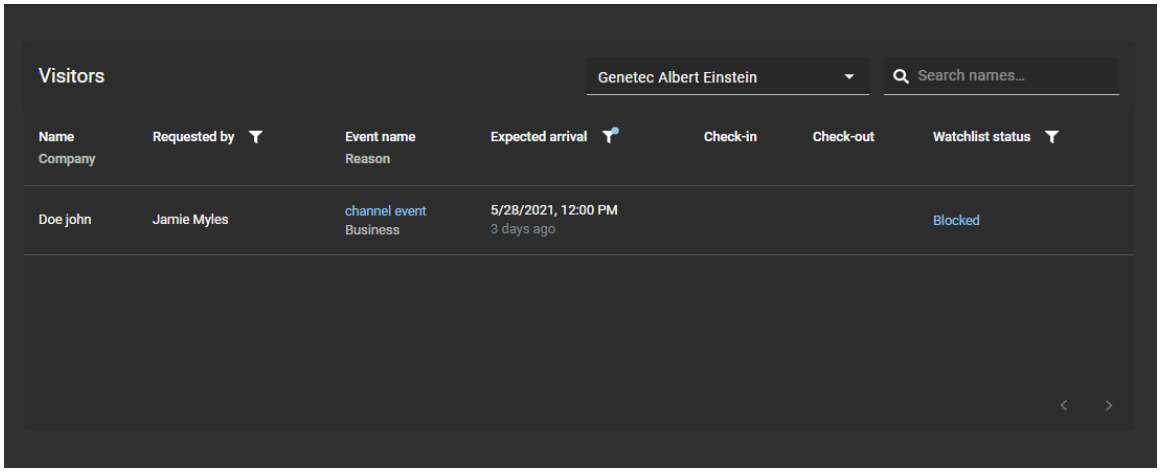
- Les *propriétaires de sites* et les *responsables de listes de surveillance* peuvent afficher le rapport de visiteurs.
- Seules les responsables de listes de surveillance peuvent débloquer ou autoriser les visiteurs bloqués.

REMARQUE : Pour les clients qui n'ont pas acheté de licence de liste de surveillance, la colonne **Statut de liste de surveillance** figure dans le rapport, mais affiche N/A, car aucune donnée de liste de surveillance n'est disponible.

Procédure

1 Sur la page d'accueil, cliquez sur **Rapports** > **Visiteurs**.

2 Sélectionnez un site dans la liste **Site**.



3 (Facultatif) Tapez un nom dans le champ de recherche.

4 (Facultatif) Cliquez sur l'icône de filtre **Demandé par** et entrez le nom du demandeur de la visite.

5 (Facultatif) Cliquez sur l'icône de filtre **Arrivée prévue** et sélectionnez une option :

- Visites actuelles et à venir
- Il y a un jour
- Il y a 7 jours
- Il y a 30 jours
- Il y a 90 jours
- Tous les événements passés

CONSEIL : En l'absence de résultat, sélectionnez une plage plus large pour le filtre **Arrivée prévue**.

6 (Facultatif) Cliquez sur l'icône de filtre **État de la liste de surveillance** et cochez une ou plusieurs cases :

- **Autorisé :** Aucune entrée de liste de blocage correspondante n'a été trouvée pour le visiteur durant la procédure de contrôle de liste de surveillance, et son accès au site a été accordé.
- **Bloqué :** Une ou plusieurs entrées de liste de blocage correspondantes ont été trouvées pour le visiteur durant la procédure de contrôle de liste de surveillance, et son accès au site a été bloqué.
- **Débloqué :** Une ou plusieurs entrées de liste de blocage correspondantes ont été trouvées pour le visiteur durant la procédure de contrôle de liste de surveillance, mais son accès au site a été accordé par le responsable de liste de surveillance.
- **En cours :** Le contrôle de liste de surveillance pour le visiteur est en cours.
- **Notifié :** Une ou plusieurs entrées de liste de notification correspondantes ont été trouvées pour le visiteur durant la procédure de contrôle de liste de surveillance. Le responsable de liste de surveillance a été notifié, et l'accès au site a été accordé au visiteur.

a) (Facultatif) Cliquez sur le lien **Bloqué** pour ouvrir la boîte de dialogue **Alerte de liste de surveillance de visiteurs**. Un responsable de liste de surveillance peut y accorder l'accès en cas de besoin.

b) (Facultatif) Cliquez sur l'icône d'information en regard d'un état de liste de surveillance débloqué pour savoir qui a débloqué le visiteur.

7 (Facultatif) Cliquez sur pour réinitialiser tous les filtres et revenir à la liste des visiteurs.

Rubriques connexes

Débloquer les visiteurs bloqués par une liste de surveillance, page 464

À propos des rapports de visiteurs, page 395

Identifiants code QR pour les visiteurs

Genetec ClearID[MC] peut utiliser des codes QR en tant qu'identifiants pour les visiteurs, afin de simplifier l'accès aux parkings, le passage de tourniquets ou l'accès à d'autres installations sécurisées.

Les solutions de code QR tierces suivantes sont actuellement prises en charge :

- Lecteurs de codes à barres Qscan
- Lecteurs de codes QR STid

Les visiteurs peuvent utiliser un code QR comme identifiant pour ouvrir les barrières d'entrée des parkings, passer les tourniquets ou accéder aux installations sécurisées :

- Le code QR contenu dans un e-mail de confirmation de visite peut être présenté à l'aide d'un smartphone.
- L'e-mail de confirmation du visiteur peut également être imprimé et utilisé pour l'enregistrement.
- Des messages SMS informent les hôtes de l'arrivée de leurs visiteurs (si la fonction de notification d'enregistrement est activée).

Rubriques connexes

Appareils pris en charge, page 78

Importer un format de carte personnalisé (identifiant code QR) dans Synergis

Avant d'utiliser les codes QR en tant qu'identifiants dans Genetec ClearID[MC], vous devez configurer Synergis[MC] pour la prise en charge du format de carte personnalisé utilisé pour les codes QR ClearID. Un code QR peut ensuite être utilisé en tant qu'identifiant pour accéder aux parkings, tourniquets et autres installations sécurisées.

Avant de commencer

- Installer le module externe ClearID
- Vérifiez que le module Gestion des visiteurs est activé dans votre licence Security Center Synergis.

À savoir

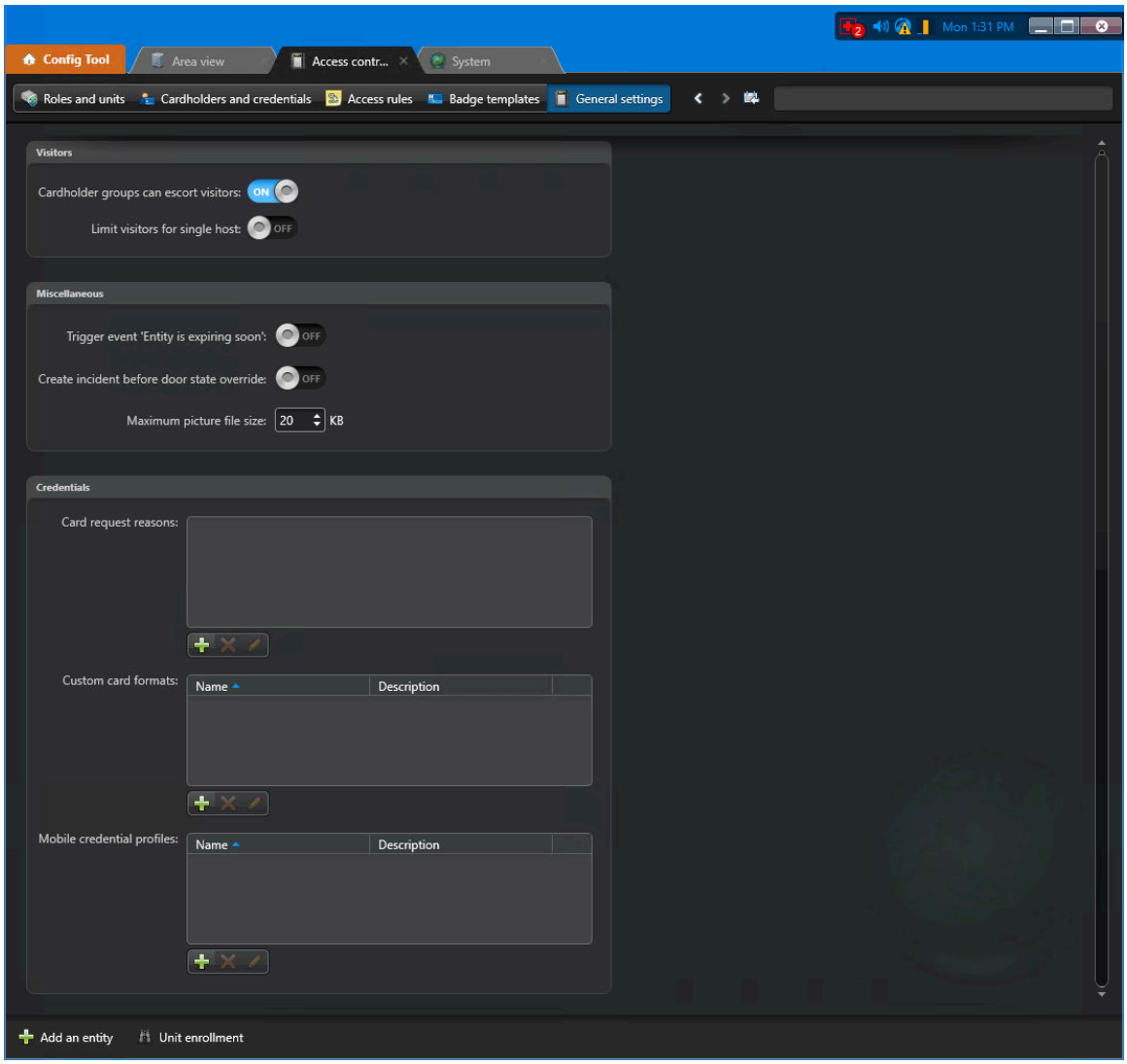
Seuls les administrateurs ou utilisateurs Security Center dotés du privilège *Modifier les propriétés d'identifiants* peuvent importer le format de carte personnalisé.

Le SDK et le module externe ClearID ne créent pas automatiquement le format de carte personnalisé pour les codes QR.

IMPORTANT : Le format de carte personnalisé est disponible sur le poste Security Center qui héberge le module externe ClearID.

Procédure

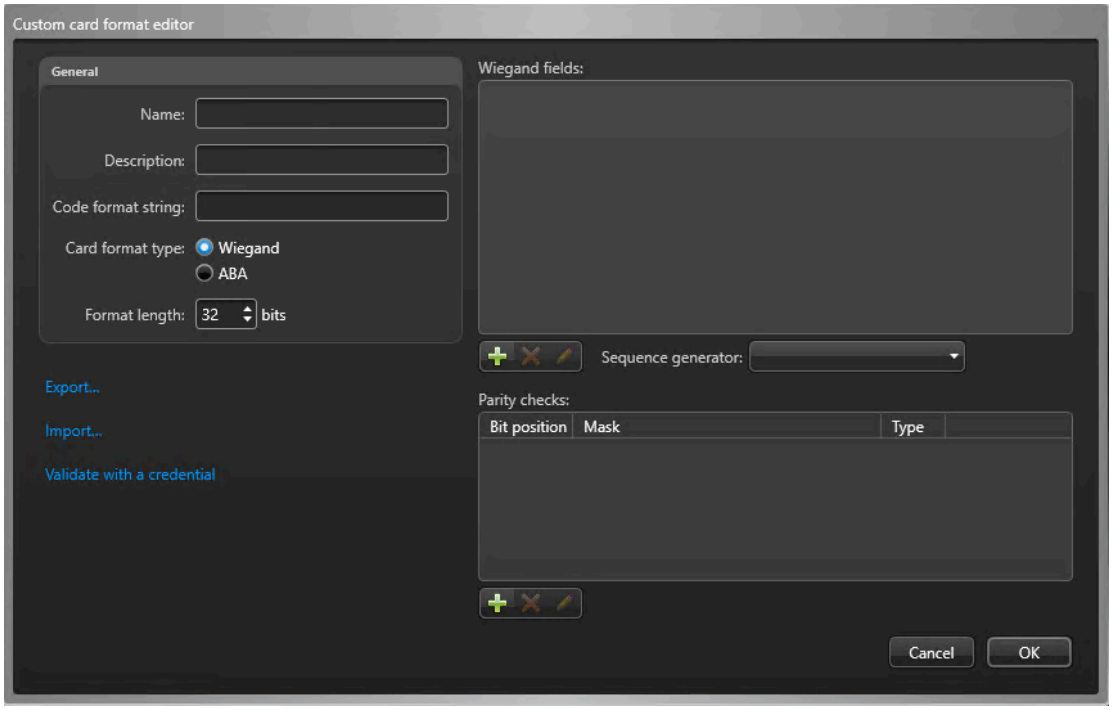
1 Dans Config Tool, ouvrez la tâche *Contrôle d'accès*, puis cliquez sur la vue **Paramètres généraux**.



2 Dans la section *Formats de carte personnalisés* sous *Identifiants*, cliquez sur **Ajouter un élément** ( ).

a) Téléchargez ce fichier QRcode.xml.

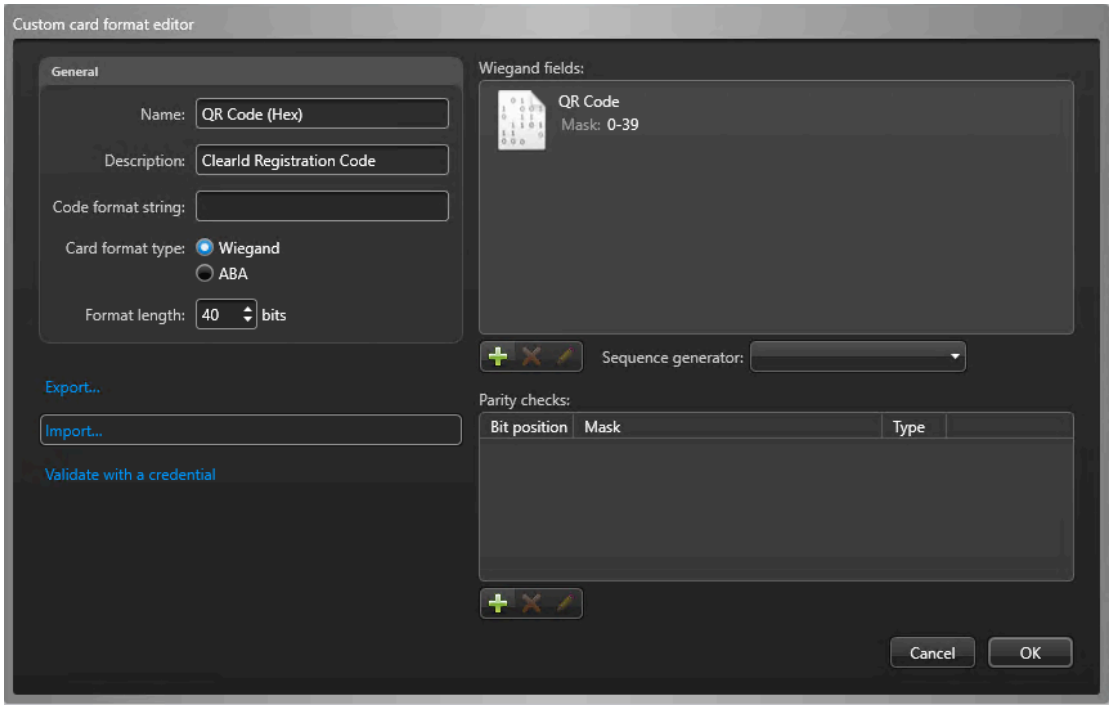
b) Dans l'*Éditeur de format personnalisé de carte*, cliquez sur **Importer**.



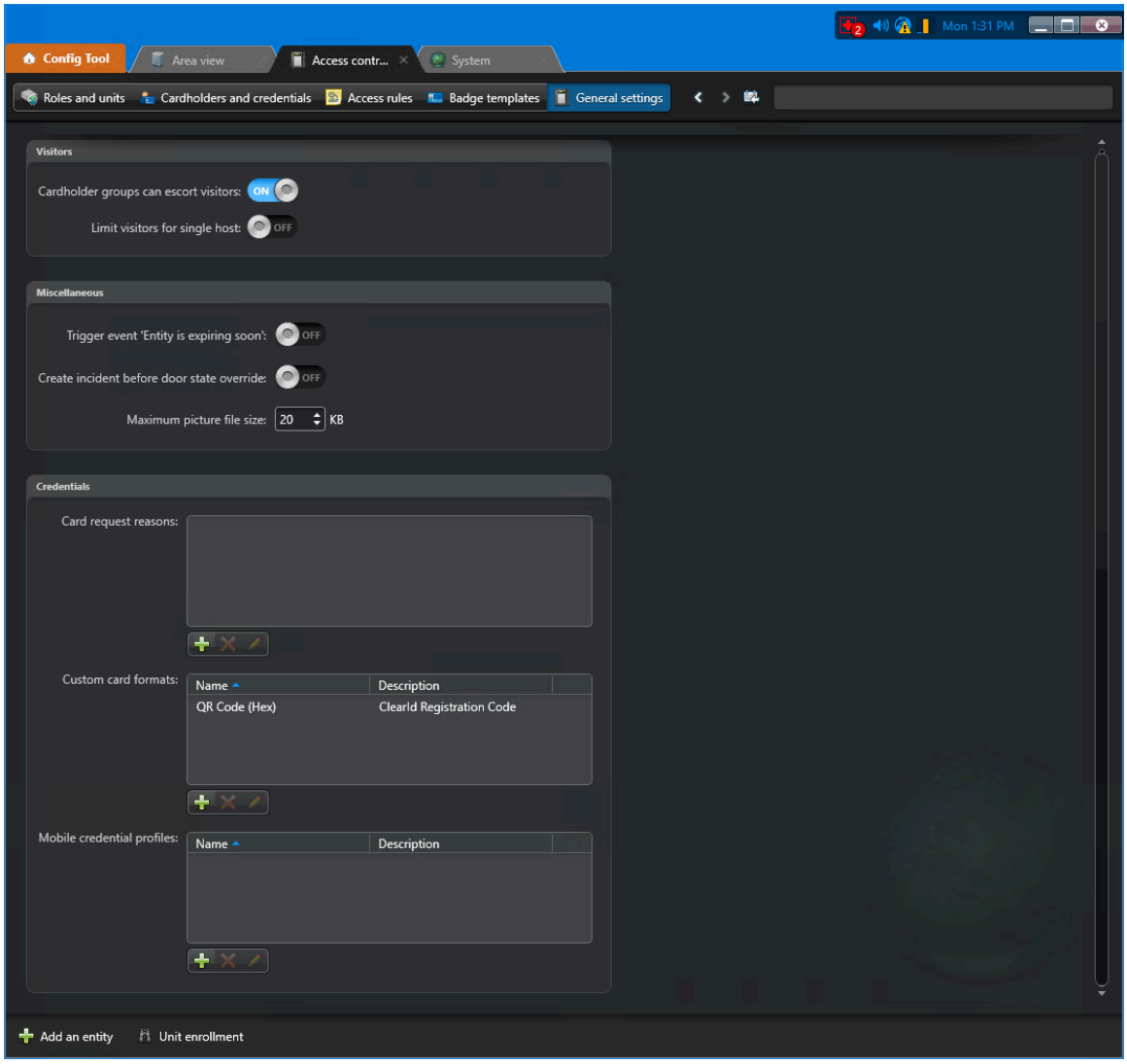
IMPORTANT : Vous devez importer le format de carte personnalisé sur le poste qui héberge le module externe ClearID. Le type de format de carte **Wiegand** est utilisé à l'importation.

c) Naviguez jusqu'au fichier *QRcode.xml* que vous avez téléchargé, puis sélectionnez-le.

d) Cliquez sur **Ouvrir** puis sur **OK**.



IMPORTANT : Vous devez utiliser ce fichier *QRCode.xml* particulier, car il contient un GUID qui est exigé par le module externe ClearID.



Dans la vue **Paramètres généraux** de la tâche *Contrôle d'accès*, le format de carte personnalisé Code QR (Hex) est désormais sélectionné et disponible.

Lorsque vous avez terminé

Activez les identifiants code QR pour les visiteurs.

Rubriques connexes

Options de licence, page 71

Activer les identifiants code QR pour les visiteurs

Pour créer automatiquement un identifiant code QR pour les visiteurs lorsqu'une demande de visite est créée, vous devez activer les identifiants code QR pour les visiteurs.

Avant de commencer

- Activer la gestion des visiteurs pour les sites dans Genetec ClearID[MC]

- Importer un format de carte personnalisé (identifiant code QR) dans Synergis[MC]

IMPORTANT : Vérifiez que le format de carte personnalisé (code QR) est importé et disponible dans le système Security Center auquel votre site est connecté.

À savoir

Seuls les propriétaires de sites et les administrateurs de comptes peuvent activer les identifiants code QR pour les visiteurs.

- Lorsqu'un code QR est créé automatiquement pour un visiteur, le visiteur est créé en état inactif, et l'identifiant du visiteur contient un code QR généré automatiquement. Le code QR dans l'identifiant correspond au code QR envoyé au visiteur dans l'e-mail de confirmation.
- L'identifiant de visiteur est actif, mais le code QR n'est pas exploitable, car le visiteur ne s'est pas encore inscrit. Lorsque le visiteur s'inscrit, le code QR est valable jusqu'à la radiation du visiteur ou de la fin de la journée de la visite.

Par exemple, les identifiants code QR pour les visiteurs peuvent servir à accorder automatiquement le passage d'un tourniquet après l'inscription.

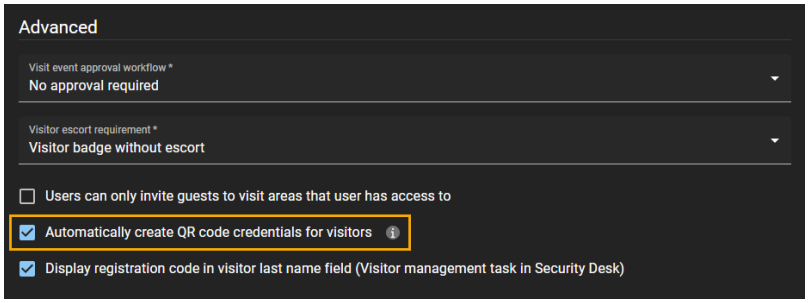
Procédure

1 Cliquez sur **Organisation** > **Sites**.

2 Recherchez et sélectionnez un site.

3 Cliquez sur **Gestion des visiteurs** pour configurer les options de gestion des visiteurs d'un site.

4 Dans la section *Avancée*, sélectionnez **Créer automatiquement un identifiant à code QR pour les visiteurs**.



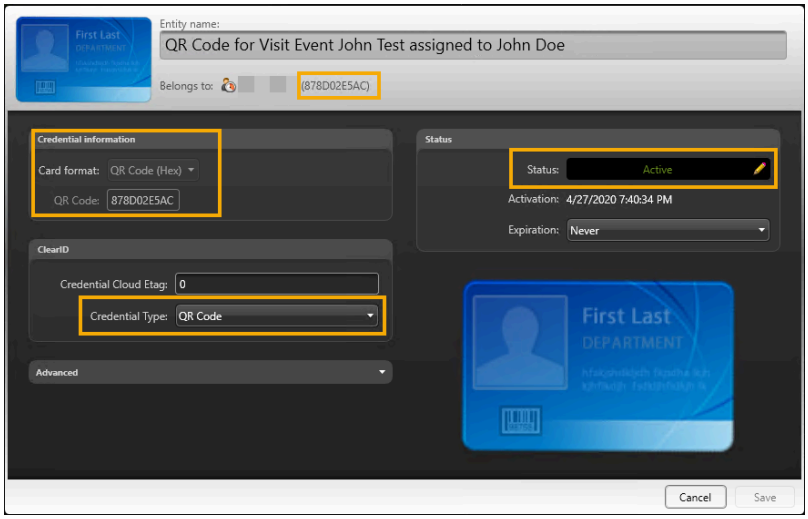
5 Cliquez sur **Enregistrer**.

À présent, lorsqu'un visiteur est invité à se rendre sur le site, ClearID crée automatiquement un identifiant code QR pour le visiteur. Le code QR est inclus dans l'e-mail de confirmation du visiteur.

Lorsque vous avez terminé

Testez l'invitation et l'inscription d'un visiteur pour vérifier que les identifiants code QR sont bien créés automatiquement.

CONSEIL : Vous pouvez rechercher un visiteur dans la tâche *Gestion des visiteurs* dans Security Desk, puis modifier l'identifiant pour vérifier les **Informations sur l'identifiant**, le **Type d'identifiant** et l'**État** du visiteur.



Rubriques connexes

Activer la gestion des visiteurs pour un site, page 257

Configurer les appareils Qscan pour ClearID

Avant d'utiliser les codes QR en tant qu'identifiants dans Genetec ClearID[MC], vous devez configurer vos appareils Qscan pour la prise en charge du format de carte personnalisé (identifiant code QR) utilisé dans ClearID. Un code QR peut ensuite être utilisé en tant qu'identifiant pour accéder aux parkings, tourniquets et autres installations sécurisées.

Avant de commencer

Prenez connaissance de la documentation Qscan :

- Guide de l'utilisateur Qscan (PDF)
- Brochure Qscan (pour les aires de stationnement, PDF)
- Brochure QscanT (pour les tourniquets, PDF)
- Brochure QscanI (version d'intérieur, PDF)

AVERTISSEMENT : Les lecteurs de codes à barres Qscan contiennent un laser de classe 2. Ne regardez pas directement le laser.

À savoir

Cette procédure s'adresse aux intégrateurs système ou aux administrateurs de comptes qui installent et configurent les scanneurs de codes à barres.

Les appareils Qscan suivants sont pris en charge par ClearID pour scanner les codes QR en tant qu'identifiants pour les visiteurs :

- Qscan (pour aires de stationnement)
- QscanT (pour les tourniquets)
- QscanI (version d'intérieur)

Procédure

1 Connectez un lecteur de codes à barres Qscan à un contrôleur Mercury.

2 Configurez le lecteur Qscan pour la prise en charge de codes QR hexadécimaux 40 bits.

Rubriques connexes

Appareils pris en charge, page 78

Connecter un lecteur de codes à barres Qscan à un contrôleur Mercury

Lorsque vous devez utiliser un lecteur de codes à barres Qscan pour accéder à un parking, un tourniquet ou une installation sécurisée, vous devez connecter le lecteur de codes à barres à un contrôleur Mercury. Cela permet au lecteur de codes à barres de communiquer avec Security Center Synergis[MC] pour gérer les accès.

Avant de commencer

AVERTISSEMENT : Les lecteurs de codes à barres Qscan contiennent un laser de classe 2. Ne regardez pas directement le laser.

À savoir

Cette procédure s'adresse aux intégrateurs système ou aux administrateurs de comptes qui installent et configurent les scanneurs de codes à barres.

Dans ce scénario, nous décrivons la connexion d'un lecteur de codes à barres Qscan à un contrôleur Mercury EP 1502.

Procédure

- Connectez le lecteur de codes à barres Qscan au bloc de connexion Reader 1 du contrôleur Mercury EP 1502.

Illustration 11 : Figure 1 : Lecteur de codes à barres Qscan

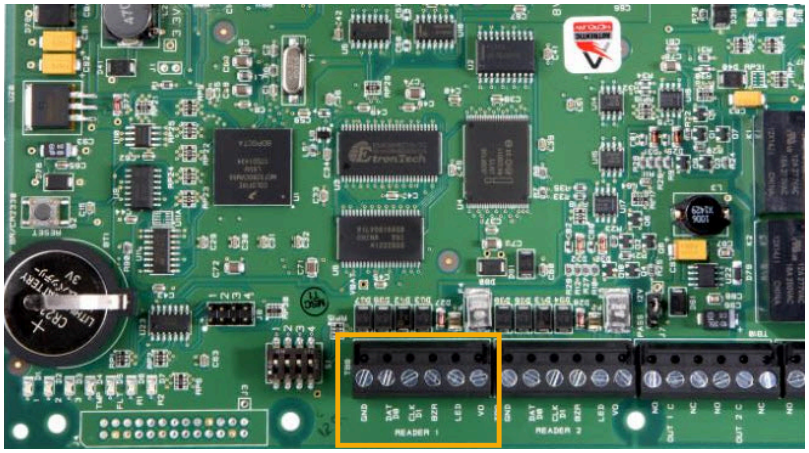
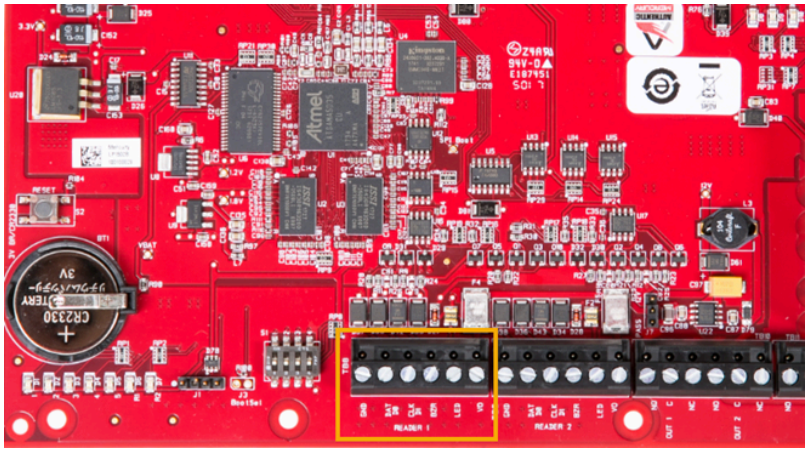


Illustration 12 : Figure 2 : Cartes du contrôleur Mercury EP 1502



REMARQUE : La couleur des cartes du contrôleur Mercury peut varier en fonction du lieu de fabrication et d'achat.

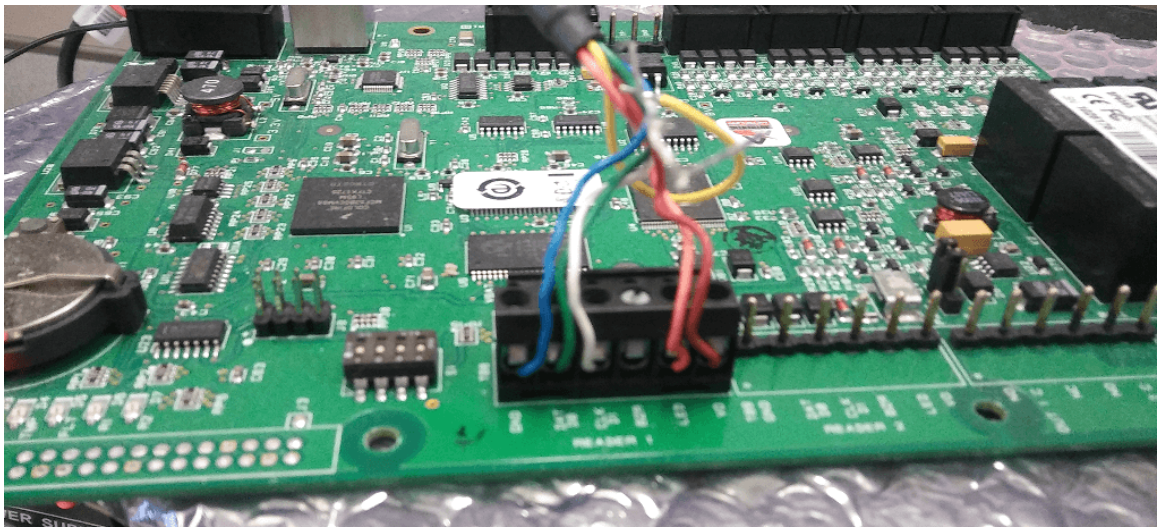


Illustration 13 : Figure 3 : Carte contrôleur Mercury EP1502 avec connexions du faisceau de câbles

Utilisez le tableau suivant pour comprendre le câblage des fils du lecteur de codes à barres Qscan au bornier du bloc de connexion *Reader 1* du contrôleur Mercury.

Câblage du lecteur Qscan et du contrôleur Mercury

Mercury EP1502 : Raccordements Reader 1	Lecteur de codes à barres Qscan : couleur des fils
GND (terre)	BLEU
DAT D0 (Données/Données 0/TR-)	VERT
CLK D1 (Horloge/Données 1/TR+)	BLANC
BZR (avertisseur)	Non applicable
LED (LED du lecteur)	ORANGE
V0 (alimentation du lecteur)	ROUGE

Lorsque vous avez terminé

Configurer le lecteur Qscan pour la prise en charge de codes QR hexadécimaux 40 bits

Configurer un lecteur Qscan pour la prise en charge de codes QR hexadécimaux 40 bits

Avant que les codes QR générés automatiquement par Genetec ClearID^{MC} pour les e-mails de confirmation envoyés aux visiteurs puissent être reconnus et traités par Synergis^{MC} Cloud Link à l'inscription, vous devez configurer votre lecteur de codes à barres Qscan pour la prise en charge des codes QR hexadécimaux sur 40 bits.

Avant de commencer

Connecter un lecteur de codes à barres Qscan à un contrôleur Mercury

AVERTISSEMENT : Les lecteurs de codes à barres Qscan contiennent un laser de classe 2. Ne regardez pas directement le laser.

À savoir

Cette procédure s'adresse aux intégrateurs système ou aux administrateurs de comptes qui installent et configurent les scanneurs de codes à barres.

Dans ce scénario, nous décrivons la manière de programmer les appareils Qscan pour la prise en charge des codes QR hexadécimaux sur 40 bits utilisés dans ClearID et envoyés vers Synergis Cloud Link.

Par exemple, un code QR scanné par Qscan est généralement lu en tant que valeur alphanumérique ABC1234567.

Synergis Cloud Link exige les codes QR au format HEX 0xAB 0xC1 0x23 0x45 0x67 pour gérer les demandes d'accès.

ATTENTION : Les étapes du processus ci-dessous suppriment la prise en charge des codes QR alphanumériques du lecteur de codes à barres Qscan. Le lecteur de codes à barres Qscan ne peut pas être utilisé en mode alphanumérique lorsque le mode hexadécimal 40 bits est actif.

Procédure

1 Pour rétablir les valeurs d'usine, scannez le code à barres qscan resetbarcode1.pdf.

REMARQUE : Le lecteur Qscan émet deux bips si la réinitialisation est réussie.

2 Pour ignorer les caractères alphanumériques, scannez le code à barres dans qscan no alpha delete.pdf.

%UX0130000

3 Pour activer la conversion HEX, scannez le code à barres dans qscan hex conversion.pdf.

4 Pour obtenir une sortie sur 40 bits, scannez les codes à barres dans qscan 40-bit.pdf.
REMARQUE : Ce fichier contient trois codes à barres à scanner l'un après l'autre.

Configurer les appareils STid pour ClearID

Avant d'utiliser les codes QR en tant qu'identifiants dans Genetec ClearID[MC], vous devez configurer vos appareils STid pour la prise en charge du format de carte personnalisé utilisé pour les codes QR dans ClearID. Un code QR peut ensuite être utilisé en tant qu'identifiant pour accéder aux parkings, tourniquets et autres installations sécurisées.

Avant de commencer

Prenez connaissance de la documentation STid :

- Lecteurs de codes QR Architect® Blue.
  - ARCS-AQ/BT - 13.56 MHz + Bluetooth® + lecteur de code QR multi-technologies
- SECard - High security programming kit
- Guide de l'utilisateur SECard

À savoir

Cette procédure s'adresse aux intégrateurs système ou aux administrateurs de comptes qui installent et configurent les lecteurs de codes QR.

Dans ce scénario, nous décrivons la manière de programmer les appareils STid pour la prise en charge des codes QR hexadécimaux sur 40 bits utilisés dans ClearID et envoyés vers Synergis[MC] Cloud Link.

Procédure

1 En savoir plus sur les codes QR STid.

2 Importez un format de carte personnalisé.

3 Configurez votre lecteur de codes QR et connectez-le à votre tableau de contrôle d'accès.

REMARQUE : La marche à suivre varie selon les tableaux de contrôle d'accès.

- Pour connecter votre lecteur OSDP à Synergis Cloud Link, voir Lecteurs OSDP connectés aux ports RS-485 de Synergis Cloud Link.
- Pour connecter votre lecteur OSDP à Mercury, voir Ajouter des lecteurs OSDP (Secure Channel) à un contrôleur Mercury.

4 Créer une configuration de lecteur de codes QR STid , page 413.

5 Transférer votre configuration de lecteur vers votre lecteur de codes QR STid , page 428.

Lorsque vous avez terminé

Ajoutez des portes aux secteurs.

À propos des lecteurs de codes QR STid

Dans Genetec ClearID[MC], les lecteurs de codes QR STid permettent de lire les identifiants de type code QR.

REMARQUE : L'image montre des lecteurs STid dont vous disposez peut-être dans votre organisation. Pour la liste des lecteurs OSDP (Open Supervised Device Protocol) pris en charge par ClearID, voir Appareils pris en charge.

Pourquoi choisir le protocole OSDP plutôt que le protocole Wiegand ?

Protocole WIEGAND

Avec Wiegand, le lecteur envoie toujours un format Wiegand de longueur fixe, quelle que soit la longueur de l'identifiant. Le *format de carte personnalisé* appelé par Security Desk est toujours le même. Le fabricant a confirmé cette limitation des lecteurs Wiegand (SY-ARCS-R31-AQBT1-XX1).

Conséquence : L'identifiant n'a pas la longueur exigée par le protocole, et un message Identifiant inconnu est affiché dans Security Desk, même si cet identifiant code QR est déjà enregistré dans la base de données Security Center Synergis[MC].

Contournement : Pour s'assurer que tous les types d'identifiants fonctionnent simultanément avec les lecteurs Wiegand et Synergis, tous les autres identifiants (RFiD ou codes QR d'autres sources comme Axis) doivent adopter la longueur de l'identifiant code QR ClearID (40 bits). Cette approche permet de garantir que Synergis reçoit toujours le même *format de carte personnalisé* (celui provenant de ClearID) et qu'il interprète correctement tous les types de données utiles transmises par le lecteur.

Protocole OSDP

Avec le protocole Open Supervised Device Protocol (OSDP), le lecteur adapte dynamiquement la longueur du format en fonction de la longueur de l'identifiant.

BONNE PRATIQUE : Utilisez OSDP avec les lecteurs de codes QR STid pour être sûr que les identifiants code QR soient compris et acceptés.

Le tableau suivant contient des exemples de lectures par un même lecteur.

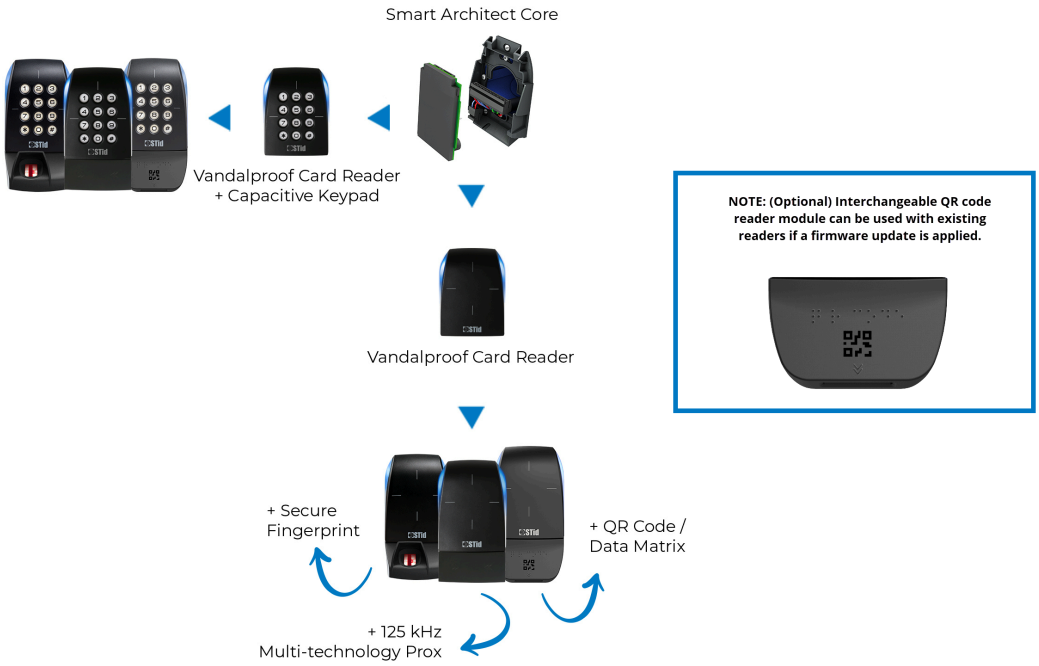
Code de l'identifiant	Format de carte	
4AE6CD6464E	Code QR (HEX)	Code QR ClearID
E01EC72022429729	64 bits	Identifiants DESFire privés 64 bits

Les exemples montrent que le *format de carte personnalisé* appelé par Security Desk est différent pour chaque lecture.

Conséquence : Le lecteur OSDP est plus souple et interprète correctement l'identifiant.

Planifier votre déploiement de lecteurs de codes QR

En fonction de vos besoins, vous pouvez utiliser les derniers lecteurs de codes QR STid Architect® Blue. Vous pouvez également ajouter des modules de code QR interchangeables si vous souhaitez réutiliser des lecteurs STid existants.



Tenez compte des considérations suivantes lorsque vous planifiez votre mise en œuvre de lecteurs de codes QR :

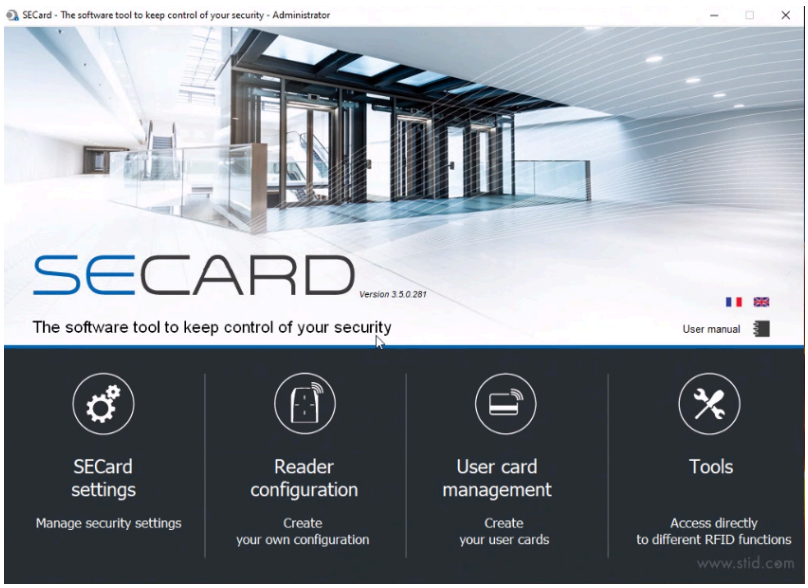
- **BONNE PRATIQUE :** Si vous prévoyez une nouvelle mise en œuvre de lecteurs de codes QR STid, songez à utiliser les derniers lecteurs de codes QR dotés du dernier micrologiciel. Par exemple, le modèle : ARCS-AQ/BT. N'utilisez que des lecteurs STid qui prennent en charge le protocole OSDP et qui ont été mis à niveau avec la **version 10 du micrologiciel**.
- Si vous avez déjà déployé de nombreux lecteurs STid au sein de votre organisation, songez à ajouter le module de lecture de code QR interchangeable, et à mettre à niveau votre micrologiciel.

  CONSEIL : L'utilisation du module interchangeable peut se traduire par des économies importantes dans le cadre d'un projet d'envergure.
- Si vous réutilisez des lecteurs existants, reportez-vous à la *documentation STid* pour savoir comment les mettre à niveau avec la **version 10 du micrologiciel**.

Programmer vos lecteurs de codes QR STid

Les lecteurs de codes QR STid peuvent être programmés à l'aide de la solution logicielle *STid SECard - High security programming kit*.

BONNE PRATIQUE : Utilisez **le logiciel SECard version 3.5** ou ultérieur de STid pour configurer vos lecteurs de codes QR STid.



Le KIT-SECARD-BT-V3.X inclut les éléments suivants :

- Lecteur, enregistreur, codeur de bureau STid Architect® ARC-G

- Clé USB contenant le logiciel SECard de STid

IMPORTANT : Genetec Inc. n'assure pas une assistance sur la solution SECard de STid. Les clients doivent utiliser la version autonome du logiciel SECard de STid pour configurer le fonctionnement des lecteurs OSDP avec le tableau du SCA ClearID.

Rubriques connexes

Appareils pris en charge, page 78

Créer une configuration de lecteur de codes QR STid

Avant d'utiliser les codes QR en tant qu'identifiants dans Genetec ClearID[MC], vous devez créer votre configuration de lecteur de codes QR STid. Vous ne pouvez utiliser les codes QR en tant qu'identifiants pour un lecteur de codes QR STid qu'après le transfert de la configuration du lecteur vers une carte mémoire STid OCB, puis vers le lecteur de codes QR STid.

Avant de commencer

Prenez connaissance de la documentation STid :

- SECard - High security programming kit

- Guide de l’utilisateur SECard
- Installez le logiciel STid SECard - High security programming kit.

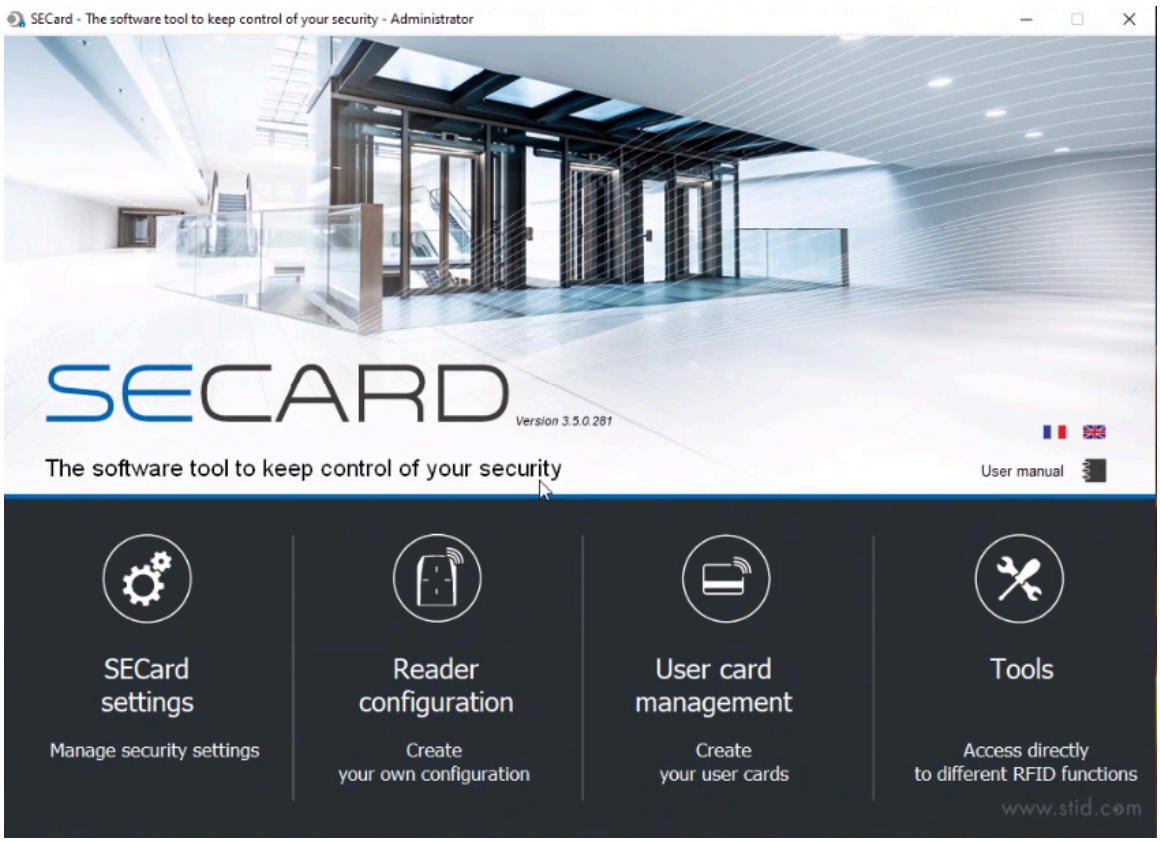
À savoir

Cette procédure s'adresse aux intégrateurs système ou aux administrateurs de comptes qui installent et configurent les lecteurs de codes QR.

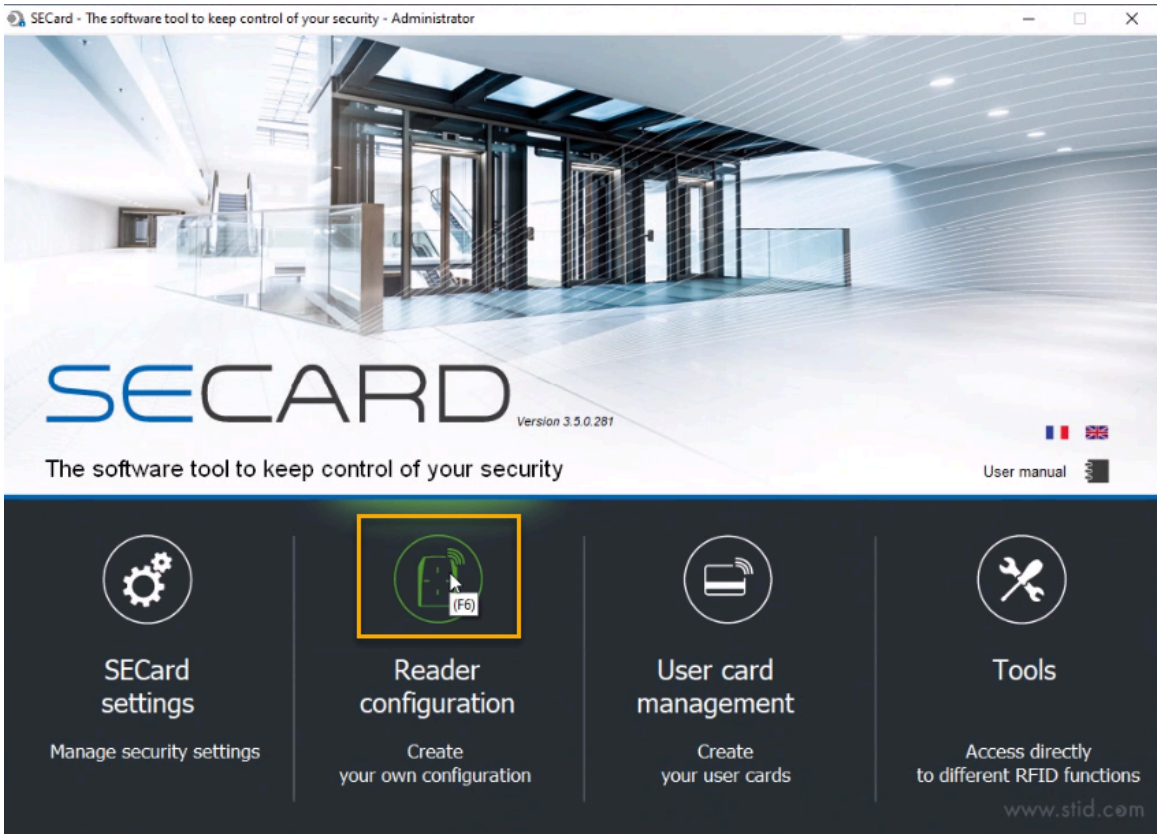
REMARQUE : Le logiciel STid SECard nécessite une licence, dont le numéro est généralement disponible sur le lecteur USB utilisé pour coder une carte à puce.

Procédure

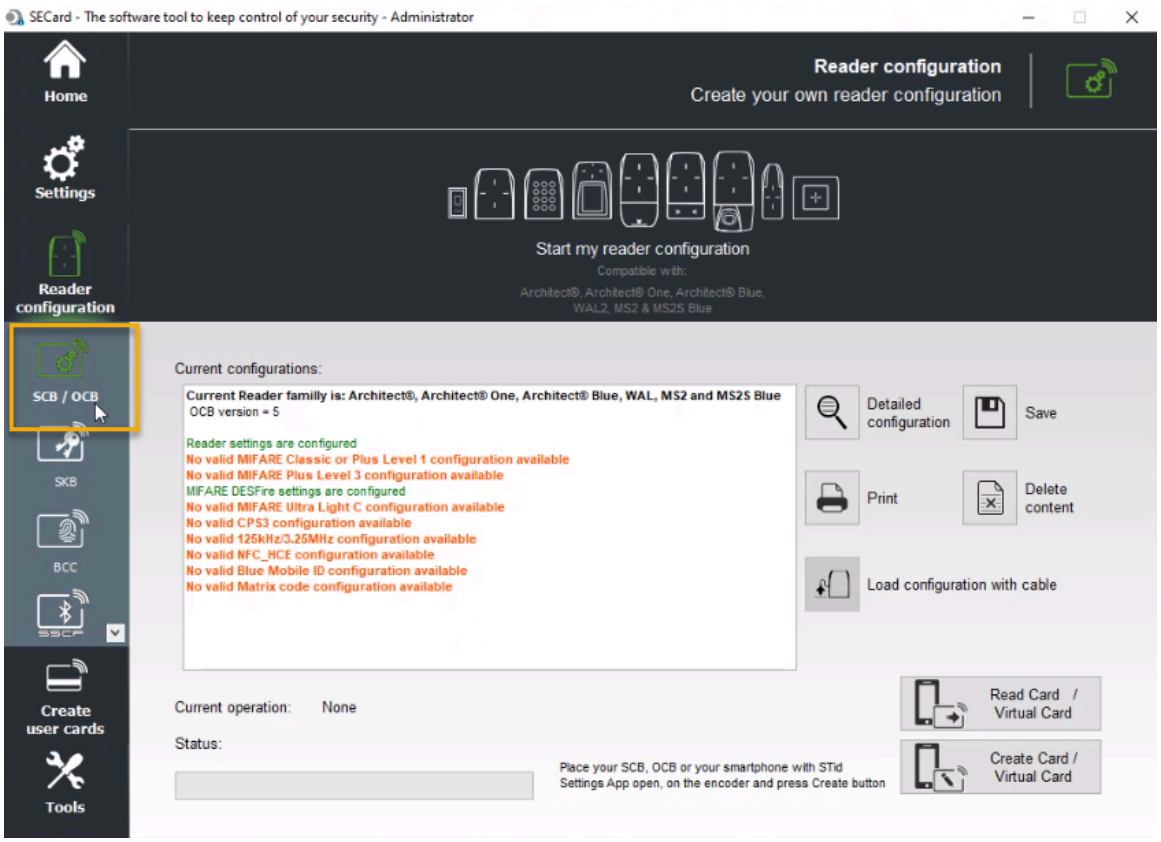
1 Lancez le logiciel STid SECard - High security programming kit pour configurer votre lecteur de codes QR STid.



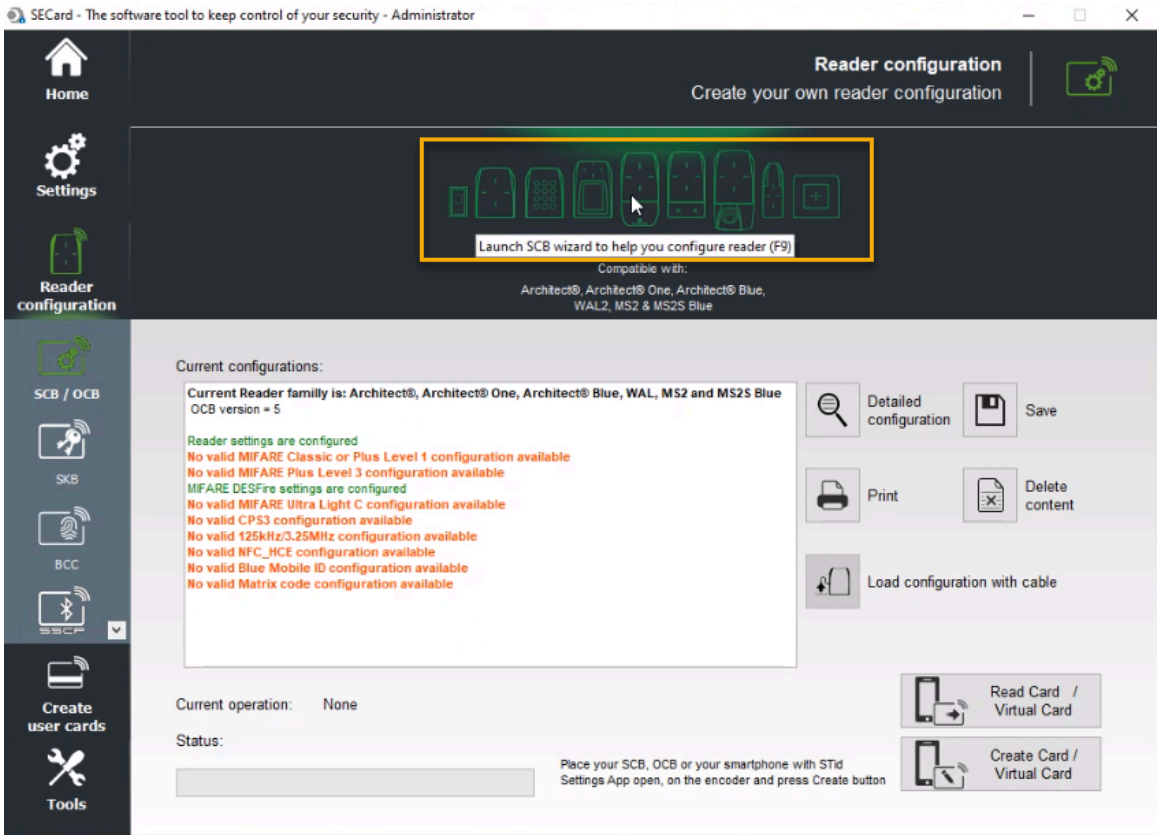
2 Cliquez sur **Reader configuration**.



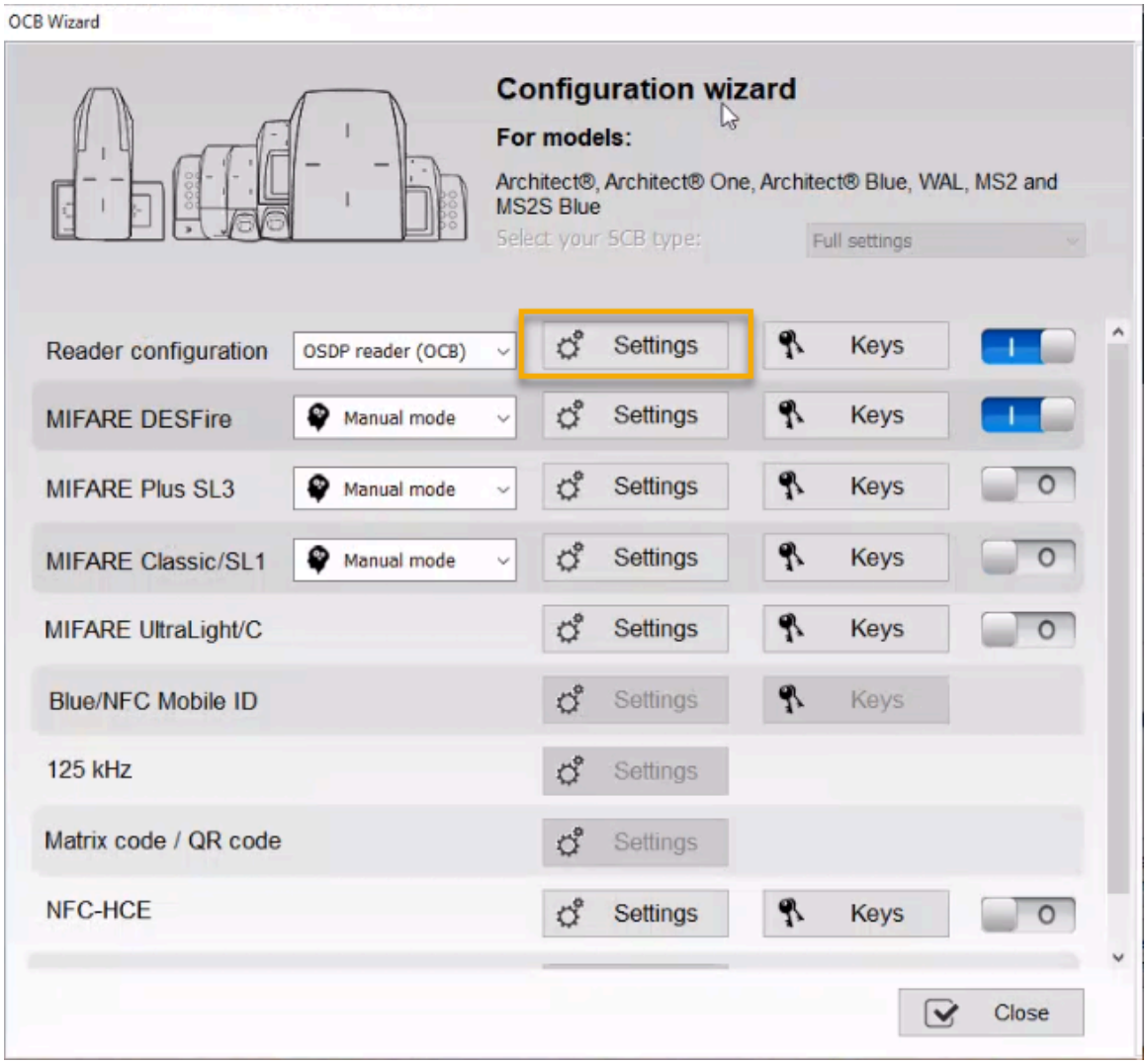
a) Dans le volet de navigation, cliquez sur **SCB / OCB**.



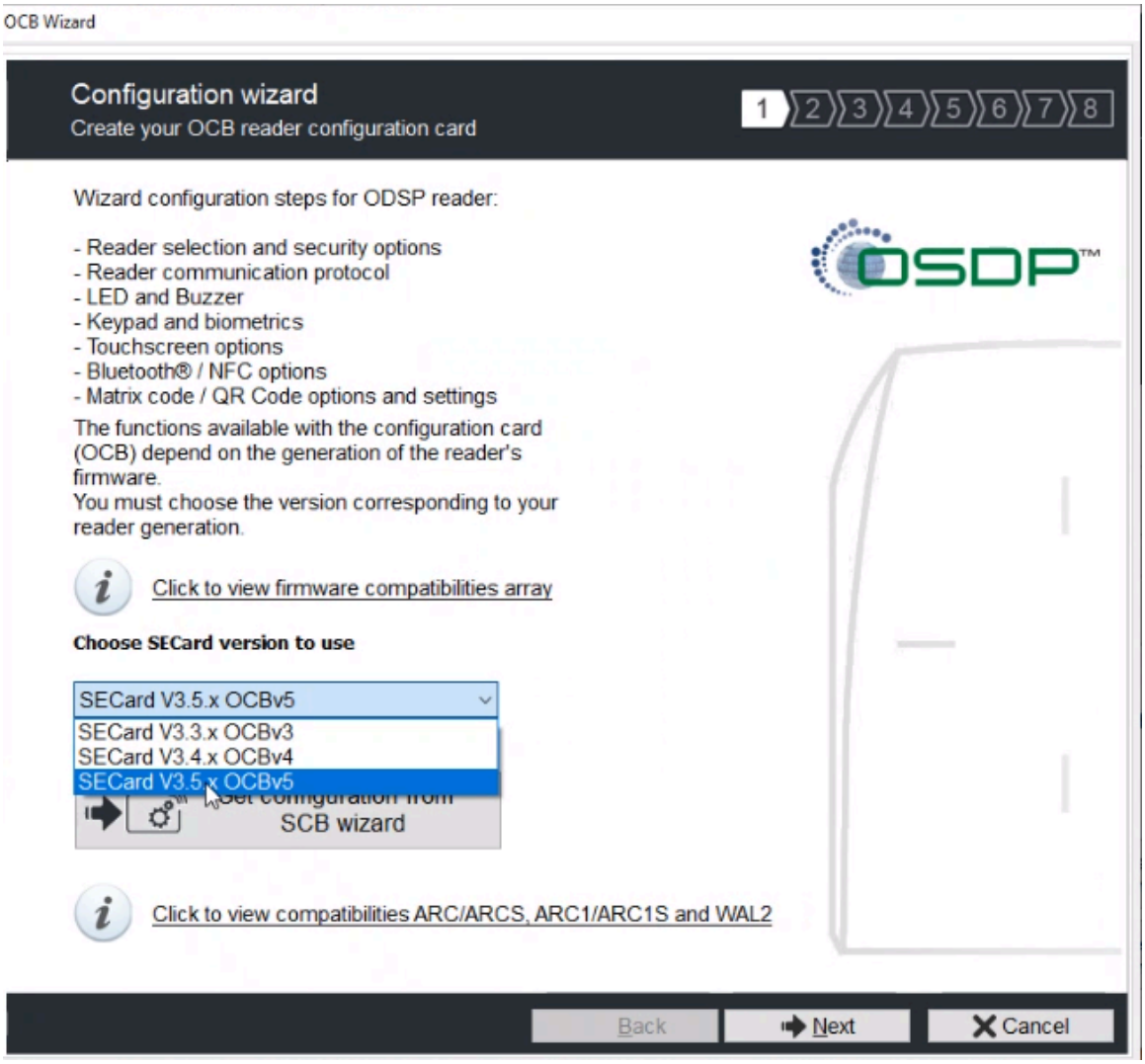
b) Cliquez sur l'image des lecteurs en haut de l'écran pour lancer l'assistant SCB.



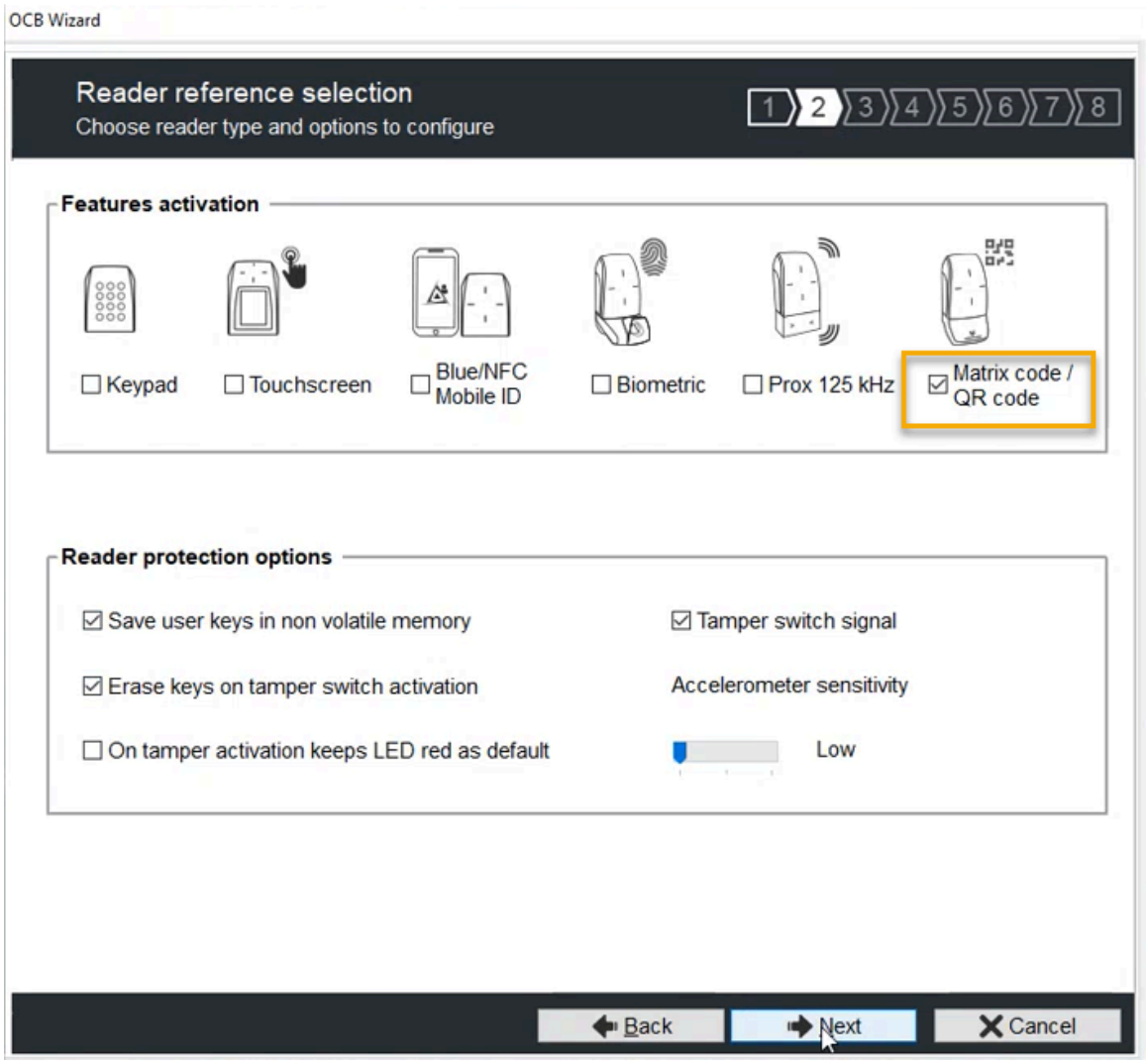
c) Dans la ligne *Reader configuration* en regard de OSDP reader (OCB), cliquez sur **Settings** pour ouvrir l'assistant de configuration.



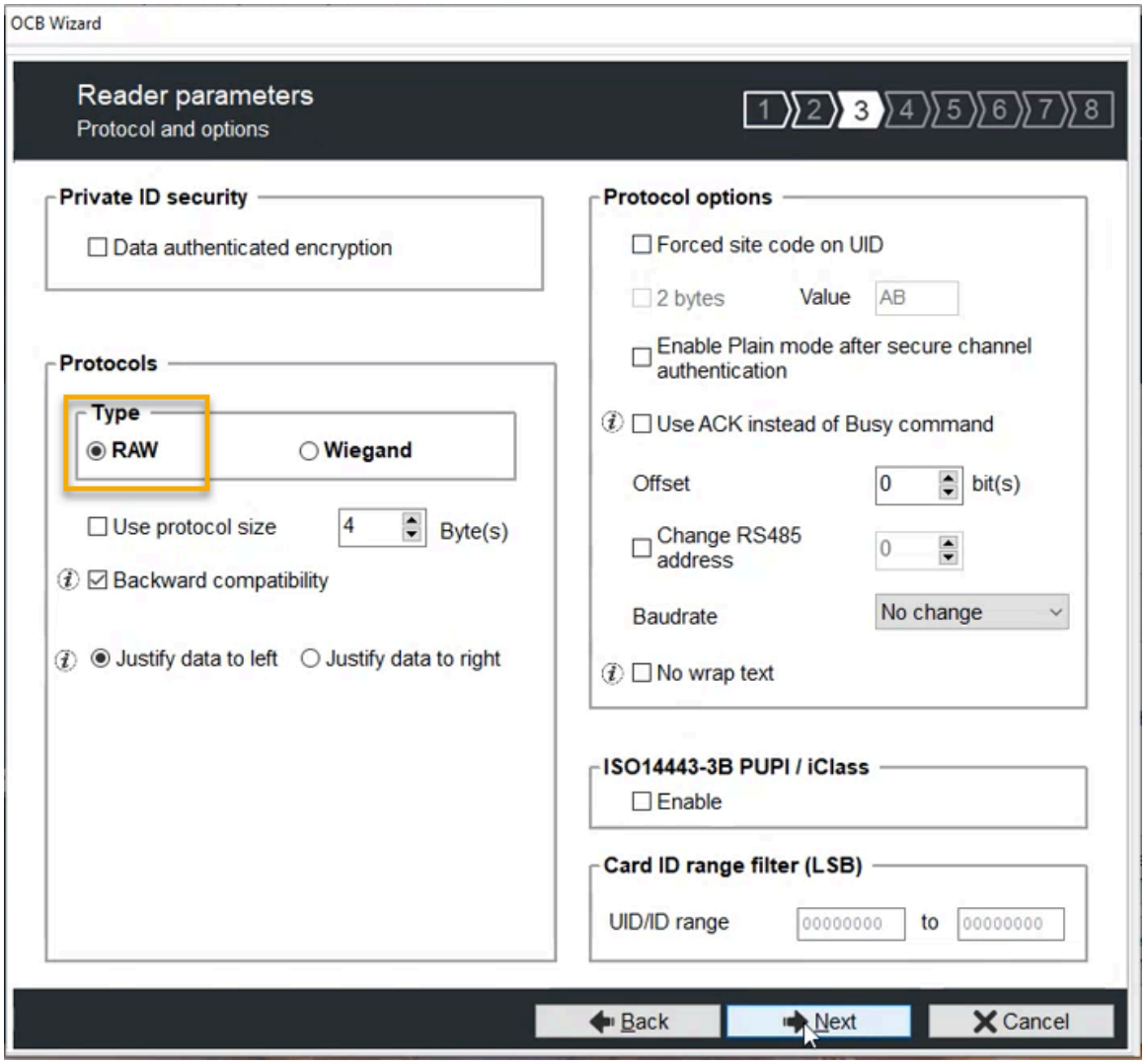
3 Dans la boîte de dialogue *Configuration wizard*, sélectionnez **SECard V3.5 x OCBv5** et cliquez sur **Next**.



a) Dans la boîte de dialogue *Reader reference selection*, cochez la case **Matrix / QR Code** et cliquez sur **Next**.



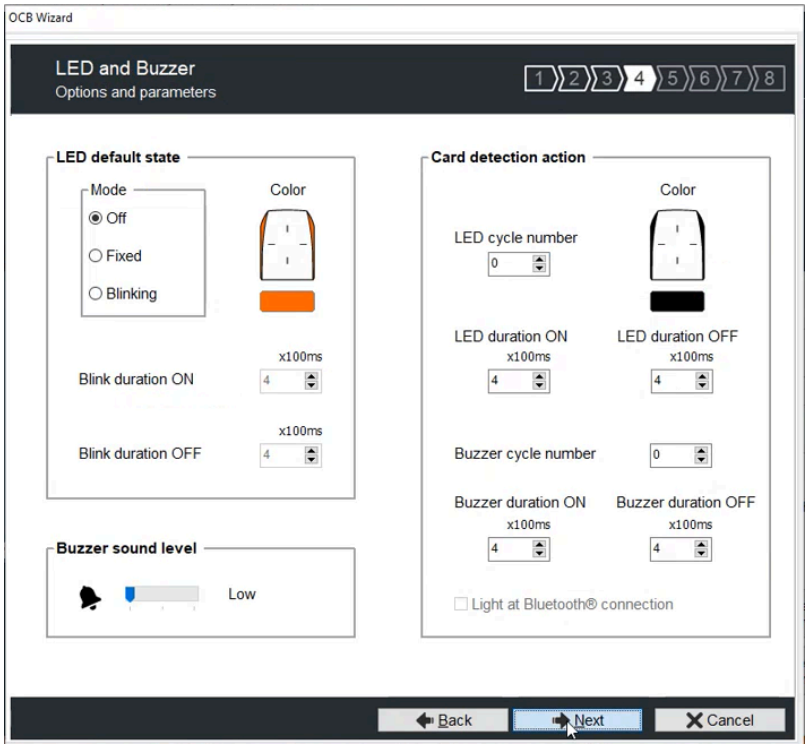
b) Dans la section *Protocols* de la boîte de dialogue *Reader parameters*, sélectionnez le type **RAW** et cliquez sur **Next**.



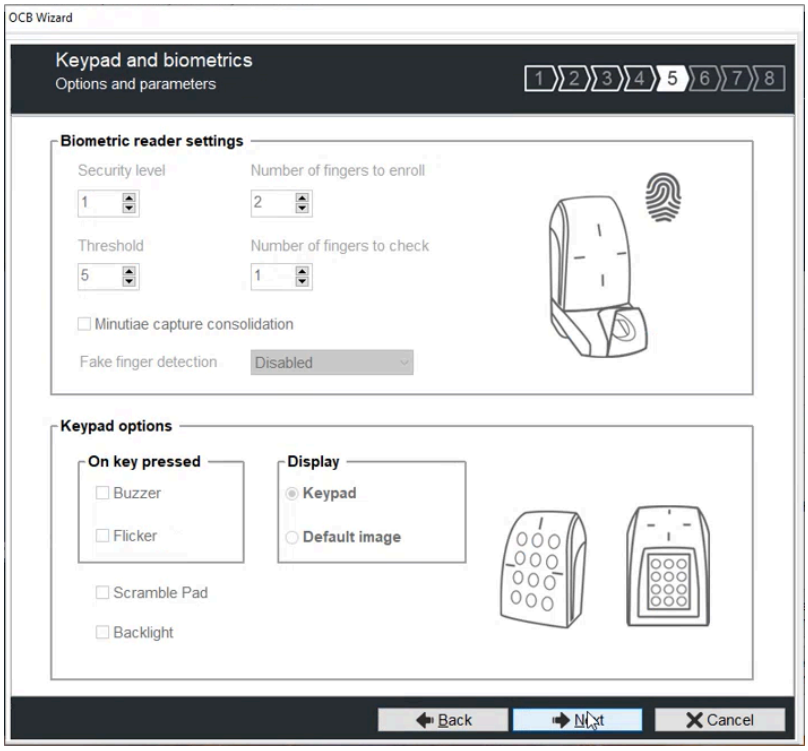
REMARQUE : Le réglage **Byte(s)** n'est pas utilisé lorsque la case **Use protocol size** n'est pas cochée. Cela permet au lecteur d'adapter la longueur à celle de l'identifiant.

4 Les étapes suivantes (4.a, page 422 à 4.d, page 423) ne sont pas obligatoires pour l'utilisation des codes QR, mais peuvent s'avérer utiles pour votre installation.

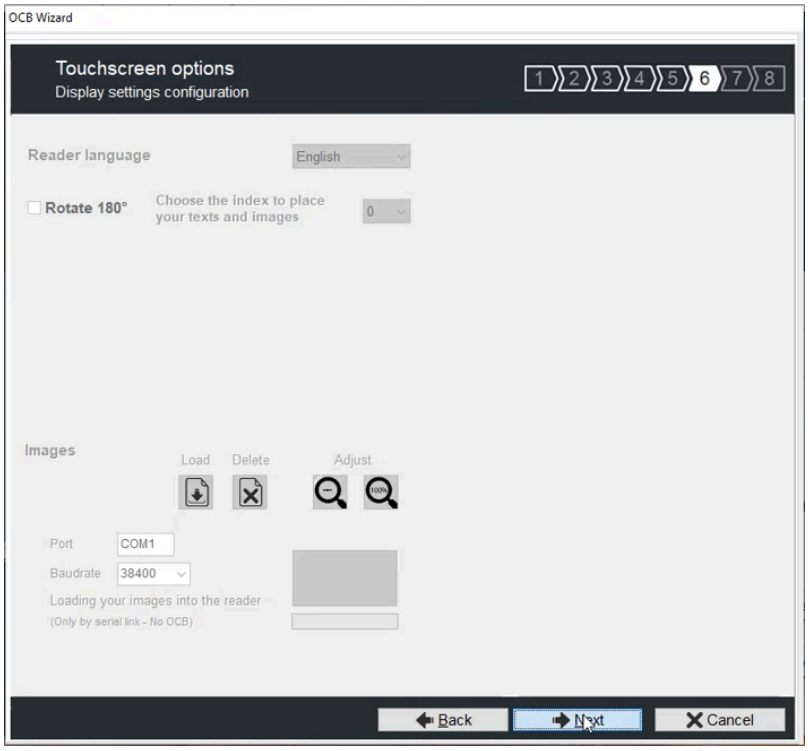
a) Cliquez sur **Next** pour ignorer la boîte de dialogue *LED and Buzzer*.



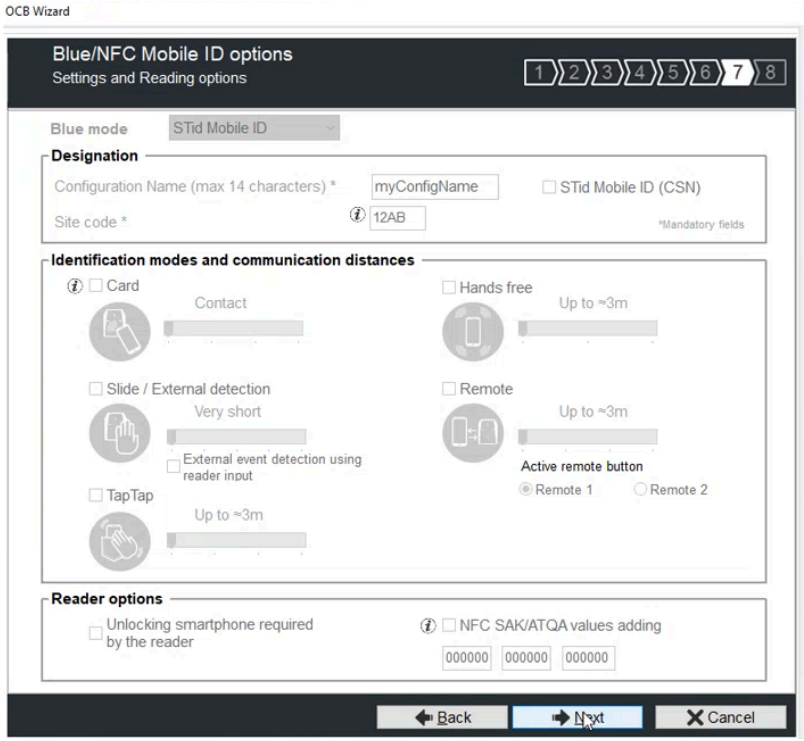
b) Cliquez sur **Next** pour ignorer la boîte de dialogue *Keypad and biometrics*.



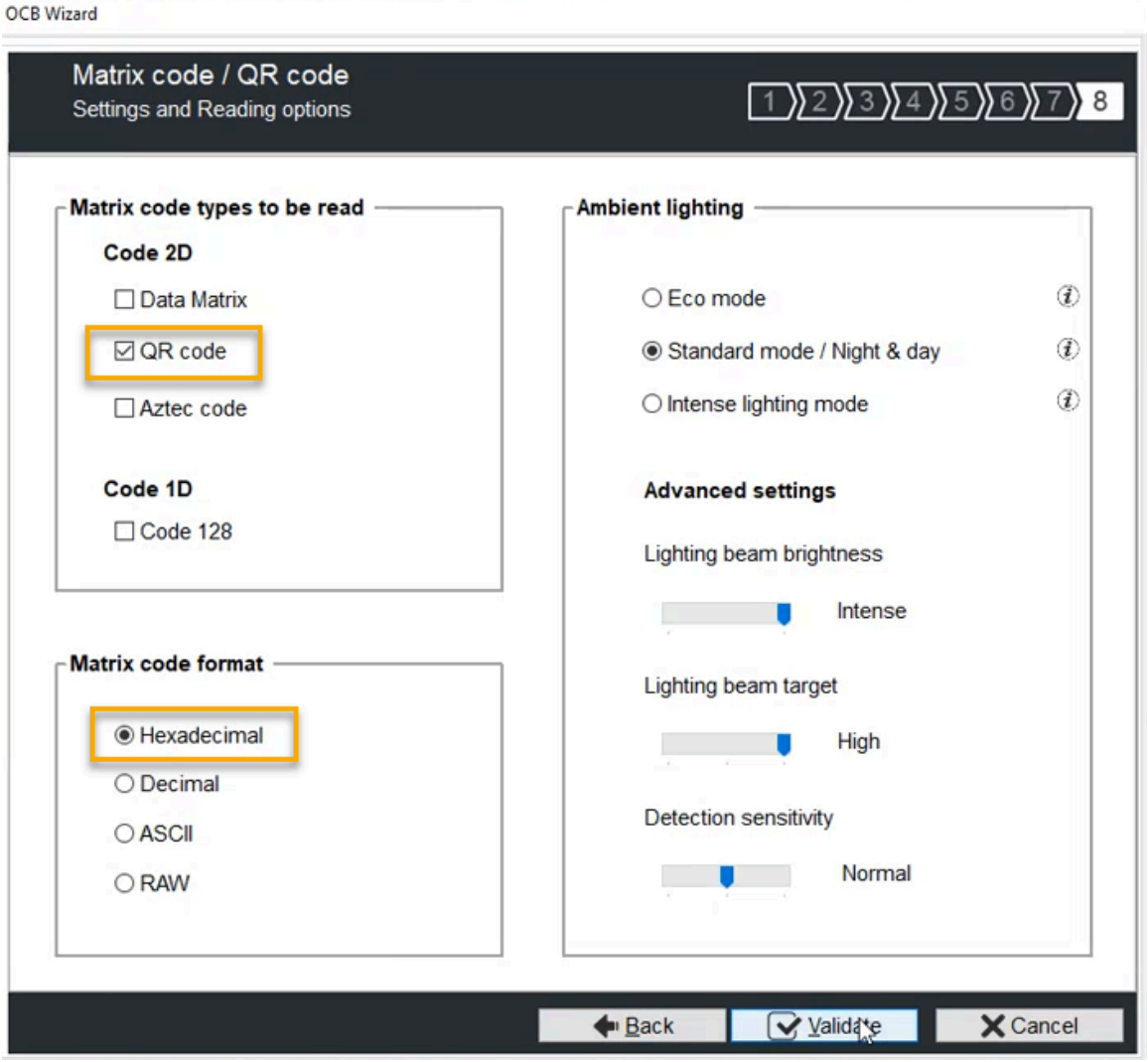
c) Cliquez sur **Next** pour ignorer la boîte de dialogue *Touchscreen options*.



d) Cliquez sur **Next** pour ignorer la boîte de dialogue *Blue/NFC Mobile ID options*.

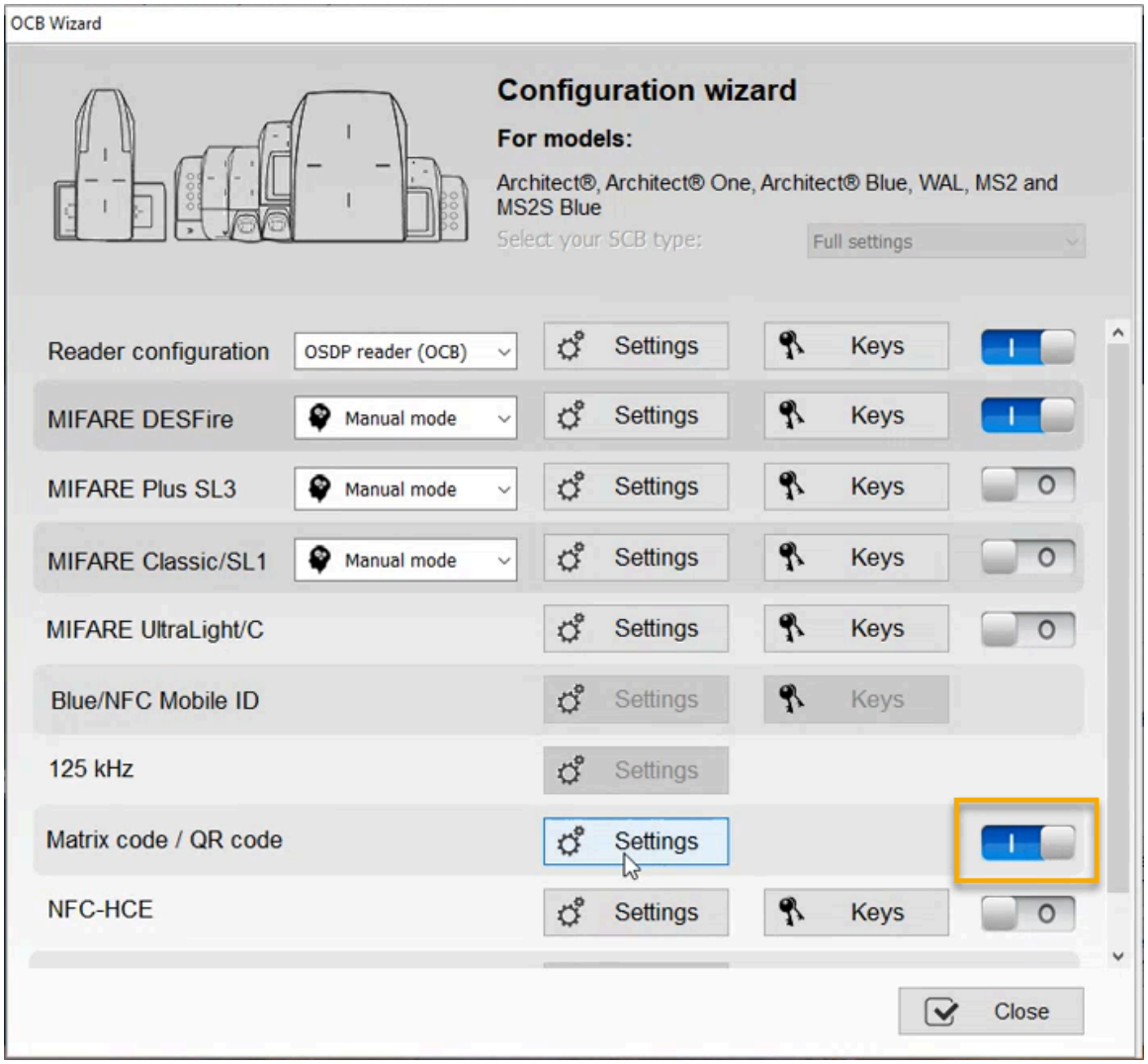


5 Dans la section *Matrix code types to be read* de la boîte de dialogue *Matrix code / QR code*, cochez uniquement la case **QR code**. Puis dans la section *Matrix code format*, cochez la case **Hexadecimal**.
Ces réglages indiquent qu'un code QR 2D peut être lu et envoyé au format hexadécimal.



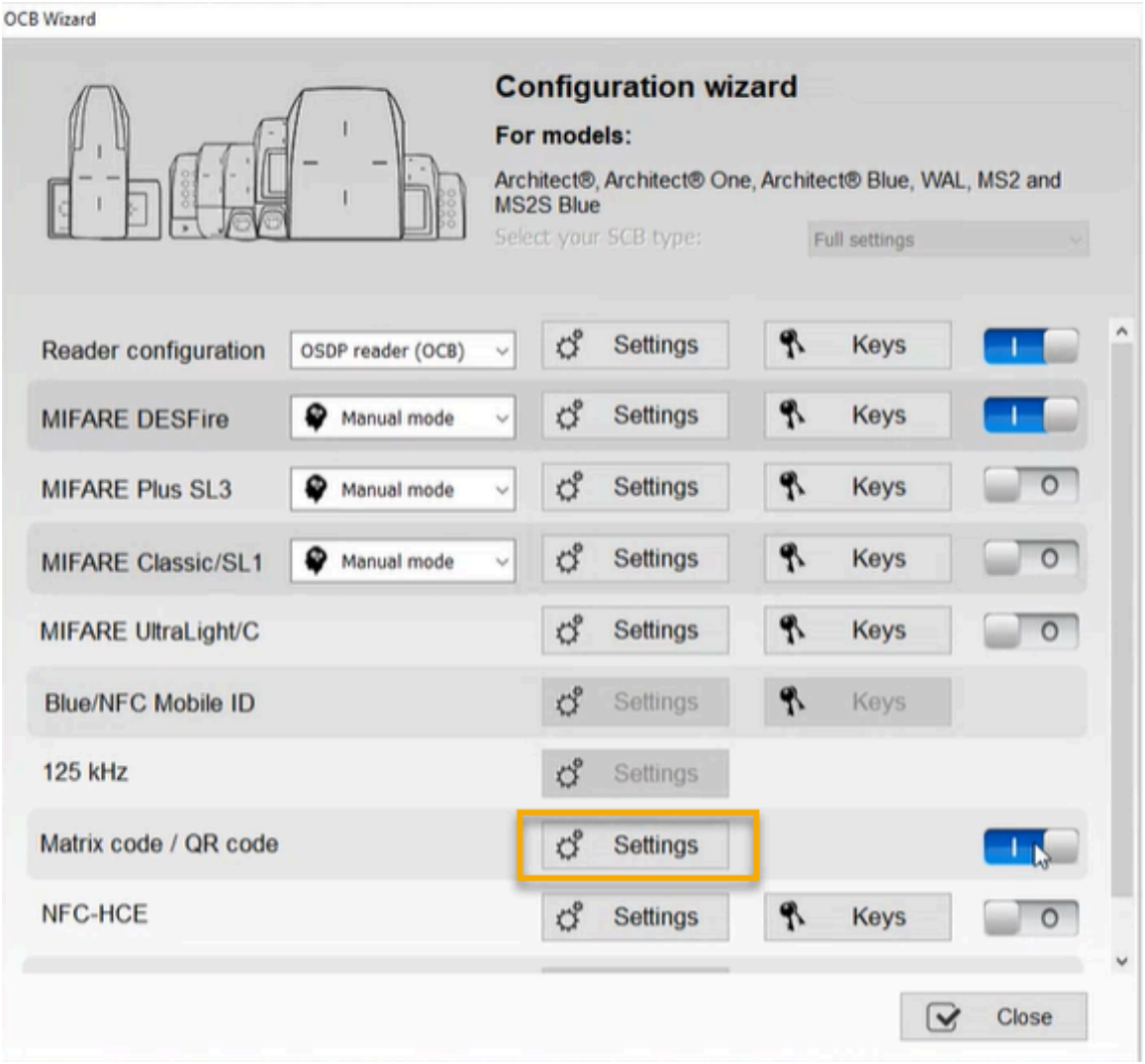
a) (Facultatif) Dans la section *Ambient lighting*, modifiez les réglages si nécessaire.
b) Cliquez sur **Valider**.

6 Dans la ligne *Matrix code / QR code*, réglez le curseur en position activé.

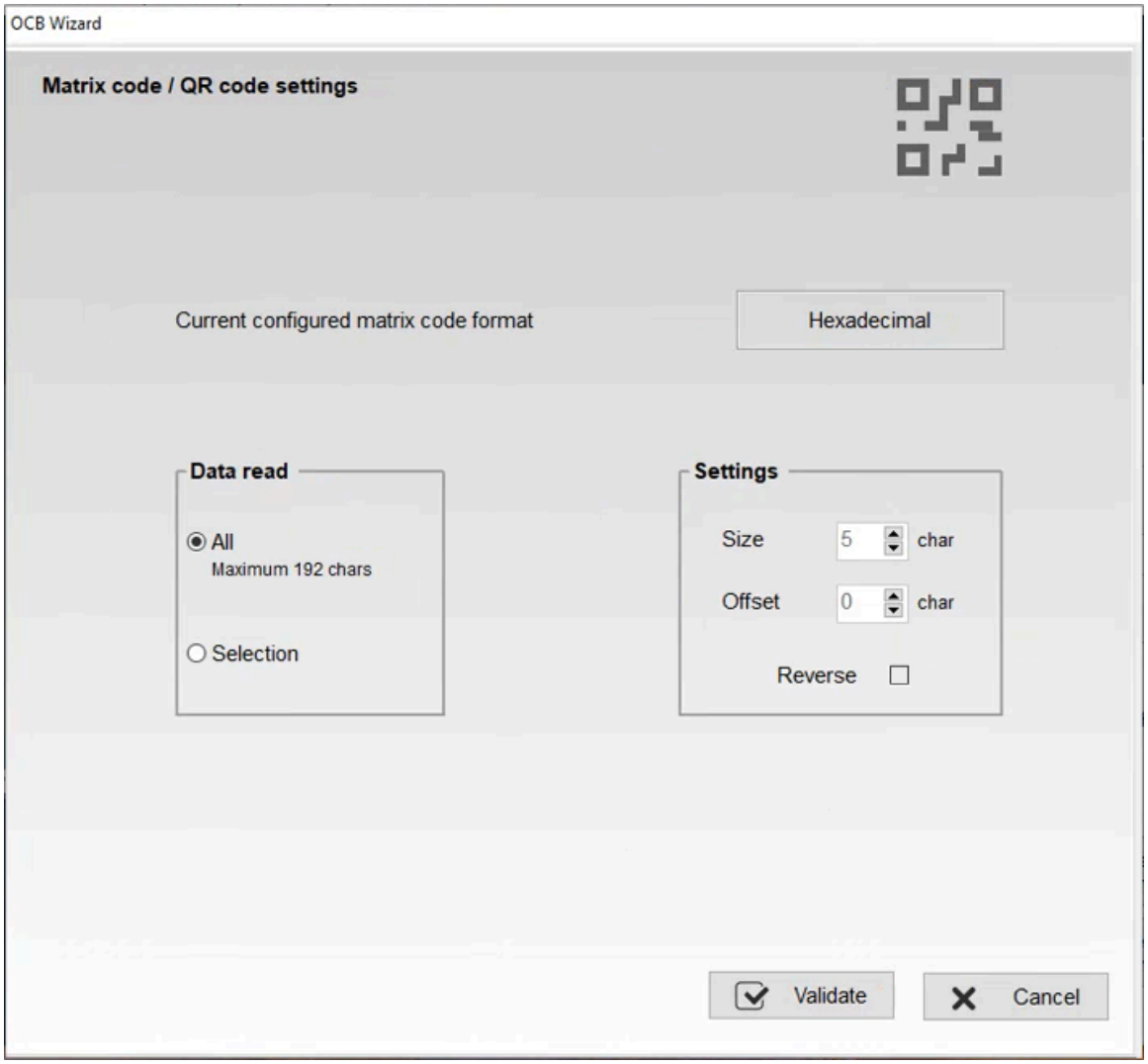


CONSEIL : Si la section *Matrix code / QR code* n'est pas disponible dans l'assistant de configuration, vérifiez que vous avez validé votre configuration de lecteur, comme indiqué plus haut.

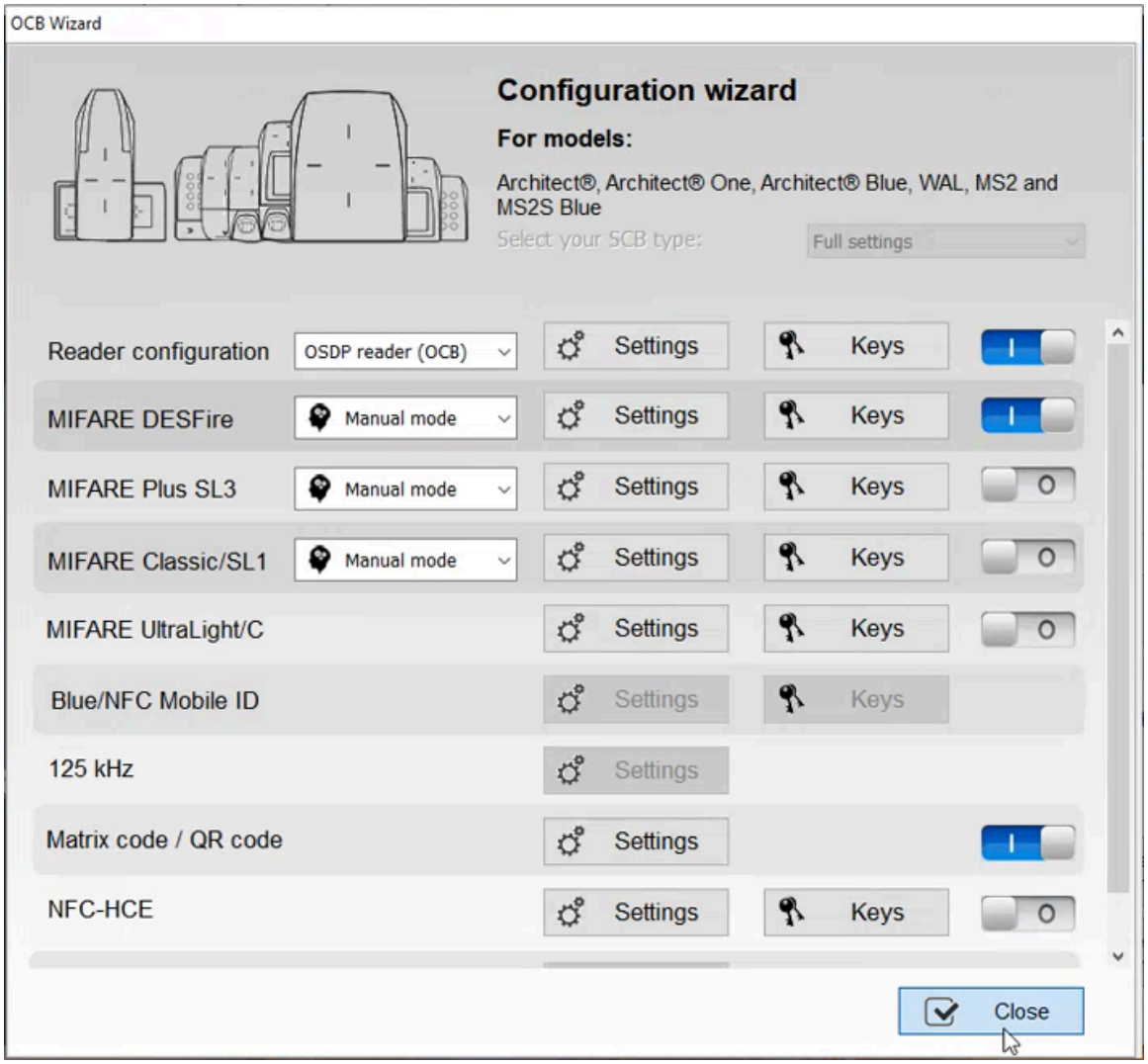
7 Dans la ligne *Matrix code / QR code*, cliquez sur **Settings**.



a) Dans la boîte de dialogue *Matrix code / QR code settings*, utilisez les réglages par défaut et cliquez sur **Validate**.



b) Cliquez sur **Fermer**.



La configuration de votre lecteur de code QR STid a été créée.

Lorsque vous avez terminé

Transférez la configuration vers votre lecteur de codes QR STid.

Transférer votre configuration de lecteur vers votre lecteur de codes QR STid

Avant d'utiliser les codes QR en tant qu'identifiants dans Genetec ClearID^{MC}, vous devez terminer de configurer votre lecteur de codes QR STid en configurant une carte à puce STid OCB pour transférer la configuration de lecteur vers le lecteur de codes QR STid.

Avant de commencer

Prenez connaissance de la documentation STid SECard :

- SECard - High security programming kit
- Guide de l'utilisateur SECard
- Installer le logiciel STid SECard - High security programming kit
- Créer votre configuration de lecteur de codes QR STid

À savoir

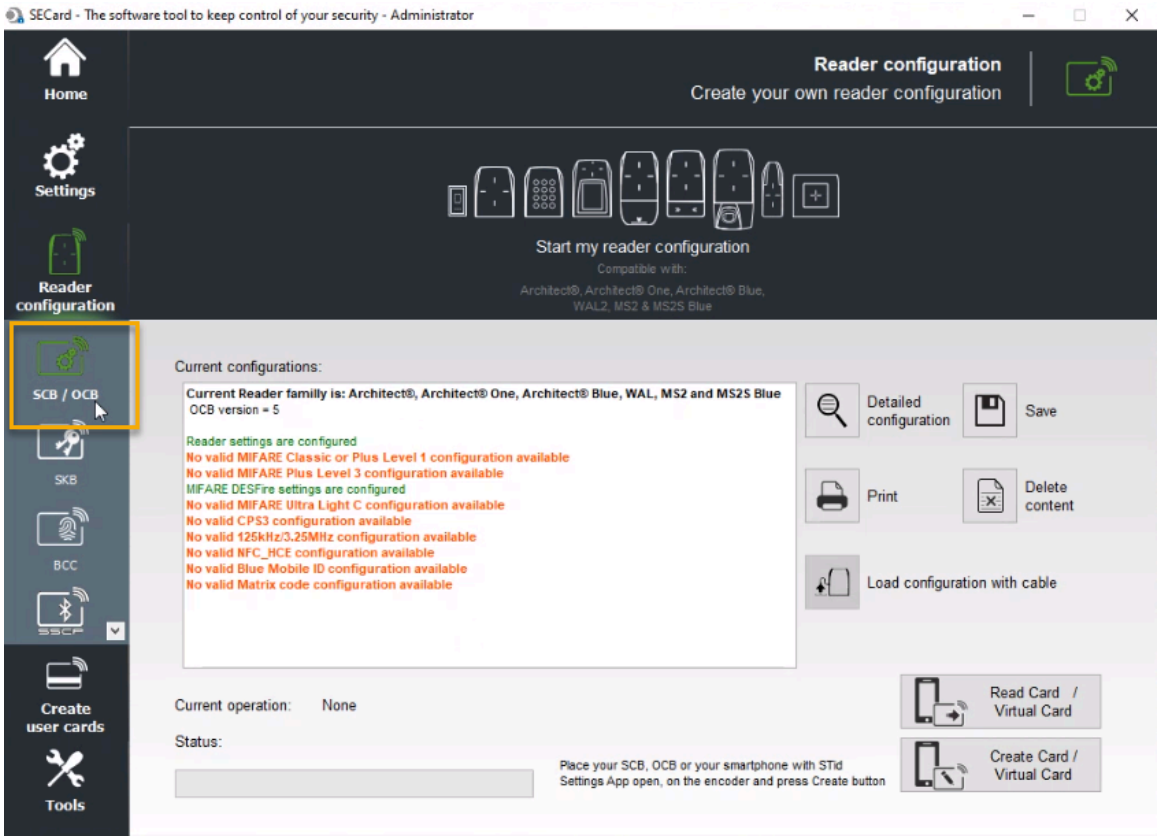
Cette procédure s'adresse aux intégrateurs système ou aux administrateurs de comptes qui installent et configurent les lecteurs de codes QR.

REMARQUE : Vérifiez que vous avez un codeur USB installé et prêt à configurer votre carte OCB. Par exemple, le lecteur, enregistreur, codeur de bureau STid Architect® ARC-G.

Procédure

1 Lancez le logiciel STid SECard pour configurer votre carte.

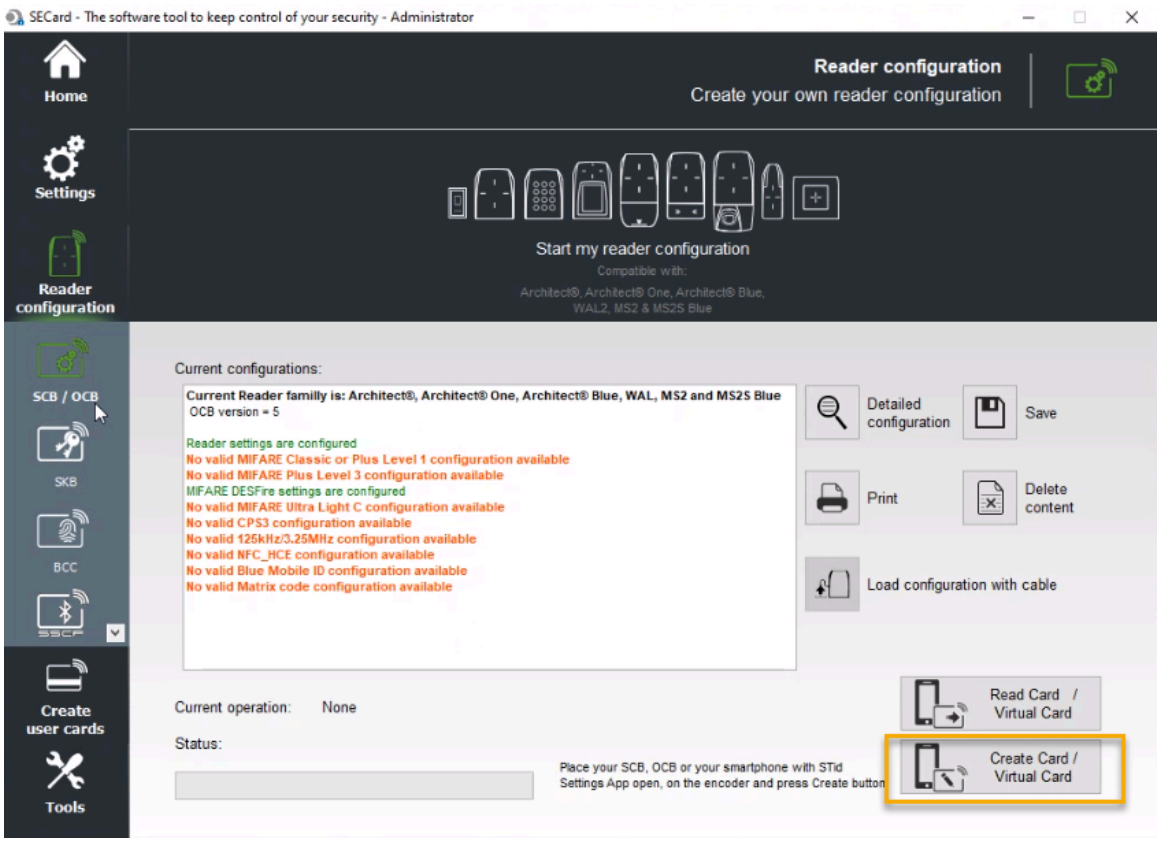
2 Dans le volet de navigation, cliquez sur **SCB / OCB**.



3 Créez votre carte STid OCB.

a) Placez la carte OCB sur le codeur (lecteur) USB.

b) Cliquez sur **Create Card / Virtual Card** pour créer votre carte de configuration.



4 Munissez-vous de la carte à puce OCB qui contient la configuration de lecteur, et passez-la sur votre nouveau lecteur de codes QR.

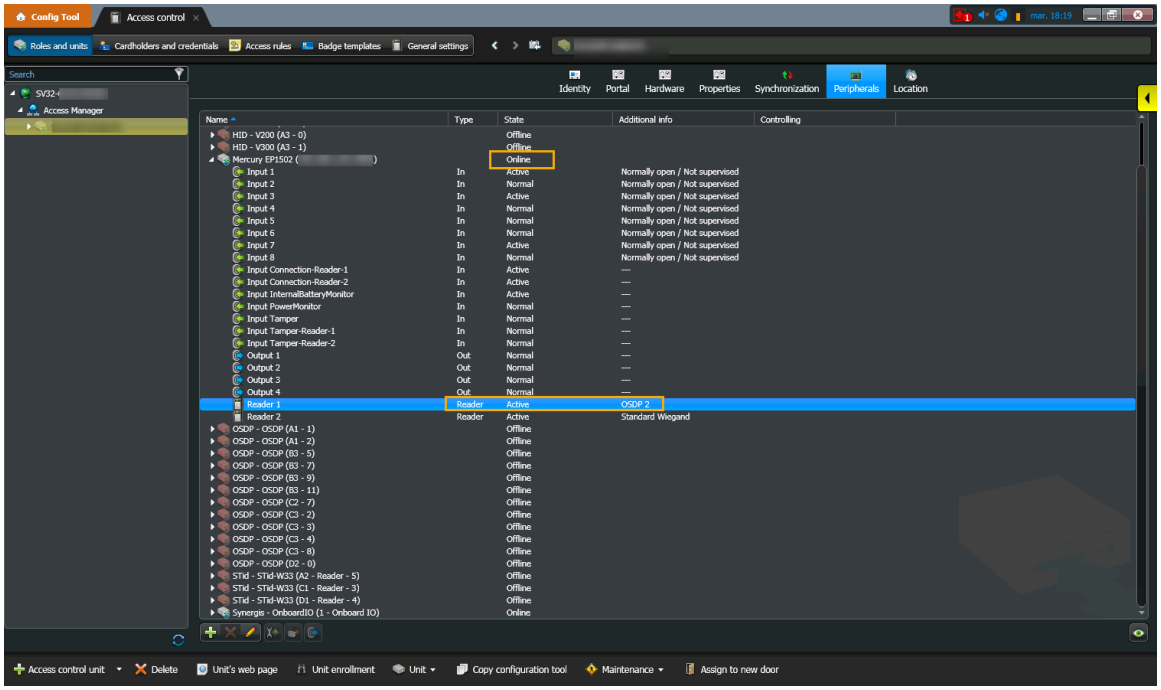
REMARQUE : Votre nouveau lecteur de codes QR doit être en ligne et disponible pour transférer la configuration de lecteur de codes QR de la carte à puce vers le lecteur.

5 Vérifiez que votre lecteur de codes QR est toujours actif après le passage de la carte OCB sur le lecteur mural.

a) Dans Config Tool, ouvrez la tâche *Contrôle d'accès*.

b) Dans la vue **Rôles et unités**, sélectionnez votre unité de contrôle d'accès.

c) Dans le champ **Nom** de l'onglet **Périphériques**, sélectionnez votre lecteur OSDP.



d) Dans le champ **Nom** de l'onglet **Périphérique**, vérifiez que l'**État** du lecteur ODSP est En ligne.

e) Dans le champ **Nom** de l'onglet **Périphérique**, vérifiez que l'**État** du lecteur est Actif.

f) Cliquez deux fois sur votre lecteur (**Lecteur 1**) dans la boîte de dialogue *Modifier le lecteur*, et vérifiez que vos réglages correspondent aux réglages du lecteur.

L'image suivante montre les réglages Mercury par défaut :

Lorsque vous avez terminé

Ajoutez des portes aux secteurs.

Automatiser l’accès et l’inscription des visiteurs à l'aide d'une macro

Vous pouvez configurer une macro du Security Center pour vérifier et accorder automatiquement l'accès aux visiteurs aux entrées de stationnement ou aux installations fermées spécifiées. La macro peut être utilisée pour les visiteurs qui ont besoin d'accéder à une entrée de parking ou à une installation fermée avant de pouvoir s'enregistrer ou à des endroits sans kiosques en libre-service.

Avant de commencer

- Importer un format de carte personnalisé (identifiant code QR) dans Synergis[MC]
- Activer les identifiants code QR pour les visiteurs

À savoir

Cette macro est uniquement à utiliser lorsque les sites souhaitent utiliser un code QR comme identifiant pour automatiser inscription des visiteurs. La macro peut accorder automatiquement l'accès à une entrée de parking spécifiée ou à une installation fermée avant inscription des visiteurs.

IMPORTANT : Cette procédure n’est compatible qu’avec Security Center 5.8 ou ultérieur.

Procédure

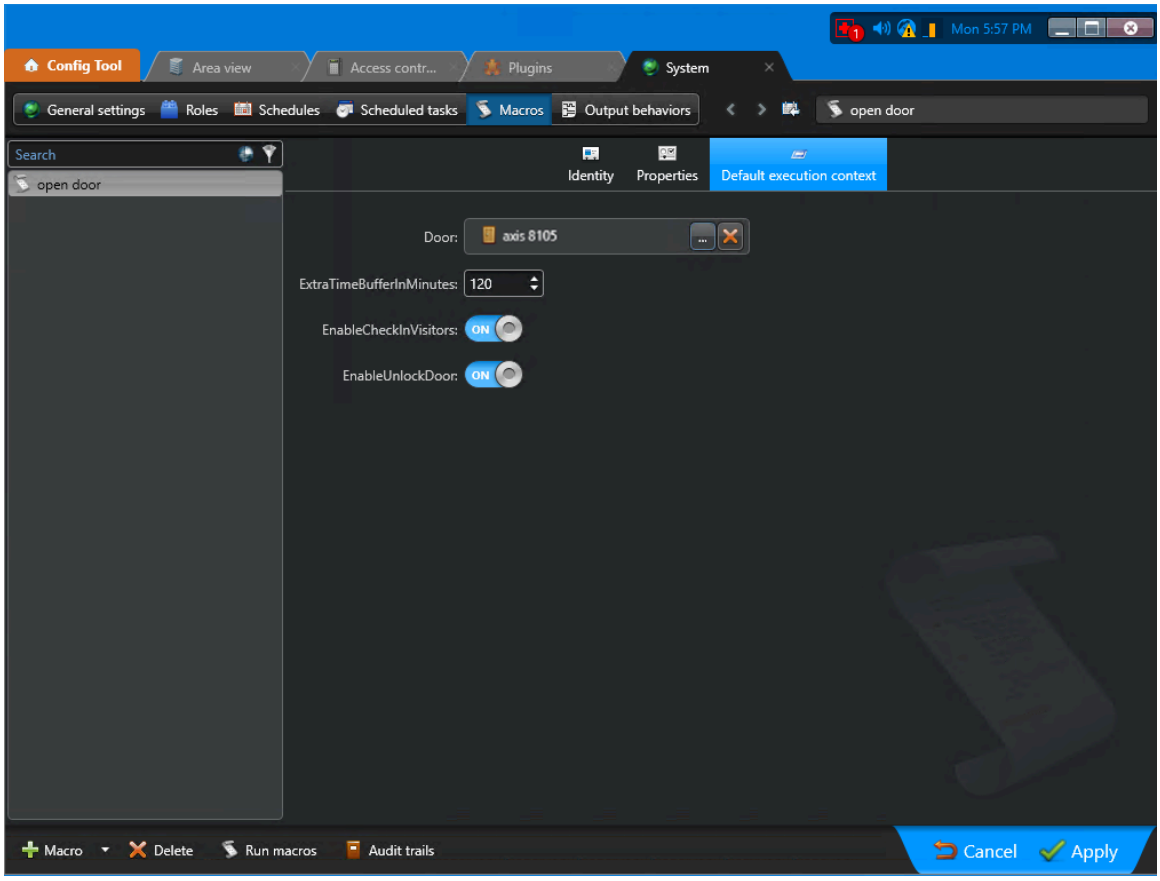
1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Système*, puis cliquez sur la vue **Macros**.

2 Cliquez sur **Macro** ( ), et entrez le nom de la macro.

3 Cliquez sur l'onglet **Propriétés**, puis procédez de l'une des manières suivantes :

- Coupez et collez le code du fichier macro dans la section *Définition de macro (C#)* de l’onglet **Propriétés** .
  - Macro 1 (exemple C#) : Compatible avec Security Center 5.7 SR4 - 5.11.2.
  - Macro 2 (exemple C#) : Compatible avec Security Center 5.11.3 ou version ultérieure.
- Importez le code source à partir d’un fichier en cliquant sur **Importer à partir**du fichier, sélectionnez le fichier contenant le code C#, puis cliquez sur **Ouvrir**.

4 Cliquez sur **Contexte d'exécution par défaut**, et configurez les réglages suivants :



REMARQUE : La porte sélectionnée dans **Contexte d'exécution par défaut** fait référence à une entrée de parking ou de secteur sécurisé particulier. Lorsqu'un visiteur présente son code QR, la macro est déclenchée pour accorder automatiquement un accès à cette porte seule.

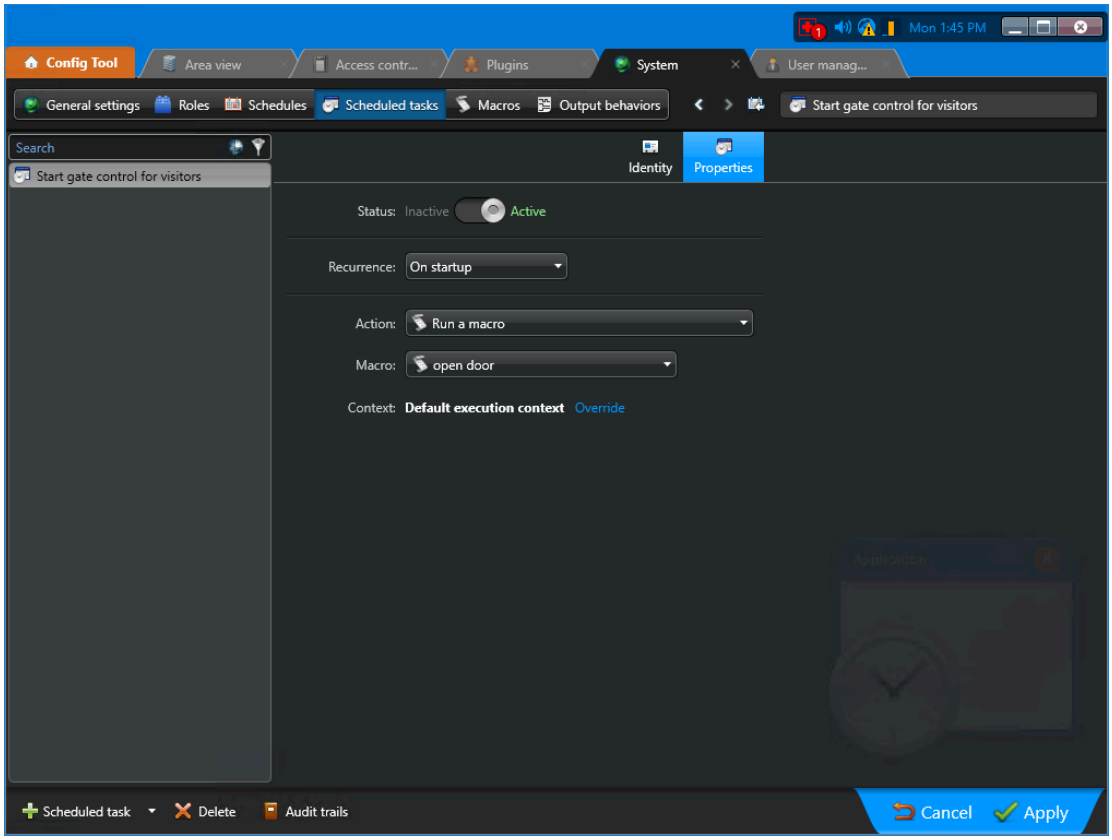
5 Cliquez sur **Appliquer**.

6 Cliquez sur **Exécuter les macros**.

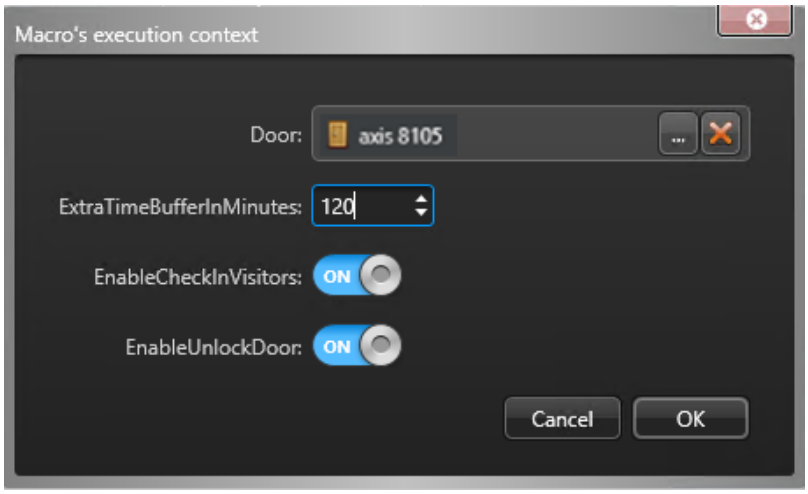
7 Sur la page d'accueil de Config Tool, ouvrez la tâche *Système*, puis cliquez sur la vue **Tâches planifiées**.

a) Cliquez sur **Tâche planifiée** (), et entrez le nom de la tâche planifiée.

b) Configurez l'onglet **Propriétés** :



c) (Facultatif) Dans la section *Contexte*, cliquez sur le lien **Ignorer** pour modifier le contexte d'exécution de la macro :



La macro du Security Center est maintenant configurée. Cela peut déclencher inscription automatique et accorder l'accès à des entrées de stationnement spécifiques ou à des installations fermées lorsque le code QR correspondant est scanné à l'entrée.

10

Gérez les listes de surveillance de visiteurs

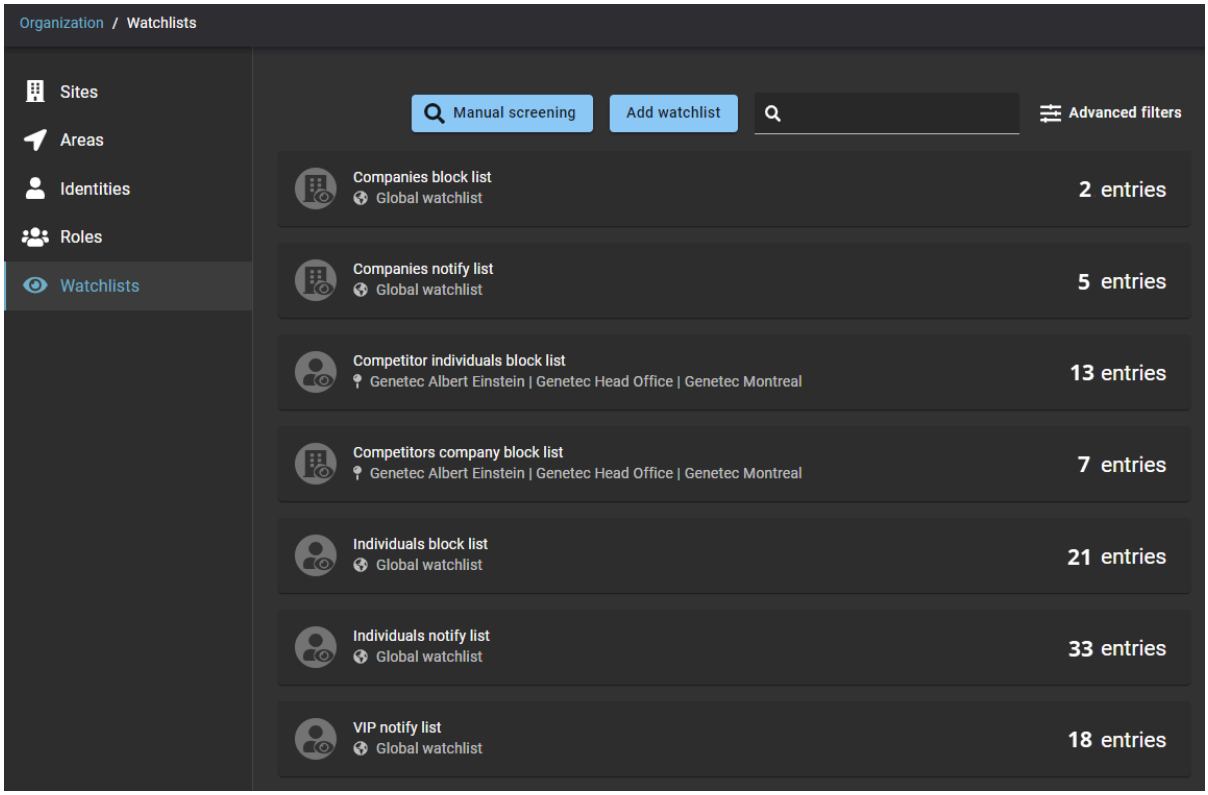
Découvrez comment gérer les accès des visiteurs à l’aide de listes de surveillance.

Cette section aborde les sujets suivants:

- " À propos des listes de surveillance ", page 437
- " Ajouter des responsables de listes de surveillance ", page 439
- " Ajouter des listes de surveillance ", page 441
- " Modifier les listes de surveillance ", page 456
- " Supprimer une liste de surveillance ", page 458
- " Contrôler les visiteurs manuellement ", page 460
- " Débloquer les visiteurs bloqués par une liste de surveillance ", page 464

À propos des listes de surveillance

Dans Genetec ClearID[MC], les listes de surveillance des visiteurs peuvent être utilisées pour filtrer les visiteurs au niveau individuel ou de l'entreprise. Vous pouvez configurer la liste de surveillance pour effectuer des actions d'autorisation, de blocage ou de notification au niveau d'un site ou au niveau mondial.



Le contrôle ne renvoie des correspondances que lorsque les conditions suivantes sont réunies :

- Personnes : Il existe une correspondance du **Prénom** et du **Nom**, du **Prénom** et du surnom pour le **Nom**, ou de l'adresse **E-mail**.
- Sociétés : Il existe une correspondance du nom de **Société**, du domaine ou d'adresse e-mail.

Il existe deux types de listes de surveillance :

- Liste de surveillance des personnes
- Liste de surveillance des sociétés

Une liste de surveillance de **Personnes** sert à comparer les inscriptions de visiteurs à des *personnes recherchées* répertoriées dans une liste de surveillance, puis à déclencher une action spécifiée dans la configuration de la liste de surveillance. Vous pouvez par exemple créer une liste de surveillance pour bloquer automatiquement les visiteurs présents dans la liste et notifier les responsables de listes de surveillance. Dans d'autres situations, vous pouvez choisir de simplement notifier les responsables de listes de surveillance. Ou vous pouvez créer une liste de surveillance de personnes pour notifier tous les responsables de listes de surveillance lorsqu'un VIP arrive sur votre site.

Une liste de surveillance de **Sociétés** sert à comparer les inscriptions de visiteurs à des *sociétés s'intérêt* répertoriées dans une liste de surveillance, puis à déclencher une action spécifiée dans la configuration de la liste de surveillance. Vous pouvez par exemple créer une liste de surveillance de sociétés pour bloquer automatiquement l'accès aux personnes associées à un nom, un domaine ou une adresse e-mail de **société** correspondant à des sociétés répertoriées dans la liste de surveillance.

REMARQUE : Les *Personnes* ou les *Sociétés* répertoriées dans une liste de surveillance peuvent être saisies individuellement ou importées par lots à partir d'un fichier *.CSV*.

Comportement de liste de surveillance

Le comportement des listes de surveillance peut être configuré de la manière suivante :

- Notifier les responsables de listes de surveillance.
- Bloquer automatiquement les visiteurs présents dans une liste de surveillance et notifier les responsables de listes de surveillance.

Listes de surveillance globales

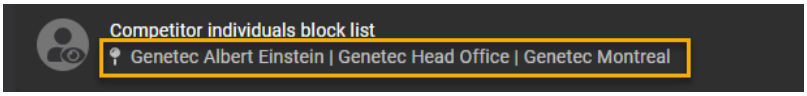
Dans Genetec ClearID[MC], une liste de surveillance globale est une liste de surveillance appliquée à tous les sites de votre système.

Les listes de surveillance globales sont indiquées par un globe ( ) dans la vue des listes de surveillance :

Listes de surveillance locales

Si une liste de surveillance n'est pas configurée en tant que *liste de surveillance globale*, elle est considérée comme s'appliquant au niveau d'un ou de plusieurs sites.

Les listes de surveillance locales sont indiquées par un identifiant de site ( ), suivi d'un ou de plusieurs sites, dans la vue des listes de surveillance :



Motifs de blocage ou de notification

Les motifs entraînant le blocage de l'accès des visiteurs répertoriés dans une liste de surveillance, ou la notification d'un responsable, comme dans les cas suivants :

- Casier judiciaire
- Menaces ou activité violente
- Fausse pièce d'identité
- Articles de contrebande
- Vol
- Infraction à la sécurité
- Autres motifs

REMARQUE : Seul un *responsable de liste de surveillance* peut consulter les motifs d'inclusion de visiteurs dans des listes de surveillance de blocage ou de notification.

Ajouter des responsables de listes de surveillance

Dans Genetec ClearID[MC], un responsable de liste de surveillance est une identité qui gère des listes de surveillance. Un responsable de liste de surveillance peut créer ou modifier des listes et leur ajouter des personnes ou des sociétés. Il configure également les listes pour déterminer si elles s'appliquent localement ou globalement. Avant de pouvoir ajouter, modifier ou configurer une liste de surveillance, vous devez ajouter des responsables de listes de surveillance.

Avant de commencer

Créez vos sites.

À savoir

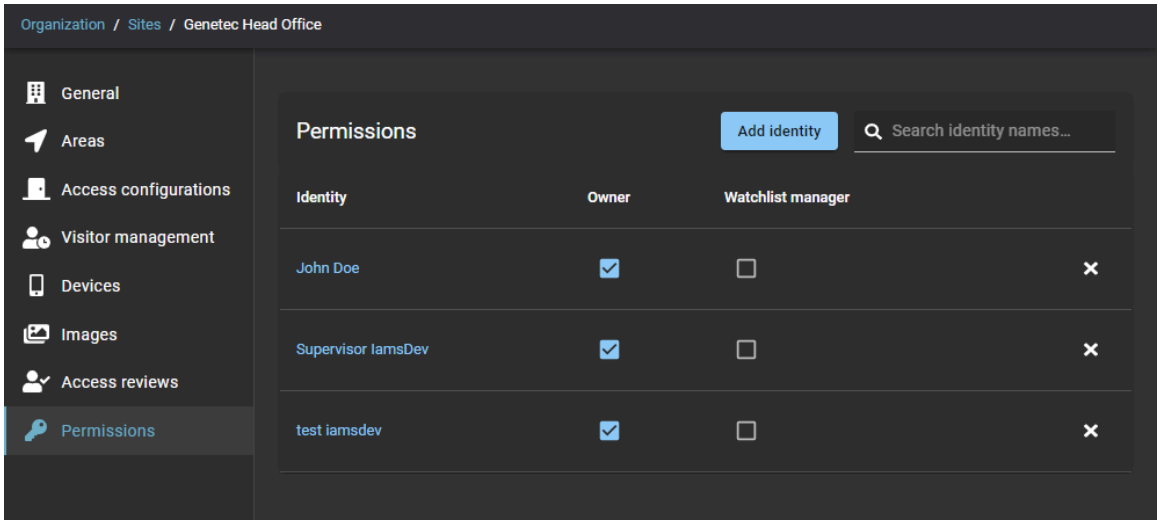
Pour ajouter des responsables de listes de surveillance dans Genetec ClearID[MC], vous devez être un administrateur de compte.

Procédure

1 Cliquez sur **Organisation** > **Sites**.

2 Sélectionnez votre site et cliquez sur **Autorisations**.

3 (Facultatif) Cliquez sur **Ajouter une identité** pour ajouter des identités à la liste des **Autorisations** du site.



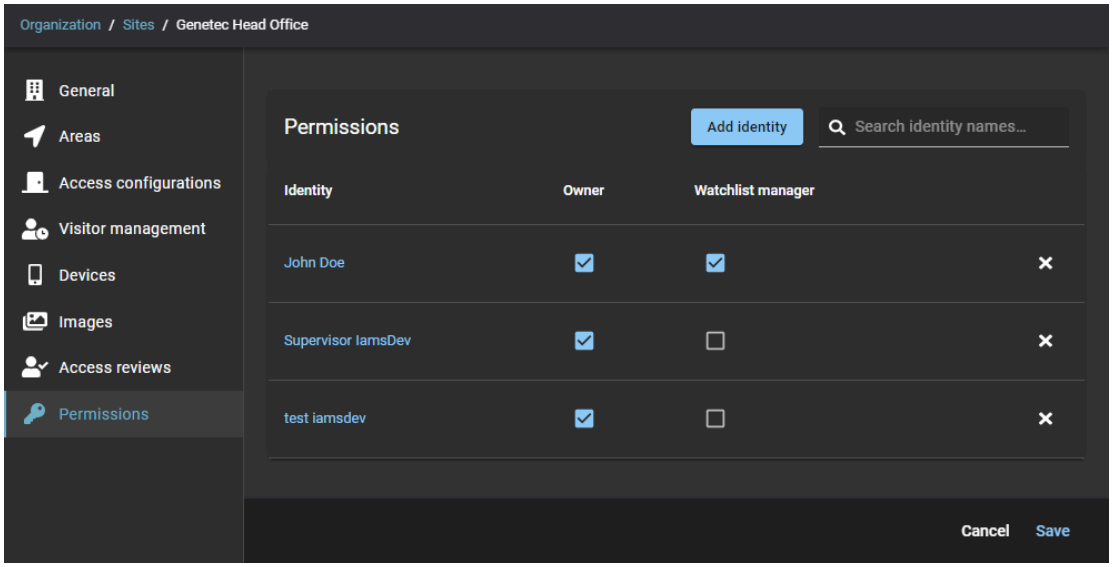
a) Recherchez ou sélectionnez les identités dont vous avez besoin et cliquez sur **Ajouter**.

CONSEIL : Vous pouvez cliquer sur le lien hypertexte d'identité dans la colonne **Identité** pour consulter les détails d'identité (entreprise, département, site d'origine, superviseur et e-mail) et vérifier que les identités correctes figurent dans la liste.

4 Cochez la case **Responsable de liste de surveillance** pour affecter des autorisations de responsable de liste de surveillance à une identité.

a) (Facultatif) Décochez les cases pour supprimer les autorisations individuelles qui ne sont plus nécessaires pour une identité.

b) (Facultatif) Cliquez sur ✖ pour supprimer toutes les autorisations qui ne sont plus nécessaires pour une identité.



5 Cliquez sur **Enregistrer**.

Lorsque vous avez terminé

Ajoutez vos listes de surveillance.

Ajouter des listes de surveillance

Ajoutez des listes de surveillance de personnes ou de sociétés pour pouvoir contrôler les visiteurs au niveau individuel ou d'une société, et déclencher automatiquement des actions de blocage ou de notification au niveau d'un site ou au niveau global, selon la configuration de la liste de surveillance.

Avant de commencer

En savoir plus sur les listes de surveillance.

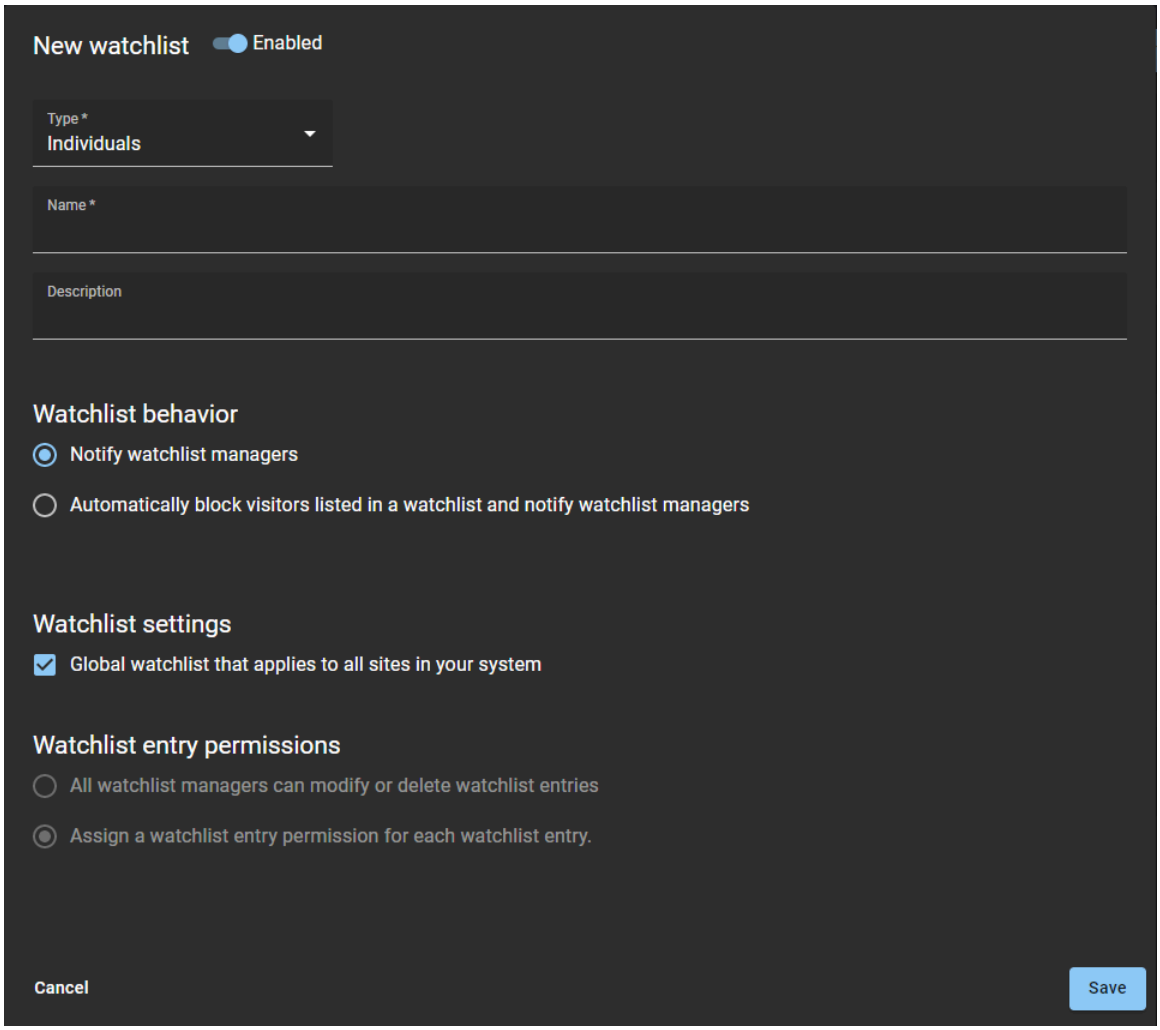
À savoir

- Tout *responsable de liste de surveillance* ou administrateur de comptes peut modifier ou supprimer les listes configurées en tant que *listes de surveillance globales*.

Procédure

1 Cliquez sur **Organisation** > **Listes de surveillance**.

2 Cliquez sur **Ajouter une liste de surveillance**.



3 Au sommet de la nouvelle liste de surveillance, cliquez sur le commutateur pour activer ou désactiver la liste.

4 Dans le champ **Type**, sélectionnez un type de liste de surveillance. Sélectionnez **Personnes** ou **Sociétés** :

- **Personnes :** Une liste de surveillance de **Personnes** sert à comparer les inscriptions de visiteurs à des *personnes recherchées* répertoriées dans une liste de surveillance, puis à déclencher une action spécifiée dans la configuration de la liste de surveillance. Vous pouvez par exemple créer une liste de surveillance pour bloquer automatiquement les visiteurs présents dans la liste et notifier les responsables de listes de surveillance. Dans d'autres situations, vous pouvez choisir de simplement notifier les responsables de listes de surveillance. Ou vous pouvez créer une liste de surveillance de personnes pour notifier tous les responsables de listes de surveillance lorsqu'un VIP arrive sur votre site.
- **Sociétés :** Une liste de surveillance de **Sociétés** sert à comparer les inscriptions de visiteurs à des *sociétés s'intérêt* répertoriées dans une liste de surveillance, puis à déclencher une action spécifiée dans la configuration de la liste de surveillance. Vous pouvez par exemple créer une liste de surveillance de sociétés pour bloquer automatiquement l’accès aux personnes associées à un nom, un domaine ou une adresse e-mail de **société** correspondant à des sociétés répertoriées dans la liste de surveillance.

5 Donnez un **Nom** à la liste de surveillance.

Vous pouvez modifier le nom d'une liste à tout moment.

CONSEIL : Utilisez si possible un *nom discret* pour éviter de divulguer des informations sensibles sur les motifs pour lesquels une personne pourrait être bloquée ou répertoriée dans une liste lors de l’envoi des notifications.

6 Donnez une **Description** à la liste de surveillance.

7 Dans la section *Comportement de la liste de surveillance*, sélectionnez l'une des options suivantes :

- **Notifier les responsables de listes de surveillance**
- **Bloquer automatiquement les visiteurs présents dans une liste de surveillance et notifier les responsables de listes de surveillance**

8 Dans la section *Réglages de la liste de surveillance*, indiquez si vous voulez une liste globale ou propre à un site.

- Pour appliquer la liste à tous les sites de votre système, sélectionnez **Liste de surveillance globale qui s'applique à tous les sites de votre système**.
- Pour appliquer la liste à un ou plusieurs sites de votre système, décochez la case **Liste de surveillance globale qui s'applique à tous les sites de votre système**.

a) Si vous optez pour une liste appliquée au niveau des sites, ajoutez les sites concernés et appuyez sur Entrée.

b) Répétez au besoin.

REMARQUE : La section *Autorisations d’entrées de listes de surveillance* est désactivée lorsque la case **Liste de surveillance globale qui s'applique à tous les sites de votre système** est cochée.

9 Si l'option **Autorisations d’entrées de listes de surveillance** est activée pour votre compte, sélectionnez l’une des options suivantes dans la section *Autorisations d’entrées de listes de surveillance* :

- **Tous les responsables de listes de surveillance peuvent modifier ou supprimer les entrées de listes de surveillance**.
- **Affecter une autorisation d’entrée de liste de surveillance à chaque entrée de liste de surveillance**
- **Tous les responsables de listes de surveillance peuvent modifier ou supprimer les entrées de listes de surveillance :** Indique que les entrées ne peuvent être modifiées ou supprimées que par les responsables de listes de surveillance des sites spécifiés.
- **Affecter une autorisation d’entrée de liste de surveillance à chaque entrée de liste de surveillance :** Indique que les autorisations d’entrées de listes de surveillance sont affectées à un

niveau plus granulaire dans chaque entrée. Cela signifie que seuls les responsables de listes de surveillance du site peuvent modifier ou supprimer des entrées.

Exemple:

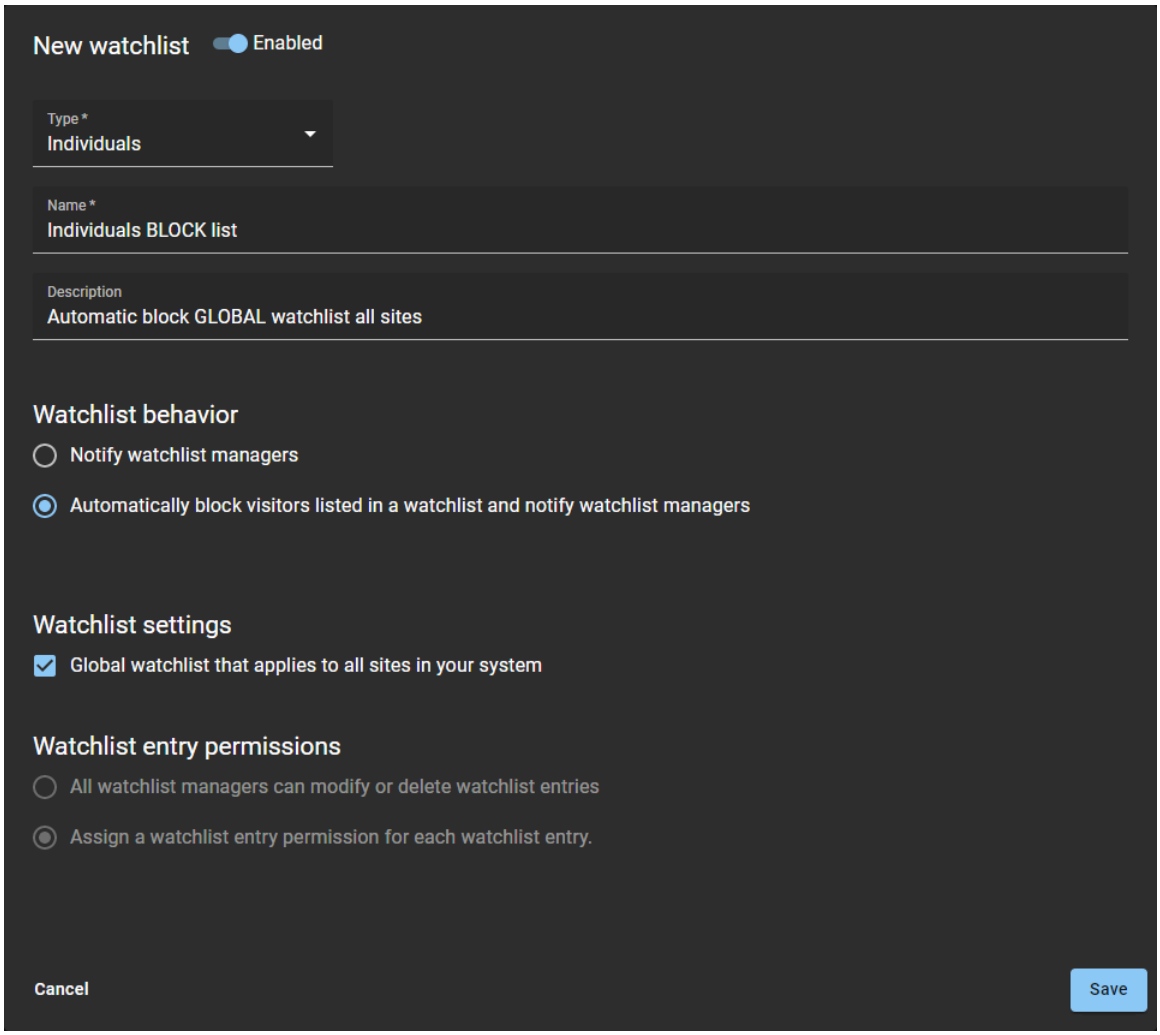


Illustration 14 : Exemple 1 : Liste de surveillance de blocage de personnes, configurée en tant que liste globale pour bloquer automatiquement les visiteurs et notifier les responsables de listes de surveillance.

Exemple:

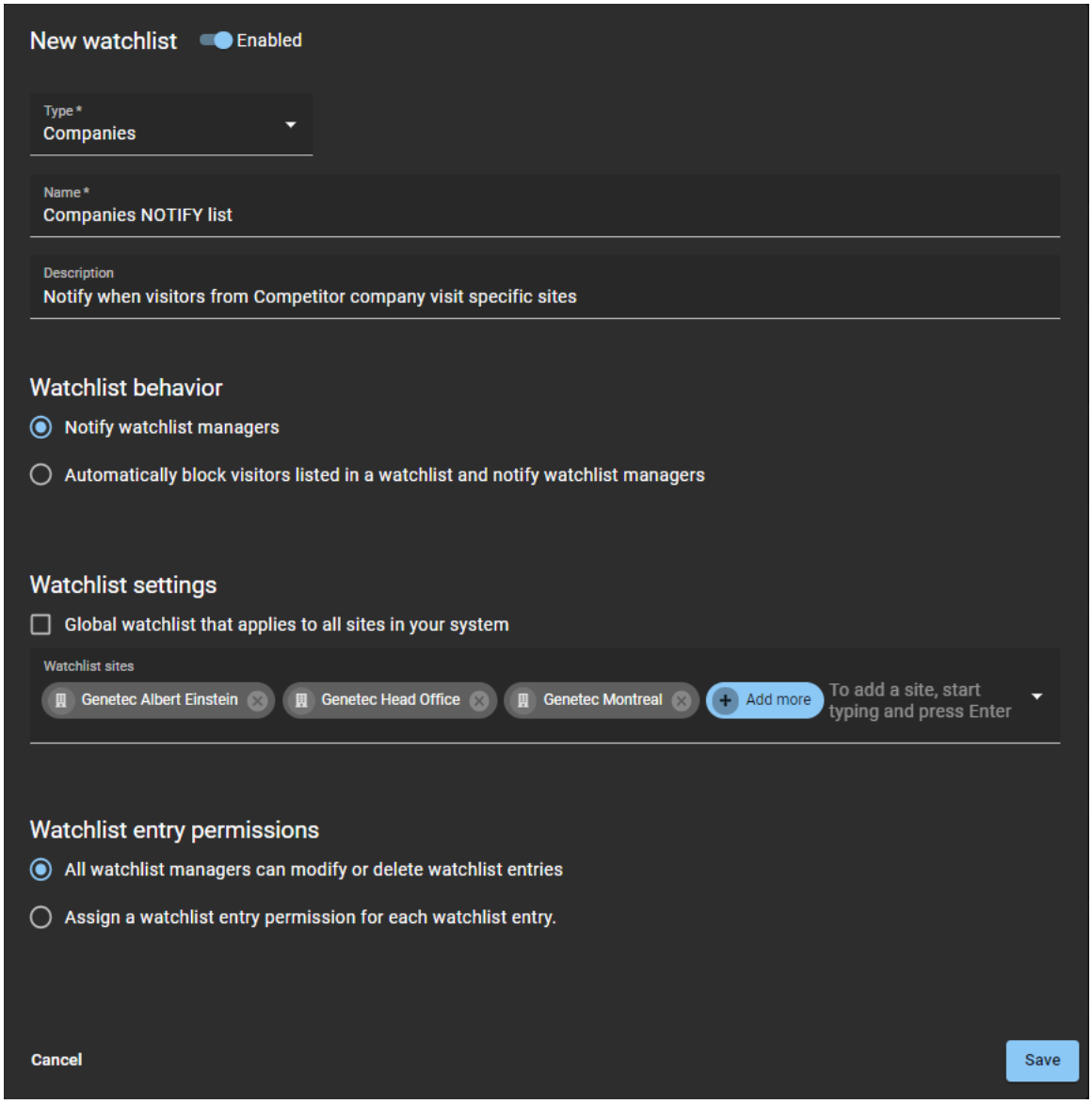


Illustration 15 : Exemple 2 : Liste de surveillance de notification de sociétés, configurée en tant que liste propre à un site pour avertir les responsables de listes de surveillance en cas d'arrivée de visiteurs d'une société concurrente.

10 Cliquez sur **Enregistrer**.

Lorsque vous avez terminé

Procédez de l'une ou de plusieurs des manières suivantes :

- Ajouter des entrées à une liste de surveillance de personnes
- Ajouter des entrées à une liste de surveillance de sociétés

Ajouter une entrée à une liste de surveillance de personnes

Ajoutez une ou plusieurs entrées à une liste de surveillance de personnes pour pouvoir contrôler les visiteurs au niveau individuel, et déclencher automatiquement des actions de blocage ou de notification au niveau d'un site ou au niveau global, selon la configuration de la liste de surveillance.

Avant de commencer

Ajoutez vos listes de surveillance.

À savoir

Seul un *responsable de liste de surveillance* peut :

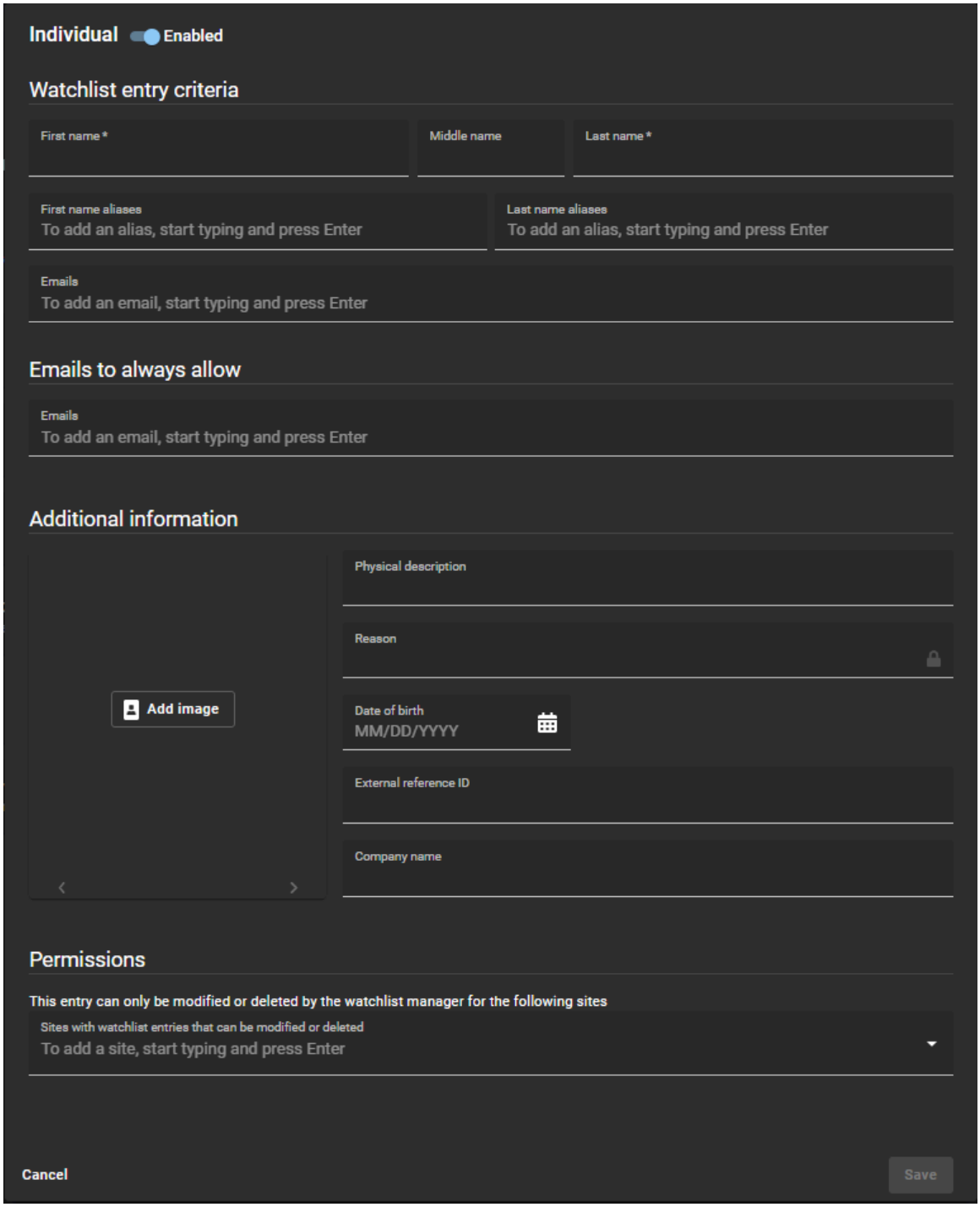
- Ajouter des entrées à une liste de surveillance de personnes.
- Consulter le motif de la présence de visiteurs dans des listes de blocage ou de notification.

Procédure

1 Cliquez sur **Organisation** > **Listes de surveillance**.

2 Sélectionnez une liste de surveillance dans la liste.

3 Cliquez sur **Ajouter une entrée**.



4 Au sommet de l'entrée de liste de surveillance, cliquez sur le commutateur pour activer ou désactiver l'entrée.

5 Dans la section *Critères d'entrée de liste de surveillance*, renseignez les champs :

- **Prénom :** Saisissez un prénom.
- **Deuxième prénom :** Entrez un deuxième prénom.
- **Nom :** Entrez un nom.
- **Alias du prénom :** Ajoutez d'éventuels surnoms pour le prénom et appuyez sur Entrée. Répétez selon vos besoins.

REMARQUE : Les alias sont affichés entre accolades dans la liste de surveillance.

- **Alias du nom :** Ajoutez d'éventuels surnoms pour le nom et appuyez sur Entrée. Répétez selon vos besoins.
- **E-mails :** Ajoutez les adresses e-mail connues et appuyez sur Entrée. Répétez selon vos besoins.

6 Dans la section *E-mails autorisés*, ajoutez toute adresse e-mail que vous souhaitez exclure du processus de contrôle par liste de surveillance.

Cette section permet d'ajouter des adresses e-mail similaires ou des faux positifs que vous souhaitez toujours autoriser. Par exemple, une correspondance possible avec le même nom, mais qui correspond à une autre personne avec une autre adresse e-mail qui doit être autorisée.

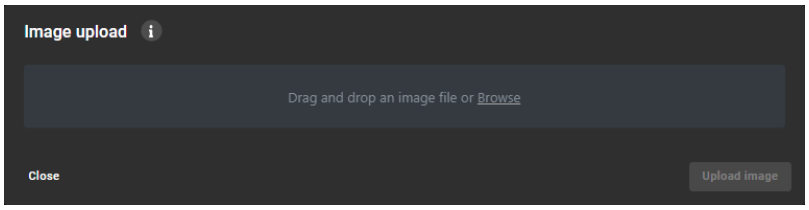
7 Dans la section *Informations complémentaires*, renseignez les champs selon vos besoins :

- **Description physique :** Entrez une description physique.
- **Motif :** Entrez le motif du blocage ou de la notification.

  REMARQUE : Le champ Motif peut contenir des informations confidentielles sensibles, et n'est visible que par le **responsable de liste de surveillance** du site.
- **Date de naissance :** Utilisez le mini calendrier pour saisir la date de naissance.

  La date de naissance peut être utile lorsqu'une inscription correspond à plusieurs personnes ayant le même nom. Elle peut servir à confirmer une identité ou à éliminer des doublons ou des faux positifs.
- **ID de référence externe :** Entrez un ID de référence externe.
- **Nom de la société :** Entrez un nom de société.

8 Dans la section *Informations complémentaires*, cliquez sur **Ajouter une image** pour ajouter une ou plusieurs images en cas de besoin.



a) Faites un glisser-déposer, ou cliquez sur **Parcourir** pour sélectionner l'image, et cliquez sur **Transférer une image**.

b) Répétez pour chaque image supplémentaire que vous souhaitez transférer.

c) (Facultatif) Cliquez sur **Supprimer l'image** pour supprimer toute image dont vous ne voulez plus.

CONSEIL : Cliquez sur **Ouvrir dans un nouvel onglet** pour afficher l'image en taille réelle.

9 Si l'option **Autorisations d'entrées de listes de surveillance** est activée pour votre compte, ajoutez les sites nécessaires dans la section *Autorisations*.

10 Cliquez sur **Enregistrer**.

Lorsque vous avez terminé

Testez vos entrées de liste de surveillance.

Ajouter une entrée à une liste de surveillance de sociétés

Ajoutez une ou plusieurs entrées à une liste de surveillance de sociétés pour pouvoir contrôler les visiteurs d'une même entreprise, et déclencher automatiquement des actions de blocage ou de notification au niveau d'un site ou au niveau global, selon la configuration de la liste de surveillance.

Avant de commencer

Ajoutez vos listes de surveillance.

À savoir

Seul un *responsable de liste de surveillance* peut :

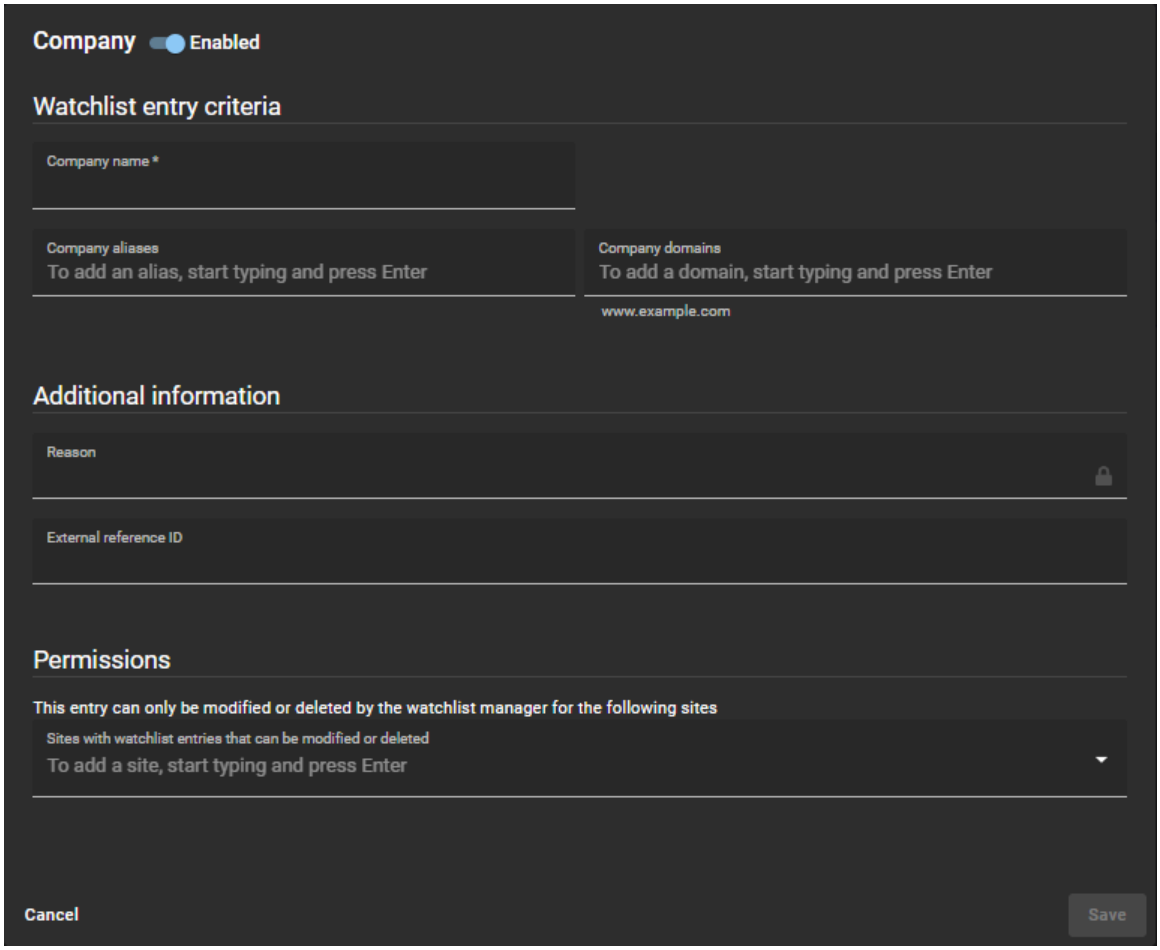
- Ajouter des entrées à une liste de surveillance de sociétés.
- Consulter le motif de la présence de visiteurs dans des listes de blocage ou de notification.

Procédure

1 Cliquez sur **Organisation** > **Listes de surveillance**.

2 Sélectionnez une liste de surveillance dans la liste.

3 Cliquez sur **Ajouter une entrée**.



4 Au sommet de l'entrée de liste de surveillance, cliquez sur le commutateur pour activer ou désactiver l'entrée.

5 Dans la section *Critères d'entrée de liste de surveillance*, renseignez les champs :

- **Nom de la société :** Entrez un nom de société.
- **Alias de société :** Ajoutez d'éventuels surnoms pour la société et appuyez sur Entrée. Répétez selon vos besoins.

  REMARQUE : Les alias sont affichés entre accolades dans la liste de surveillance.
- **Domaines de société :** Ajoutez d'autres domaines de la société et appuyez sur Entrée. Répétez selon vos besoins.

6 Dans la section *Informations complémentaires*, renseignez les champs selon vos besoins :

- **Motif :** Entrez le motif du blocage ou de la notification.

  REMARQUE : Le champ Motif peut contenir des informations confidentielles sensibles, et n'est visible que par le **responsable de liste de surveillance** du site.
- **ID de référence externe :** Entrez un ID de référence externe.

7 Si l'option **Autorisations d'entrées de listes de surveillance** est activée pour votre compte, ajoutez les sites nécessaires dans la section *Autorisations*.

8 Cliquez sur **Enregistrer**.

Lorsque vous avez terminé

Testez vos entrées de liste de surveillance.

Importer des entrées de liste de surveillance depuis un fichier

Pour accélérer la configuration de votre liste de surveillance, vous pouvez importer vos entrées depuis un fichier *.CSV*. Vous pouvez également télécharger un fichier *.CSV* exemple pour vous aider à préparer votre fichier d'entrées de liste de surveillance au bon format.

Avant de commencer

Préparez vos entrées de liste de surveillance dans un fichier *.CSV* pour l'importation.

À savoir

Seul un *responsable de liste de surveillance* peut importer des entrées de liste de surveillance.

Vous pouvez importer des données d'entrées de liste de surveillance préexistantes à partir d'un fichier *.CSV* provenant de l'une ou plusieurs des sources suivantes :

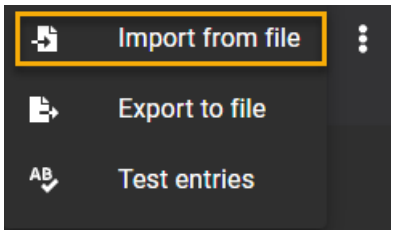
- Sharepoint
- Excel
- Liste « BOLO » (Be on the look-out, ou soyez aux aguets), un terme utilisé par les forces de l'ordre.
- Liste entrée interdite (no entry list)
- Liste d'interdiction d'accès (Deny entry list ou DEL)

Procédure

1 Cliquez sur **Organisation** > **Listes de surveillance**.

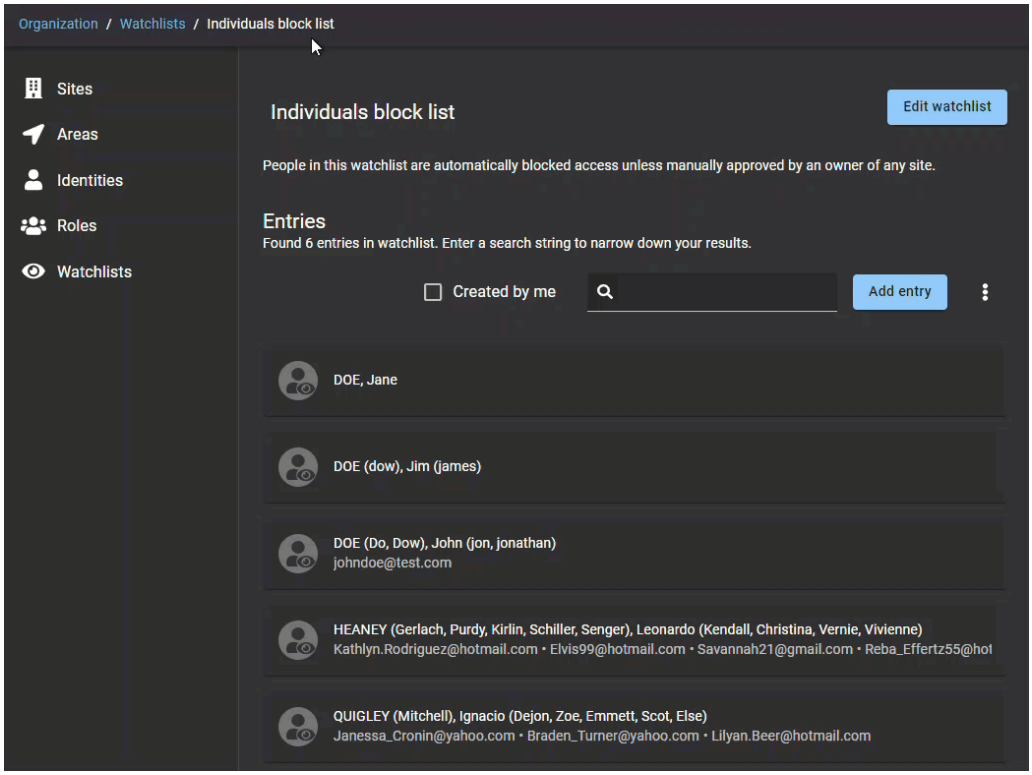
2 Sélectionnez une liste de surveillance.

3 Cliquez sur puis cliquez sur **Importer à partir d'un fichier**.



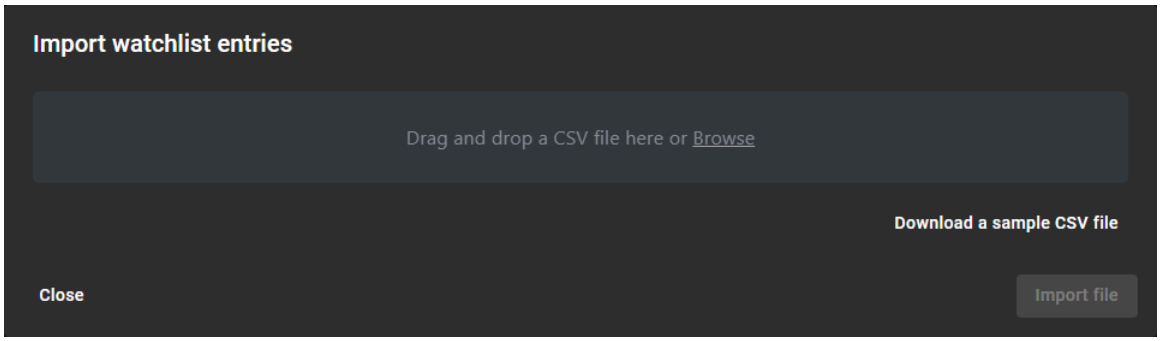
4 (Facultatif) Cliquez sur **Télécharger un fichier .CSV exemple** pour vous aider à préparer votre fichier d'entrées de liste de surveillance au bon format.

REMARQUE : Les colonnes et les entrées dans le fichier CSV exemple (*watchlist-sample.csv*) peut varier en fonction du type de liste de surveillance sélectionné (**Personnes** ou **Sociétés**) lorsque vous téléchargez le fichier.

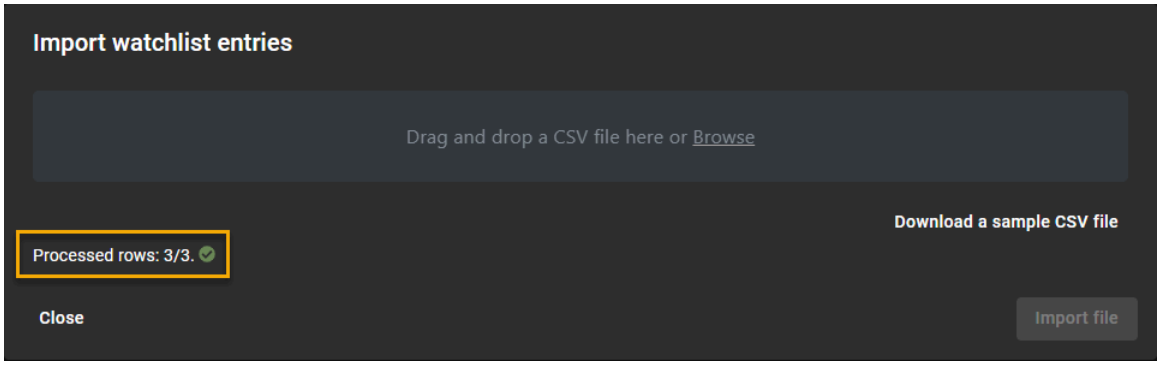


CONSEIL : Cliquez sur l'animation pour la voir en taille réelle.

5 Faites glisser un fichier CSV dans la boîte de dialogue *Importer les entrées de liste de surveillance* ou cliquez sur **Parcourir** pour sélectionner un fichier.



6 Cliquez sur **Importer un fichier**.



REMARQUE : Le champ **Lignes traitées** dans la boîte de dialogue *Importer des entrées de liste de surveillance* indique le nombre d'entrées qui ont été traitées.

Lorsque vous avez terminé

Testez vos entrées de liste de surveillance.

Exporter les entrées de liste de surveillance dans un fichier

Vous pouvez exporter vos entrées de liste de surveillance dans un fichier *.CSV* pour une modification globale ou à des fins de sauvegarde. Vous pouvez par exemple exporter vos entrées de liste de surveillance vers Microsoft Excel, modifier les entrées, supprimer les doublons, puis fusionner des listes de surveillance ou consolider des entrées dans une nouvelle liste de surveillance.

Avant de commencer

Procédez de l'une ou de plusieurs des manières suivantes :

- Ajoutez des entrées à votre liste de surveillance de personnes.
- Ajoutez des entrées à votre liste de surveillance de sociétés.
- Importez vos entrées de liste de surveillance.

À savoir

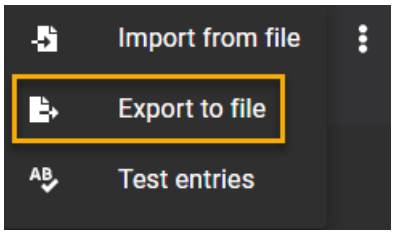
Seul un *responsable de liste de surveillance* peut exporter des entrées de liste de surveillance.

Procédure

1 Cliquez sur **Organisation** > **Listes de surveillance**.

2 Sélectionnez une liste de surveillance.

3 Cliquez sur puis cliquez sur **Exporter dans un fichier**.



Les entrées sont exportées dans un fichier *.CSV* dans le dossier de téléchargement par défaut de votre navigateur. Par défaut, le fichier exporté est créé d'après le nom de votre liste de surveillance. Par exemple, *Liste de blocage de personnes.csv*.

4 Suivez les instructions dans votre navigateur pour télécharger le fichier exporté.

Lorsque vous avez terminé

(Facultatif) Traitez les données des entrées de liste de surveillance selon les besoins.

Tester les entrées de liste de surveillance

Pour tester de nouvelles entrées de liste de surveillance, vous pouvez saisir les informations pour une personne recherchée ou une société d'intérêt pour vérifier qu'il existe bien une correspondance.

Avant de commencer

Procédez de l'une ou de plusieurs des manières suivantes :

- Ajoutez des entrées à une liste de surveillance de personnes
- Ajoutez des entrées à une liste de surveillance de sociétés

À savoir

Seul un *responsable de liste de surveillance* peut tester des entrées de liste de surveillance.

Le contrôle ne renvoie des correspondances que lorsque les conditions suivantes sont réunies :

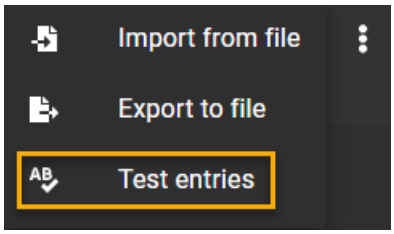
- Personnes : Il existe une correspondance du **Prénom** et du **Nom**, du **Prénom** et du surnom pour le **Nom**, ou de l'adresse **E-mail**.
- Sociétés : Il existe une correspondance du nom de **Société**, du domaine ou d'adresse e-mail.

Procédure

1 Cliquez sur **Organisation** > **Listes de surveillance**.

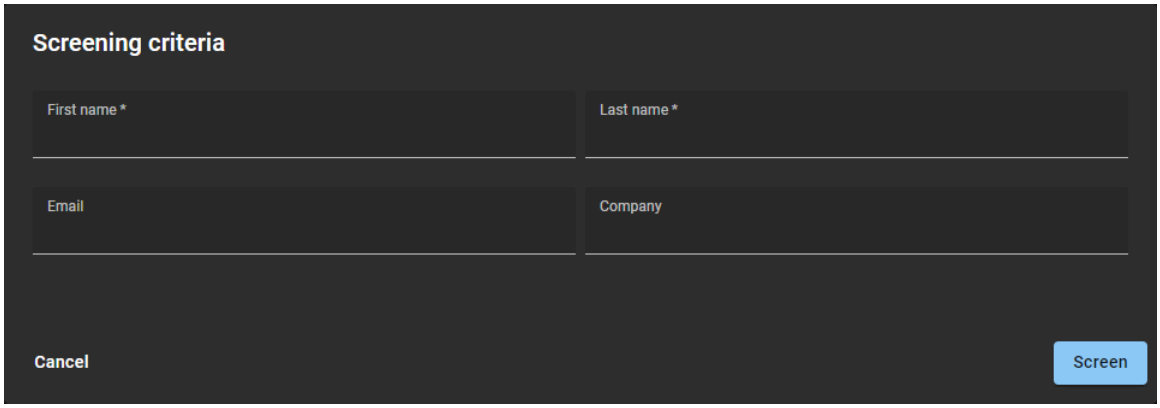
2 Sélectionnez une liste de surveillance.

3 Cliquez sur puis cliquez sur **Tester les entrées**.



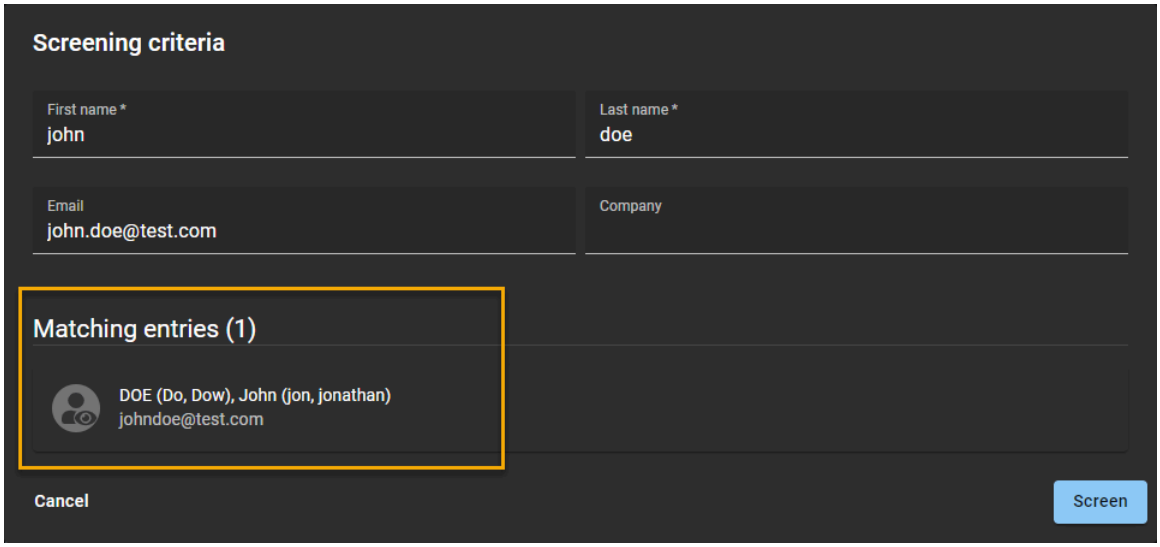
4 Dans la boîte de dialogue *Critères de contrôle*, renseignez les informations sur l'entrée que vous souhaitez tester.

REMARQUE : Les champs obligatoires sont indiqués par un astérisque (*).



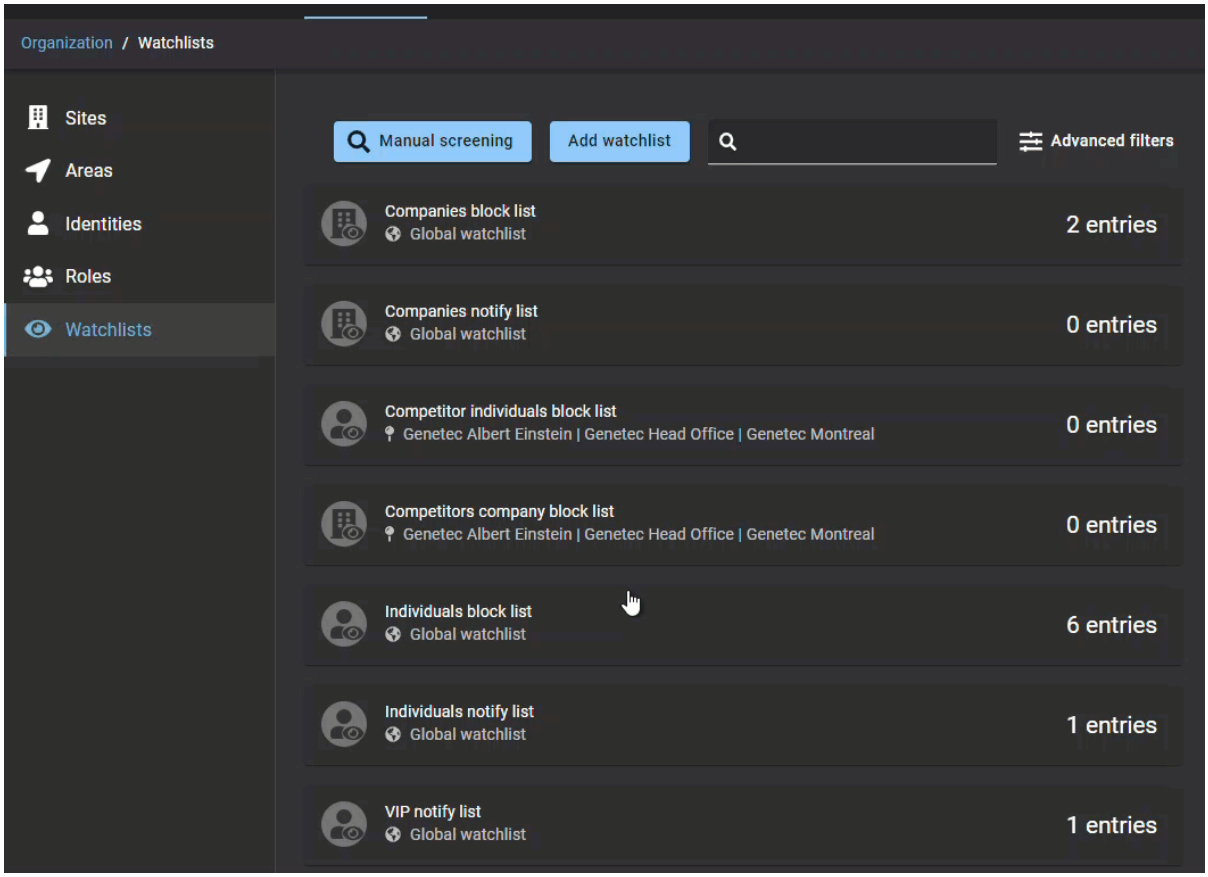
5 Cliquez sur **Contrôler**.

Les entrées correspondantes sont affichées dans la liste *Entrées correspondantes* de la boîte de dialogue *Critères de contrôle*.



6 (Facultatif) Cliquez sur une entrée correspondante dans la liste pour afficher l'intégralité des informations de l'entrée de liste de surveillance.

7 Cliquez sur **Annuler** pour fermer la boîte de dialogue *Critères de contrôle*.



Supprimer les entrées de liste de surveillance

Un responsable de liste de surveillance peut supprimer les entrées de listes de surveillance de personnes ou de sociétés qui sont obsolètes ou ne sont plus nécessaires.

Avant de commencer

Procédez de l'une ou de plusieurs des manières suivantes :

- Ajoutez des entrées à une liste de surveillance de personnes
- Ajoutez des entrées à une liste de surveillance de sociétés

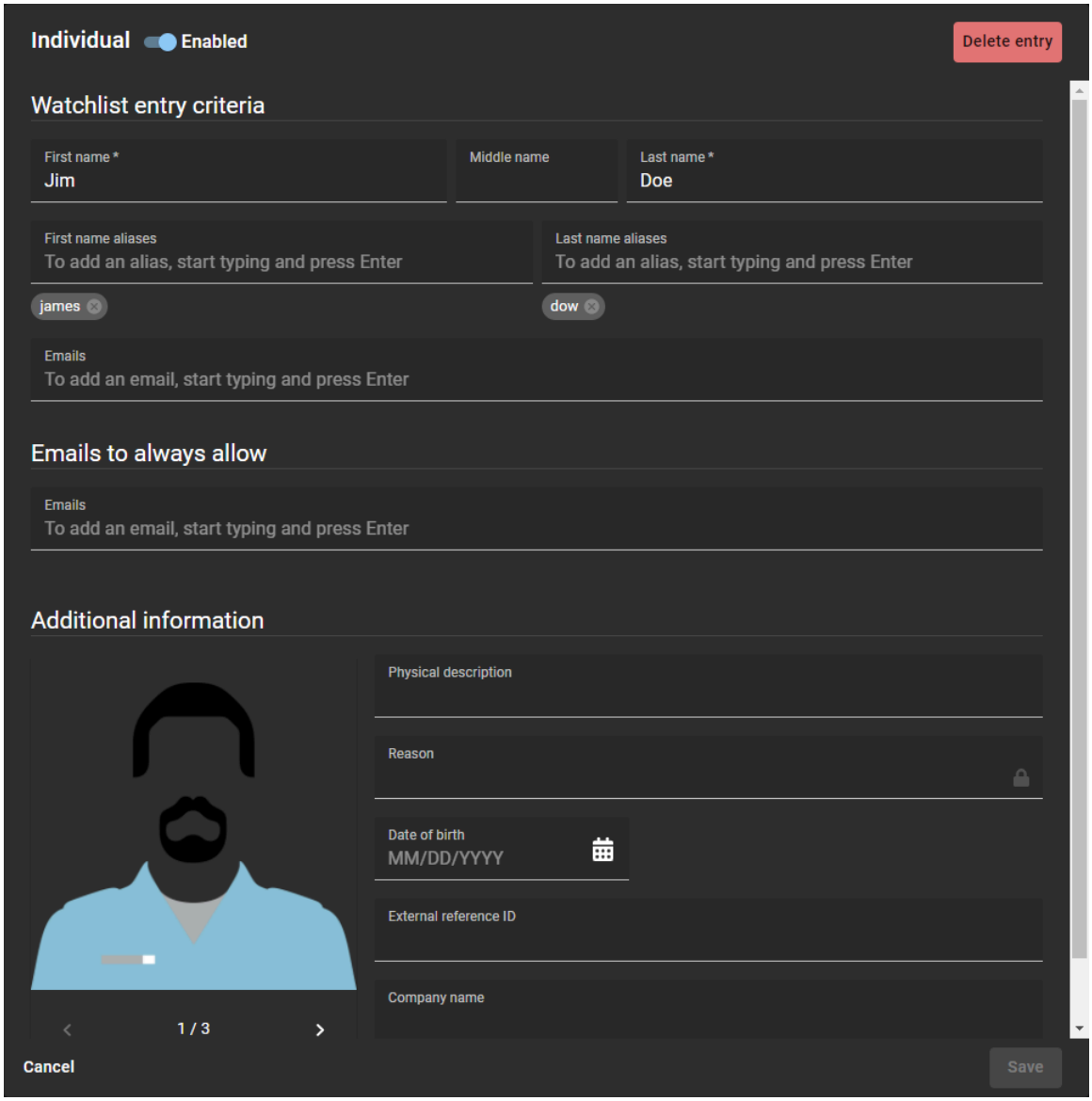
À savoir

Une entrée de liste de surveillance ne peut être supprimée que par le *responsable de liste* qui l'a créée.

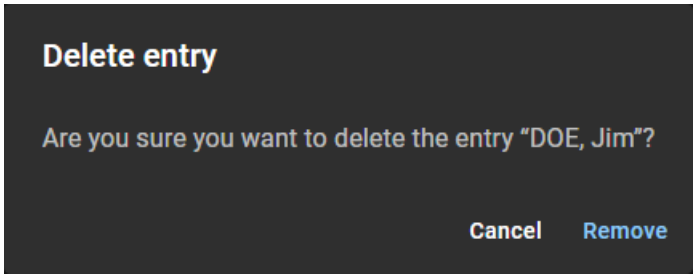
Procédure

1 Cliquez sur **Organisation** > **Listes de surveillance**.
2 Sélectionnez une liste de surveillance dans la liste.
3 (Facultatif) Si la liste est longue, sélectionnez **Créé par moi** pour filtrer les résultats.
4 Procédez de l'une des manières suivantes :
   - Cliquez sur une entrée dans la liste pour la sélectionner.
   - Recherchez l'entrée que vous souhaitez supprimer.

5 Faites défiler la page jusqu'au bas de l'entrée, et cliquez sur **Supprimer l'entrée**.



6 Dans la boîte de dialogue *Supprimer l'entrée*, cliquez sur **Supprimer** pour confirmer votre choix.



Modifier les listes de surveillance

Une fois que vous avez ajouté vos listes de surveillance, vous pouvez modifier certains de leurs réglages. Un responsable de liste de surveillance peut désactiver une liste, modifier le nom ou la description, et modifier le comportement de la liste.

Avant de commencer

Ajoutez vos listes de surveillance.

À savoir

Tenez compte des points suivants lorsque vous modifiez une liste de surveillance :

- Vous ne pouvez pas transformer une *liste de surveillance globale* en *liste de surveillance locale*.
- Vous ne pouvez pas transformer une *liste de surveillance locale* en *liste de surveillance globale*.
- Vous ne pouvez pas modifier les **Autorisations d'entrées de listes de surveillance** une fois que la liste a été créée.

Tout *responsable de liste de surveillance* ou administrateur de comptes peut modifier les listes configurées en tant que *listes de surveillance globales*.

Procédure

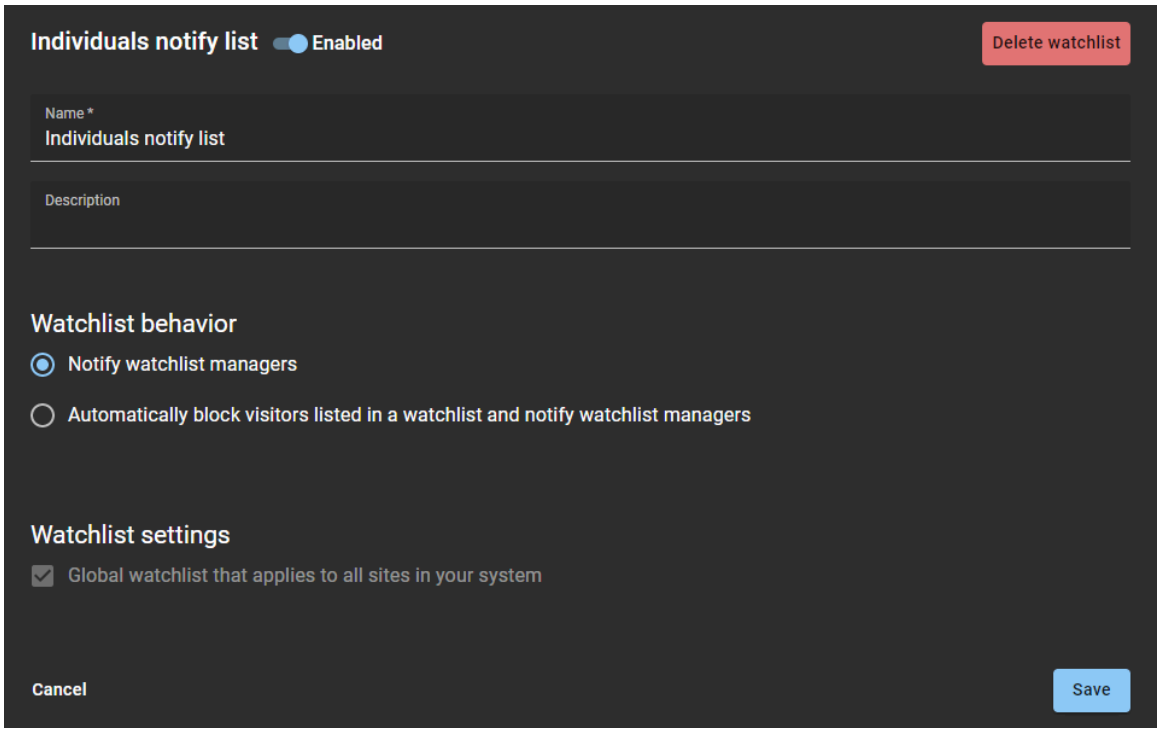
1 Cliquez sur **Organisation** > **Listes de surveillance**.

2 (Facultatif) Utilisez le champ de recherche pour rechercher une liste particulière.

3 (Facultatif) Cliquez sur **Filtres avancés** pour filtrer le résultat par **Site** ou **Type de liste de surveillance**.
Sélectionnez les critères de filtre nécessaires :
   a) Dans la liste **Site**, sélectionnez un site.
   b) Faites une sélection dans la liste **Types de listes de surveillance**.
   c) Cliquez sur **Fermer**.

4 Sélectionnez une liste de surveillance dans la liste.

5 Cliquez sur **Modifier la liste de surveillance**.



6 Modifiez la liste de surveillance en fonction de vos besoins de la manière suivante :

a) Au sommet de la boîte de dialogue Liste de surveillance, cliquez sur le commutateur pour activer ou désactiver la liste.

Vous pouvez par exemple vouloir désactiver une liste de taille importante, et vous y reporter pendant que vous réorganisez les entrées dans d'autres listes.

b) Dans le champ **Nom**, modifiez le **nom** de la liste de surveillance.

c) Dans le champ **Description**, modifiez la **description** de la liste de surveillance.

d) Dans la section *Comportement de la liste de surveillance*, modifiez le **comportement de la liste**. Sélectionnez soit **Notifier les responsables de listes de surveillance** ou **Bloquer automatiquement les visiteurs présents dans une liste de surveillance et notifier les responsables de listes de surveillance**.

7 Cliquez sur **Enregistrer**.

Supprimer une liste de surveillance

Un responsable de liste de surveillance peut supprimer des listes de surveillance obsolètes ou qui ne sont plus nécessaires. Ou vous voudrez parfois supprimer une liste lorsque vous voulez transformer une *liste de surveillance de site* en *liste de surveillance globale*, ou inversement.

Avant de commencer

Ajoutez vos listes de surveillance.

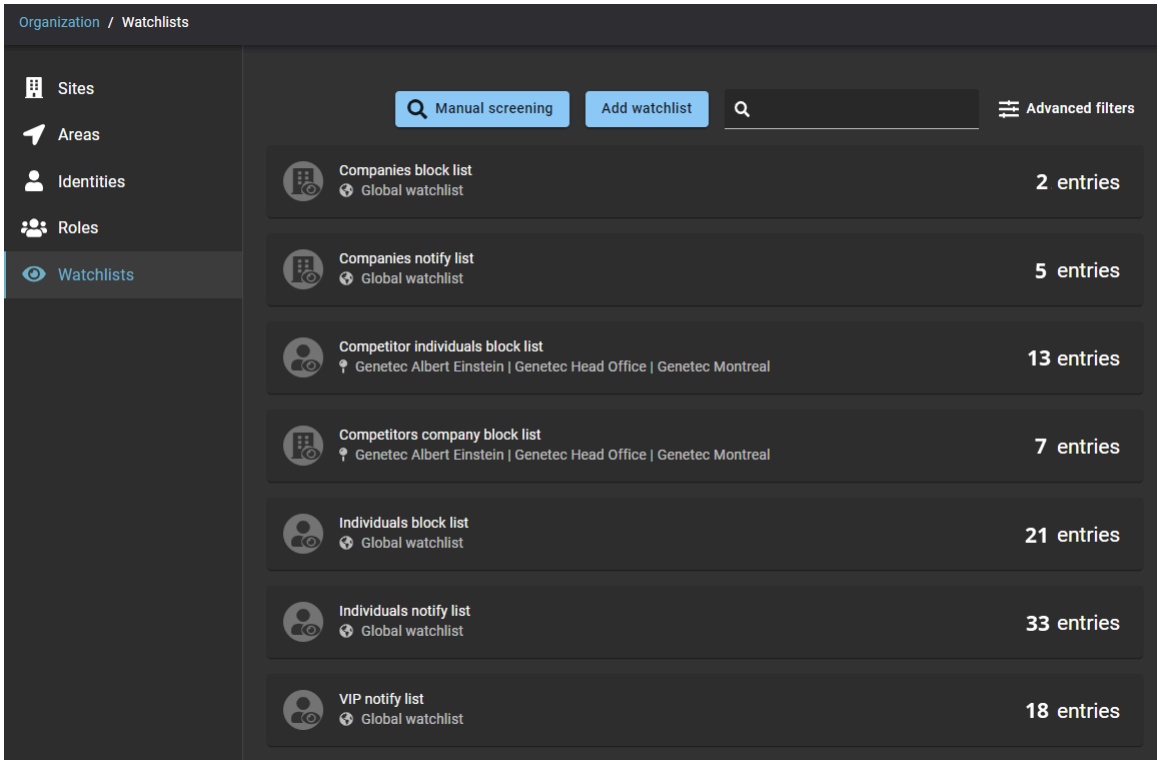
À savoir

Une liste de surveillance ne peut être supprimée que par le *responsable de liste* qui l'a créée.

REMARQUE : Tout responsable de liste de surveillance ou administrateur de comptes peut modifier les listes configurées en tant que listes de surveillance globales.

Procédure

1 Cliquez sur **Organisation** > **Listes de surveillance**.



2 (Facultatif) Utilisez le champ de recherche pour rechercher une liste particulière.

3 (Facultatif) Cliquez sur **Filtres avancés** pour filtrer le résultat par **Site** ou **Type de liste de surveillance**. Sélectionnez les critères de filtre nécessaires :

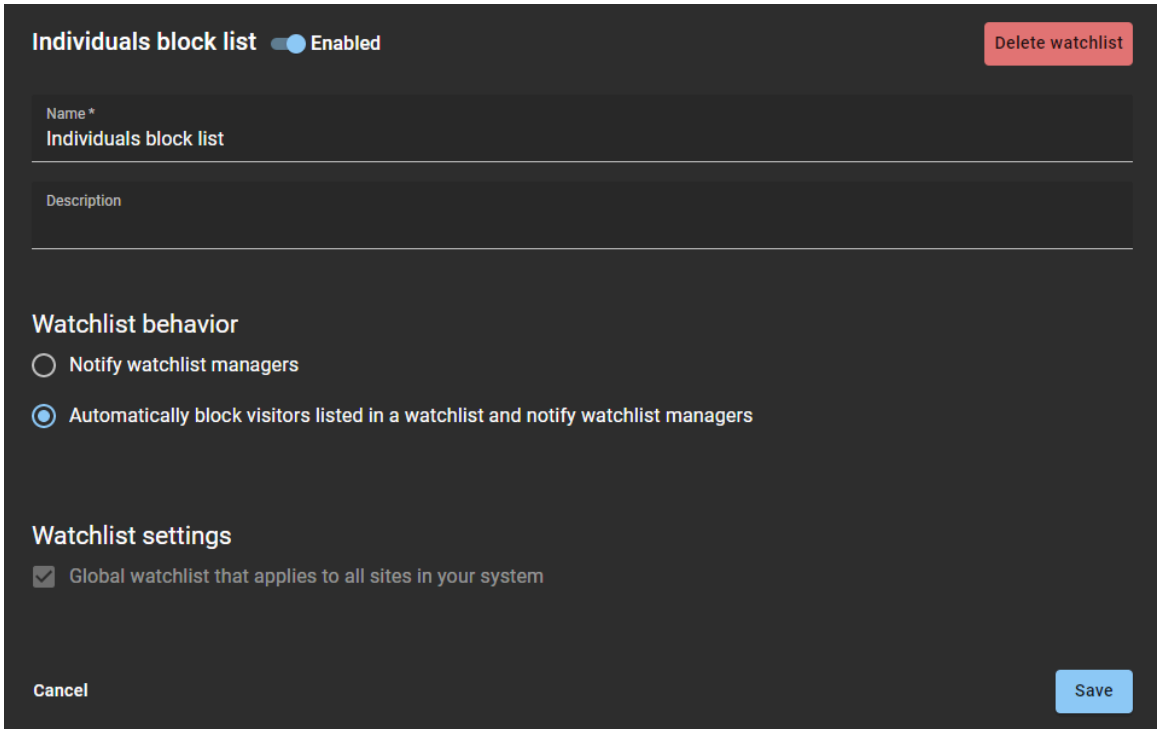
   a) Dans la liste **Site**, sélectionnez un site.

   b) Faites une sélection dans la liste **Types de listes de surveillance**.

4 Sélectionnez une liste de surveillance dans la liste.

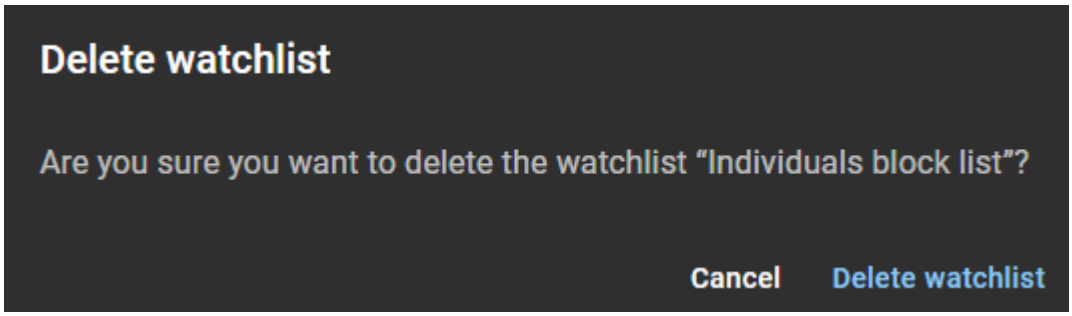
5 Cliquez sur **Modifier la liste de surveillance**.

6 Vérifiez que vous avez sélectionné la bonne liste et cliquez sur **Supprimer la liste de surveillance**.



Procédez de l'une des manières suivantes :

a) Dans la boîte de dialogue *Supprimer la liste de surveillance*, cliquez sur **Supprimer la liste de surveillance** pour confirmer la suppression.



b) (Facultatif) Cliquez sur **Annuler** pour annuler la suppression.

Contrôler les visiteurs manuellement

Pour contrôler un visiteur manuellement, vous pouvez saisir des informations pour rechercher des correspondances. Par exemple, tester une nouvelle liste de surveillance pour y trouver des listes qui contiennent une personne ou une société particulière, ou pour valider une nouvelle recrue en interrogeant une liste de surveillance interne.

Avant de commencer

Ajoutez des entrées à votre liste de surveillance de personnes.

À savoir

Seuls les *responsables de listes de surveillance* ou les administrateurs de comptes peuvent contrôler manuellement les visiteurs pour :

- Trouver des listes de surveillance qui contiennent une personne recherchée.
- Valider une nouvelle recrue en interrogeant une liste de surveillance de **personnes** ou de **sociétés**.

  Le contrôle ne renvoie des correspondances que lorsque les conditions suivantes sont réunies :

  - Personnes : Il existe une correspondance du **Prénom** et du **Nom**, du **Prénom** et du surnom pour le **Nom**, ou de l'adresse **E-mail**.
  - Sociétés : Il existe une correspondance du nom de **Société**, du domaine ou d'adresse e-mail.

Si la *sécurité* ou l'*accueil* doit contrôler manuellement des visiteurs, l'autorisation *Responsable de liste de surveillance* doit être ajoutée à leur identité.

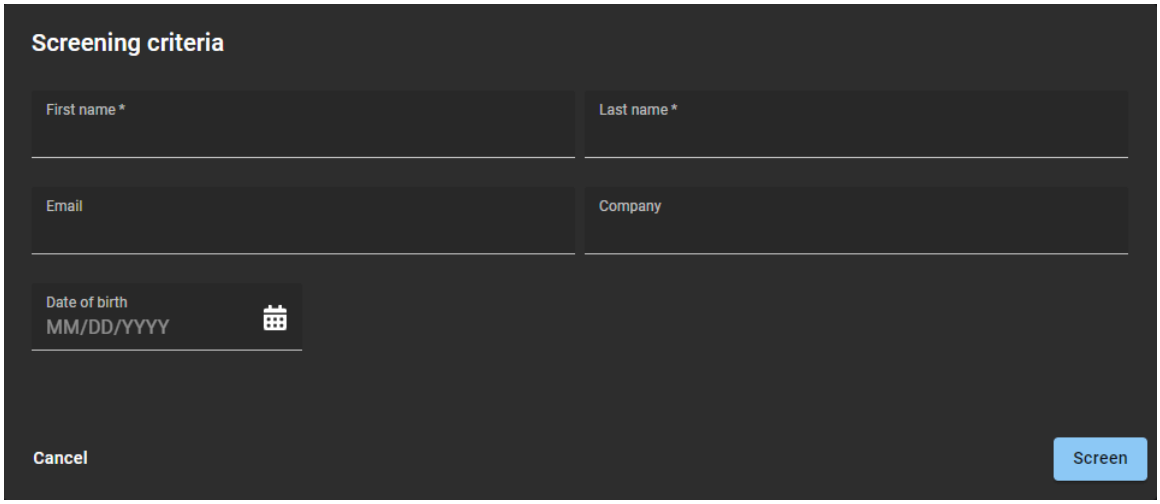
Procédure

1 Cliquez sur **Organisation** > **Listes de surveillance**.

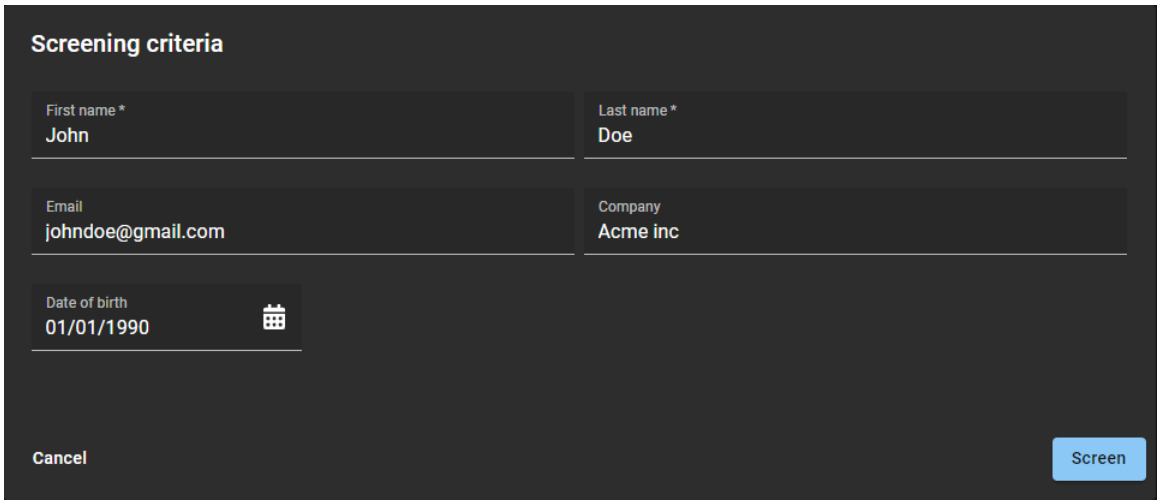
2 Cliquez sur **Contrôle manuel**.

3 Dans la boîte de dialogue *Critères de contrôle*, renseignez les informations sur le visiteur que vous souhaitez vérifier.

REMARQUE : Les champs obligatoires sont indiqués par un astérisque (*).

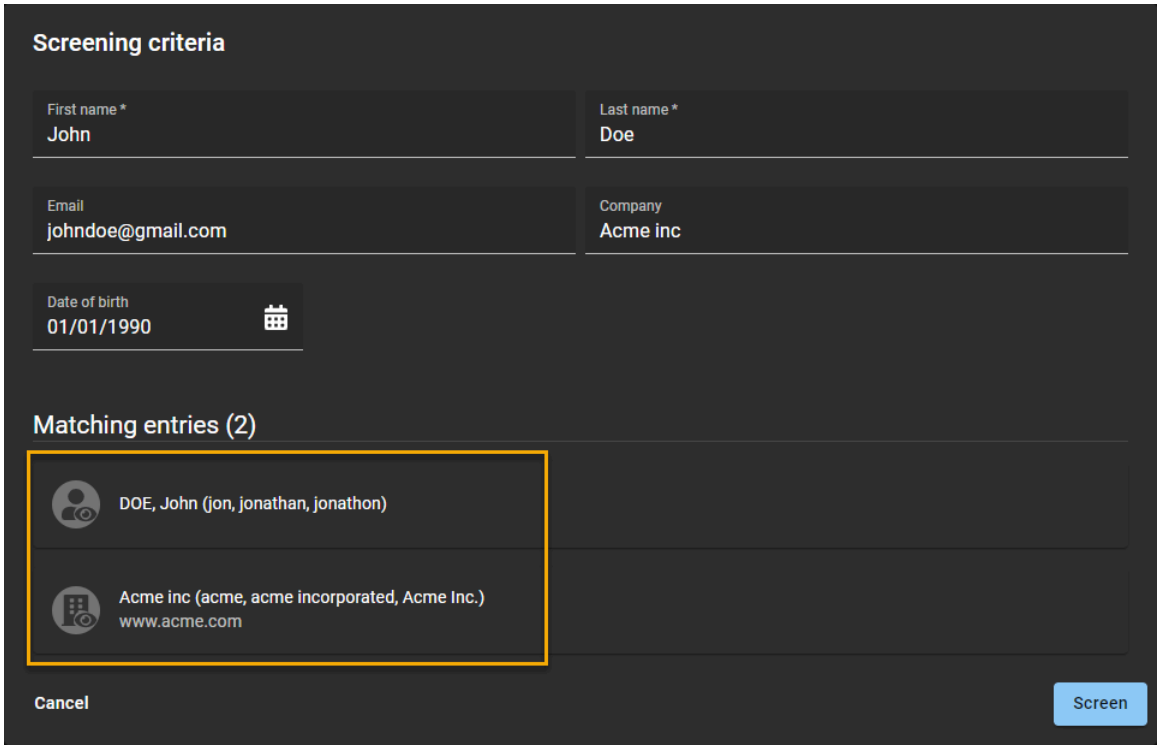


- **Prénom :** Saisissez un prénom.
- **Nom :** Entrez un nom.
- **E-mail :** Entrez l'adresse e-mail du visiteur.
- **Société :** Entrez le nom de la société du visiteur.
- **Date de naissance :** Utilisez le mini calendrier pour saisir la date de naissance du visiteur. La date de naissance peut être utile lorsqu'une inscription correspond à plusieurs personnes ayant le même nom. Elle peut servir à confirmer une identité ou à éliminer des doublons ou des faux positifs.



4 Cliquez sur **Contrôler**.

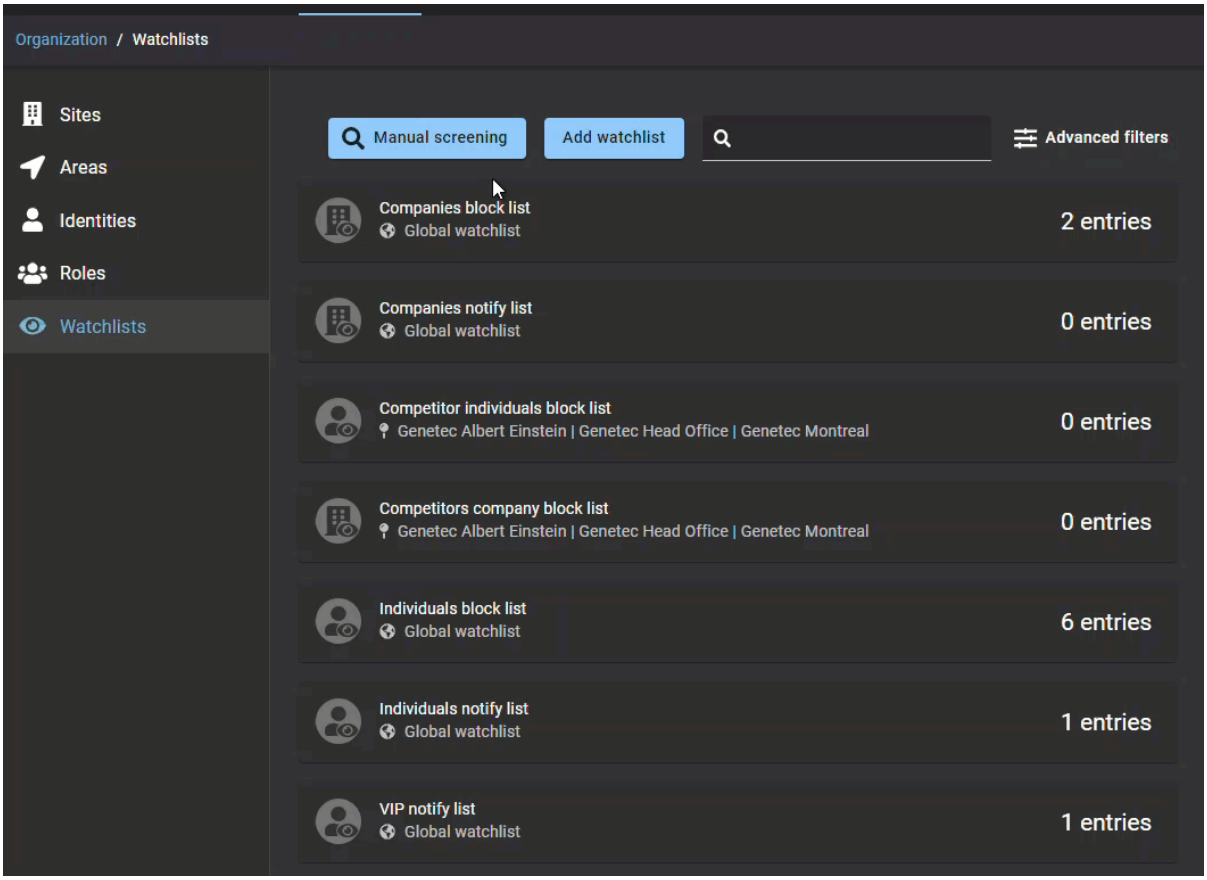
Les personnes ou les sociétés correspondantes sont affichées dans la liste *Entrées correspondantes* de la boîte de dialogue *Critères de contrôle*.



5 (Facultatif) Cliquez sur une personne dans la liste **Entrées correspondantes** pour afficher l'intégralité des informations de l'entrée de liste de surveillance de personnes.

6 (Facultatif) Cliquez sur une société dans la liste **Entrées correspondantes** pour afficher l'intégralité des informations de l'entrée de liste de surveillance de sociétés.

7 Cliquez sur **Annuler** pour fermer la boîte de dialogue *Critères de contrôle*.



CONSEIL : Cliquez sur l'animation pour la voir en taille réelle.

Rubriques connexes

Ajouter des responsables de listes de surveillance, page 439

Débloquer les visiteurs bloqués par une liste de surveillance

Pour débloquer des visiteurs bloqués à tort par une liste de surveillance, vous pouvez placer leur adresse e-mail sur liste blanche.

Avant de commencer

Ajouter des entrées à votre liste de surveillance de personnes.

À savoir

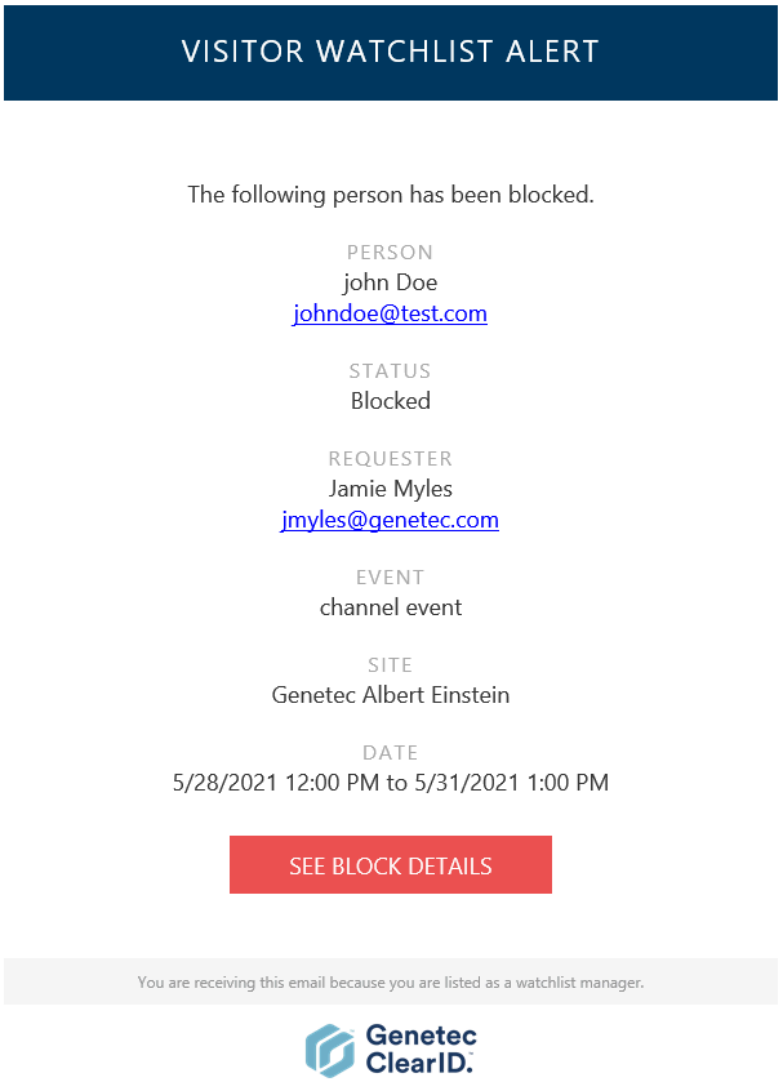
Seul un *responsable de liste de surveillance* ou un administrateur de comptes peut débloquer un visiteur bloqué.

- Les correspondances d'e-mail dans une liste de surveillance de personnes ne peuvent pas être réglées sur **Toujours autoriser**.
- Les correspondances d'entrées dans une liste de surveillance de sociétés ne peuvent pas être réglées sur **Toujours autoriser**.
- Les correspondances d'entrées dans une liste de surveillance de notification ne peuvent pas être réglées sur **Toujours autoriser**.

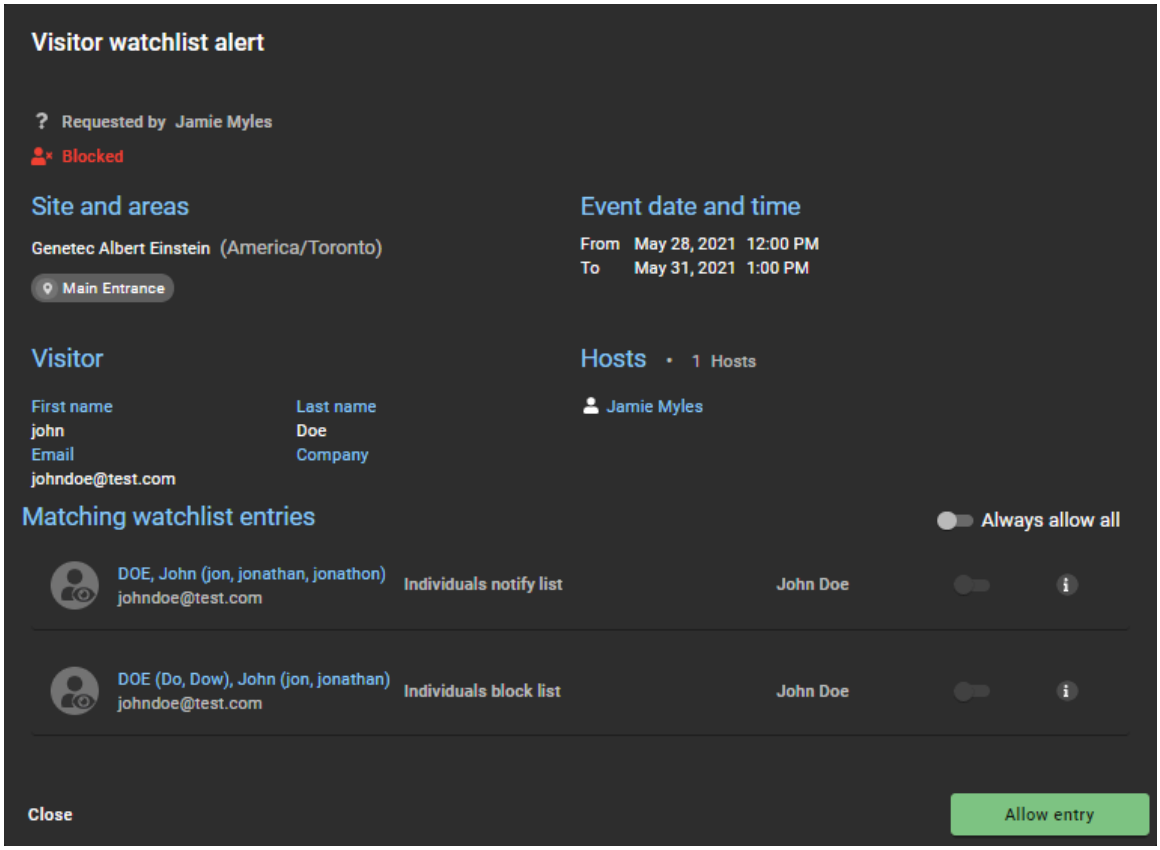
Utilisez cette procédure pour ajouter des adresses e-mail similaires ou des faux positifs que vous souhaitez autoriser une fois ou indéfiniment. Par exemple, une correspondance possible avec le même nom, mais qui correspond à une autre personne avec une autre adresse e-mail qui doit être autorisée.

Procédure

1 Dans l'e-mail *Alerte de liste de surveillance pour <personne ou société d'intérêt>*, cliquez sur **AFFICHER LES DÉTAILS DU BLOCAGE**.



La boîte de dialogue d'alerte de liste de surveillance de visiteurs est affichée sur le portail Web Genetec ClearID[MC].



a) Dans la section *Entrées de liste de surveillance correspondantes*, survolez l'icône d'information pour afficher les détails de l'entrée associée au visiteur.

b) (Facultatif) Cliquez sur une entrée de liste de surveillance pour l'ouvrir et consulter les informations détaillées.

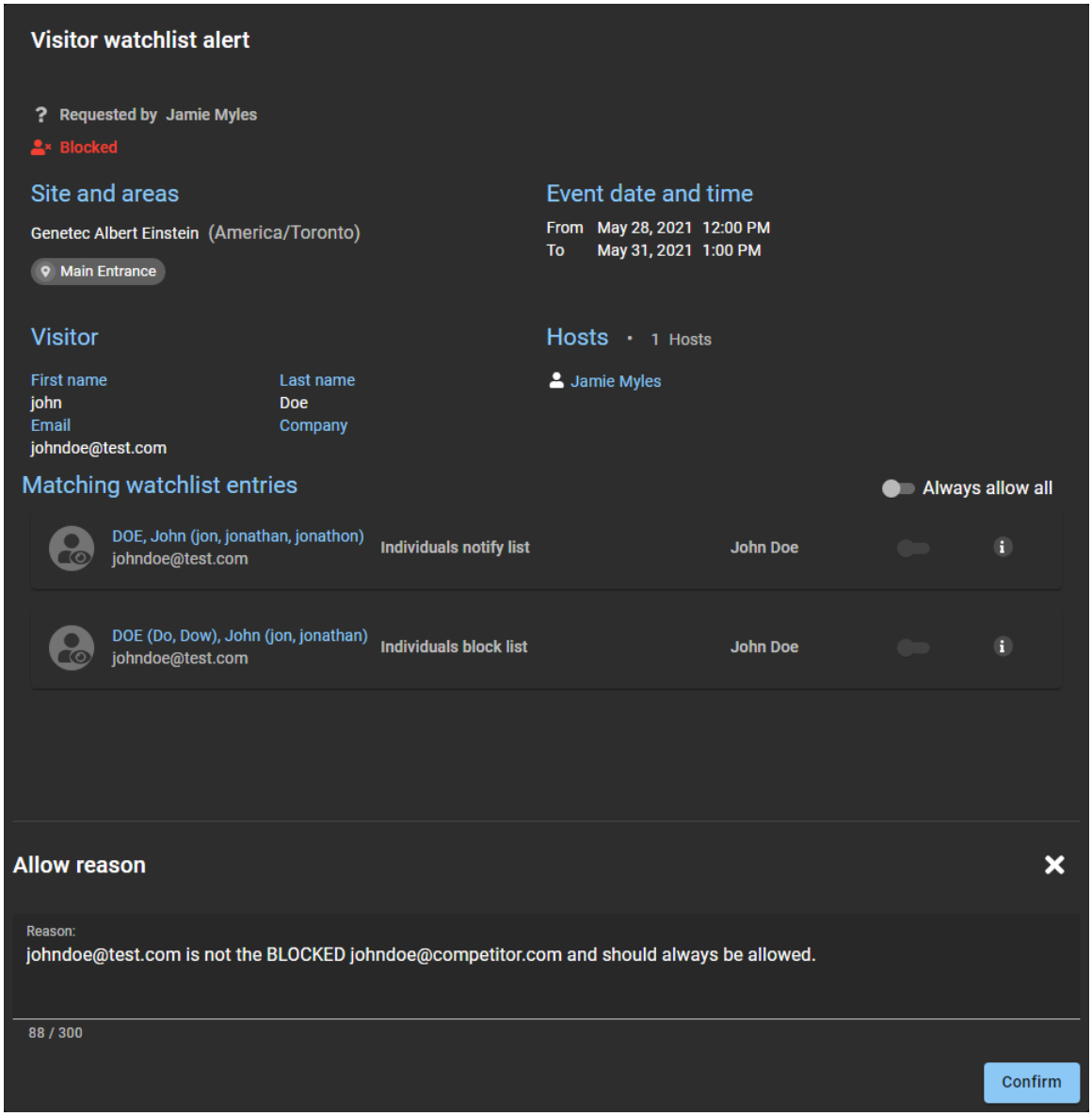
L'entrée de liste de surveillance est ouverte dans un nouvel onglet de navigateur.

2 Indiquez si vous souhaitez accorder l'accès une seule fois ou indéfiniment. Procédez de l'une des manières suivantes :

- Si vous ne souhaitez accorder l'accès qu'une seule fois pour cette alerte de liste de surveillance de visiteurs, cliquez sur **Accorder l'accès**.
- Si vous souhaitez toujours autoriser les entrées qui correspondent à ce visiteur à l'avenir, dans la liste **Entrées de liste de surveillance correspondantes**, activez le commutateur **Toujours autoriser** pour chaque entrée que vous souhaitez autoriser, puis cliquez sur **Accorder l'accès**.
- Si vous souhaitez autoriser toutes les entrées qui correspondent à ce visiteur à l'avenir, dans la liste **Entrées de liste de surveillance correspondantes**, activez le commutateur **Toujours autoriser tout**, puis cliquez sur **Accorder l'accès**.

  REMARQUE : Seules les commandes de réglage des entrées de liste de surveillance qui peuvent être réglées sur **Toujours autoriser** sont activées.

3 Dans le champ **Motif**, entrez la raison pour laquelle le visiteur a été débloqué et autorisé à poursuivre sa visite.



4 (Facultatif) Dans la section **Motif d'autorisation**, cliquez sur ✕ pour annuler le déblocage, puis cliquez sur **Fermer**.

5 Cliquez sur **Confirmer**.

11

Contrôle d'accès basé sur les rôles

Découvrez le contrôle d'accès basé sur les rôles.

Cette section aborde les sujets suivants:

- " À propos du contrôle d'accès basé sur les rôles ", page 469
- " Ajouter des rôles ", page 472
- " Configurer les responsables de rôles ", page 474
- " Configurer les stratégies de contrôle d'accès basé sur les rôles ", page 476
- " Ajouter des attributs de provisionnement personnalisés à une identité ", page 482
- " Ajouter des membres aux rôles ", page 484
- " À propos du rapport d'activité de rôle ", page 486
- " Afficher un rapport d'activité de rôle ", page 487

À propos du contrôle d'accès basé sur les rôles

Le contrôle d'accès basé sur les rôles utilise des identités avec divers attributs pour gérer automatiquement le contrôle d'accès. Définir des stratégies de provisionnement permet de s'assurer que les niveaux d'autorisation d'accès des membres de votre organisation restent à jour. Si un employé change de poste, de service ou de site, le système ajuste automatiquement ses accès lorsque ses attributs d'identité sont modifiés.

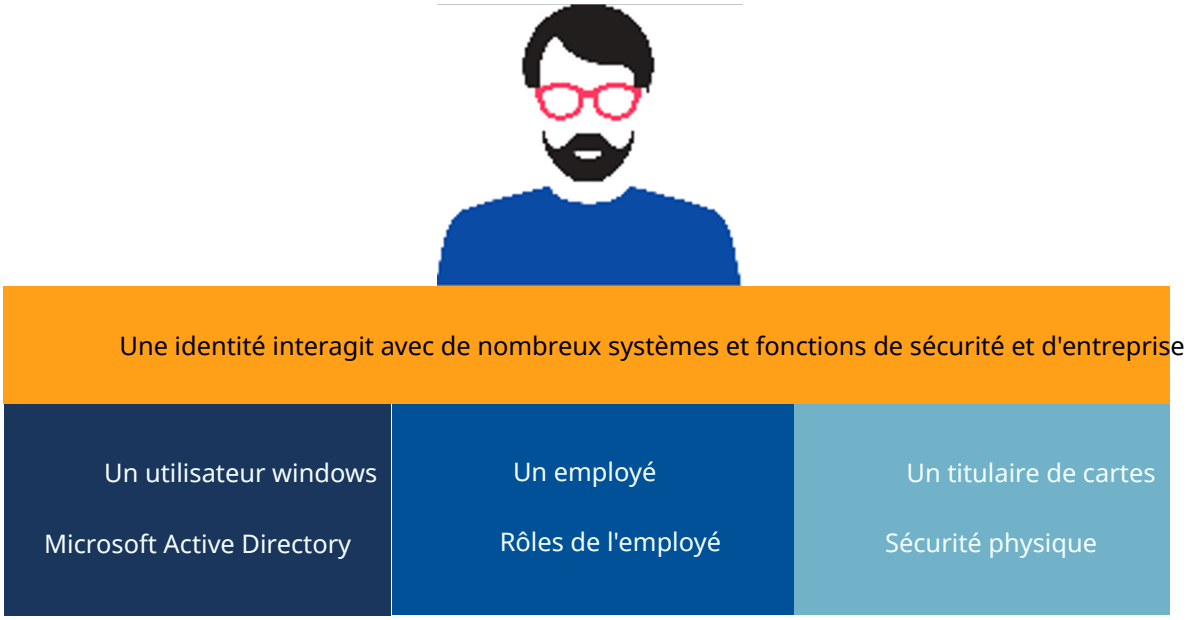
Les stratégies de provisionnement basées sur les rôles peuvent être utilisées pour attribuer ou révoquer automatiquement l'accès dans différentes situations :

- Accorder ou révoquer l’accès en fonction de l’emplacement géographique des employés.
- Accorder ou révoquer l'accès en fonction de *rôles* spécifiques, de postes ou de supérieurs hiérarchiques au sein de l'entreprise.
- Accorder l'accès à un secteur uniquement si les personnes ont des qualifications ou certifications spécifiques.
- Accorder ou révoquer l'accès en fonction d'une liste d'attributs personnalisés synchronisés à partir d'une source externe.

REMARQUE : Bien d'autres scénarios sont possibles, en fonction de vos exigences et de votre configuration. Vous pouvez également ajouter, modifier ou supprimer les accès manuellement à tout instant.

Qu'est-ce qu'une identité ?

Dans Genetec ClearID[MC], une identité représente une personne et détermine ce qu’elle peut faire sur une variété de plates-formes, de systèmes de sécurité, de systèmes d’entreprise et de fonctions. Chaque identité a un ou plusieurs badges de contrôle d'accès (identifiants) et est associée à un titulaire de cartes dans Synergis[MC]. Par exemple, les identifiants peuvent être un utilisateur Windows (Active Directory), un employé (ressources humaines et paie), un vendeur (outils CRM ou de création de devis) et un titulaire de cartes (sécurité physique).



Plus qu'un profil d'un titulaire de cartes, une identité est un profil numérique unique. L'identité représente une personne qui dispose d'un badge de contrôle d'accès, qui utilise le portail en libre-service, ou les deux.

REMARQUE : Dans ClearID, un visiteur ou un titulaire de cartes temporaire n'est pas une identité.

- Une identité correspond une personne à qui un badge permanent a été attribué.
- Un visiteur correspond une personne à qui un badge papier ou temporaire a été attribué.
- Un sous-traitant peut être une identité ou un visiteur. Lorsqu'un sous-traitant est défini en tant que visiteur, il reçoit une carte HID valable un jour et saisie en tant que visiteur dans ClearID.

L'accès est généralement permanent pour les employés, semi-permanent pour les sous-traitants et temporaire pour les invités.

Attributs d'identité

Dans Genetec ClearID^{MC}, les attributs sont les traits ou les caractéristiques qui forment une identité. Parmi les exemples d'attributs figurent le service, l'emplacement, le rôle, l'ancienneté, le niveau de rémunération, les certifications de formation et l'habilitation de sécurité.

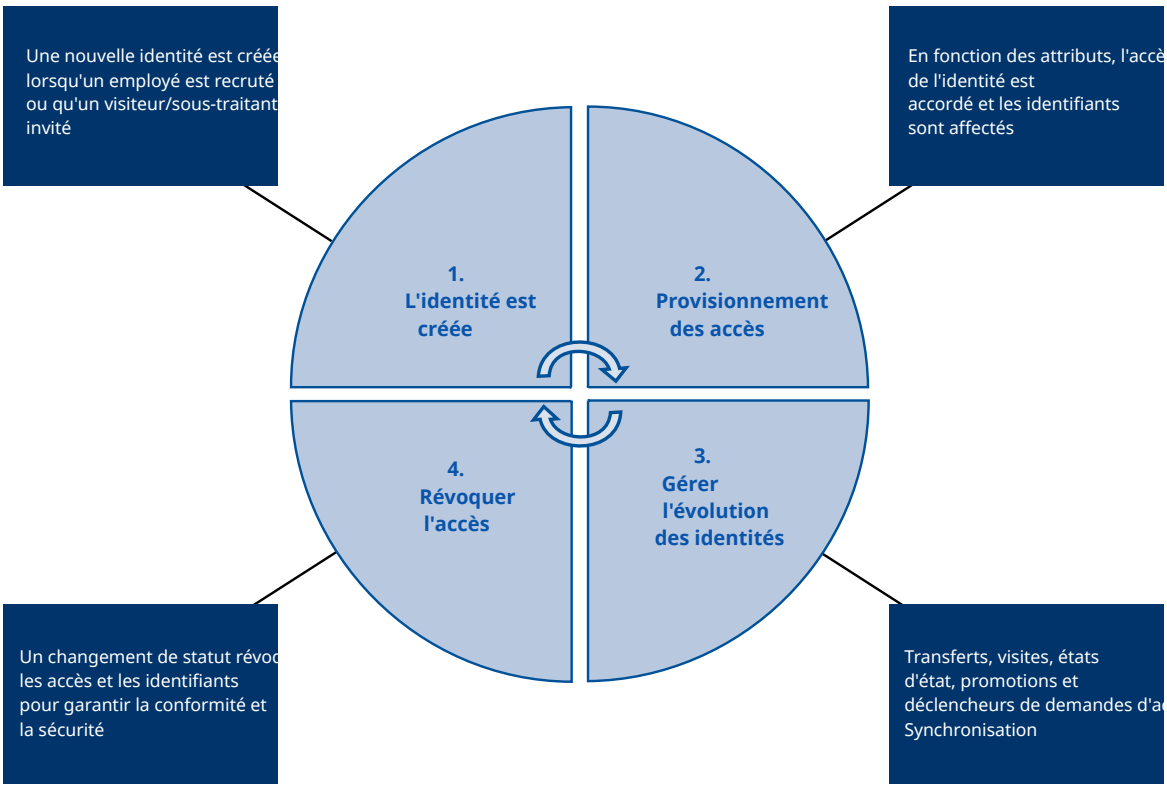
Le contrôle d'accès basé sur les rôles repose sur des **stratégies** (*règles de provisionnement*) qui attribuent automatiquement des droits aux **identités** (personnes) en fonction des **attributs** (traits ou caractéristiques).

Dans Genetec ClearID^{MC}, un responsable de rôle est une identité qui a autorité sur les personnes affectées à un rôle. Un responsable de rôle peut ajouter des personnes à un rôle et en supprimer. Il est également chargé de l'approbation des analyses d'accès.

Le cycle de vie d'une identité

Dans ClearID, le cycle de vie complet d'une identité peut être géré automatiquement.

Le diagramme suivant illustre le cycle de vie d'une identité lorsqu'une stratégie de provisionnement est activée :


Une nouvelle identité est créée lorsqu'un employé est recruté ou qu'un visiteur/sous-traitant invité
1. L'identité est créée
2. Provisionnement des accès
En fonction des attributs, l'accès de l'identité est accordé et les identifiants sont affectés
4. Révoquer l'accès
3. Gérer l'évolution des identités
Un changement de statut révoc les accès et les identifiants pour garantir la conformité et la sécurité
Transferts, visites, états d'état, promotions et déclencheurs de demandes d'a Synchronisation

Ajouter des rôles

Avant de pouvoir configurer vos stratégies de contrôle d'accès automatique basées sur les rôles, vous devez définir vos rôles.

Avant de commencer

Familiarisez-vous avec le contrôle d'accès basé sur les rôles.

À savoir

Dans Genetec ClearID[MC], un rôle est un groupe de personnes dotées des mêmes accès. Une personne peut se voir attribuer plusieurs rôles. Les rôles sont associés aux groupes de titulaires de cartes dans Synergis[MC]. Un responsable de rôle contrôle les accès aux groupes.

- Seuls les administrateurs de comptes peuvent ajouter des rôles.
- Pensez à créer des rôles pour chaque service, groupe ou poste dans votre organisation. Par exemple, vous pouvez créer des rôles pour les services ressources humaines, informatique, marketing, les équipes de développeurs, le service de traitement des salaires, les sous-traitants, etc.

Procédure

1 Sur la page d'accueil, cliquez sur **Organisation** > **Rôles**.

2 Cliquez sur **Ajouter un rôle**.

3 Dans la section *Général*, remplissez les champs.

a) Saisissez un nom pour le rôle.

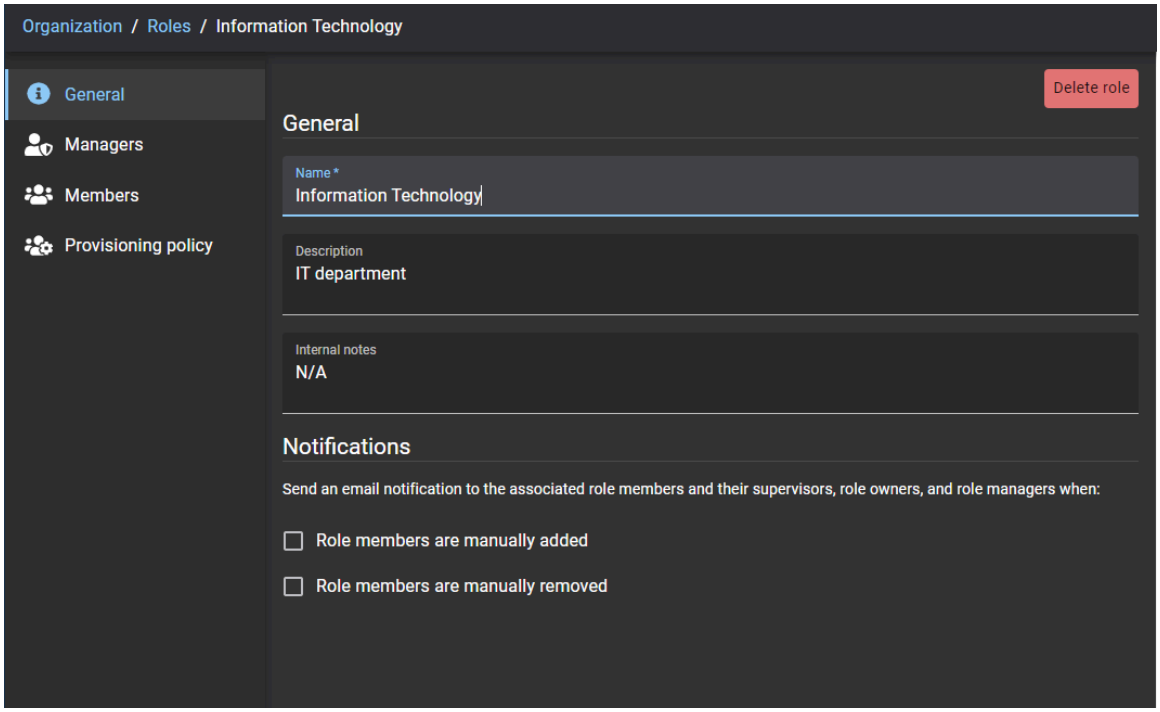
b) Saisissez une description significative.

c) Ajoutez des notes internes.

REMARQUE : Le champ notes internes permet de consigner des instructions ou des informations spéciales qui ne sont visibles que par l'administrateur du compte, le propriétaire du rôle et le gestionnaire du rôle. Les autres utilisateurs du système ne peuvent pas voir les notes internes. Le champ notes internes peut par exemple contenir les informations suivantes :

Only permanent employees based in Montreal should be in this role. Discuss with security before adding employees to this role.

4 (Facultatif) Dans la section *Notifications*, sélectionnez les options de notification nécessaires.



5 Cliquez sur **Enregistrer**.

Lorsque vous avez terminé

Configurez vos stratégies de contrôle d'accès basées sur les rôles.

Rubriques connexes

Afficher un rapport d'activité de rôle, page 487

Configurer les responsables de rôles

Les responsables de rôles sont composés de deux rôles distincts : les propriétaires de rôles et les responsables de rôles. Avant de pouvoir définir des stratégies pour un rôle, ou encore ajouter ou supprimer des identités d'un rôle, vous devez désigner un ou plusieurs employés en tant que responsables de rôles.

Avant de commencer

Ajoutez vos rôles.

À savoir

- Seuls les propriétaires de rôles peuvent configurer les responsables de rôles.

Procédure

1 Sur la page d'*accueil*, cliquez sur **Organisation** > **Rôles** et sélectionnez un rôle.

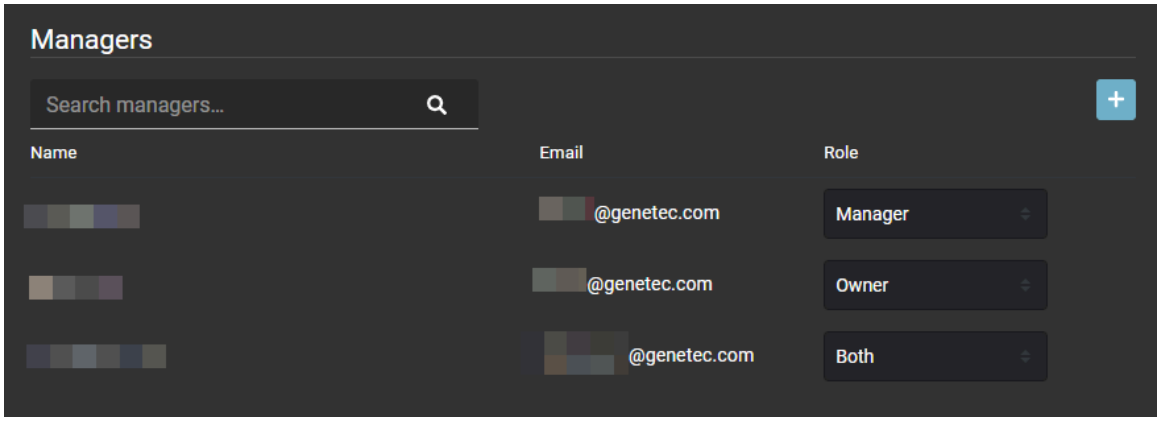
2 Cliquez sur **Responsables** pour configurer les paramètres du responsable de rôles.

a) Utilisez le champ de recherche pour trouver des gestionnaires existants, ou cliquez sur **Ajouter** ( ).

b) Sélectionnez le ou les utilisateurs requis, puis cliquez sur **Confirmer**.

3 Choisissez le type de **Rôle** pour les utilisateurs que vous venez d'ajouter parmi les options suivantes :

- **Responsable :** Un responsable de rôle est une identité qui a autorité sur les personnes affectées à un rôle. Un responsable de rôle peut ajouter des personnes à un rôle et en supprimer.
- **Propriétaire :** Un propriétaire de rôle est chargé d'affecter les responsables de rôle et de configurer les politiques basées sur les rôles.
- **Les deux :** Utilisez cette option lorsqu'une personne est responsable de la gestion des rôles, de l'affectation des responsables de rôle et de la configuration des politiques.



4 (Facultatif) Pour supprimer les gestionnaires dont vous n'avez plus besoin, placez la souris sur un nom et cliquez sur .

5 Cliquez sur **Enregistrer**.

Les personnes sélectionnées sont ajoutées à la liste en tant que gestionnaires, propriétaires ou les deux.

Lorsque vous avez terminé

Ajoutez des membres de rôle.

Rubriques connexes

Afficher un rapport d'activité de rôle, page 487

Configurer les stratégies de contrôle d'accès basé sur les rôles

Pour vous assurer que les membres de votre organisation disposent toujours de niveaux d'autorisation d'accès à jour, vous pouvez définir des règles de provisionnement qui affectent automatiquement les personnes à des rôles spécifiques en fonction de leurs attributs d'identité. Si un employé change de poste, de service ou intègre un autre site, le système ajuste automatiquement son accès.

Avant de commencer

- Ajoutez vos rôles.

À savoir

- Seuls les administrateurs de compte ou les propriétaires de rôles peuvent créer ou modifier des stratégies de provisionnement qui associent automatiquement les personnes à un rôle spécifique.
- Un maximum de 25 stratégies avec un maximum de 25 conditions de stratégie peut être défini pour chaque rôle.

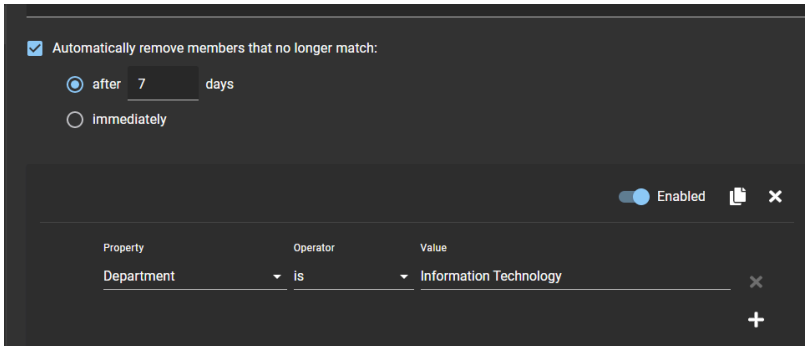
Procédure

1 Sur la page d'*accueil*, cliquez sur **Organisation** > **Rôles** et sélectionnez un *Rôle*.

2 Cliquez sur **Stratégie de provisionnement** et cliquez ou faites glisser le curseur sur **Actif**.

3 Dans le champ *Description*, décrivez adéquatement la stratégie.

4 (Facultatif) Configurez les réglages de suppression automatique des membres du rôle :



a) Cochez la case **Supprimer automatiquement les membres qui ne correspondent plus**.

b) Indiquez quand vous souhaitez supprimer automatiquement les membres du rôle. Choisissez l'une des options suivantes :

- Après un nombre de jours prédéfini. La valeur par défaut est de 7 jours.
- Immédiatement.

Par exemple pour un rôle SI qui donne accès aux salles des serveurs. Lorsqu'un membre du rôle SI évolue vers un poste de développeur, il aura peut-être besoin d'accéder à la salle des serveurs pendant 7 jours à des fins d'assistance ou de passation de pouvoir. Les membres sont supprimés du rôle lorsque leurs réglages d'identité ne correspondent plus aux réglages de stratégies de contrôle d'accès basé sur les rôles.

5 Ajoutez les règles de stratégie pour le rôle que vous configurez.

a) Sélectionnez le type de **Propriété** dont vous avez besoin.

Les types de propriétés affichés ici sont les attributs de champs d'identité par défaut disponibles dans la section **Général** de toute identité.

REMARQUE : Vous ne pouvez sélectionner que les rôles pour lesquels vous êtes un responsable de rôle.

- **Société :** Saisissez le nom de l'entreprise.
- **Pays :** Sélectionnez un pays dans la liste.
- **Département :** Saisissez un nom de service.
- **Description :** Saisissez une description.
- **Délai d'accès prolongé :** Utilisé pour sélectionner True ou False.
- **ID externe :** Entrez un ID externe
- **Intitulé du poste :** Saisissez un poste.
- **Site principal :** Entrez ou sélectionnez le lieu du site principal.
- **Attributs de provisionnement :** Saisissez un attribut de provisionnement personnalisé et appuyez sur Entrée. Voici quelques exemples : vérification des antécédents, test de dépistage de drogues et d'alcool, NDA, formation de sécurité, formation initiale au site, etc.
- **État :** Choisissez **Actif** ou **Inactif**.
- **Nom du superviseur :** Saisissez un nom.
- **Superviseurs :** Ajoutez plusieurs superviseurs.
- **Code type d'employé :** Saisissez un code de type de travailleur
- **Description du type de travailleur :** Entrez une description significative pour le type de travailleur.

b) Sélectionnez un **opérateur** parmi les options suivantes :

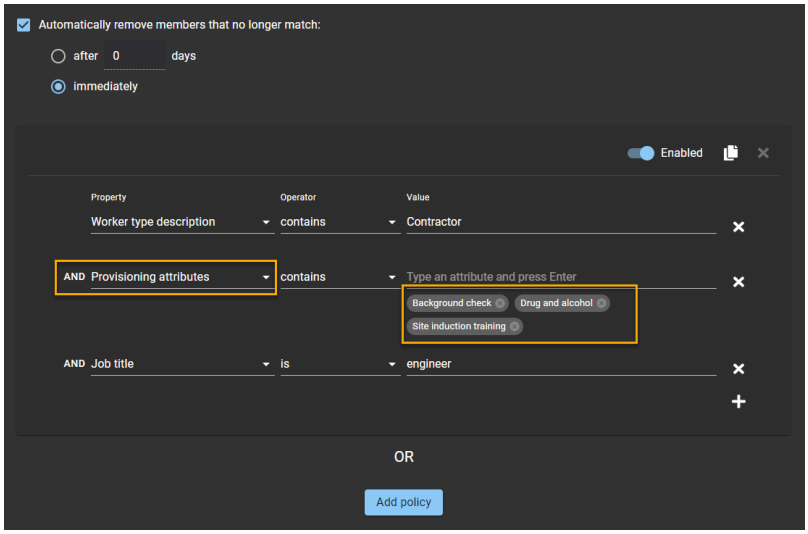
- Contient
- Ne contient pas
- Est
- N'est pas

REMARQUE : Les **opérateurs** affichés varient en fonction du type de **Propriété** que vous sélectionnez.

a) Saisissez une valeur ou sélectionnez une option relative au type de **Propriété** que vous avez sélectionné.

REMARQUE : Les options ou les champs de **Valeur** affichés varient en fonction du type de **Propriété** que vous sélectionnez.

6 (Facultatif) Ajoutez des attributs de provisionnement personnalisés à votre stratégie de provisionnement.
   a) Sélectionnez la propriété **Attributs de provisionnement**.
   b) Sélectionnez un **opérateur** parmi les options suivantes :
      - Contient
      - Ne contient pas
   c) Entrez les valeurs d'attributs personnalisés dont vous avez besoin.



   REMARQUE : Pour les attributs personnalisés, la règle de provisionnement n'est déclenchée que lorsqu'une identité intègre au moins toutes les valeurs d'attributs de provisionnement spécifiées dans cette stratégie.

7 (Facultatif) Pour désactiver temporairement une règle de stratégie, déplacez le curseur de la valeur **Activé** sur **Désactivé**.

8 (Facultatif) Cliquez sur **Copier la stratégie** ( ) lorsque vous souhaitez copier une règle ou un ensemble de règles.

9 (Facultatif) Cliquez sur pour supprimer toutes les règles de stratégie dont vous n'avez plus besoin.

10 Cliquez sur **Enregistrer**.

Les utilisateurs peuvent à présent être automatiquement affectés à des rôles ou supprimés de rôles particuliers en fonction de leurs attributs d'identité.

Lorsque vous avez terminé

Ajoutez des responsables de rôles.

Rubriques connexes

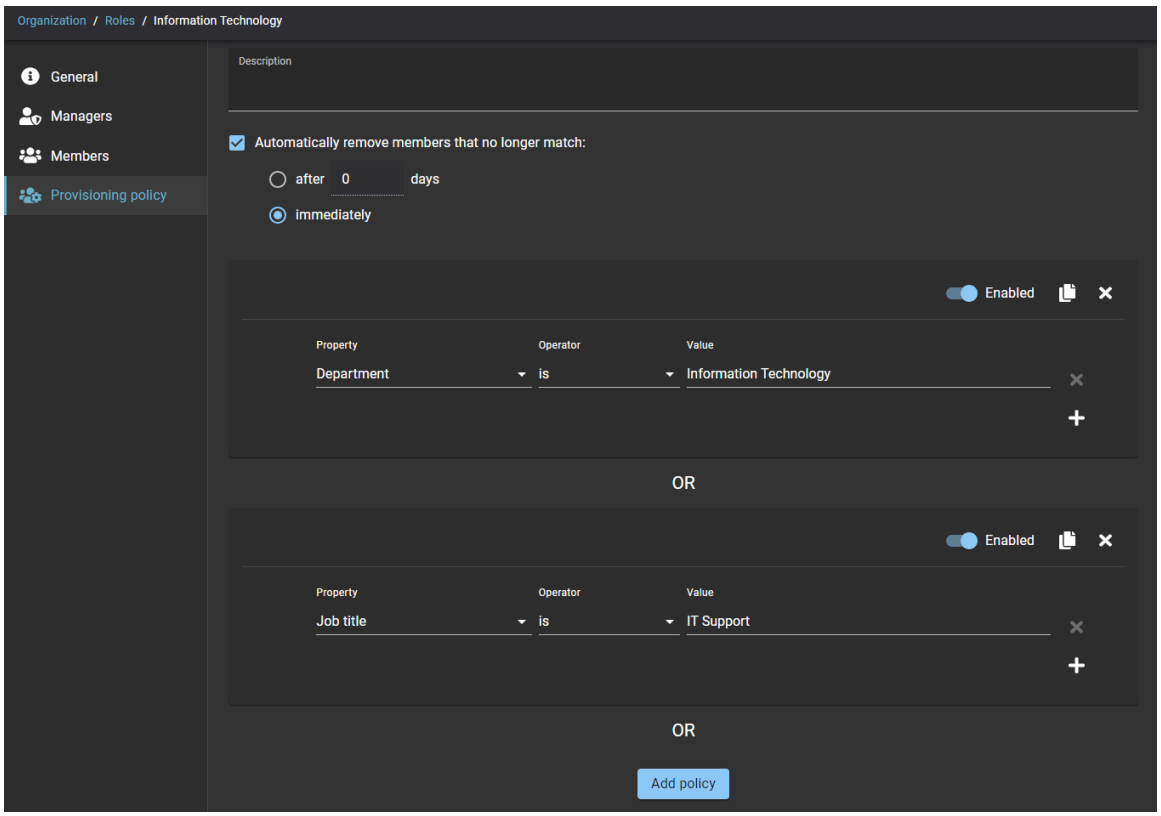
Ajouter des rôles, page 472
Champs d'identité, page 115

Scénario 1 : Ajouter des employés à un rôle d'informaticien

Dans cet exemple, une stratégie est utilisée pour affecter automatiquement des employés à un rôle d'informaticien en fonction de leurs attributs d'identité.

L'exemple suivant montre une stratégie configurée pour ajouter automatiquement des employés à un rôle d'informaticien si les critères suivants sont réunis :

- Service informatique
- Le titre du poste est Support informatique.

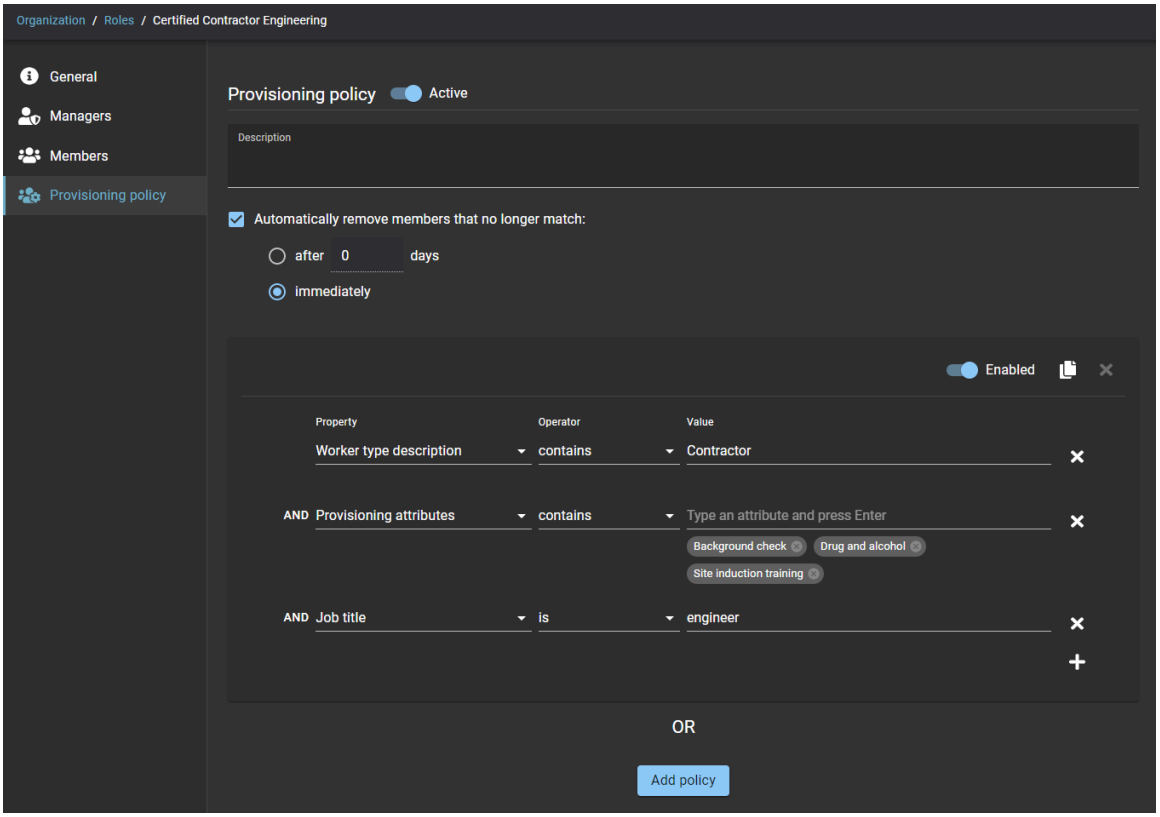


Scénario 2 : Ajouter des sous-traitants à un rôle d'ingénieur certifié

Dans cet exemple, une stratégie est utilisée pour affecter automatiquement des sous-traitants à un rôle d'ingénieur certifié en fonction de leurs attributs d'identité.

L'exemple suivant montre une stratégie configurée avec des attributs personnalisés pour ajouter automatiquement des sous-traitants à un rôle d'ingénieur certifié si les critères suivants sont réunis :

- L'identité contient un sous-traitant de type travailleur
- Des attributs de provisionnement existent
- L'intitulé du poste est ingénieur.

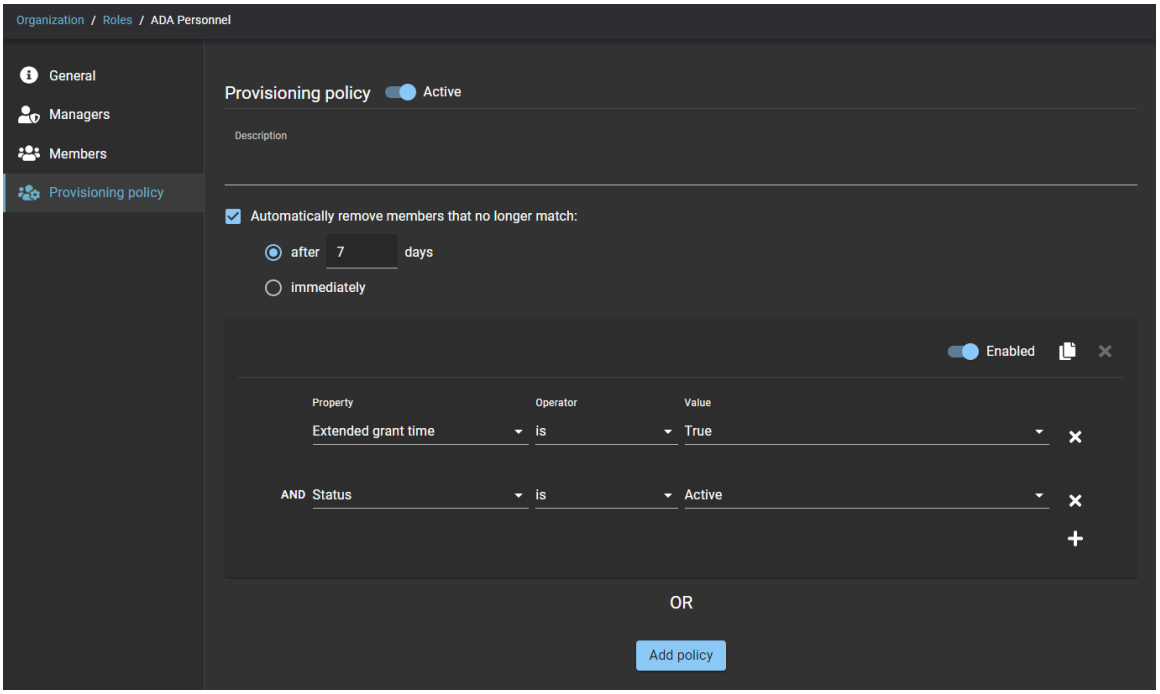


Scénario 3 : Ajouter des employés à un rôle de personnel ADA

Dans cet exemple, une stratégie est utilisée pour affecter automatiquement des employés qui ont besoin d'une assistance en matière d'accès à un rôle de personnel ADA en fonction de leurs attributs d'identité.

L'exemple suivant montre une stratégie configurée pour ajouter automatiquement des employés à un rôle de personnel ADA si les critères suivants sont réunis :

- La propriété de délai d'accès prolongé est trouvée.
- Leur état est actif.


Organization / Roles / ADA Personnel
General
Managers
Members
Provisioning policy
Provisioning policy
Active
Description
Automatically remove members that no longer match:
after 7 days
immediately
Enabled
Property
Operator
Value
Extended grant time
is
True
AND
Status
is
Active
OR
Add policy

Ajouter des attributs de provisionnement personnalisés à une identité

Si les attributs par défaut des stratégies Genetec ClearID[MC] ne répondent pas à vos besoins, vous pouvez affecter manuellement des attributs de provisionnement personnalisés à l'enregistrement d'identité d'un employé. Ces attributs peuvent ensuite être utilisés dans une stratégie de contrôle d'accès basée sur les rôles.

Avant de commencer

- Ajoutez vos rôles.

À savoir

- Seuls les administrateurs de comptes peuvent ajouter des attributs personnalisés.
- Les attributs personnalisés sont généralement utilisés lorsque vous importez ou synchronisez vos attributs depuis une source externe.
- L'état actuel des attributs personnalisés peut être géré à l'aide d'une intégration, et ceux qui deviennent obsolètes peuvent être supprimés automatiquement.
- Les attributs personnalisés peuvent également être ajoutés ou supprimés manuellement.

Voici quelques exemples d'attributs de provisionnement personnalisés : vérification des antécédents, test de dépistage de drogues et d'alcool, NDA, formation à la sécurité, formation à l'arrivée sur un site, etc.

Procédure

1 Sur la page d'*accueil*, cliquez sur **Entreprise** > **Identités** et sélectionnez une identité.

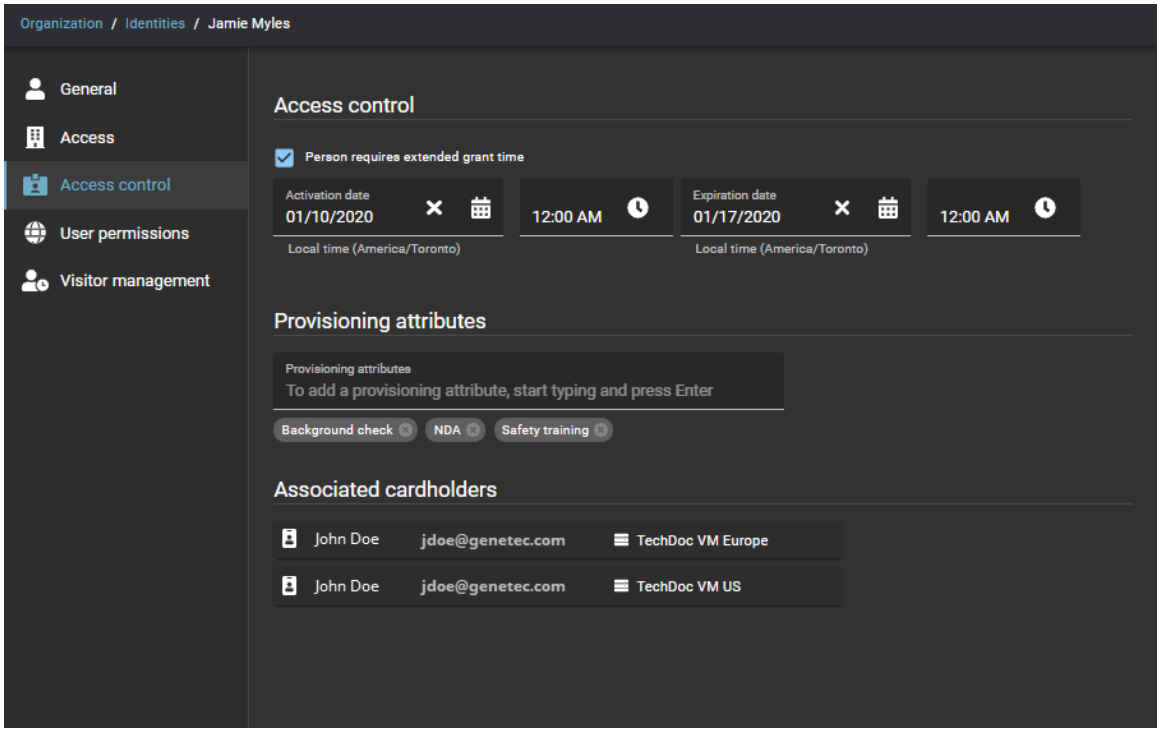
2 Cliquez sur **Contrôle d'accès**.

3 Dans la section *Attributs de provisionnement*, commencez à taper et appuyez sur Entrée pour ajouter vos attributs personnalisés.

4 (Facultatif) Ajoutez des attributs personnalisés supplémentaires si nécessaire.

5 (Facultatif) Cliquez sur ✕ pour supprimer les attributs ayant expiré ou qui ne sont plus pertinents.

6 Cliquez sur **Enregistrer**.



Ajouter des membres aux rôles

Pour ajouter des membres de rôle qui ne correspondent pas aux critères de la stratégie de provisionnement basée sur les rôles par défaut, ajoutez-les manuellement.

Avant de commencer

Ajoutez des responsables de rôles.

À savoir

- Seuls les responsables de rôles peuvent ajouter des membres à un rôle.
- Lorsqu'une stratégie de provisionnement est activée, les membres du rôle sont ajoutés automatiquement en fonction des règles définies dans la stratégie. Les membres qui sont ajoutés automatiquement ont la mention Stratégie de provisionnement dans la colonne **Autorisé par**.
- Les membres peuvent aussi être ajoutés manuellement. Les membres qui sont ajoutés manuellement ont la mention Manuel dans la colonne **Autorisé par**.
- Les membres qui correspondent à une stratégie de provisionnement sont verrouillés et ne peuvent pas être supprimés.
- Les membres qui ne correspondent plus à une stratégie de provisionnement sont immédiatement déverrouillés. Ils sont supprimés automatiquement à l'issue du délai spécifié dans une stratégie de provisionnement.

Procédure

1 Sur la page d'*accueil*, cliquez sur **Organisation** > **Rôles** et sélectionnez un rôle.

2 Cliquez sur **Membres** pour configurer la liste des membres du rôle.

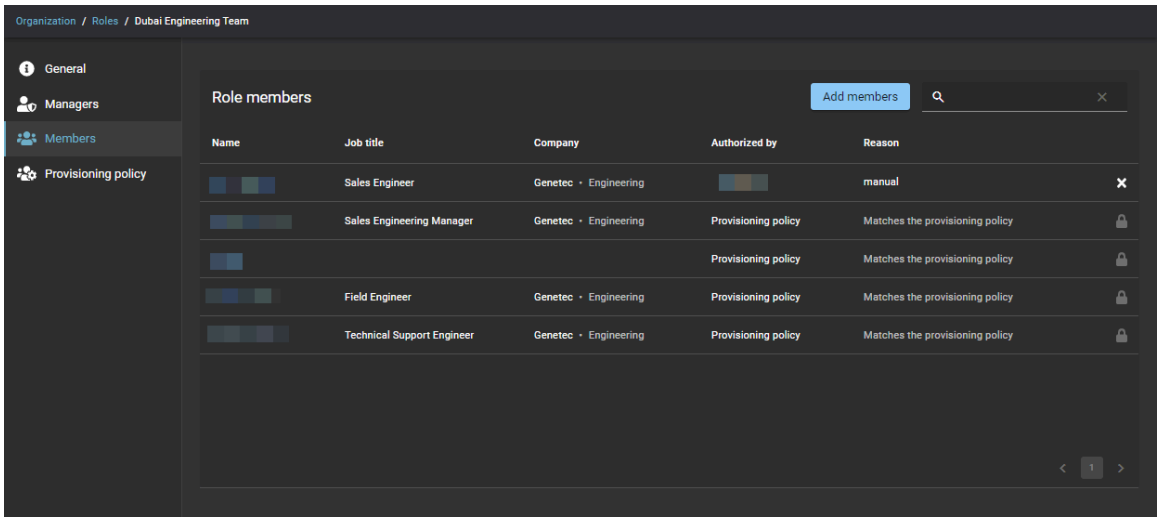
3 Cliquez sur **Ajouter des membres**.

4 Recherchez ou sélectionnez un ou plusieurs membres.

5 Entrez un `motif` et cliquez sur **Ajouter**.

L'exemple suivant illustre les membres du rôle Équipe d'ingénierie de Dubaï.

REMARQUE : La colonne **Autorisé par** contient deux membres qui ont été ajoutés automatiquement (Stratégie de provisionnement) et un membre qui a été ajouté manuellement (Manuel).



CONSEIL : Vous pouvez cliquer sur le texte bleu dans la colonne **Nom** pour afficher ou modifier les détails de l'identité.

6 (Facultatif) Pour supprimer immédiatement les membres de rôle qui ne répondent plus aux critères de la stratégie ou qui ont été ajoutés manuellement, cliquez sur ✕ puis sur **Supprimer**.

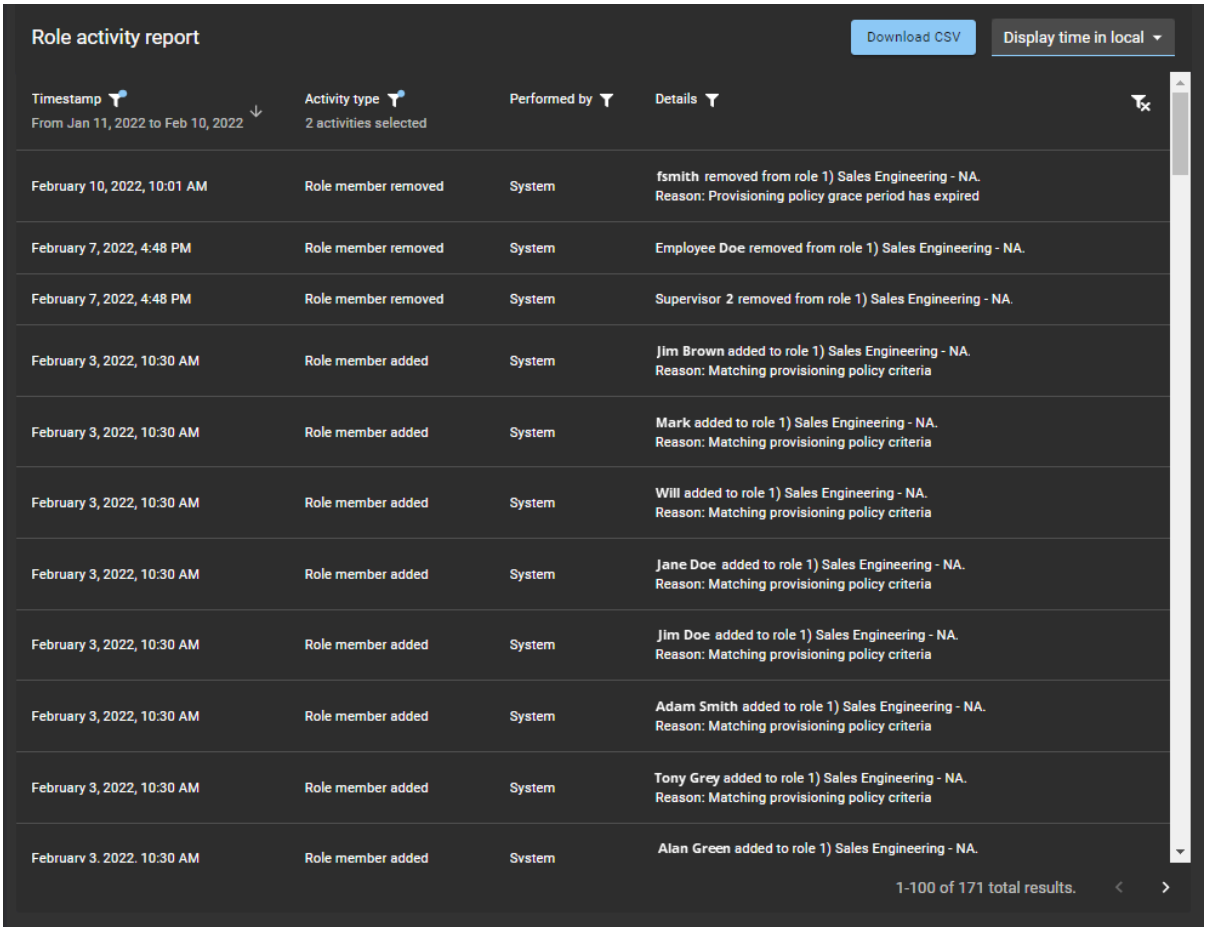
Rubriques connexes

Afficher un rapport d'activité de rôle, page 487

À propos du rapport d'activité de rôle

Dans Genetec ClearID[MC], le rapport d'activité de rôle est un historique de toutes les activités associées aux rôles. Le rapport contient des informations d'horodatage, de type d'activité, sur les personnes ayant effectué l'activité, ainsi qu'une section détails qui contient des informations de motif.

Rapport d'activité de rôle



Le rapport d'activité de rôle permet aux administrateurs de comptes d'examiner toutes les activités associées aux rôles. Lorsque le rapport est consulté par un gestionnaire ou un propriétaire de rôle, seule l'activité associée à leurs rôles est affichée. Par exemple, accès au rôle accordé ou supprimé, responsable de rôle ajouté ou supprimé, propriétaire de rôle ajouté ou supprimé et membre de rôle ajouté ou supprimé.

Des filtres peuvent être utilisés pour affiner le résultat de la recherche par horodatage, type d'activité, effectué par et détails.

Rubriques connexes

Afficher un rapport d'activité de rôle, page 487

Afficher un rapport d'activité de rôle

En tant *qu'administrateur de comptes*, *gestionnaire*de rôle ou *propriétaire de rôle*, vous pouvez afficher une trace d'audit des activités liées au rôle, telles que les informations horodatage , le type d'activité, la personne qui a effectué l'activité, etc.

Avant de commencer

Vous devez être *administrateur de comptes*, gestionnaire de *rôle*ou *propriétaire de rôle* pour afficher un **rapport d'activité de rôle** et consulter les informations de trace d'audit pour les activités liées au rôle.

Procédure

1 Sur la page d'*accueil*, cliquez sur **Organisation** > **Rôles**.

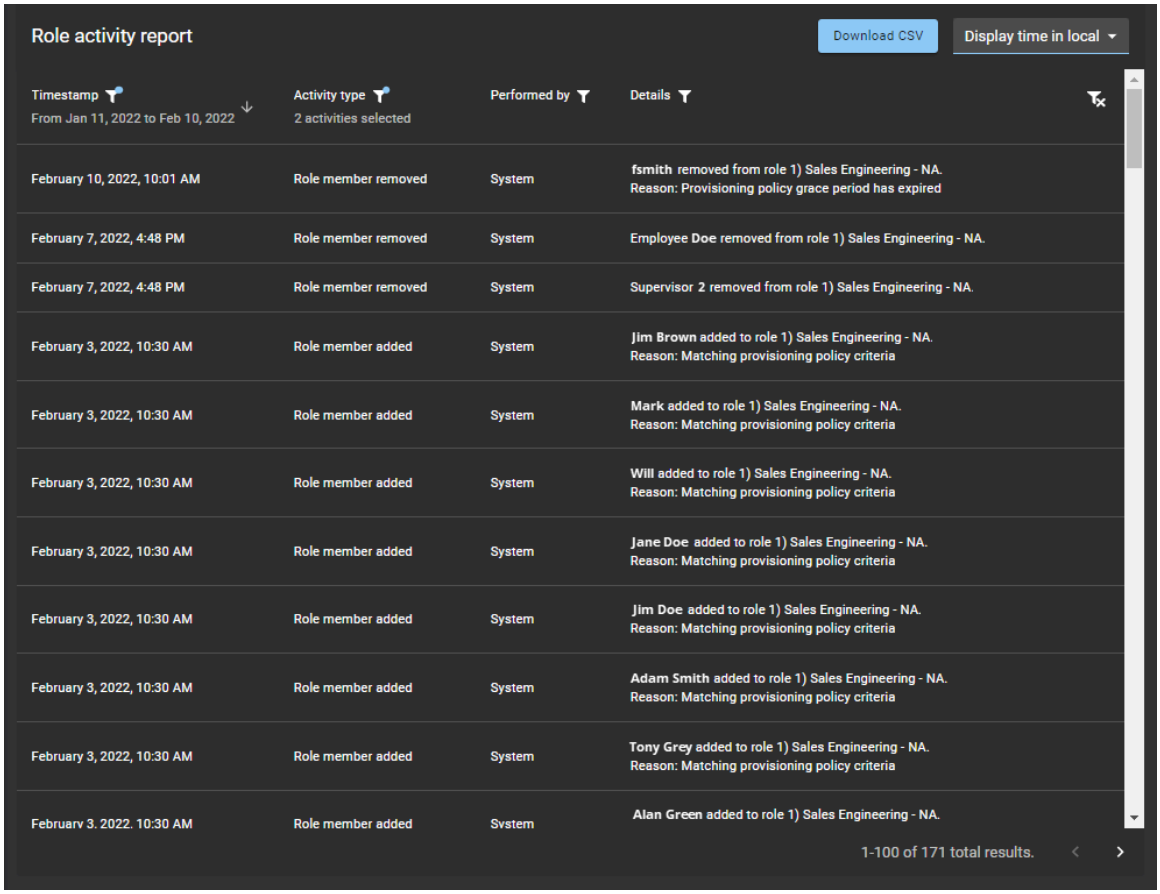
2 Recherchez ou sélectionnez le rôle dont vous avez besoin dans la colonne **Nom**.

3 Cliquez sur **Activité de rôle**.

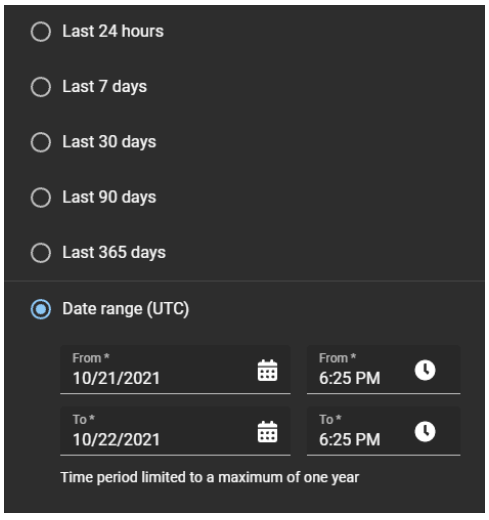
4 Dans le menu **Heure d'affichage**, sélectionnez le format d'heure d'affichage requis.

- **Heure d'affichage locale :** Les heures d'affichage sont affichées via l'heure du système de l'ordinateur de l'utilisateur connecté.
- **Heure d'affichage UTC :** Les heures du rapport sont affichées au format UTC (temps universel coordonné).

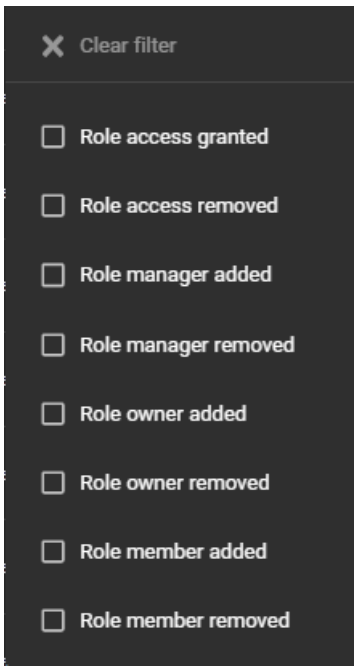
5 Filtrez le rapport en fonction de vos critères requis :



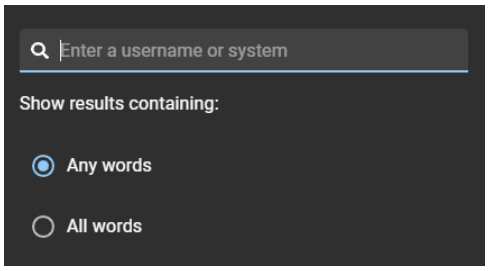
- **Horodatage :** Dans la colonne **Horodatage**, cliquez sur pour filtrer le résultat par date. Sélectionnez une plage de dates prédéfinie parmi les choix disponibles, ou spécifiez une plage particulière à l'aide du sélecteur de plage de dates.



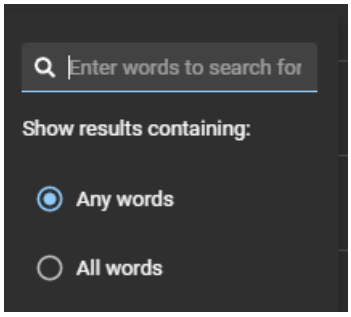
  (Facultatif) Utilisez les icônes de tri (et) pour afficher le résultat en ordre croissant ou décroissant.
- **Type d'activité :** (Facultatif) Utilisez les icônes de tri (et) pour afficher le résultat en ordre croissant ou décroissant.



- **Effectué par :** Dans la colonne **Effectué par**, cliquez sur pour ouvrir une boîte de dialogue de recherche et filtrer les résultats sur la personne ayant effectué une activité. Il peut s'agir de tâches effectuées par un utilisateur particulier ou de tâches effectuées automatiquement par le système.



- **Détails :** Dans la colonne **Détails**, cliquez sur pour ouvrir une boîte de dialogue qui permet de rechercher dans les détails ou les motifs à l'aide de critères de recherche.



- **(Facultatif) :** Cliquez pour réinitialiser les sélections de filtre.

6 Cliquez sur **Télécharger CSV** pour télécharger une copie du rapport d'activité de rôle au format CSV. Le rapport peut ensuite être utilisé à des fins d'audit, pour conserver un exemplaire physique, pour le joindre

à une demande d'audit, pour une analyse hors ligne ou encore pour traiter ou consolider les données dans un tableur pour d'autres publics.

a) Suivez les instructions dans votre navigateur pour télécharger le fichier exporté.

   Le fichier est exporté sous la forme d'un fichier *.CSV* dans le dossier de téléchargement par défaut de votre navigateur. Par défaut, le fichier exporté est créé d'après le nom de votre site. Par exemple, RoleActivity_*rolename*_*fromdate*_to_*todate*_SiteActivityReport.csv (*RoleActivity_All active contracotrs_2024-09-23.csv*).

   REMARQUE : Les colonnes et les entrées dans le fichier CSV peuvent varier en fonction des filtres sélectionnés au moment de télécharger le rapport.

Rubriques connexes

À propos du rapport d'activité de rôle, page 486
Ajouter des membres aux rôles, page 484
Configurer les responsables de rôles, page 474
Ajouter des rôles, page 472

12

Connexion à d’autres systèmes

Découvrez comment connecter ClearID à d'autres systèmes.

Cette section aborde les sujets suivants:

- " Authentifier votre connexion ", page 492
- "Configurer la synchronisation des données", page 494
- "Synchroniser les identités à l'aide d'une API", page 496
- " Synchroniser les identités à l'aide de l’intégration SCIM ", page 498
- " Synchroniser les identités avec One Identity ", page 518
- " Synchroniser les identités par LDAP ", page 569

Authentifier votre connexion

Avant de vous connecter à Genetec ClearID[MC] pour synchroniser des données ou envoyer des commandes d’API, vous devez d’abord authentifier vos applications (ou votre environnement d’API) afin que vos applications ou API puissent communiquer avec ClearID.

À savoir

Utilisez la clé d'intégration d'API pour authentifier vos applications lorsque vous exécutez des demandes dans votre compte ClearID.

- Le protocole OAUTH 2.0 est utilisé pour authentifier les communications ou connexions système non-utilisateur avec ClearID.
- Stockez votre clé de manière sécurisée et ne la partagez pas.

IMPORTANT : Lorsque vous recréez votre clé, vous devez mettre à jour les applications qui ont accès à ce compte pour utiliser la nouvelle clé.

Vous pouvez créer une intégration d'API pour authentifier les communications pour les tâches suivantes :

- Genetec ClearID[MC] API
- Intégration SCIM (System for Cross-domain Identity Management)
- Genetec ClearID[MC] One Identity Synchronization Tool (Azure AD, base de données, fichier)
- Genetec ClearID[MC] LDAP Synchronization Agent

Procédure

1 Ajouter une intégration d'API
   a) Dans ClearID, cliquez sur **Administration** > **Intégrations d'API**.
   b) Cliquez sur **Ajouter une intégration d'API**.
      - **Nom :** Saisissez un nom pour l'intégration d'API. Par exemple, Synchronisation Active Directory LDAP, Connexions utilisateur API ou Synchronisation d'une identité.
      - **Description :** Entrez une description claire de l’intégration d'API.
   c) Cliquez sur **Enregistrer**.

2 Sélectionnez un utilisateur dans la liste d'intégration d'API.
   a) Cliquez sur **Générer une clé**, puis cliquez sur **Confirmer** pour générer la clé d'authentification pour votre intégration d'API.
      ATTENTION : La clé d'intégration d’API existante est immédiatement invalidée et n'est plus récupérable.
   b) Cliquez sur **Télécharger la clé d'authentification**.
      CONSEIL : Notez l’emplacement de téléchargement du fichier pour plus tard.

      Par défaut, la clé d'authentification pour votre intégration d'API est appelée *key-systemID-APIintegrationname.json*.

Vous êtes prêt à configurer vos applications pour synchroniser des données ou envoyer des commandes d’API.

Lorsque vous avez terminé

Selon la façon dont les attributs sont configurés dans votre organisation, procédez de l'une des manières suivantes :

- Synchronisez les attributs d'identité avec des commandes d'API REST.
- Synchronisez les attributs d'identité à l’aide de l’intégration SCIM.
- Synchronisez les attributs d'identité via One Identity (Azure AD, Base de données, Fichier).
- Synchronisez les attributs d'identité par LDAP.

Rubriques connexes

À propos de la sécurité des informations dans ClearID, page 9
Se connecter à ClearID, page 34

Configurer la synchronisation des données

Configurer la synchronisation des données dans Genetec ClearID[MC] nécessite l’apprentissage de certains concepts, la configuration de la solution de synchronisation pour vos données d'identité, et les options d'intégration des webhooks pertinentes pour votre organisation.

1. Examinez les exigences de ports du pare-feu.
2. Connectez-vous à ClearID.
3. Accordez l’accès au portail web.
4. Authentifiez vos connexions système non utilisateur pour synchroniser les données ou transmettre des commandes d’API.
5. Choisissez une solution de synchronisation pour vos données d'identité :
   - Synchronisez les attributs d'identité avec l’API ClearID :
     - Synchronisez les identités avec une API.
       - À propos de l’API ClearID.
   - Synchronisez les attributs d'identité avec l’intégration SCIM ClearID :
     - Synchronisez les identités avec l’intégration SCIM.
       - En savoir plus sur la norme SCIM.
       - En savoir plus sur les champs d'attributs Microsoft Entra ID.
       - Configurez l’intégration SCIM ClearID.
         - Générez une clé SCIM.
         - Créez une application d’entreprise Microsoft Azure.
         - Connectez votre intégration SCIM ClearID à Microsoft Azure.
         - Désactivez le réglage Groupes Microsoft Entra ID.
         - Configurez les réglages d’utilisateurs Microsoft Entra ID.
         - Configurez les réglages de synchronisation de l’intégration SCIM ClearID.
       - (Facultatif) Réinitialisez les données d'identité de l’intégration SCIM.
       - Examinez l’état de la synchronisation de l’intégration SCIM ClearID.
   - Synchronisez les attributs d'identité avec ClearID One Identity Synchronization Tool :
     - Synchronisez vos identités avec One Identity Synchronization Tool.
       - En savoir plus sur l'outil de synchronisation One Identity.
       - En savoir plus sur les champs d'attributs One Identity Synchronization Tool.
       - En savoir plus sur l'application Web Azure.
       - Installez l'outil de synchronisation One Identity.
       - Configurez l'outil de synchronisation One Identity.
     - Examinez l’état de la synchronisation.
     - En savoir plus sur les journaux One Identity Synchronization Tool.
     - Consultez les journaux One Identity Synchronization Tool.
     - Mettre à jour les identités existantes à partir d'une source de données externe.
   - Synchronisez les attributs d'identité avec ClearID LDAP Synchronization Agent :
     - En savoir plus sur ClearID LDAP Synchronization Agent.
     - En savoir plus sur l’association des attributs LDAP et des attributs ClearID.
     - Configurez ClearID LDAP Synchronization Agent.

6. Configurez et gérez vos intégrations webhook :
   - En savoir plus sur les webhooks.
     - Créez vos webhooks.
     - Modifiez vos webhooks.
     - Consulter les journaux des webhooks.
7. (Facultatif) Informations de dépannage.
   a. One Identity Synchronization Tool : Problèmes de connectivité
   b. One Identity Synchronization Tool : Problèmes de synchronisation des données

Synchroniser les identités à l'aide d'une API

Utilisez l’API Genetec ClearID[MC] pour programmer vos propres solutions afin d’automatiser diverses fonctions dans ClearID. L’API REST sert principalement à synchroniser les identités, mais bien d'autres utilisations sont possibles.

À propos de l’API ClearID

L’API Genetec ClearID[MC] est une interface de programmation que les développeurs peuvent utiliser pour aider leurs clients et partenaires à intégrer des logiciels supplémentaires ou des fonctions personnalisées.

Genetec ClearID[MC] est un service conçu en priorité autour d'une API, et l’interface Web est bâtie sur cette API REST. La majorité des fonctionnalités de l’interface Web sont donc accessibles en utilisant des points de terminaison REST (Representational State Transfer).

L’API ClearID est conçue pour répondre à deux objectifs principaux :

- **Indépendance de la plateforme :** Tout client doit pouvoir appeler l’API, indépendamment de la mise en œuvre interne de l’API. Cette indépendance de la plate-forme exige l’utilisation de protocoles standard, et de disposer d'un mécanisme permettant au client et au service Web de s'entendre sur le format des données à échanger.
- **Évolution du service :** L'API web doit pouvoir évoluer et intégrer de nouvelles fonctionnalités, indépendamment de l’application client. En cas d’évolution de l’API, les applications client doivent continuer à fonctionner sans modification.

L’API ClearID suit les meilleures pratiques REST (Representational State Transfer) et exploite les actions HTTP standard : `GET`, `POST`, `PUT`, `PATCH` et `DELETE`.

Exemples

L’API REST sert principalement à synchroniser les identités, mais bien d'autres utilisations sont possibles.

Voici quelques exemples de rapports ou de données que vous pouvez obtenir de ClearID en exploitant l’API REST :

- La liste de tous les événements de visite à venir et passés.
- La liste de tous les hôtes de visiteurs approuvés.
- La liste de tous les événements de visite à venir et passés pour un demandeur, un hôte ou un site particulier.
- La liste de tous les hôtes actifs ou inactifs, les autorisations de chaque hôte, les coordonnées, la fonction, le service et la société.

Pour chaque visite, vous pouvez obtenir les éléments suivants :

- Événement
- Nom de l'événement
- Dates et heures d'arrivée et de départ prévues
- Demandeur de visite
- Liste d'invités
- Type de visite
- Emplacement de stationnement
- Lieu de rendez-vous
- Site visité
- Secteurs de ce site
- Détails de l’approbation

Pour en savoir plus sur l’automatisation des fonctions à l'aide de l’API REST de ClearID, voir la documentation pour Développeurs Genetec[MC].

Synchroniser les identités à l'aide de l’intégration SCIM

Pour synchroniser les attributs système d'un fournisseur d'identité externe compatible avec les attributs d'identité Genetec ClearID[MC], vous pouvez utiliser l’intégration SCIM (System for Cross-domain Identity Management). Ces attributs d’identité peuvent ensuite être utilisés dans ClearID pour affecter des personnes à des rôles et pour automatiser le contrôle d'accès basé sur les rôles.

À savoir

Seul Microsoft Entra ID est pris en charge pour l’instant. Si vous souhaitez intégrer un autre fournisseur d'identité, contactez votre chargé de déploiement.

Procédure

1 En savoir plus sur la norme SCIM.
2 En savoir plus sur les champs d'attributs Microsoft Entra ID.
3 Configurez l’intégration SCIM.
4 (Facultatif) Réinitialisez les données d'identité de l’intégration SCIM.
5 Examinez l’état de la synchronisation de l’intégration SCIM.

À propos de la norme SCIM

La norme SCIM (System for Cross-domain Identity Management ou Système de gestion des identités interdomaines) est un protocole ouvert conçu pour échanger les données d’identité entre différentes entités. Il est très utilisé pour automatiser le processus de gestion des identités des utilisateurs à l'aide de systèmes informatiques. L'intégration SCIM assure la synchronisation automatique de toute modification des attributs d'identité avec d'autres systèmes.

- **Système :** SCIM crée un format commun pour l’échange de données d'identité.
- **Interdomaines :** SCIM communique les données d’identité de manière sécurisée entre différentes plates-formes.
- **Gestion des identités :** SCIM automatise les flux d'informations entre un fournisseur d'identité ou un système de gestion des identités et des accès (IAM) et les applications dans le cloud.

Avantages

- L’utilisation de SCIM limite l’effort nécessaire pour créer, modifier et synchroniser les données d'identité.
- L'intégration SCIM utilise Microsoft Entra ID dans le cloud, ce qui signifie que vous n’avez pas d’ordinateurs ou d'infrastructure à gérer.
- Il n’est pas nécessaire de configurer des ports de pare-feu.

REMARQUE : L’intégration SCIM ne synchronise que les attributs d'identité qui ont changé. Cette approche réduit considérablement le débit et le traitement nécessaires. D’autres solutions synchronisent tous les attributs d'identité à intervalles réguliers pour obtenir les dernières données d'identité.

À propos des champs d'attributs Microsoft Entra ID

Lorsque vous synchronisez un système externe avec Genetec ClearID[MC] en exploitant la norme SCIM (System for Cross-domain Identity Management), les attributs du système externe sont importés dans les attributs d'identité ClearID. L'importation utilise les correspondances de champs dans Microsoft Entra ID.

La plupart des champs d'identité ClearID sont créés sous forme d'attributs personnalisés.

Chaque champ doit avoir les préfixes suivants : urn:ietf:params:scim:schemas:extension:clearid:2.0:User

Attributs d'identité

Champs d'attributs	Remarques
Champs de base : active username displayname	• Ces champs sont les seuls champs du schéma SCIM de base que nous utilisons. • displayName est obligatoire pour la correspondance.
Champs d'identité de base : urn:ietf:params:scim:schemas:extension:clearid:2.0:User:description urn:ietf:params:scim:schemas:extension:clearid:2.0:User:firstName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:lastName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:middleName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:countryCode urn:ietf:params:scim:schemas:extension:clearid:2.0:User:email	• firstName ou lastName doit être indiqué dans la correspondance (comme dans le formulaire d'identité du portail). • email doit être un format d’e-mail valable pour la création de l’identité. • countryCode doit être un code composé de 3 lettres. Il est recommandé d’utiliser une valeur fixe de Microsoft Entra ID pour l’instant.
Champs CompanyData : urn:ietf:params:scim:schemas:extension:clearid:2.0:User:employeeNumber urn:ietf:params:scim:schemas:extension:clearid:2.0:User:secondaryEmail urn:ietf:params:scim:schemas:extension:clearid:2.0:User:cityOfResidence urn:ietf:params:scim:schemas:extension:clearid:2.0:User:stateOfResidence urn:ietf:params:scim:schemas:extension:clearid:2.0:User:zipCode urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberPrimary urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberSecondary	• secondaryEmail doit être un format d’e-mail valable pour la création de l’identité.
Champs PrivateData : urn:ietf:params:scim:schemas:extension:clearid:2.0:User:supervisorName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:departmentName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:jobTitle urn:ietf:params:scim:schemas:extension:clearid:2.0:User:companyName urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeDescription urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeCode	
Champs SystemData : urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasExtendedTime urn:ietf:params:scim:schemas:extension:clearid:2.0:User:externalId	• Les champs booléens ne fonctionnent qu'avec le drapeau de fonctionnalité SCIM 2.0. • externalId est obligatoire et doit être unique. Cette valeur sert à gérer la création des identités (comme dans OneIdentity). La façon la plus simple d'utiliser cette valeur

Champs d'attributs	Remarques
	consiste à utiliser une adresse e-mail ou un nom d'utilisateur.
Autres champs personnalisés : (qui n’appartiennent pas directement au modèle d’identité) urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasWebPortalAccess urn:ietf:params:scim:schemas:extension:clearid:2.0:User:isAdmin	• Les champs booléens ne fonctionnent qu'avec le drapeau de fonctionnalité SCIM 2.0.

Champs d'attributs non pris en charge

Champ de date :

- birthday
- activationDateUtc
- expirationDateUtc
- externalSyncTimeUtc

Champs avec des ID (identityIds) :

- creationOnBehalf
- approvers
- siteId
- provisioningAttributes
- customFields

Configurer l’intégration SCIM

Avant de synchroniser un système externe avec Genetec ClearID[MC], vous devez d'abord configurer l’intégration SCIM (System for Cross-domain Identity Management) dans ClearID et Microsoft Azure.

Avant de commencer

- En savoir plus sur la norme SCIM.
- En savoir plus sur les champs d'attributs Microsoft Entra ID.

À savoir

Cette procédure s'adresse à l'équipe de déploiement de ClearID, votre service informatique ou les personnes responsables de l'administration Microsoft Entra ID dans votre organisation.

Seul Microsoft Entra ID est pris en charge pour l’instant. Si vous souhaitez intégrer un autre fournisseur d'identité, contactez votre chargé de déploiement.

IMPORTANT : Ne sautez pas l’étape de désactivation des groupes. ClearID ne prend pas en charge la synchronisation des groupes.

Procédure

1 Générez votre clé SCIM.

2 Créez votre application d’entreprise Microsoft Azure.

3 Connectez votre intégration SCIM ClearID à Microsoft Azure.

4 Configurez les correspondances d’attributs.
   a) Désactivez le réglage Groupes de Microsoft Entra ID.
   b) Configurez les réglages d’utilisateurs Microsoft Entra ID.

5 Configurez les réglages de synchronisation de l’intégration SCIM ClearID.

Lorsque vous avez terminé

Examinez l’état de la synchronisation de l’intégration SCIM.

Générer une clé SCIM

Pour que votre intégration SCIM avec Genetec ClearID[MC] puisse communiquer avec Microsoft Entra ID, vous devez générer une clé SCIM (System for Cross-domain Identity Management).

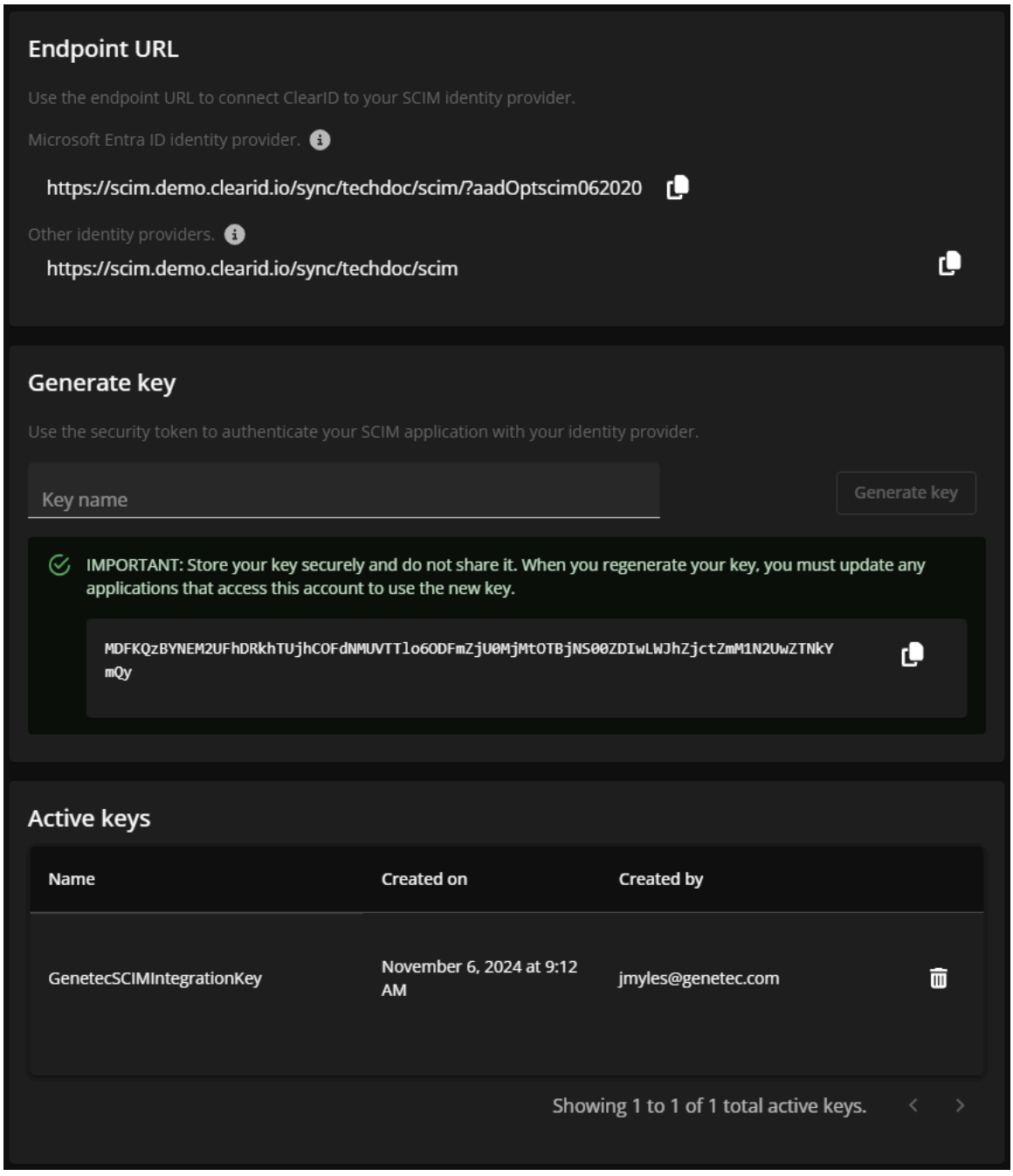
À savoir

Seul un *administrateur* du portail ClearID peut effectuer cette tâche.

Procédure

1 Sur le portail ClearID, cliquez sur **Administration** > **Intégration SCIM**.

2 Dans la section *Générer la clé*, entrez un nom de clé et cliquez sur **Générer la clé**.
Par exemple, vous pourriez nommer la clé `CléIntégrationGenetecSCIM`.



Lorsque vous avez terminé

Créez votre application d'entreprise Microsoft Azure.

Créer une application d’entreprise Microsoft Azure

Votre organisation peut automatiser l’approvisionnement d'attributs d'identité à l’aide de l’intégration SCIM Genetec ClearID^{MC} en utilisant Microsoft Entra ID en tant que fournisseur d'identité. Pour utiliser l’intégration, vous devez d'abord créer une application d’entreprise dans Microsoft Azure.

À savoir

Cette procédure s'adresse à l'équipe de déploiement de ClearID, votre service informatique ou les personnes responsables de l'administration Microsoft Entra ID dans votre organisation.

Procédure

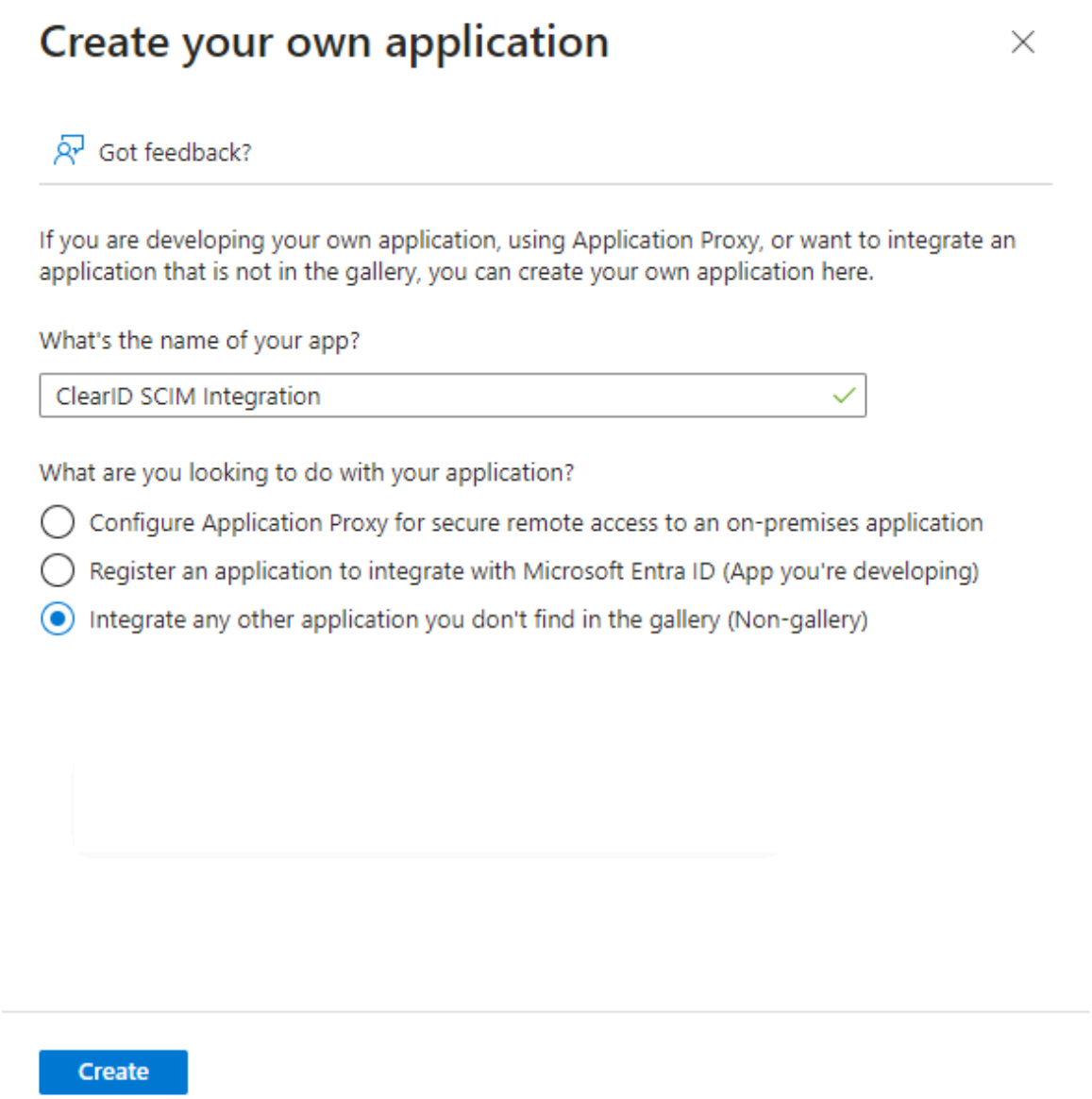
1 Sur le portail Microsoft Azure, repérez et cliquez sur **Applications d’entreprise**.

2 Dans la section *Applications d’entreprise*, cliquez sur **Nouvelle application**.

3 Cliquez sur **Créer votre propre application**.

4 Sélectionnez **Intégrer toute autre application que vous ne trouvez pas dans la galerie (hors galerie)**.

5 Entrez le nom de votre application et cliquez sur **Créer**.
Par exemple, vous pourriez nommer l’application `Intégration SCIM ClearID`.



REMARQUE : Une notification d'ajout réussi doit apparaître dans le coin supérieur droit de l’écran.

Lorsque vous avez terminé

Connectez votre intégration SCIM ClearID à Microsoft Azure.

Connecter votre intégration SCIM ClearID à Microsoft Azure

Avant d’utiliser l’intégration SCIM dans Genetec ClearID^{MC} pour synchroniser les attributs d'identité, vous devez fournir les identifiants qui connectent l’API de l’intégration SCIM ClearID à Microsoft Azure.

Avant de commencer

Créez votre application d’entreprise Microsoft Azure.

À savoir

Cette procédure s'adresse à l'équipe de déploiement de ClearID, votre service informatique ou les personnes responsables de l'administration Microsoft Entra ID dans votre organisation.

Procédure

1 Sur le portail Microsoft Azure, repérez et cliquez sur **Applications d’entreprise**.

2 Dans la section *Applications d’entreprise*, repérez votre application d’**Intégration SCIM ClearID**.

3 Dans la section *Gérer*, cliquez sur **Approvisionnement**, puis à nouveau sur **Approvisionnement**.

4 Dans la liste **Mode d’approvisionnement**, sélectionnez **Automatique**.

5 Développez la section *Identifiants d'administrateur*.

6 Dans l’onglet **Intégration SCIM** du portail ClearID, repérez la section *URL de point de terminaison* et cliquez sur **Copier dans le presse-papier** en regard du fournisseur d'identité Microsoft Entra ID.

L’URL de point de terminaison est copiée dans votre presse-papiers.

7 Revenez sur la page *Approvisionnement* de Microsoft Azure et collez l’URL dans le champ **URL de locataire**.

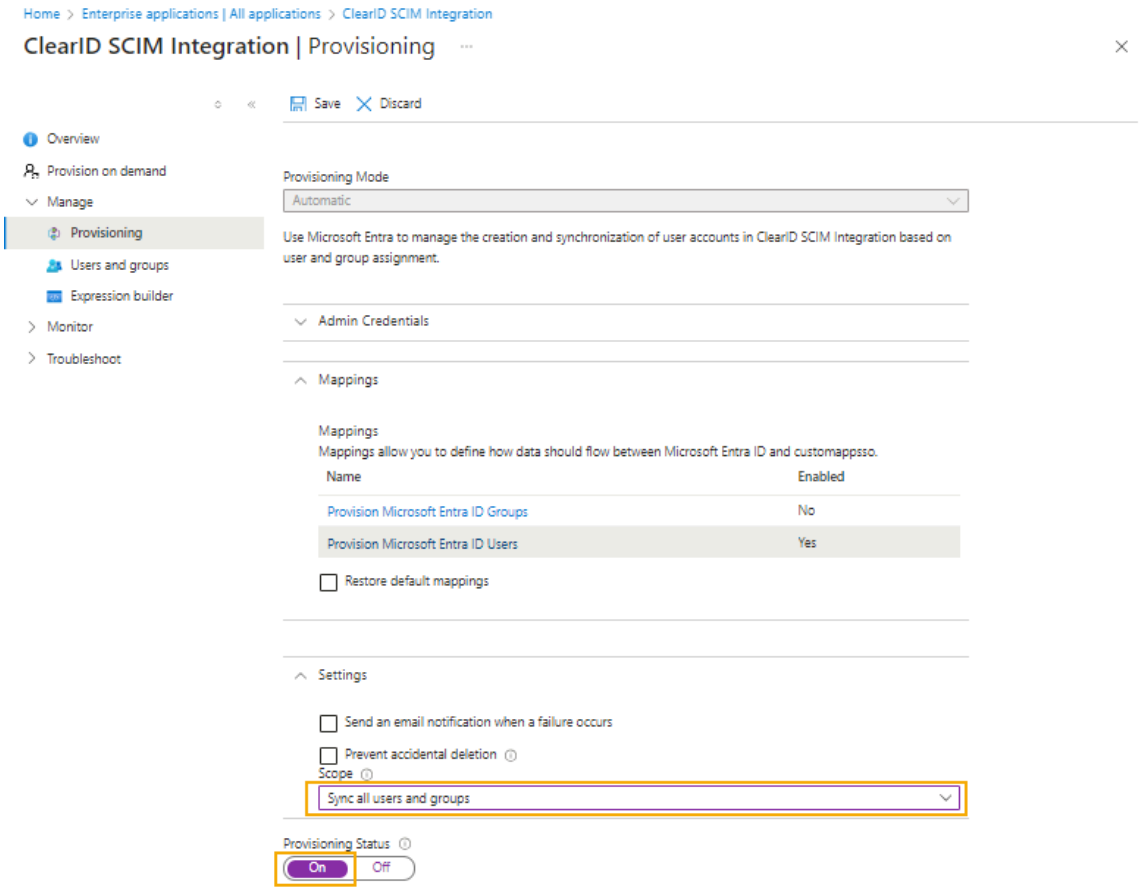
L’URL de point de terminaison sert à connecter ClearID aux systèmes d'authentification SCIM et à Microsoft Entra ID.

8 Dans l’onglet **Intégration SCIM** du portail ClearID, repérez la section *Générer la clé* et cliquez sur **Copier dans le presse-papiers**.

9 Revenez sur la page *Approvisionnement* de Microsoft Azure et collez la clé dans le champ **Jeton secret**.

La clé SCIM sert à authentifier votre application auprès de Microsoft Entra ID.

10 Cliquez sur **Tester la connexion**.



11 Cliquez sur **Enregistrer**.

CONSEIL : Une notification de mise à jour réussie doit apparaître dans le coin supérieur droit de l’écran.

Lorsque vous avez terminé

Désactivez vos réglages de groupes Microsoft Entra ID.

Désactiver le réglage Groupes Microsoft Entra ID

Genetec ClearID[MC] ne prend pas en charge la synchronisation des groupes. Pour éviter la synchronisation des réglages ou attributs de groupes, désactivez le réglage Groupes de Microsoft Entra ID dans votre application d’entreprise Microsoft Azure.

Avant de commencer

Connectez votre intégration SCIM ClearID à Microsoft Azure.

À savoir

Cette procédure s'adresse à l'équipe de déploiement de ClearID, votre service informatique ou les personnes responsables de l'administration Microsoft Entra ID dans votre organisation.

IMPORTANT : ClearID ne prend pas en charge la synchronisation des groupes. Ce réglage doit être désactivé.

Procédure

1 Sur le portail Microsoft Azure, repérez et cliquez sur **Applications d’entreprise**.

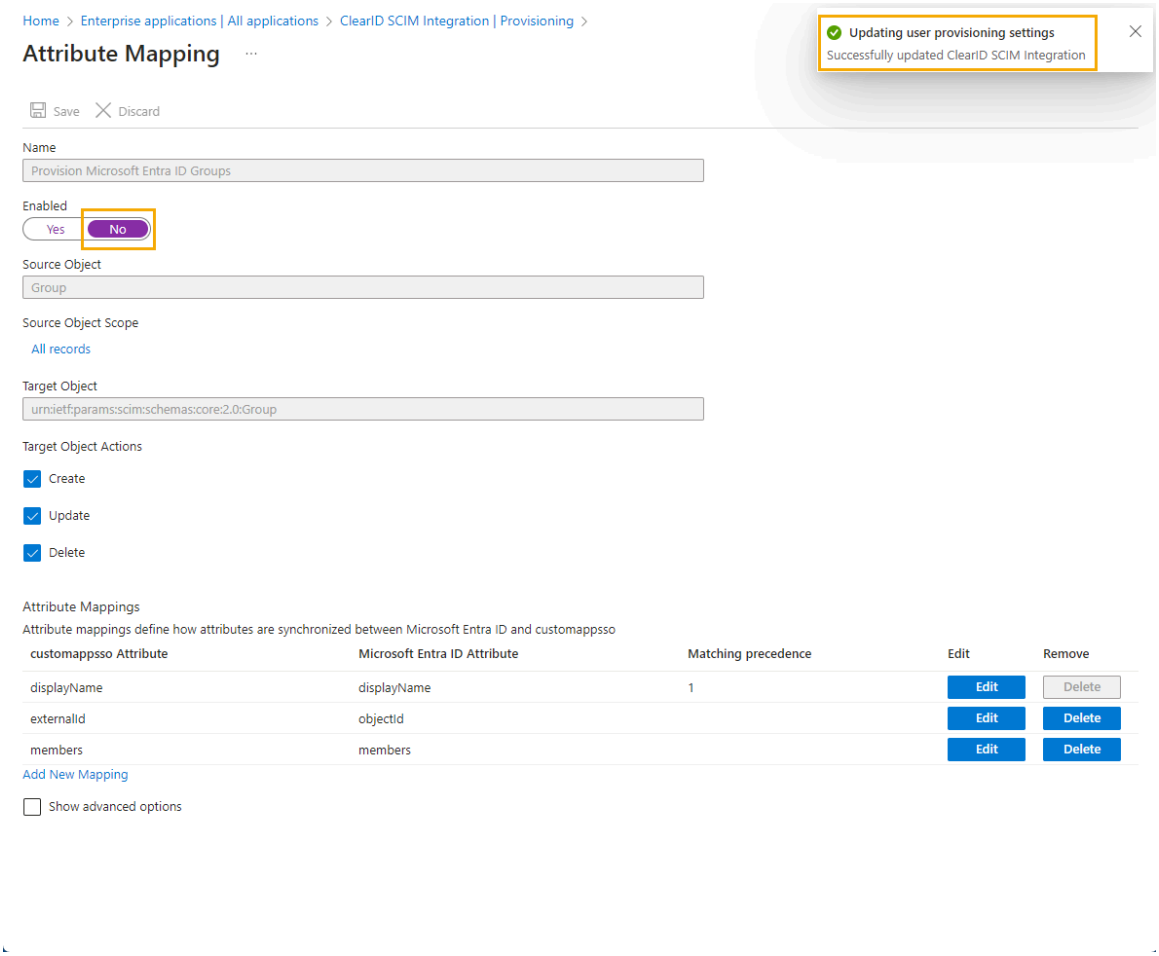
2 Dans la section *Applications d’entreprise*, repérez votre application d’**Intégration SCIM ClearID**.

3 Dans la section *Gérer*, cliquez sur **Approvisionnement**, puis à nouveau sur **Approvisionnement**.

4 Développez la section *Mappages* de la page *Approvisionnement*.

5 Cliquez sur **Approvisionner les groupes Microsoft Entra ID**.

6 Réglez le curseur **Activé** sur **Non**.



7 Cliquez sur **Enregistrer** puis cliquez sur **Oui** pour confirmer vos modifications.

8 Fermez la fenêtre et revenez à la page *Approvisionnement*.
L'actualisation de la page peut prendre quelques instants.

Lorsque vous avez terminé

Configurez les réglages d’utilisateurs Microsoft Entra ID.

Configurer les réglages d’utilisateurs Microsoft Entra ID

Pour spécifier la manière dont les données doivent circuler entre Microsoft Entra ID et Genetec ClearID[MC], vous devez configurer les réglages d’utilisateurs et spécifier les correspondances d'attributs pour la synchronisation automatique.

Avant de commencer

Désactivez le réglage Groupes Microsoft Entra ID.

À savoir

Cette procédure s'adresse à l'équipe de déploiement de ClearID, votre service informatique ou les personnes responsables de l'administration Microsoft Entra ID dans votre organisation.

Procédure

1 Sur le portail Microsoft Azure, repérez et cliquez sur **Applications d’entreprise**.

2 Dans la section *Applications d’entreprise*, repérez votre application d’intégration SCIM ClearID.

3 Dans la section *Gérer*, cliquez sur **Approvisionnement**, puis à nouveau sur **Approvisionnement**.

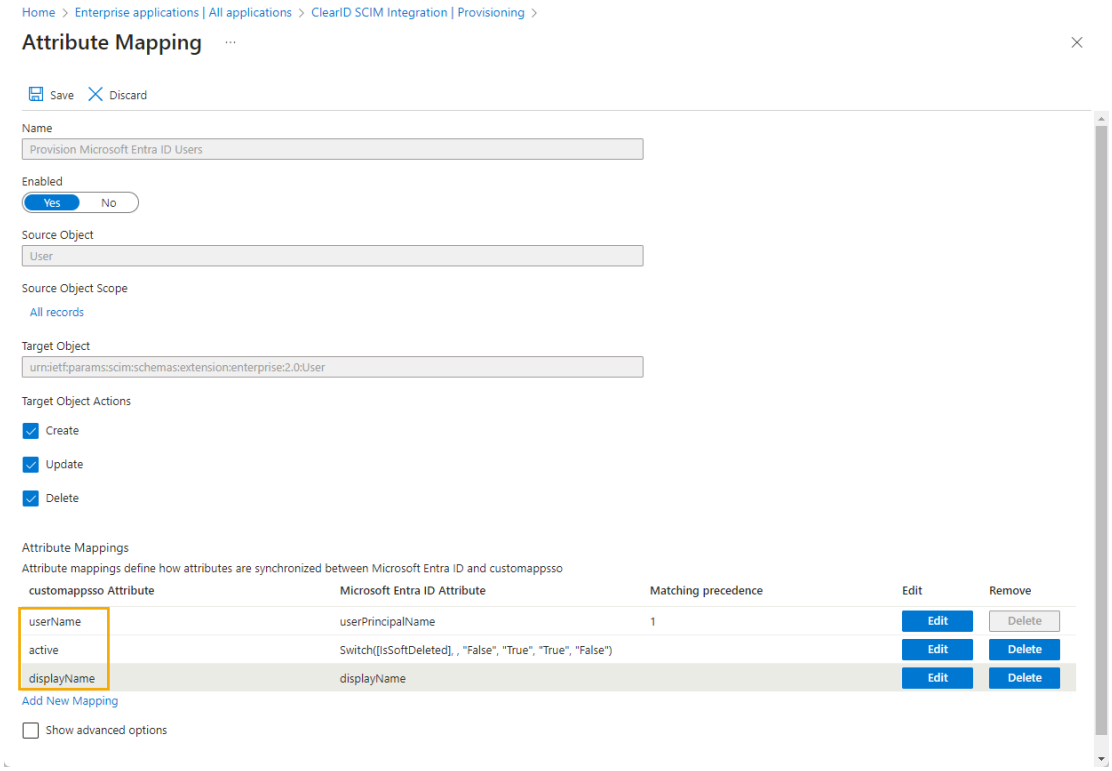
4 Développez la section *Mappages* et cliquez sur **Approvisionner les utilisateurs Microsoft Entra ID**.

5 Modifier les correspondances d'attributs par défaut.

a) Sur la page *Mappage d'attributs*, cliquez sur **Supprimer** pour supprimer les attributs par défaut qui sont inutilisés.

Conservez uniquement les suivants :

- userName
- active
- displayName



b) Cliquez sur **Enregistrer** puis cliquez sur **Oui** pour confirmer vos modifications.

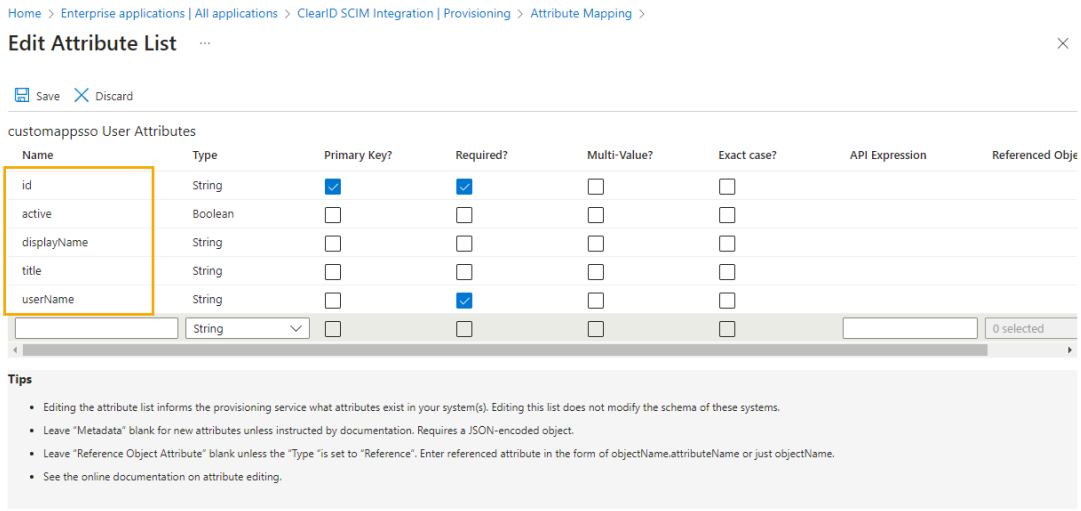
6 Modifiez les attributs utilisateur customappsso.

a) Sur la page *Mappage d'attributs*, cliquez sur **Afficher les options avancées**.

b) Cliquez sur **Modifier la liste d'attributs pour customappsso**, puis cliquez sur **Supprimer** pour supprimer tous les attributs par défaut qui sont inutilisés.

Conservez uniquement les suivants :

- id
- active
- displayName
- title
- userName



c) Cliquez sur **Enregistrer** puis cliquez sur **Oui** pour confirmer vos modifications.

7 Ajoutez les attributs du schéma ClearID.

Ajoutez uniquement la liste d'attributs disponibles pour ClearID :

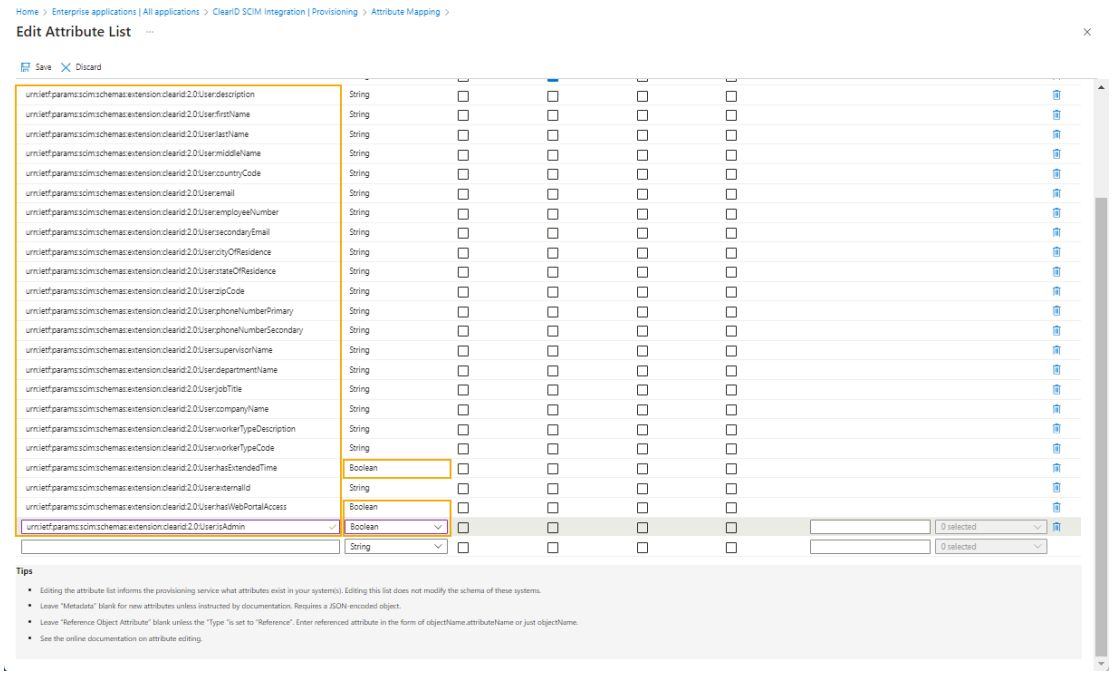
```
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:description
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:firstName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:lastName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:middleName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:countryCode
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:email
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:employeeNumber
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:secondaryEmail
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:cityOfResidence
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:stateOfResidence
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:zipCode
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberPrimary
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:phoneNumberSecondary
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:supervisorName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:departmentName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:jobTitle
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:companyName
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeDescription
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:workerTypeCode
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasExtendedTime
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:externalId
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:hasWebPortalAccess,
 Boolean
urn:ietf:params:scim:schemas:extension:clearid:2.0:User:isAdmin, Boolean
```

a) Sur la page *Modifier la liste d'attributs*, copiez et collez un nom d'attribut de l'exemple de code du schéma ClearID précédent dans le champ **Nom** et sélectionnez le **Type** d'attribut.

Quasiment tous les attributs sont de type **Chaîne**, à l'exception de trois attributs qui sont de type **Booléen** : hasExtendedTime hasWebPortalAccess et UserisAdmin.

IMPORTANT : L'attribut ClearID externalId est l'identifiant unique utilisé par ClearID pour la synchronisation. Il est associé à l'attribut unique objectId dans Microsoft Entra ID.

b) Répétez pour chaque attribut cité dans l'exemple de code d'attribut du schéma ClearID précédent.



c) Cliquez sur **Enregistrer** puis cliquez sur **Oui** pour confirmer vos modifications.

8 Ajoutez les mappages d'attributs ClearID.

a) Sur la page *Mappage d'attributs*, cliquez sur **Ajouter un nouveau mappage**.

b) Sur la page *Modifier l’attribut*, ajoutez les attributs nécessaires correspondant aux attributs ajoutés à l’étape 7.

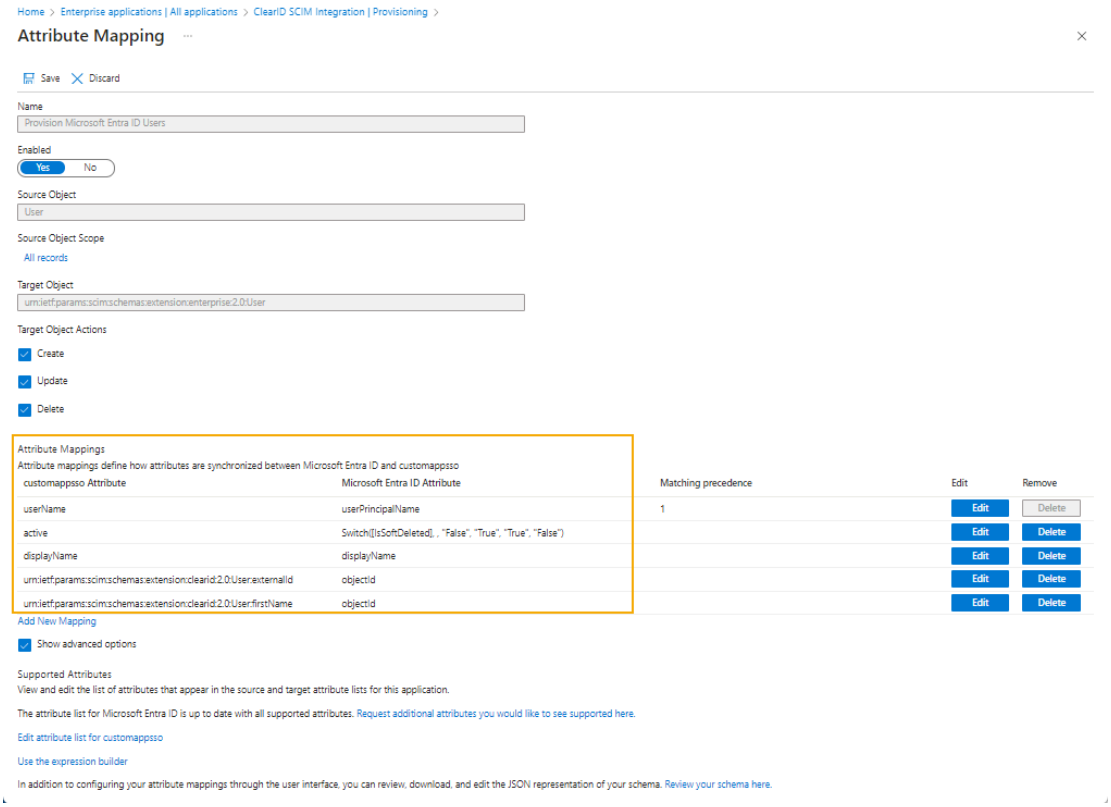
Incluez les éléments suivants :

- Type de mappage : **Direct**
- Attribut source : **objectid**
- Attribut cible : <*votre valeur d'attribut*>

c) Cliquez sur **OK**.

d) Répétez pour chaque attribut ajouté plus tôt, et remplacez la valeur d'attribut cible avec l'attribut suivant.

Pour une synchronisation initiale réussie, les attributs suivants sont nécessaires. Vous pouvez en ajouter d’autres par la suite.



REMARQUE : objectid correspond au GUID dans Azure. Vous ne pouvez pas manipuler le objectid d'un utilisateur dans Azure. Il s'agit d'un champ codé en dur qui n’est pas modifiable.

e) Cliquez sur **Enregistrer** puis cliquez sur **Oui** pour confirmer vos modifications.

Vous pouvez à présent fermer la fenêtre et revenir à la page *Approvisionnement*.

Lorsque vous avez terminé

Configurez les réglages de synchronisation de l’intégration SCIM ClearID.

Configurer les réglages de synchronisation de l’intégration SCIM ClearID

Pour déterminer les données d'identité qui sont synchronisées avec Genetec ClearID[MC], vous devez sélectionner les réglages de synchronisation adaptés et activer l’approvisionnement dans Microsoft Azure.

Avant de commencer

Configurez les réglages d’utilisateurs Microsoft Entra ID.

À savoir

Cette procédure s'adresse à l'équipe de déploiement de ClearID, votre service informatique ou les personnes responsables de l'administration Microsoft Entra ID dans votre organisation.

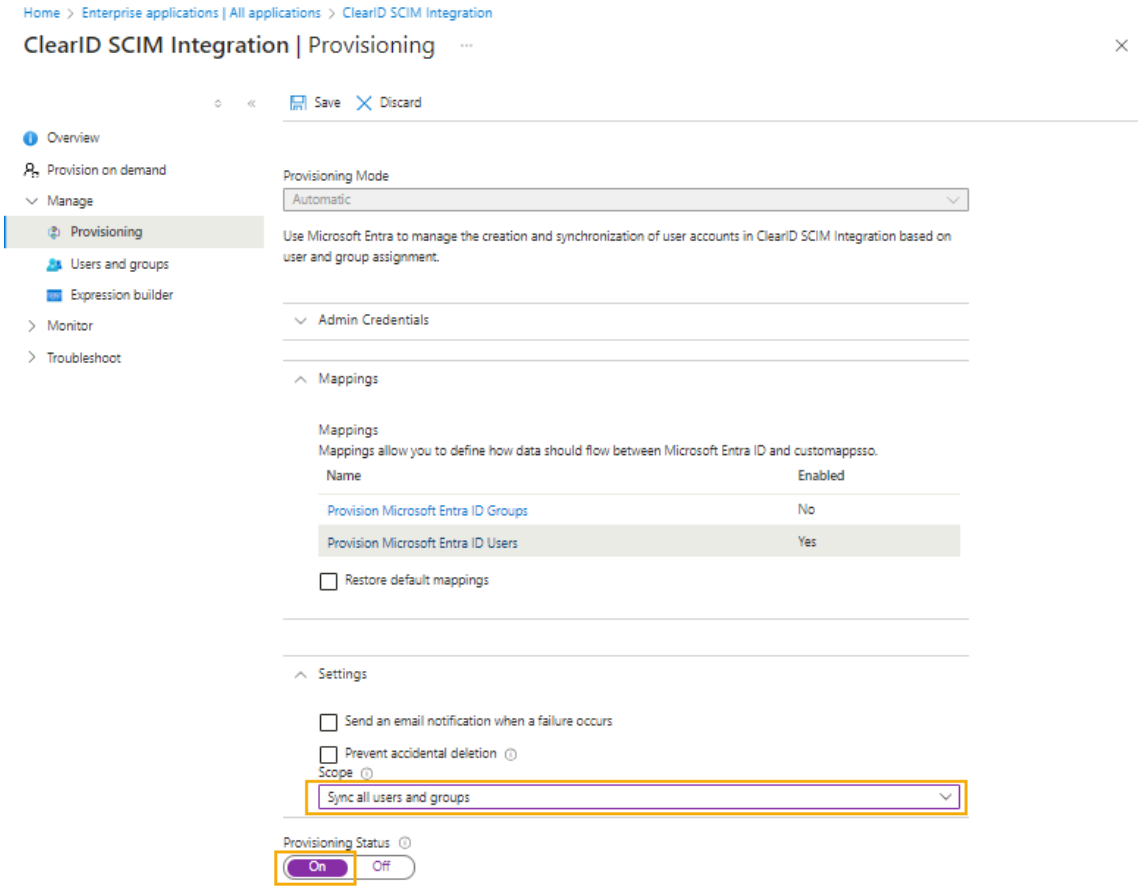
Procédure

1 Sur la page *Approvisionnement*, cliquez sur **Réglages** et sélectionnez les utilisateurs à synchroniser avec ClearID :

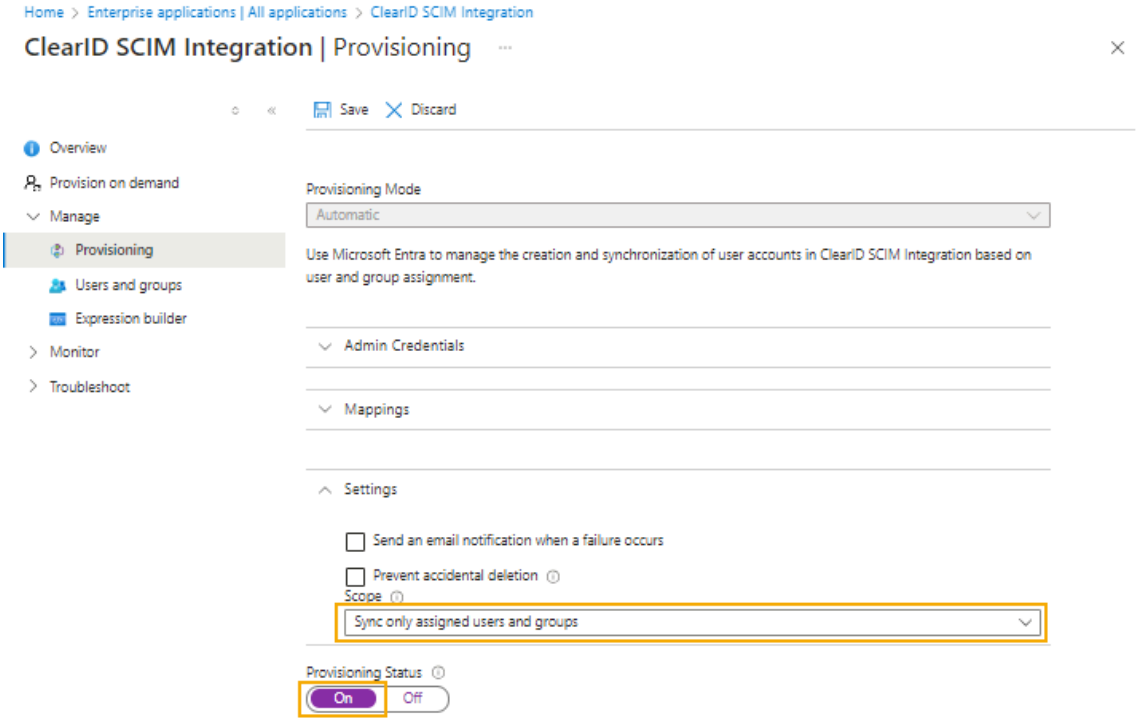
- **Synchroniser tous les utilisateurs et groupes :** Synchronise tout avec Microsoft Entra ID.
- **Ne synchroniser que les utilisateurs et groupes affectés :** Seuls les utilisateurs et groupes sélectionnés sont synchronisés.

IMPORTANT : ClearID ne prend pas en charge la synchronisation des groupes. En fonction des réglages d'approvisionnement que vous sélectionnez, tout ou partie des données d'identité des utilisateurs sélectionnés sont synchronisés.

2 Si vous avez choisi **Synchroniser tous les utilisateurs et groupes**, dans la section *Statut de l'approvisionnement*, réglez le curseur sur **Activé** et cliquez sur **Enregistrer**.



3 Si vous avez choisi **Ne synchroniser que les utilisateurs et groupes affectés**, paramétrez les options d'approvisionnement.
   a) Cliquez sur **Utilisateurs et groupes** dans la barre de navigation à gauche.
   b) Cliquez sur **Ajouter un groupe**.
   c) Cliquez sur **Aucun sélectionné**, recherchez et sélectionnez le groupe désiré, et cliquez sur **Sélectionner**.
   d) Cliquez sur **Affecter**, et répétez pour chaque groupe que vous souhaitez ajouter.
   e) Revenez à la page *Approvisionnement* et cliquez sur **Paramètres**.
   f) Dans la section *Statut d'approvisionnement*, réglez le curseur sur **Activé** et cliquez sur **Enregistrer**.



Lorsque vous avez terminé

Examinez l'état de la synchronisation de l'intégration SCIM ClearID.

Réinitialiser les données d'identité d'une intégration SCIM

Pour corriger les problèmes liés aux données d'identité, vous pouvez réinitialiser et remplacer toutes les données d'identité SCIM (System for Cross-domain Identity Management) dans Genetec ClearID^{MC}. Cette procédure de réinitialisation utilise les dernières données de Microsoft Entra ID.

À savoir

Cette procédure s'adresse à l'équipe de déploiement de ClearID, votre service informatique ou les personnes responsables de l'administration Microsoft Entra ID dans votre organisation.

N'utilisez la réinitialisation que pour résoudre les problèmes liés aux données d'identité. Par exemple, en cas de divergence après la modification manuelle de vos données d'identité, ou si les données d'identité ont été supprimées dans ClearID.

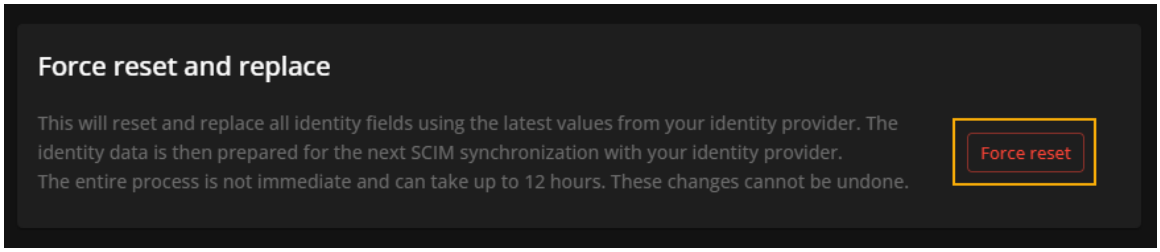
La réinitialisation prépare les données d’identité pour la prochaine synchronisation SCIM entre ClearID et Microsoft Entra ID. Cette procédure ne transmet les modifications de données d'identité que dans un sens, vers Entra ID.

IMPORTANT : Ce processus peut prendre jusqu’à 12 heures. Ces modifications ne peuvent pas être annulées.

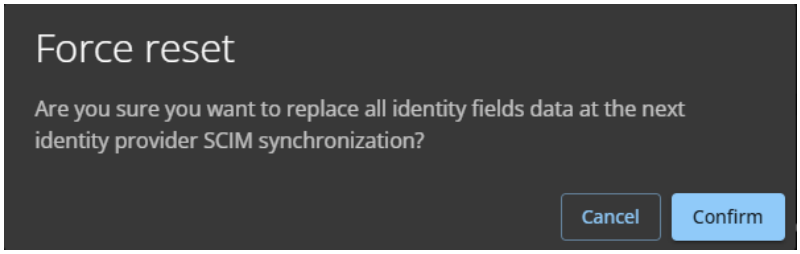
Procédure

1 Sur le portail ClearID, cliquez sur **Administration** > **Intégration SCIM**.

2 Dans la section *Forcer la réinitialisation et le remplacement*, cliquez sur **Forcer la réinitialisation**.



3 Cliquez sur **Confirmer** pour réinitialiser et remplacer vos données d’identité.



Lorsque vous avez terminé

Vérifiez l'état de la synchronisation de l’intégration SCIM pour confirmer que vos données d'identité ont bien été réinitialisées.

Examiner l’état de la synchronisation de l’intégration SCIM

Vous pouvez consulter l’état général de la synchronisation d'identités SCIM (System for Cross-domain Identity Management). Vous pouvez également consulter les journaux d'approvisionnement dans Microsoft Azure pour obtenir des informations plus détaillées sur l'activité de synchronisation de l’intégration SCIM Genetec ClearID^{MC} concernant une personne ou une identité particulière.

À savoir

Cette procédure s'adresse à l'équipe de déploiement de ClearID, votre service informatique ou les personnes responsables de l'administration Microsoft Entra ID dans votre organisation.

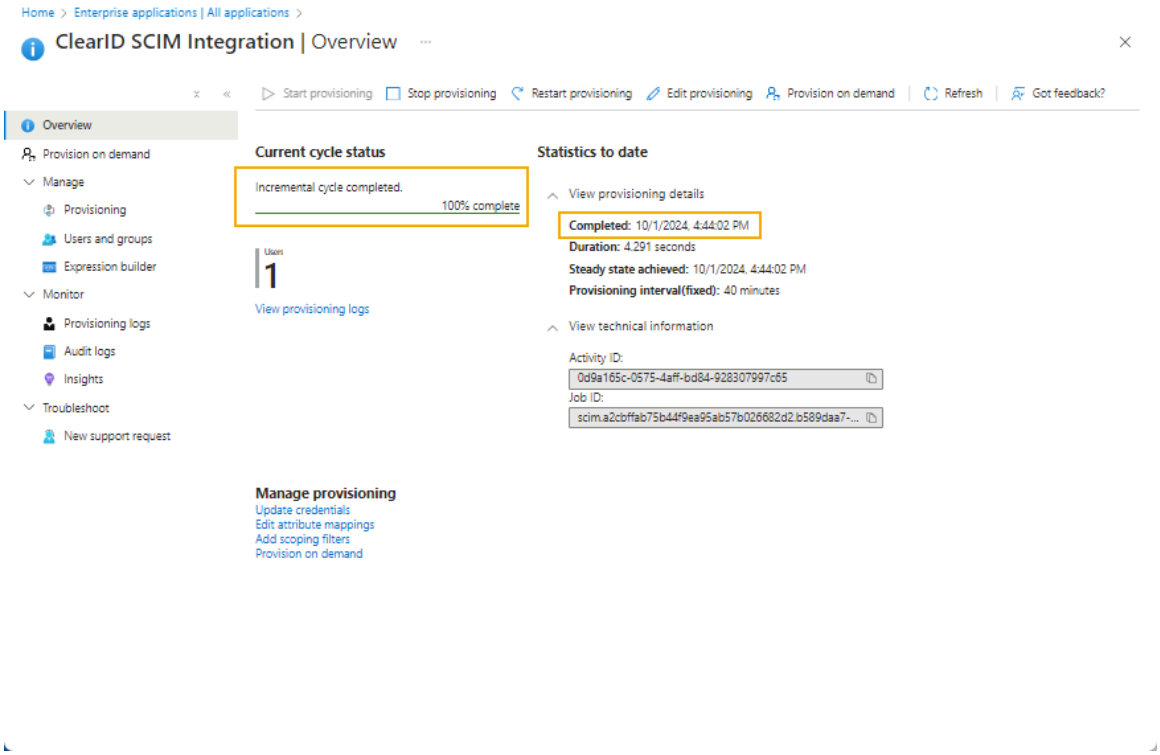
Les journaux d'approvisionnement peuvent servir à vérifier que l’intégration SCIM ClearID est bien configurée et opérationnelle. En cas de problème de configuration, des messages d'erreur sont générés et consignés dans les journaux d'approvisionnement.

Procédure

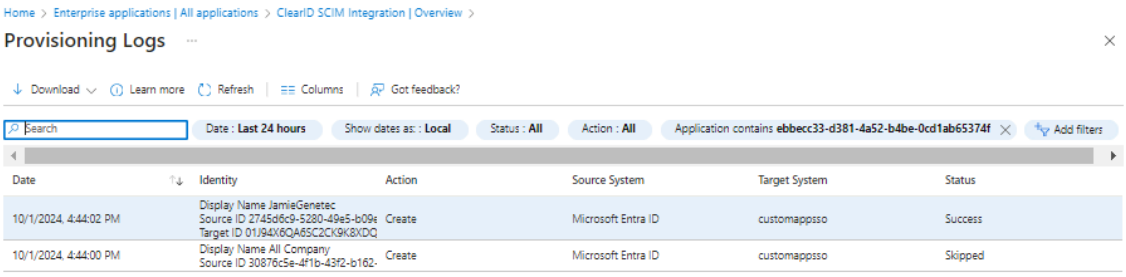
1 Sur le portail Microsoft Azure, repérez et cliquez sur **Applications d’entreprise**.

2 Dans *Applications d'entreprise*, sélectionnez votre application d'intégration SCIM.

3 Sur la page *Présentation*, vérifiez que la dernière synchronisation s'est déroulée avec succès, et l'heure de la dernière synchronisation.



4 (Facultatif) Cliquez sur **Afficher les journaux d'approvisionnement** pour obtenir des informations plus détaillées sur la synchronisation des identités.



REMARQUE : Si les journaux sont trop longs, la page *Journaux d'approvisionnement* intègre des filtres utiles pour manipuler les données.

Synchroniser les identités avec One Identity

Utilisez Genetec ClearID[MC] One Identity Synchronization Tool pour synchroniser les attributs d'un système externe avec les attributs d'identité Genetec ClearID[MC]. Ces attributs d'identité dans ClearID peuvent ensuite être utilisés pour affecter des personnes à des rôles et pour automatiser le contrôle d'accès basé sur les rôles.

À savoir

À l'aide de l'outil de synchronisation One Identity, vous pouvez synchroniser les attributs système externes à partir des sources de données suivantes :

- Azure AD
- Base de données (Microsoft SQL Server, Oracle Database, ODBC)
- Fichier (CSV)

Procédure

1 En savoir plus sur l'outil de synchronisation One Identity.

2 En savoir plus sur les champs d'attribut One Identity.

3 En savoir plus sur l'application Web Azure.

4 Installez l'outil de synchronisation One Identity.

5 Configurez l'outil de synchronisation One Identity.

6 Consulter l'état de la synchronisation.

Rubriques connexes

Problèmes de connectivité (One Identity Synchronization Tool), page 685
Problèmes de synchronisation des données (One Identity Synchronization Tool), page 686

À propos de One Identity Synchronization Tool

Genetec ClearID[MC] One Identity Synchronization Tool est un service Windows qui permet d'importer des informations d'identités à partir d'un système externe dans Genetec ClearID[MC].

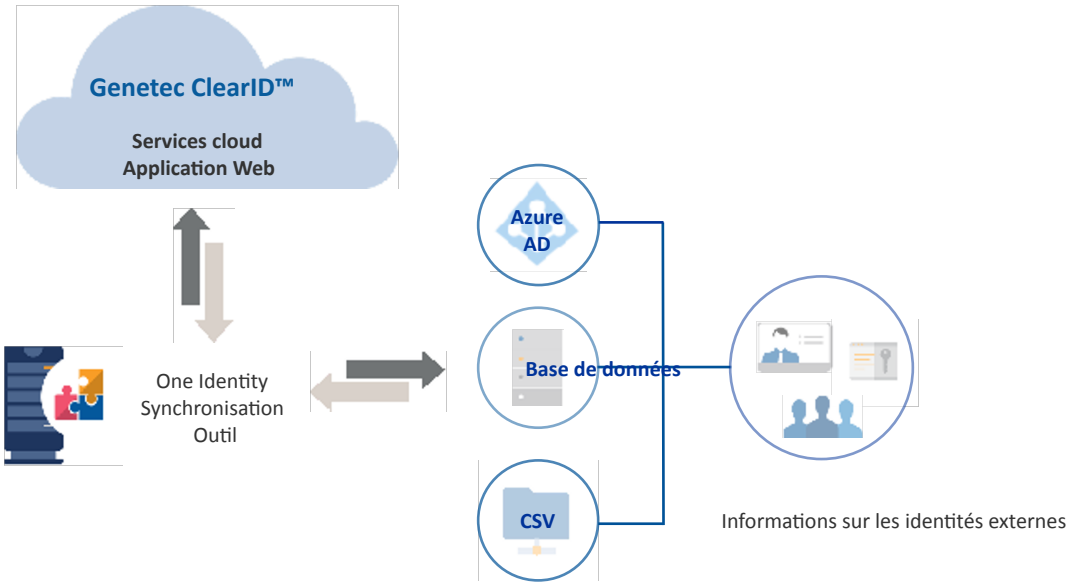
ClearID One Identity Synchronization Tool inclut les composants suivants :

- **Genetec.ClearID.OneIdentity.SynchronizationTool** (*OneIdentityConfigurationTool.exe*) est le composant d'interface utilisateur de l'application Windows qui est utilisé pour configurer l'outil de synchronisation.
- **Genetec.ClearID.OneIdentity.SynchronizationService** (*OneIdentityService.exe*) est le composant de service Windows de l’application qui effectue la synchronisation des attributs des systèmes externes

avec les attributs d'identité ClearID automatiquement, en arrière-plan et à la fréquence spécifiée dans Synchronization Tool.

Sources de données

Vous pouvez sélectionner une ou plusieurs sources de données à synchroniser à partir d'un système externe. À l'aide de la boîte de dialogue *Configuration des sources de données*, vous configurez les **sources de données** et mappez les attributs One Identity à leurs attributs système externes associés.



- **Azure Active Directory :** La source de données Azure AD est un annuaire Azure Active Directory à partir duquel vous pouvez importer des informations sur les identités. Par exemple, pour importer des identités, des identifiants ou des photos dans ClearID.
- **Base de données :** La source de données de la base de données peut être une base de données Microsoft SQL Server, une base de données Oracle ou une base de données compatible ODBC qui suit le mappage des attributs One Identity. La base de données doit être accessible depuis le serveur qui héberge ClearID One Identity Synchronization Tool. Une base de données peut contenir une table ou une vue pour les informations sur les identités.
- **Fichier :** La source de données du fichier est un fichier texte délimité. Par exemple, un fichier CSV qui suit l'association des attributs One Identity et qui doit être accessible depuis le serveur sur lequel ClearID One Identity Synchronization Tool est installé. Chaque fichier contient des informations sur des identités.

Synchronisation

Dans ClearID, les identités peuvent provenir de différentes sources de données (bases de données, RH, sources externes) et peuvent être synchronisées à l'aide de différents outils (Genetec ClearID^{MC} LDAP Synchronization Agent, l'API Genetec ClearID^{MC} ou Genetec ClearID^{MC} One Identity Synchronization Tool).

- LDAP est généralement utilisé pour la synchronisation des attributs Active Directory avec les identités ClearID.
- L'API est généralement utilisée pour les mises à jour en temps réel. Par exemple, pour supprimer rapidement des personnes. L'option de synchronisation de l'API est la plus souple, mais elle est coûteuse.

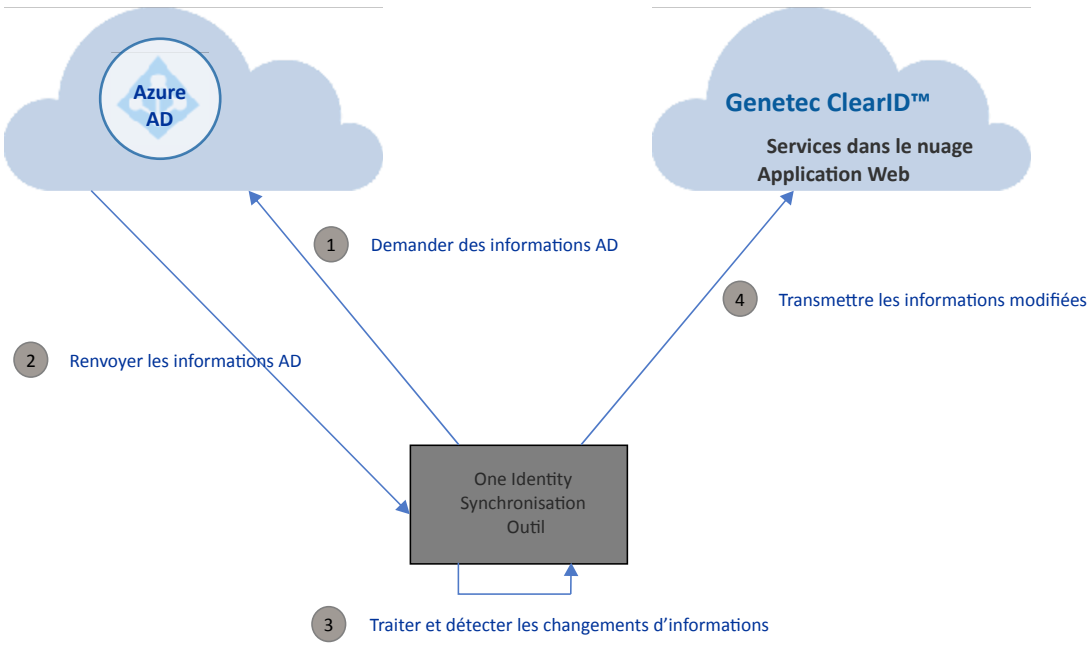
- One Identity est généralement utilisé pour les systèmes RH. Par exemple, pour synchroniser tous les employés tous les jours ou toutes les 4 heures. ClearID One Identity Synchronization Tool est configuré pour se synchroniser à la même fréquence.

Synchronisation de données One Identity

Les informations suivantes décrivent la synchronisation One Identity :

- La synchronisation des attributs du système externe avec les attributs d'identité ClearID ne fonctionne qu’en mode ENTRANT.
  ATTENTION : Toute modification apportée aux identités dans ClearID peut être remplacée lors de la synchronisation suivante avec le système externe.
- La synchronisation peut être effectuée manuellement à l'aide de l'option **Synchroniser maintenant** ( ) ou automatiquement aux intervalles de **synchronisation automatique** spécifiés dans l'outil de synchronisation One Identity.
  - Pour chaque **champ One Identity** configuré, un mappage personnalisé vers le **champ Externe** du système externe est créé. Cette correspondance garantit de pouvoir synchroniser les attributs du système externe avec les champs d'attributs One Identity.

Le diagramme suivant illustre une synchronisation de données Azure AD :



Le workflow de synchronisation est fondamentalement identique pour toutes les sources de données :

1. Demande des informations de la source de données.
2. Renvoi des informations de la source de données.
3. Traitement et détection des changements d'informations éventuels.
4. Les informations de source de données sont transmises à l'application Web ClearID.

Exemples de fichiers SQL

Pour l'option de source de données **Base de données**, des exemples de fichiers de script SQL sont fournis avec l'outil et sont disponibles ici :

C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service

- *Identities_Oracle.sql*
- *Identities_SqlServer.sql*

Les exemples de fichiers SQL peuvent être utilisés pour tester la solution de source de données **Base de données**, ou pour vous aider à comprendre le format de données SQL.

Exemples de fichiers CSV

Pour l'option de source de données **Fichier**, un exemple de fichier CSV est fourni avec l'outil, et il est disponible ici :

C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service

- *Identities.csv*

L'exemple de fichier CSV peut être utilisé pour tester la solution de source de données **Fichier**, ou pour vous aider à comprendre le format de données CSV.

À propos des champs d'attributs One Identity Synchronization Tool

Lorsque vous synchronisez un système externe avec Genetec ClearID[MC] avec Genetec ClearID[MC] One Identity Synchronization Tool, les attributs du système externe sont synchronisés (importés) dans les attributs d'identité ClearID en fonction des correspondances de champs dans One Identity Synchronization Tool.

REMARQUE : L'ordre des sources de données est important car la première source de données remplace toujours les champs communs.

Attributs d'identité

Champ One Identity	Type de donnée	Description
ID unique* * Ce champ est obligatoire.	Champ texte	Un identifiant unique pour l'identité. L'identifiant unique peut être un code alphanumérique ou une adresse e-mail. Par exemple, le numéro d'employé *xyz12345*. **IMPORTANT :** (Azure Active Directory uniquement) La modification du mappage de l'ID unique peut entraîner des problèmes de duplication des données.
Date d'activation	DateTime	La date à laquelle l'identité est activée. Par exemple, 1/11/2022. **REMARQUE :** Tous les formats d'horodatage standard sont pris en charge.
Ville	Champ texte	La ville où se trouve l'identité. Par exemple, Paris.
Société	Champ texte	Le nom de l'entreprise. Par exemple, Genetec[MC].
Code postal	Champ texte	Le code du pays à trois lettres (MAJUSCULES). Par exemple, USA ou CAN. **REMARQUE :** Les codes pays à trois lettres sont basés sur les codes Alpha-3 de la norme de codes pays ISO 3166-1.
Date de naissance	DateTime	La date de naissance de l'identité. Par exemple, 7/21/2022.

Champ One Identity	Type de donnée	Description
		REMARQUE : Tous les formats d'horodatage standard sont pris en charge.
Département	Champ texte	Le nom du département. Par exemple, informatique ou marketing.
Description	Champ texte	La description d'identité.
Adresse e-mail	Champ texte	Adresse e-mail principale (e-mail professionnelle) de l'identité. Par exemple, johndoe@test.com
Numéro d'employé	Champ texte	Le numéro d'employé de l’identité.
Date d'expiration	DateTime	La date à laquelle l'identité expire. **REMARQUE :** Tous les formats d'horodatage standard sont pris en charge.
Prénom	Champ texte	Le prénom de l'identité.
Intitulé du poste	Champ texte	Le titre du poste de l'identité.
Nom	Champ texte	Le nom de famille de l'identité.
Deuxième prénom	Champ texte	Le deuxième prénom de l'identité
Numéro de téléphone mobile	Champ texte	Le numéro de téléphone secondaire (numéro de téléphone mobile) Par exemple, 555-555-5555.
e-mail personnel	Champ texte	L'adresse e-mail secondaire (e-mail personnelle) de l'identité. Par exemple, johndoe2@test.com
Numéro de téléphone	Champ texte	Le numéro de téléphone principal (numéro de téléphone Office) Par exemple, 555-555-5555.
Photo	Image	Une image au format d'un objet blob, d'une chaîne en base64 ou d'un chemin vers une image. Valeurs prises en charge : • Chemin de fichier - utilise un chemin de fichier Windows standard. Le chemin doit être accessible depuis le serveur. • Chaîne codée en base64 - utilise un codage base64 standard. • Binaire - données binaires. Formats d'image pris en charge : png, jpeg et bmp.
Nom souhaité	Champ texte	Le nom préféré de l'identité.
Attributs de provisionnement	Champ texte	Attributs de provisioning tels que définis et configurés par le client pour son environnement. Les éléments de la liste sont séparés par le caractère « | ». Par exemple, A1| A2| Un3.
État ou province	Champ texte.	L'État ou la province où se trouve l'identité.

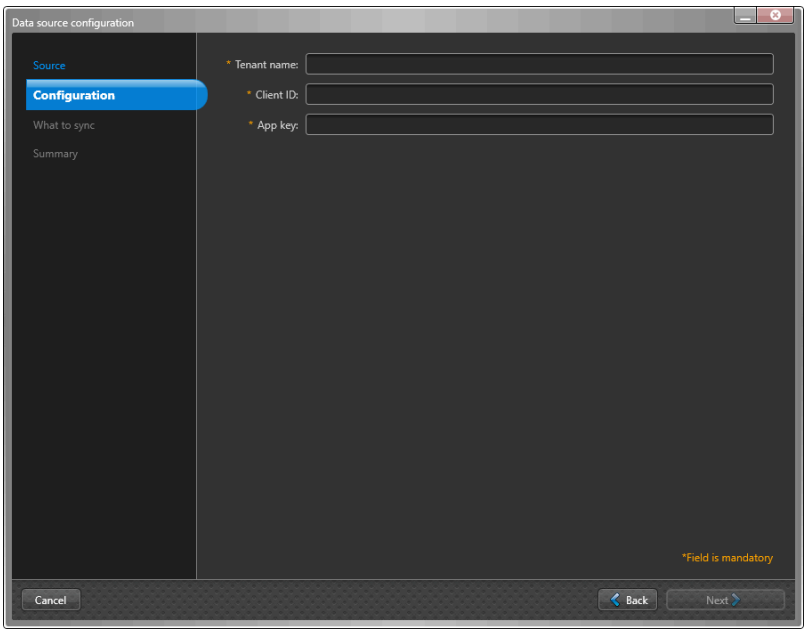
Champ One Identity	Type de donnée	Description
État	Champ texte	L'état d'activation de l'identité. Par exemple, Active ou Inactif.
Nom du superviseur	Champ texte	Le nom du superviseur de l’identité.
Superviseurs	Champ texte	La liste des ID de superviseur uniques pour l’identité. Les éléments de la liste sont séparés par le caractère « | ». Par exemple, A1| A2| Un3.
Utiliser le délai d’accès prolongé	Valeur booléenne	La valeur qui active ou désactive l'option **Utiliser le délai d'accès prolongé**. Par exemple, TRUE ou FALSE.
Type d'utilisateur	Champ texte	Le type d'utilisateur. Par exemple, **Admin** ou **User**.
Nom d’utilisateur	Champ texte	L’adresse e-mail utilisée par l’identité pour se connecter à ClearID.
Accès au portail Web	Champ texte	La valeur qui active ou désactive **l'accès au portail Web**. Par exemple, 0 FALSE ou 1 TRUE.
Code type d'employé	Champ texte	The worker type code.
Description du type de travailleur	Champ texte	The worker type description.
Code postal	Champ texte.	Le code postal du lieu de l’identité.

À propos de l’application Web Azure

L'application Web Azure sert à connecter l’application Genetec ClearID[MC] One Identity Synchronization Tool aux données Azure AD afin de pouvoir consulter et synchroniser les informations sur les utilisateurs Active Directory.

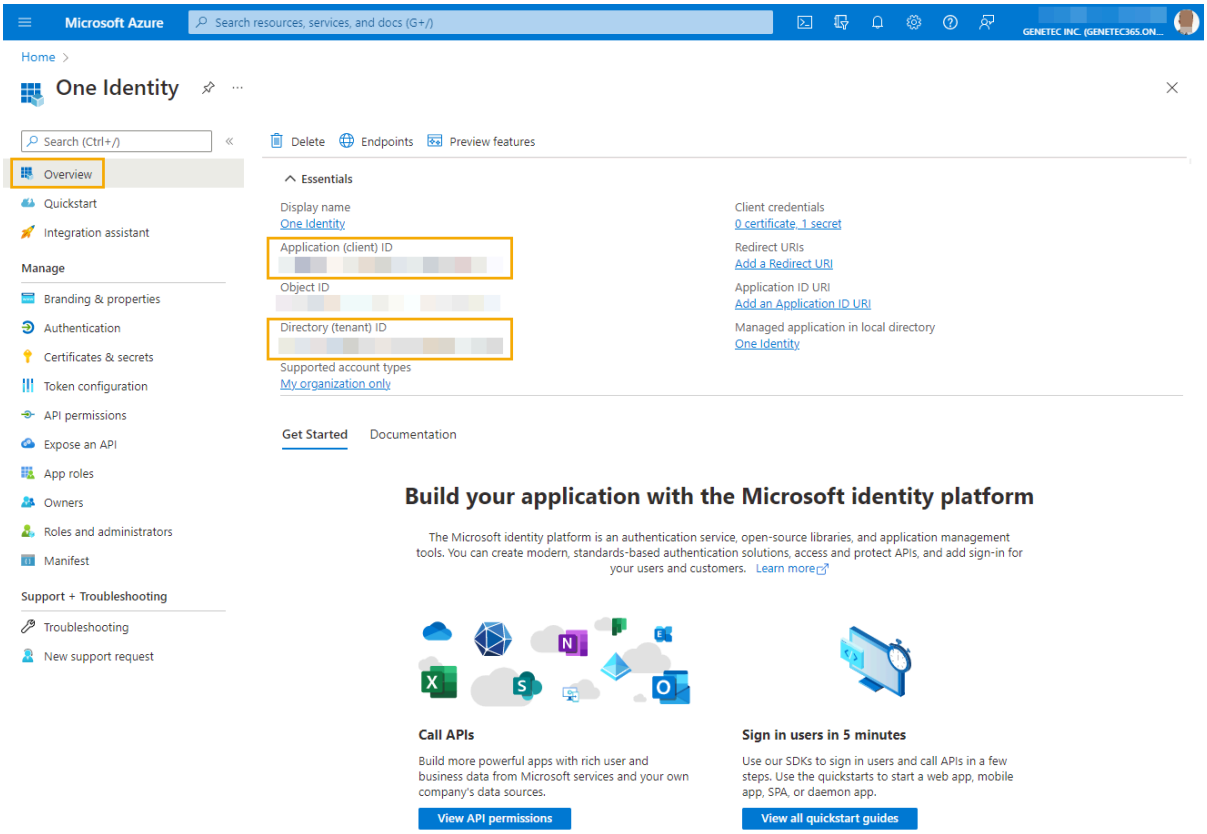
Informations de connexion pour l'application Web Azure

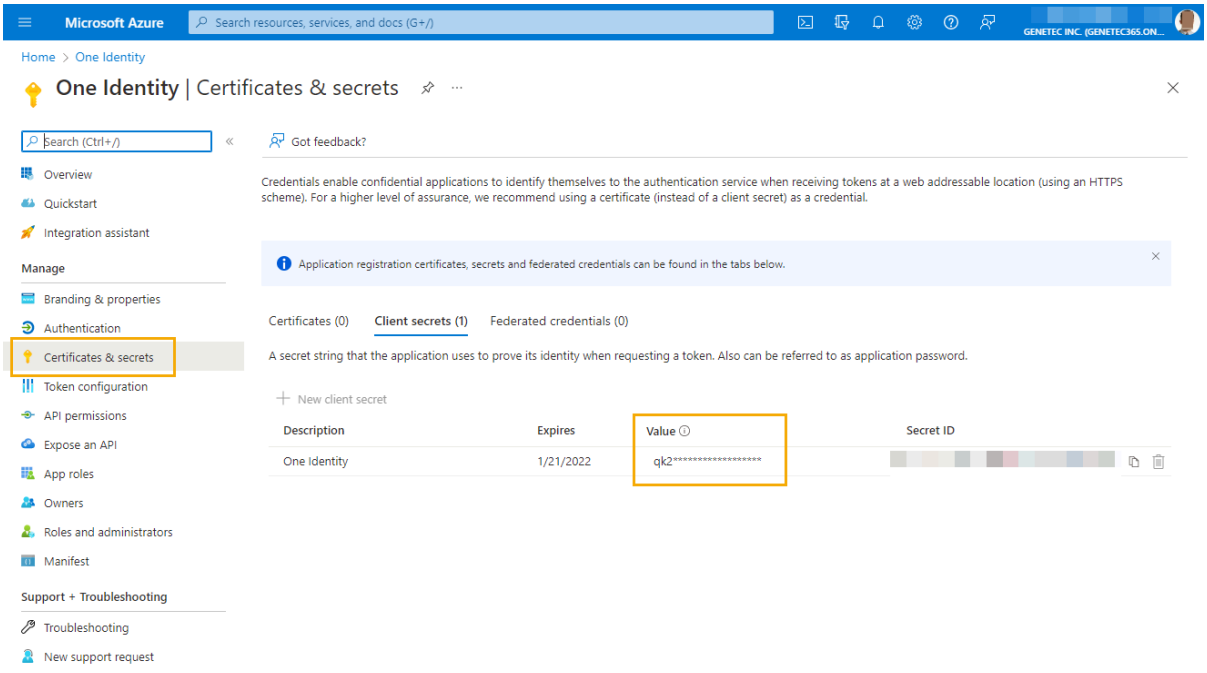
Pour connecter l'application web Azure à ClearID One Identity Synchronization Tool, vous devez disposer des informations suivantes :



- Nom du locataire (ID de répertoire pour le compte)
- ID client (ID d'application)
- Clé d'application (valeur du code client)

CONSEIL : Le nom du locataire, l'ID client et la clé d'application peuvent être obtenus via votre inscription à l'application Azure Active Directory.





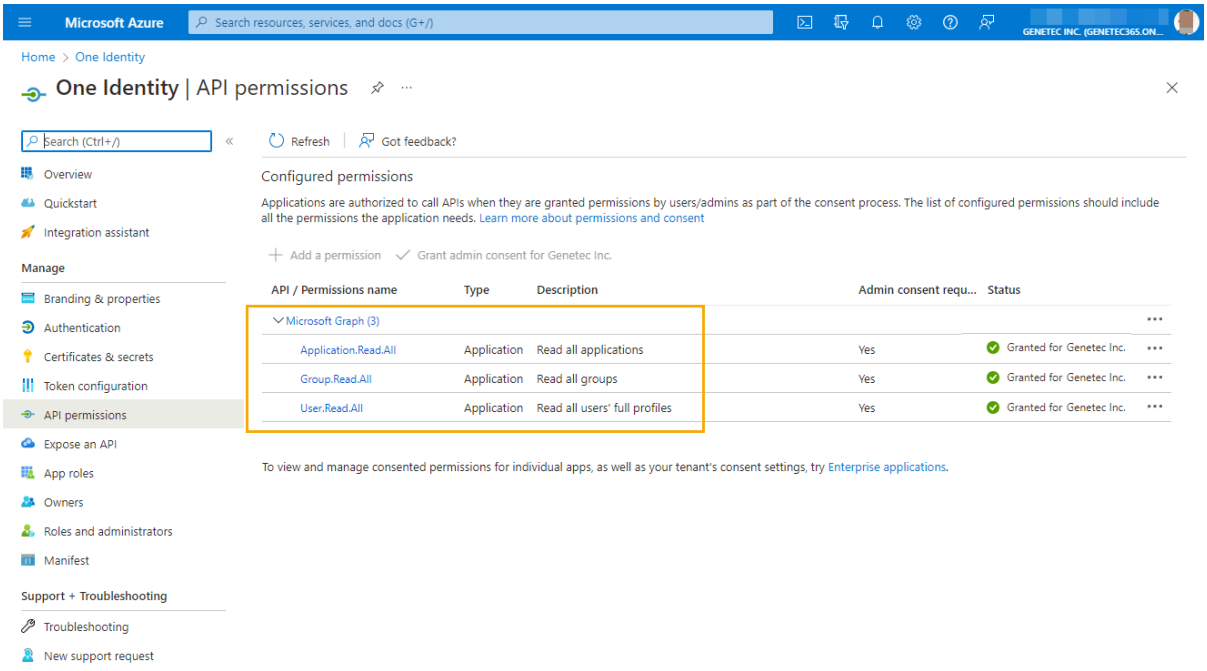
Autorisations d'API Azure AD

Avant de synchroniser des données avec ClearID, un administrateur des attributs du système externe (membre de l’équipe informatique ou de sécurité) doit définir et configurer les privilèges de lecture de l’API suivants dans Azure AD :

Microsoft Graph (configuration requise) :

- *Application.Read.All* - Utilisé pour récupérer les attributs d’extensions.
  - Permet à l'application de lire les applications et les principaux de services sans utilisateur connecté.

  Pour en savoir plus, voir List extensionProperties (extensions d'annuaire)
- *User.Read.All* - Utilisé pour récupérer des informations sur l’utilisateur.
  - Permet à l'application de lire les informations sur les risques de l’utilisateur d’identité dans votre organisation sans utilisateur connecté.
- *Group.Read.All* - Utilisé pour récupérer des informations sur les groupes.
  - Permet à l’application de lire les propriétés et les membres des groupes, et de lire les conversations de tous les groupes, sans utilisateur connecté.



Pour en savoir plus, voir Référence des autorisations Microsoft Graph.

Installer One Identity Synchronization Tool

Avant d'importer des informations sur les identités depuis un système externe dans Genetec ClearID^{MC}, vous devez installer Genetec ClearID^{MC} One Identity Synchronization Tool.

Avant de commencer

Obtenez le dernier pack d'installation auprès de votre contact de déploiement.

À savoir

Cette procédure est destinée au personnel informatique ou de sécurité chargé de l'administration des attributs système externes.

Installez l'outil de synchronisation One Identity sur un serveur dédié. Il ne doit pas forcément s'agir d’un serveur Security Center.

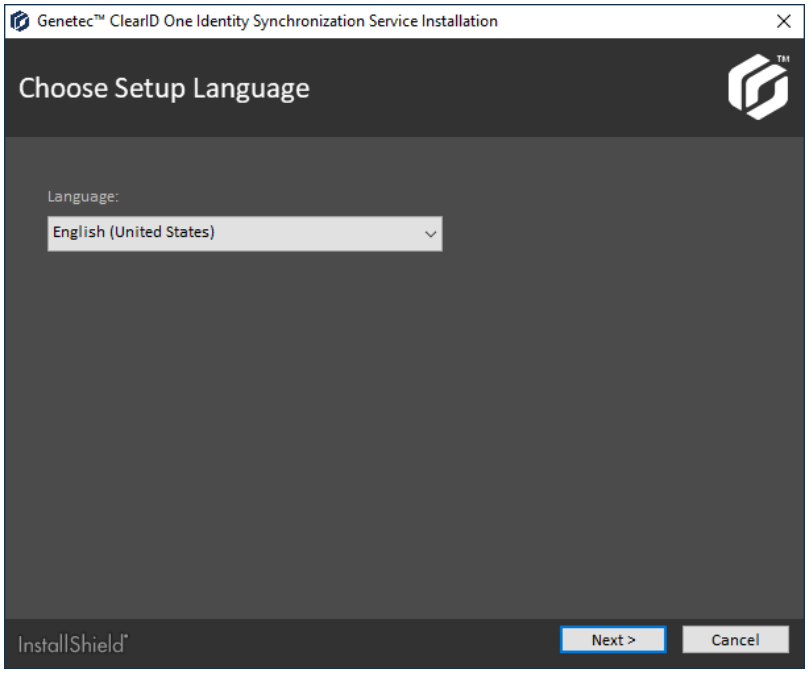
REMARQUE : L'outil de synchronisation One Identity n'est généralement pas disponible en téléchargement public. Le lien de téléchargement de l’outil de synchronisation est fourni par votre contact de déploiement en cas de besoin.

Procédure

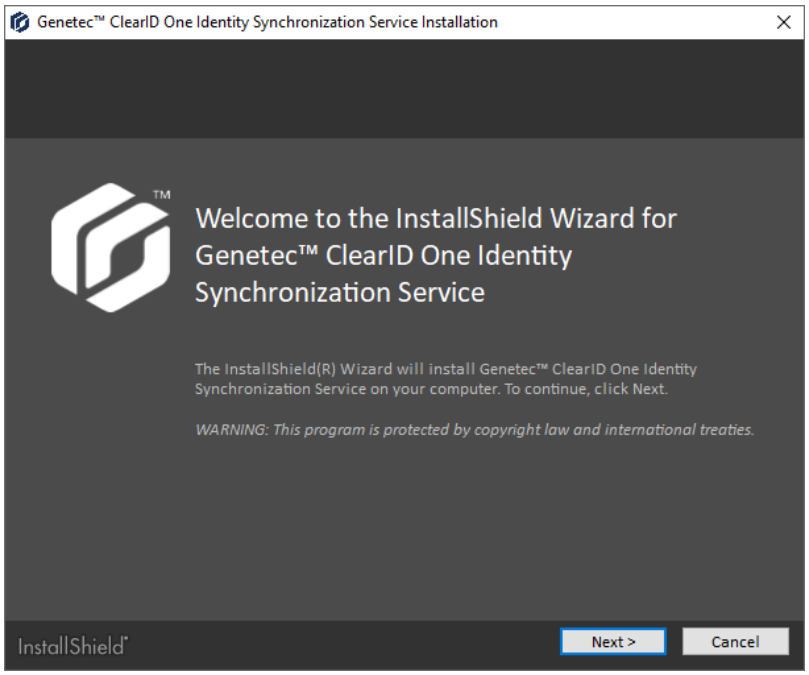
1 Naviguez jusqu’au programme d’installation de ClearID One Identity Synchronization Tool fourni par votre contact de déploiement.

2 Faites un clic droit sur le fichier *setup.exe*. Cliquez sur **Exécuter en tant qu'administrateur** et suivez les instructions d'installation.

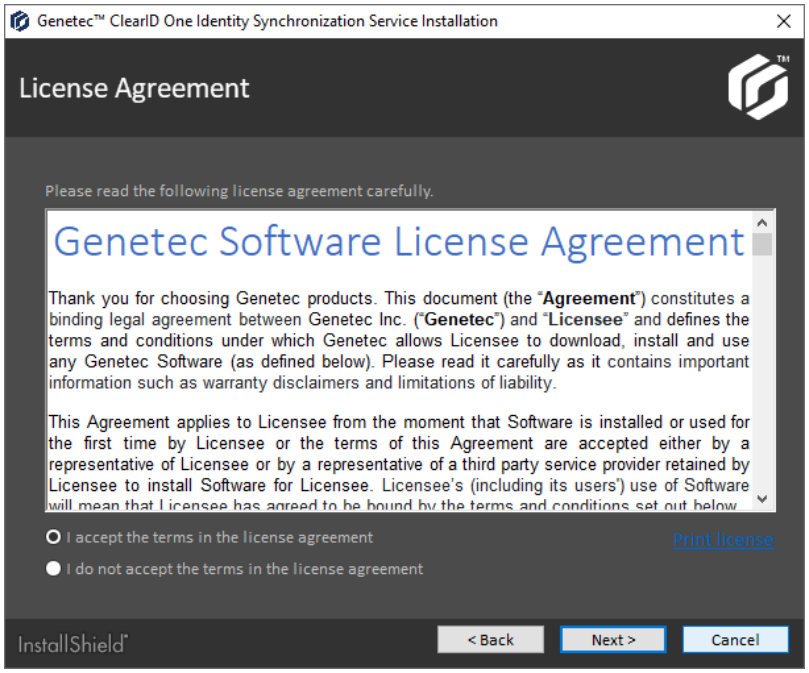
3 Dans la boîte de dialogue *Installation du service Genetec ClearID*[MC] *One Identity Synchronization*, sélectionnez une langue d'installation et cliquez sur **Suivant**.



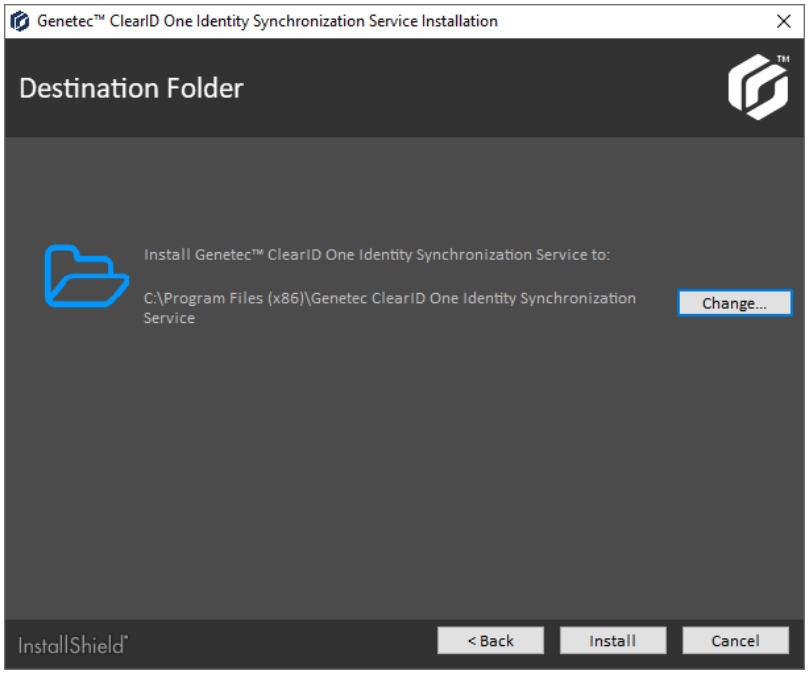
4 Dans la section *Bienvenue dans l'Assistant InstallShield*, cliquez sur **Suivant**.



5 Lisez et acceptez l'accord de licence, puis cliquez sur **Suivant**.



6 Spécifiez votre dossier de destination.

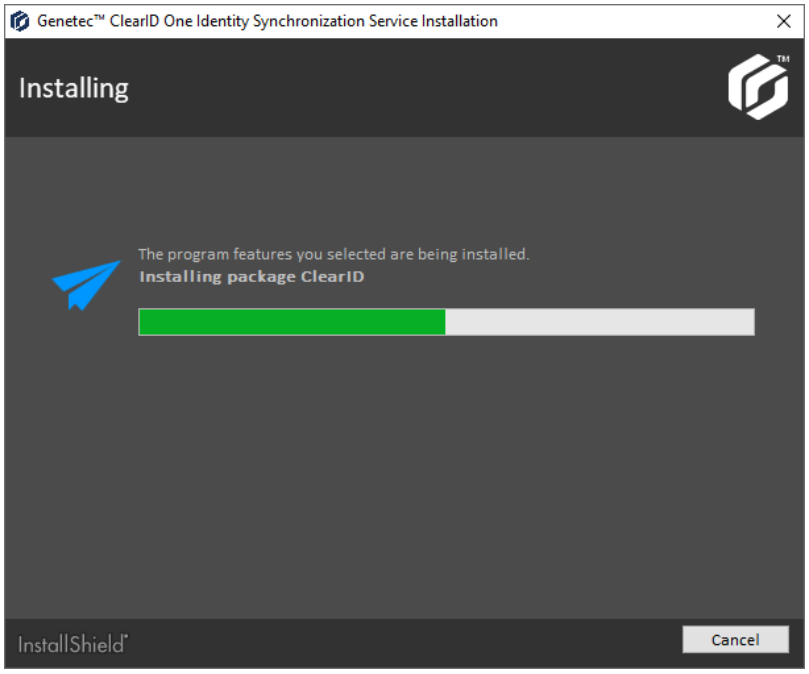


Par défaut, le service est installé dans *C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service*.

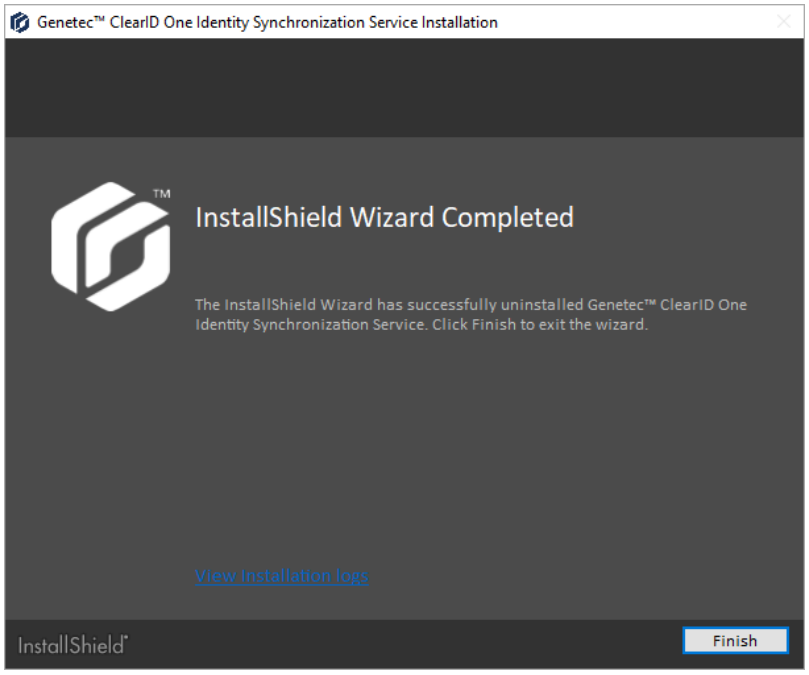
7 (Facultatif) Cliquez sur **Modifier** pour modifier le dossier de destination.

a) Dans la boîte de dialogue **Rechercher un dossier**, recherchez et sélectionnez le dossier dans lequel vous souhaitez installer le service, puis cliquez sur **OK**.

8 Cliquez sur **Installer**.



9 Cliquez sur **Terminer** pour terminer l'installation.



ClearID One Identity Synchronization Tool est à présent installé.

Lorsque vous avez terminé

Configurez l'outil de synchronisation.

Désinstaller One Identity Synchronization Tool

De temps à autre, vous voudrez potentiellement désinstaller Genetec ClearID[MC] One Identity Synchronization Tool pour résoudre un problème ou installer une version plus récente.

Avant de commencer

Genetec ClearID One Identity Synchronization Tool doit être installé.

À savoir

Cette procédure est destinée au personnel informatique ou de sécurité chargé de l'administration des attributs système externes.

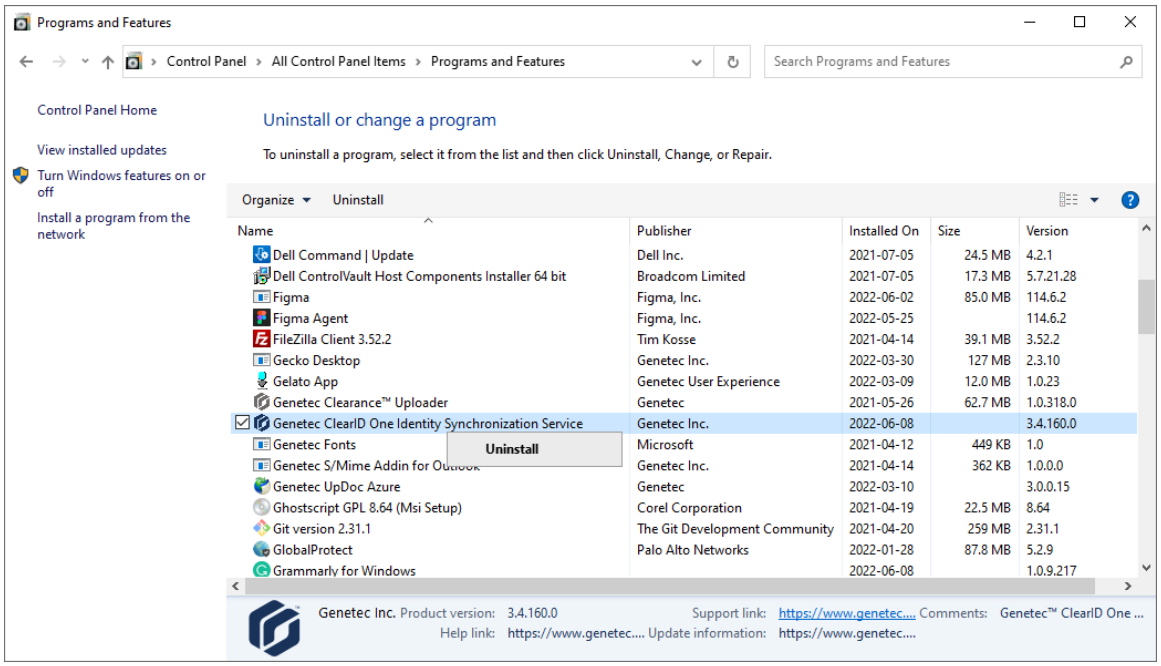
- Les options que vous rencontrez lors de la désinstallation d'un programme (service) peuvent varier en fonction de la version de Windows que vous exécutez.
- Cette procédure décrit comment désinstaller l'outil de synchronisation (service) d'un client Windows 10.

ATTENTION : Le processus de désinstallation supprime toutes les données de configuration. Si vous effectuez une mise à niveau, veillez à sauvegarder les données du programme dans le dossier de configuration *C:\ProgramData\Genetec\OneIdentity\Configuration*.

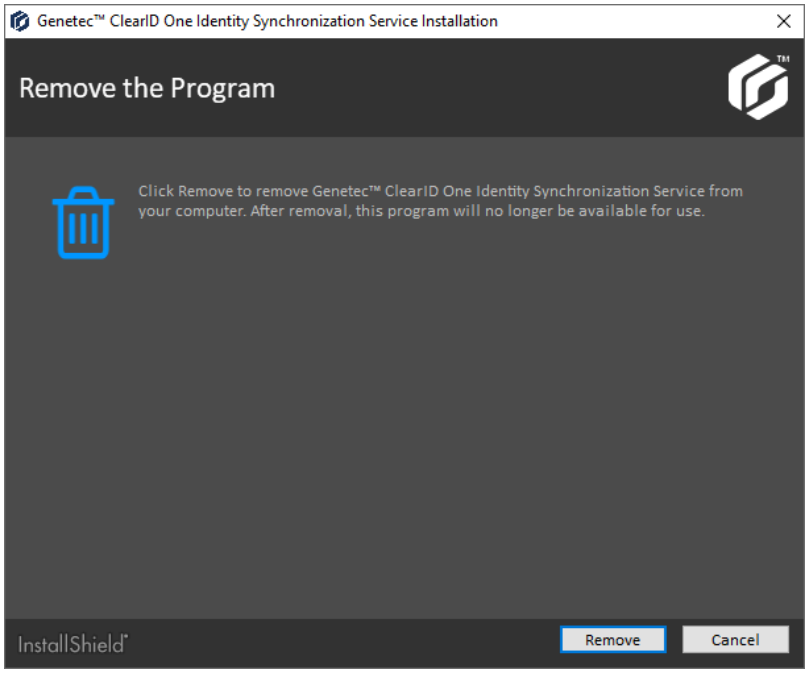
Procédure

1 Ouvrez le **Panneau de configuration** Windows, allez dans la section *Programmes* et cliquez sur **Désinstaller un programme** pour accéder à **Applications et fonctionnalités**.

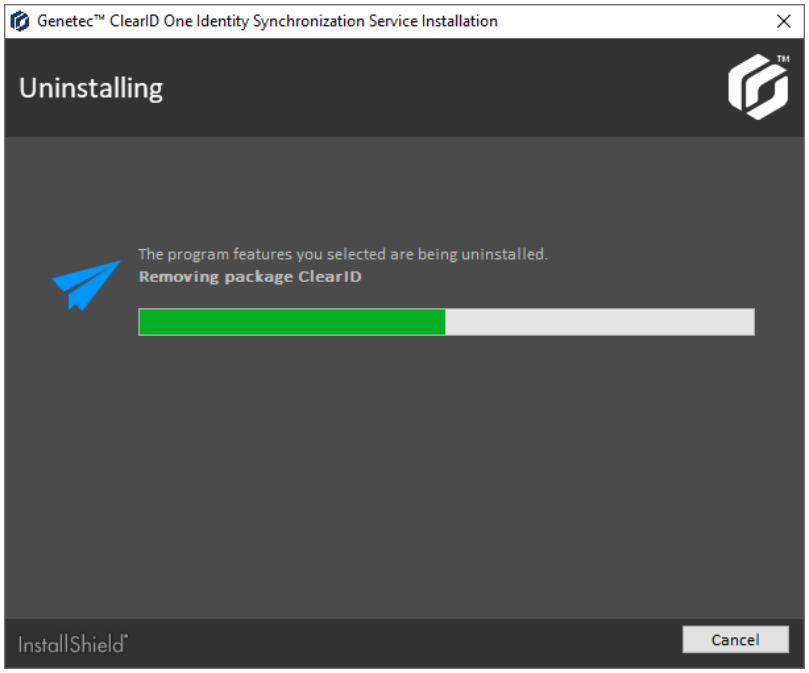
2 Repérez le service ClearID One Identity Synchronization Tool et faites un clic droit pour afficher l'option **Désinstaller**, puis cliquez sur **Désinstaller**.



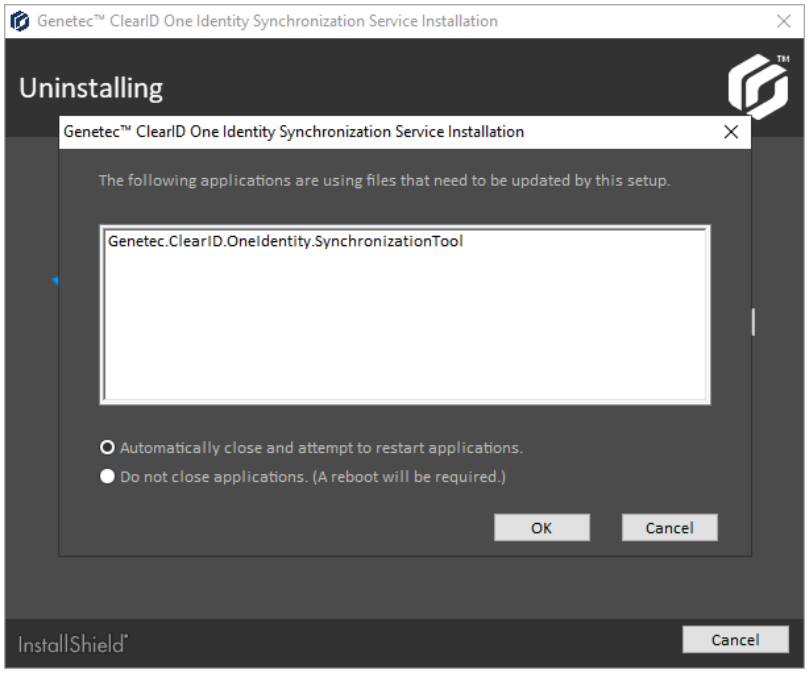
3 Cliquez sur **Supprimer** pour supprimer le programme.



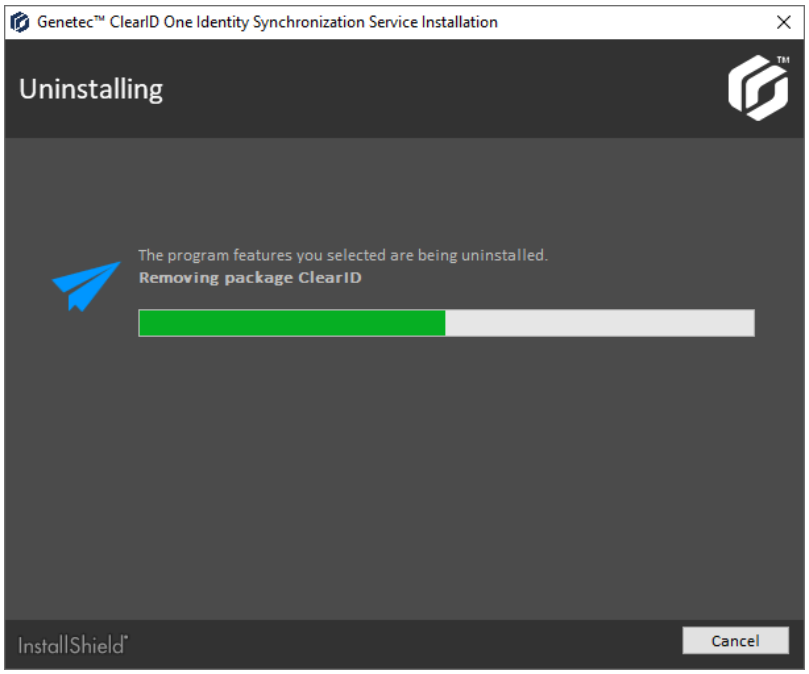
La désinstallation du programme commence.



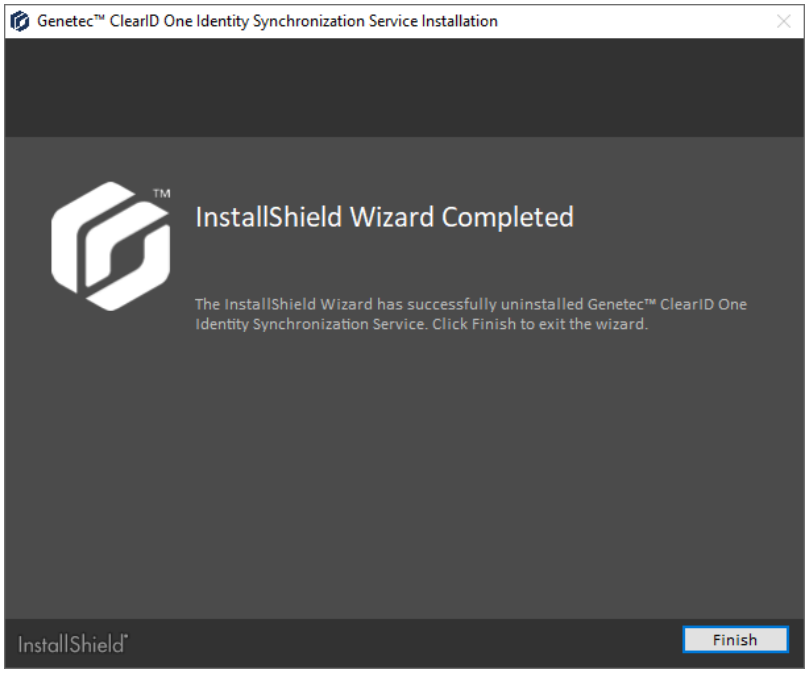
4 (Facultatif) Si la boîte de dialogue suivante s'affiche, sélectionnez **Fermer automatiquement et tenter de redémarrer les applications**, puis cliquez sur **OK**.



Le pack continue de se désinstaller.



5 Cliquez sur **Terminer** pour terminer la désinstallation.



ClearID One Identity Synchronization Tool est à présent désinstallé.

Mettre à niveau One Identity Synchronization Tool

Effectuez la mise à niveau de Genetec ClearID[MC] One Identity Synchronization Tool vers la dernière version disponible pour pouvoir profiter de nouvelles fonctionnalités.

Avant de commencer

Genetec ClearID One Identity Synchronization Tool doit être installé.

À savoir

Cette procédure est destinée au personnel informatique ou de sécurité chargé de l'administration des attributs système externes.

Procédure

1 Sauvegardez le dossier de configuration *C:\ProgramData\Genetec\OneIdentity\Configuration*.

Le dossier contient les paramètres de configuration. Par exemple, *ApiConfiguration.dat*, *ClearIdEntityMappingFile.xml*, *Configuration.xml* et *SingleCardEntityMapping.xml*.

REMARQUE : Les fichiers *.dat* ou *.xml* présents dans le dossier de configuration varient en fonction des réglages configurés dans ClearID One Identity Synchronization Tool.

2 Désinstallez ClearID One Identity Synchronization Tool (version précédente).

3 Installez ClearID One Identity Synchronization Tool (dernière version).

4 Vérifiez que ClearID One Identity Synchronization Tool fonctionne comme prévu.

REMARQUE : Vous devez avoir les mêmes configurations de sources de données qu'avant la mise à niveau.

ClearID One Identity Synchronization Tool est à présent mis à niveau.

Configurer One Identity Synchronization Tool

Avant de synchroniser un système externe avec Genetec ClearID[MC], vous devez configurer Genetec ClearID[MC] One Identity Synchronization Tool.

Avant de commencer

- Familiarisez-vous avec les champs d'attribut One Identity.
- Préparez un les valeurs des attributs d'identités que vous souhaitez importer et synchroniser avant de procéder à la synchronisation.
- Téléchargez une clé d'authentification de service.
- Installez l'outil de synchronisation One Identity.
- Consultez vos informations de licence : La référence CD-IDSYNC-SERVICE-1Y est requise pour l’importation One Identity Synchronization Tool.

IMPORTANT : Vérifiez que le fichier n'est pas en cours d'édition et qu'il est fermé, car l'outil de synchronisation verrouille le fichier pendant le processus de synchronisation.

À savoir

Cette procédure est destinée au personnel informatique ou de sécurité chargé de l'administration des attributs système externes.

La synchronisation des attributs du système externe avec les attributs d'identité ClearID ne fonctionne qu’en mode ENTRANT.

ATTENTION : Toute modification apportée aux identités dans ClearID peut être remplacée lors de la synchronisation suivante du système externe.

Procédure

1 Configurez vos paramètres de connexion.

2 Configurez les paramètres de source de données pour l'une des sources suivantes :

- Azure AD
- Base de données (Microsoft SQL Server, Oracle Database, ODBC)
- Fichier (CSV)

3 Configurez vos paramètres de synchronisation.

4 Cliquez sur **Enregistrer**.

Lorsque vous avez terminé

Vérifiez que les nouveaux attributs du système externe ont été synchronisés et contiennent les bons attributs.

Configurer les réglages de connexion

Avant de synchroniser un système externe avec Genetec ClearID[MC], vous devez configurer les réglages de connexion de Genetec ClearID[MC] One Identity Synchronization Tool.

Avant de commencer

- Vérifiez les valeurs des attributs d'identités que vous souhaitez importer avant de procéder à la synchronisation.
- Téléchargez une clé d'authentification de service.

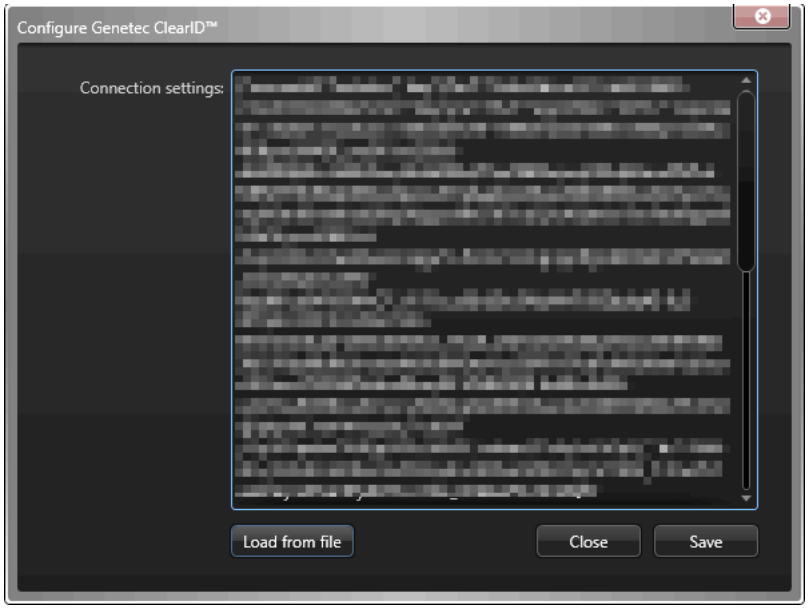
- Consultez vos informations de licence : La référence CD-IDSYNC-SERVICE-1Y est requise pour l’importation One Identity Synchronization Tool.

À savoir

Procédure

1 Ouvrez l'outil de synchronisation One Identity (*OneIdentityConfigurationTool.exe*) et configurez vos paramètres.

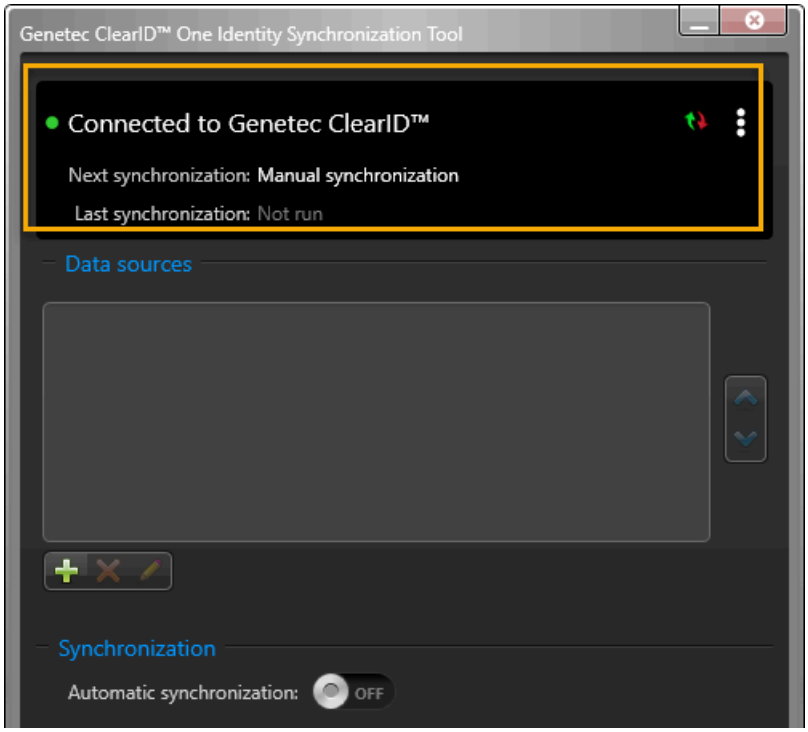
2 Configurez vos paramètres de connexion.
   a) Dans l'outil de synchronisation One Identity, cliquez sur **Configurer**.
   b) Dans la boîte de dialogue *Configurer Genetec ClearID*^{MC}, cliquez sur **Charger à partir du fichier**.
   c) Accédez à et sélectionnez votre clé d'authentification.



3 Cliquez sur **Enregistrer**.

   REMARQUE : Le service One Identity redémarre automatiquement lorsque les réglages de connexion pour la clé d'authentification sont modifiés.

One Identity Synchronization Tool est à présent connecté à ClearID.



Lorsque vous avez terminé

Configurez vos sources de données. Choisissez l'une des options suivantes :

- Configurer la source de données pour la synchronisation avec Azure AD, page 538
- Configurer la source de données pour la synchronisation d’une base de données, page 547
- Configurer la source de données pour la synchronisation de fichiers, page 556

Configurer la source de données pour la synchronisation avec Azure AD

Avant de synchroniser un système externe avec Genetec ClearID[MC], vous devez configurer les sources de données Genetec ClearID[MC] One Identity Synchronization Tool pour la synchronisation avec Azure Active Directory.

Avant de commencer

- Familiarisez-vous avec les champs d'attribut One Identity.
- Familiarisez-vous avec l'application Web Azure.
  - Notez les paramètres de connexion de l'application Web Azure pour une utilisation ultérieure.
  - Vérifiez que les autorisations d'API Azure AD sont configurées.
- Préparez un annuaire Azure Active Directory contenant les attributs d'identités que vous souhaitez importer et synchroniser.
- Consultez vos informations de licence : La référence CD-IDSYNC-SERVICE-1Y est requise pour l’importation One Identity Synchronization Tool.

À savoir

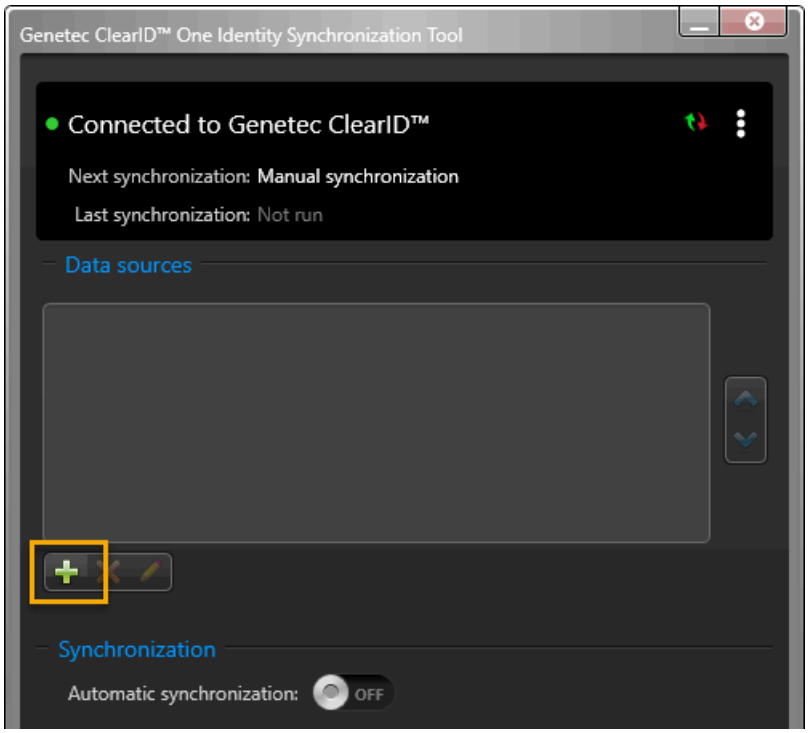
Cette procédure est destinée au personnel informatique ou de sécurité chargé de l'administration des attributs système externes.

Cette procédure décrit uniquement comment configurer la source de données pour **Azure AD**.

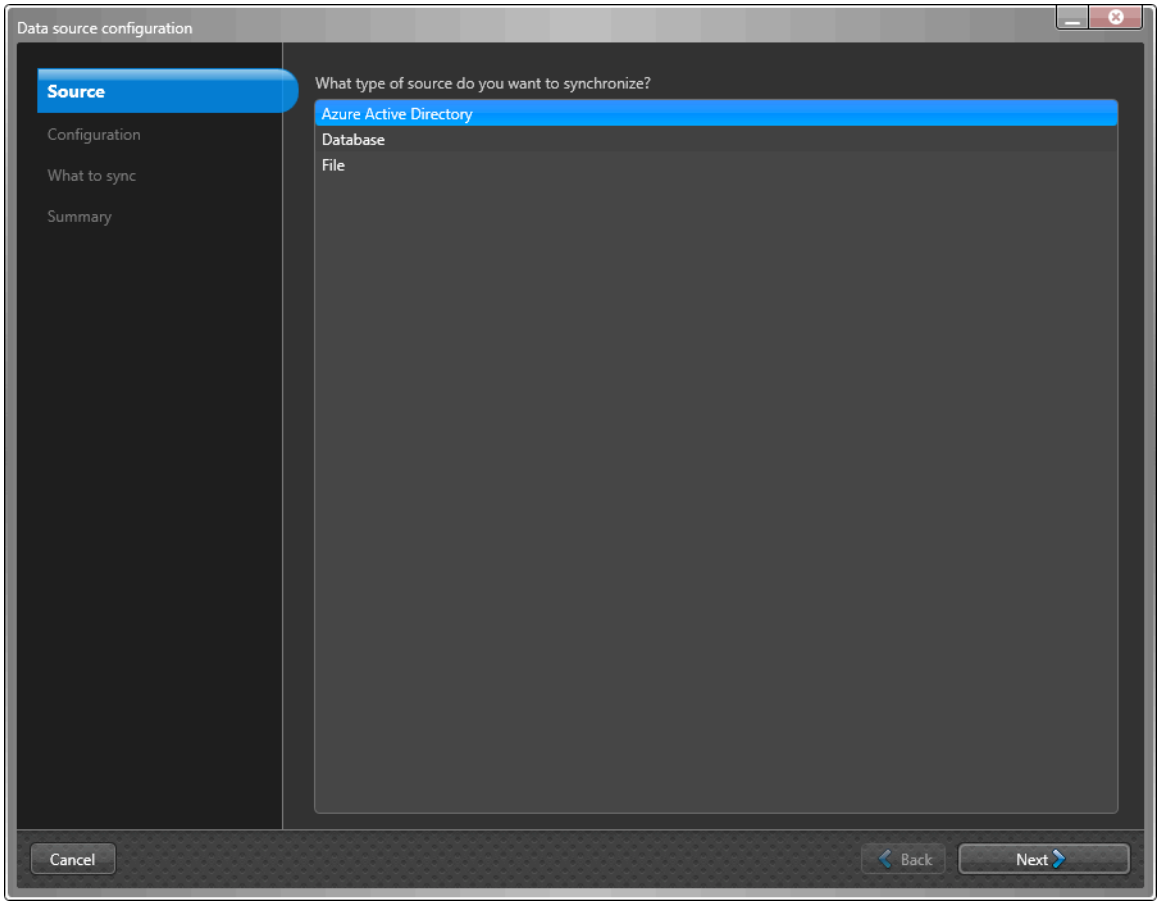
- L'ordre des sources de données est important car la première source de données remplace toujours les champs communs.
- Il n'y a pas de limite au nombre de sources de données. Cependant, plus la source de données est volumineuse, plus les besoins en mémoire augmentent.
- Lorsque vous utilisez une source de données Azure pour synchroniser les identités, le seul champ possible pour **ID unique** est le champ **UserId**. Lorsque la source de données Azure est sélectionnée, les champs **ID unique** ne peuvent pas être configurés et l'utilisation du champ **UserId** Azure est déclenchée par défaut.

Procédure

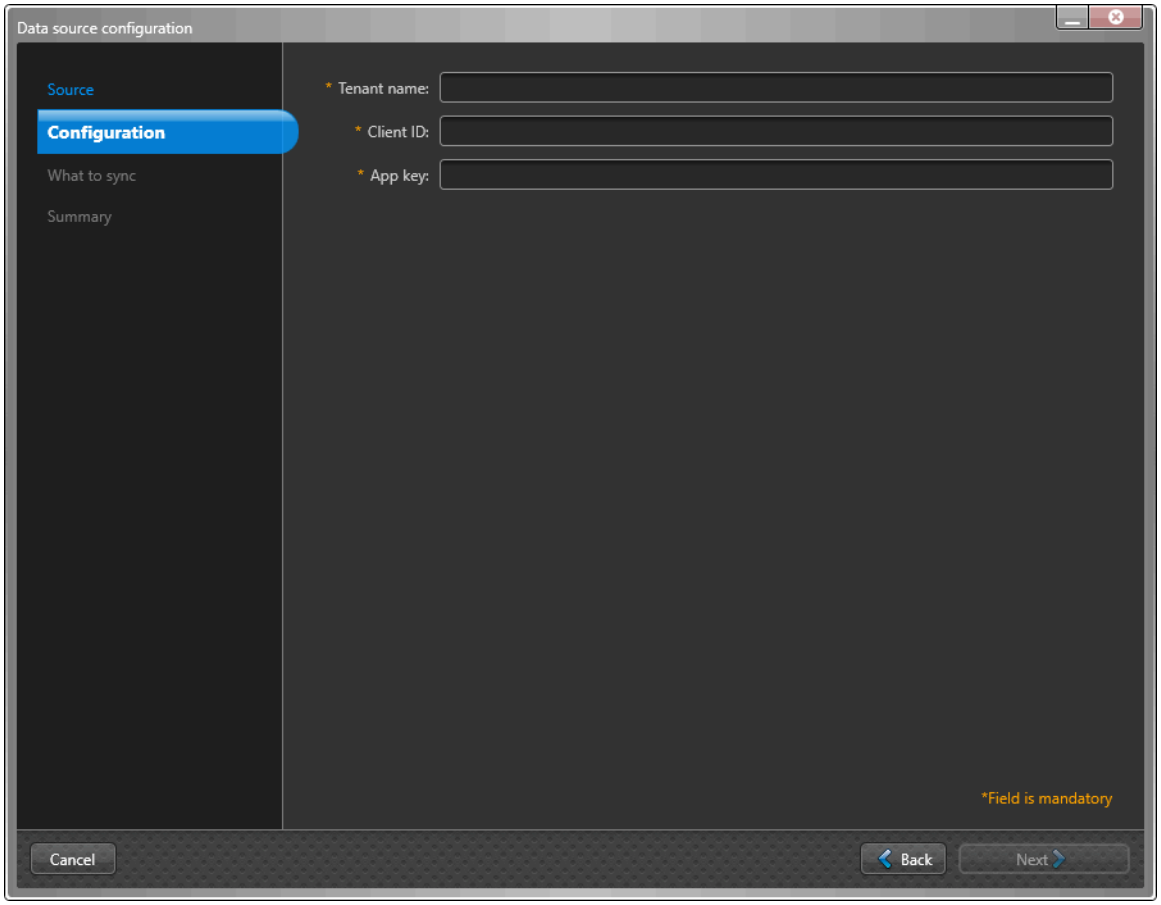
1 Dans la section *Sources de données* de l'outil de synchronisation One Identity, cliquez sur **Ajouter une source de données** ( ).



2 Dans la section *Source* de la boîte de dialogue *Configuration de la source de données*, cliquez sur **Azure Active Directory**, puis sur **Suivant**.



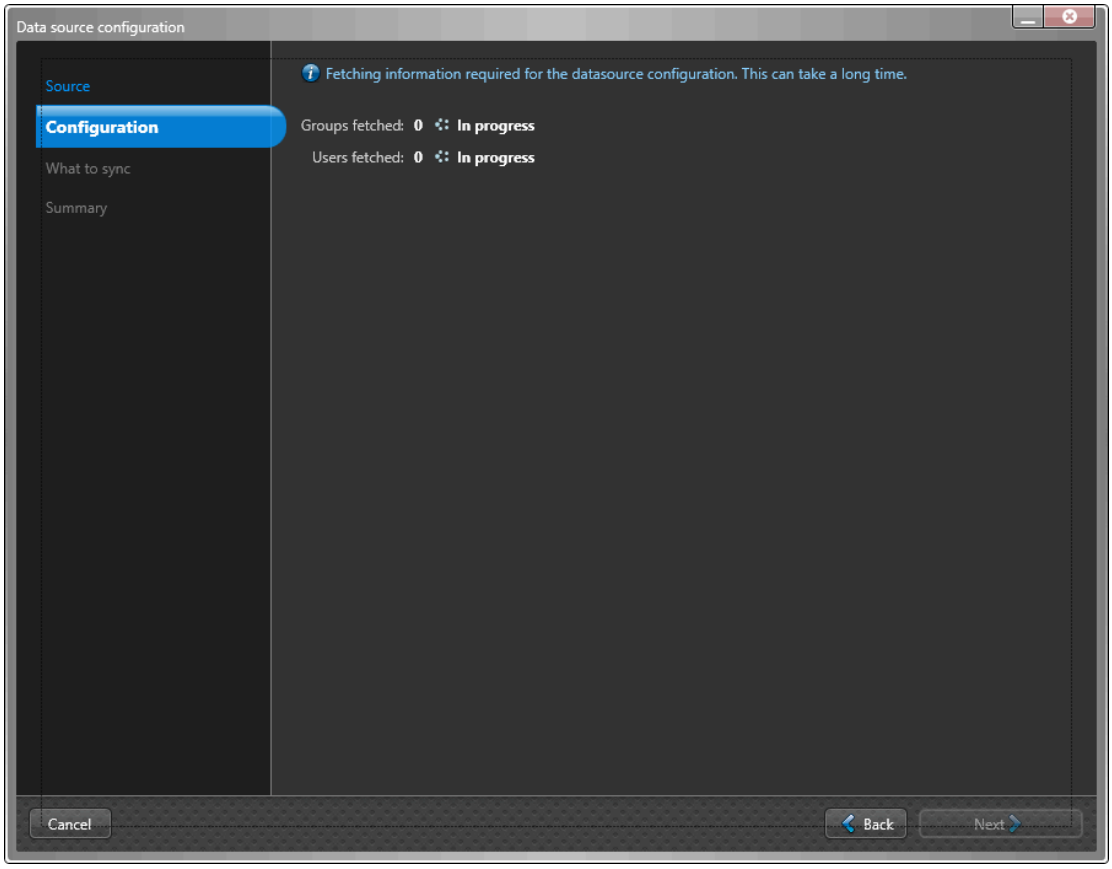
3 Dans la section *Configuration* de la boîte de dialogue *Configuration de la source de données*, renseignez les champs obligatoires suivants :



- **Nom de locataire :** Dans le champ **Nom du locataire**, saisissez votre nom de locataire (nom de compte). Le nom du locataire est utilisé pour se connecter au Répertoire du compte. Par exemple, une adresse d'hôte *account.onmicrosoft.com* ou un GUID nxxnxnxx-nnnn-nxnn-nnnx-nxnnnxnnxnnn.
- **ID client :** Dans le champ **ID client**, saisissez votre ID client. L'ID client est utilisé pour se connecter à l'application cliente. Le format **ID client** est un code alphanumérique comme suit : nxnxnxxn-xxnn-nnnx-xxnn-nxxxnxnnnxnn.
- **Clé d’app :** Dans le champ **Clé d'application**, saisissez votre clé d'application. La clé d'application sert à authentifier les communications avec ClearID. Le format de la **clé d'application** est un code alphanumérique comme suit : nXnxxxxXxxXnxxxXXXxXXnxxXXXnnxxxXXnXXXXXxxx = .

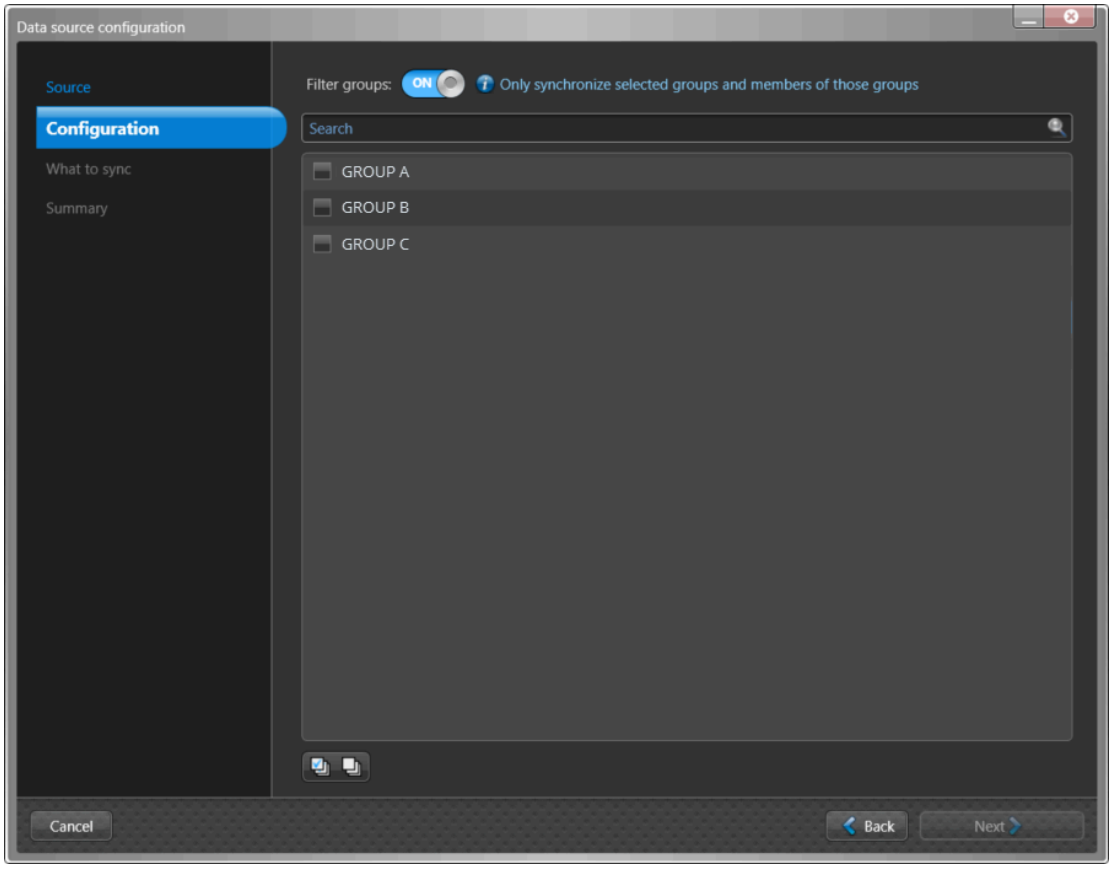
CONSEIL : Le nom du locataire, l'ID client et la clé d'application peuvent être obtenus via votre inscription à l'application Azure Active Directory.

a) Cliquez sur **Suivant**.



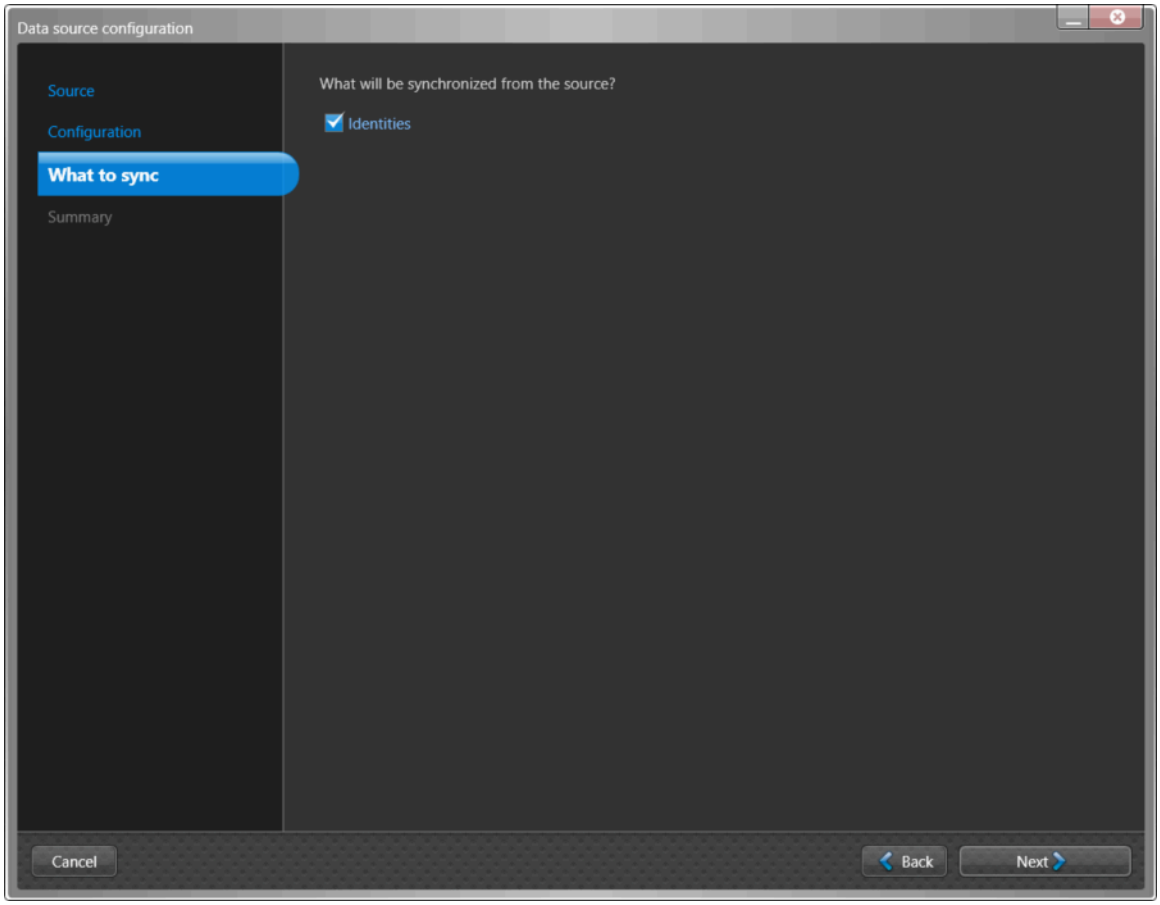
REMARQUE : La récupération des informations requises pour la configuration de la source de données peut prendre du temps et varie en fonction du nombre de groupes et d'utilisateurs.

b) (Facultatif) Utilisez l'option **Filtrer les groupes** pour synchroniser uniquement un sous-ensemble de groupes et de membres de groupe Azure AD sélectionnés. Recherchez ou sélectionnez les groupes dont vous avez besoin et cliquez sur **Suivant**.



REMARQUE : Si votre liste Azure AD est longue, vous pouvez également utiliser l'icône **Tout sélectionner** ou **Tout désélectionner** pour vous aider dans le processus de sélection.

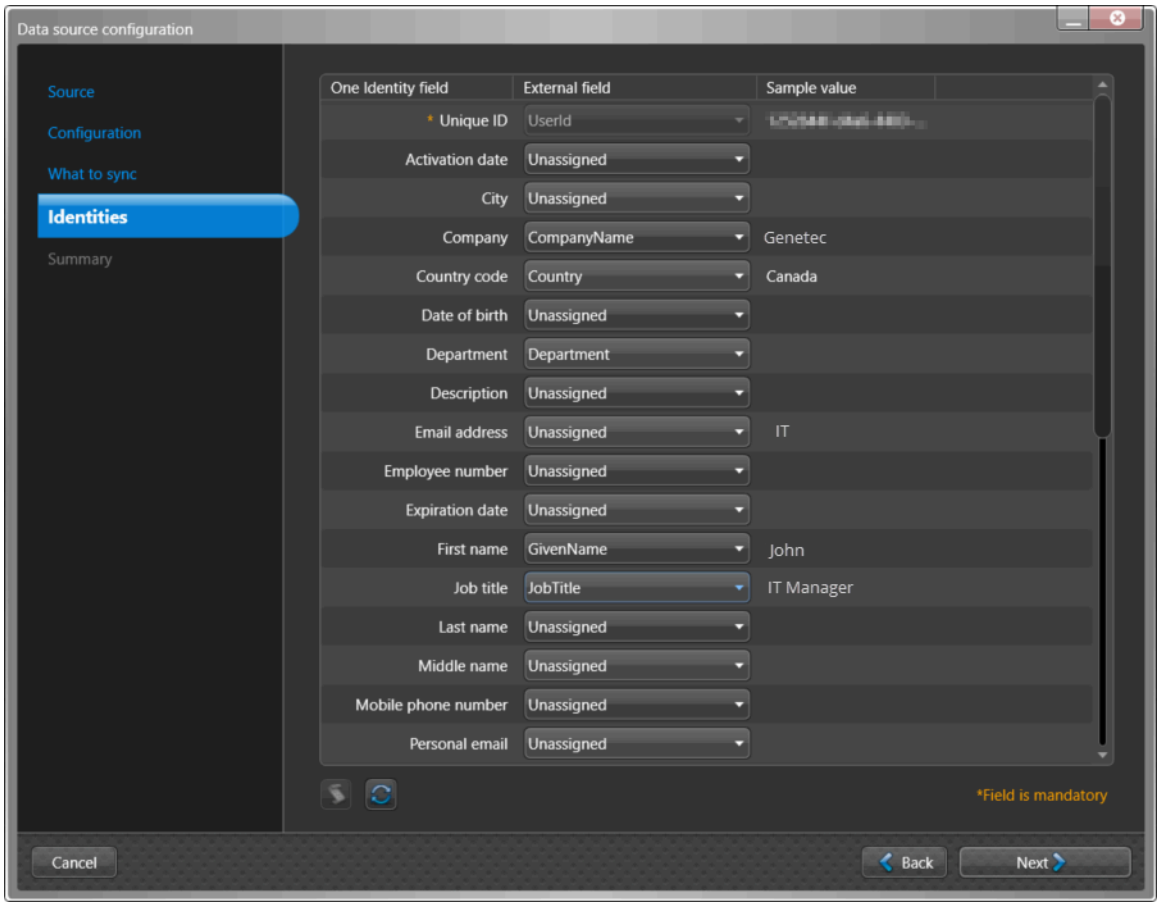
4 Dans la section *Éléments à synchroniser* de la boîte de dialogue *Configuration de la source de données*, sélectionnez **Identités** pour synchroniser avec la source de données du système externe.



5 Si vous avez sélectionné **Identités** comme source de données, dans la section *Éléments à synchroniser*, configurez les paramètres des attributs d'identité.

REMARQUE : Les champs affichés dans la section *Identités* dépendant de la source de données sélectionnée dans la section *Source*.

L'image suivante montre les options qui s'affichent après la sélection d'une source de données **Azure AD**.



a) Configurez vos mappages d'attributs de **champ externe**.

- **Champ One Identity :** Affiche les attributs d'identité ClearID. Les champs obligatoires sont indiqués par un astérisque (*).
- **Champ externe :** Sélectionnez les attributs système dans les colonnes **Champ externe** du système externe que vous souhaitez associer aux attributs d'identité ClearID affichés dans la colonne **Champ One Identity**.

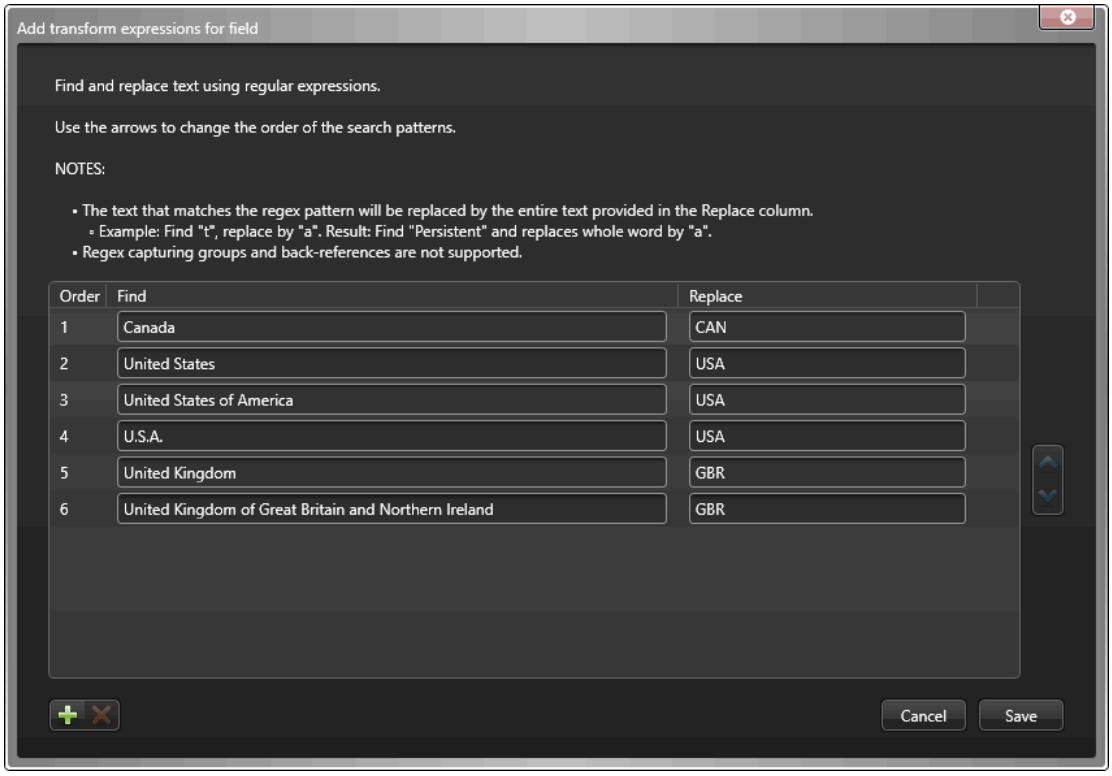
ATTENTION : Lors de l'utilisation d'**Azure AD** comme source de données, le champ **ID unique** de One Identity doit être mappé vers le champ externe **ID utilisateur** d'Azure AD pour garantir que les attributs d'identité sont correctement mappés et synchronisés.

- **Valeur témoin :** Si un **Champ externe** est sélectionné, un exemple des données de champ externe sélectionnées dans votre source de données s'affiche (le cas échéant) dans le texte de la colonne **Valeur échantillon**, à côté de la colonne **Champ externe**.

CONSEIL : Utilisez la colonne Valeur témoin pour valider le format des données d’attribut que vous êtes sur le point d'importer depuis votre système externe dans ClearID.

b) (Facultatif) Cliquez sur **Script** ( ) pour ajouter une expression de transformation afin de rechercher et de remplacer le texte de champ externe à l'aide d'expressions régulières.

Par exemple, vous pouvez rechercher des variantes d'un nom de pays à remplacer par un code de pays correct.



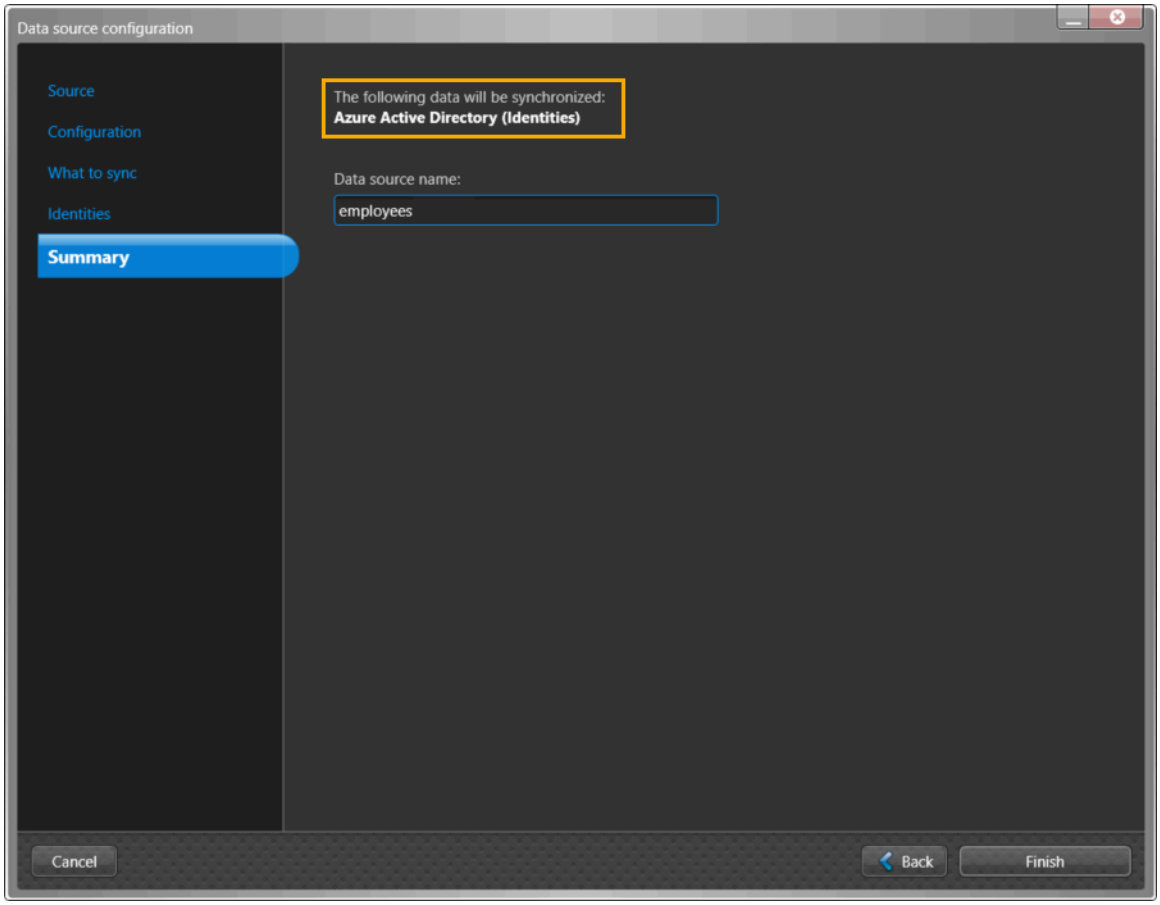
- Une icône de script ( ) est affichée dans la colonne **Exemple de valeur** lorsque le texte du champ est remplacé par une expression régulière.
- Les expressions de transformation sont traitées dans l'ordre spécifié dans la boîte de dialogue *Ajouter des expressions de transformation pour le champ*.

CONSEIL : Si nécessaire, vous pouvez sélectionner la ligne des expressions dont vous n'avez plus besoin et cliquer sur **Supprimer** .

c) (Facultatif) Cliquez sur **Actualiser** ( ) pour mettre à jour les données des champs externes à partir de votre source de données. Cette option d'actualisation est utilisée dans les situations où les données existantes ont été modifiées, de nouvelles lignes de données ont été ajoutées ou de nouvelles colonnes d'attributs ont été ajoutées.

d) Cliquez sur **Suivant**.

6 Dans la section *Résumé*, examinez les données qui seront synchronisées.



REMARQUE : Si plusieurs sources de données sont sélectionnées, seul le premier fichier de source de données s'affiche dans la section *Résumé* pour le champ **Nom de la source de données**. Si vous souhaitez que chacun des fichiers de données soit répertorié dans la section **Sources de données**, vous devez les ajouter individuellement.

a) Si les détails de la synchronisation des données semblent corrects, cliquez sur **Terminer**.

Lorsque vous avez terminé

Configurez vos paramètres de synchronisation.

Rubriques connexes

À propos des champs d'attributs One Identity Synchronization Tool, page 522

Configurer la source de données pour la synchronisation d’une base de données

Avant de synchroniser un système externe avec Genetec ClearID^{MC}, vous devez configurer les sources de données Genetec ClearID^{MC} One Identity Synchronization Tool pour la synchronisation avec une base de données.

Avant de commencer

- Familiarisez-vous avec les champs d'attribut One Identity.
- Préparez les attributs d'identités que vous souhaitez importer et synchroniser.
- Consultez vos informations de licence : La référence CD-IDSYNC-SERVICE-1Y est requise pour l’importation One Identity Synchronization Tool.

À savoir

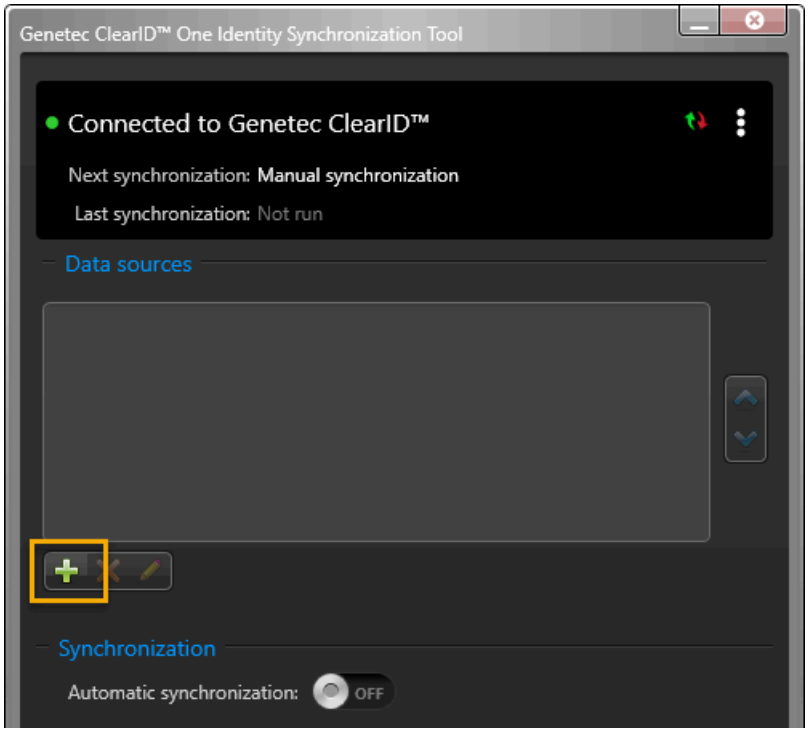
Cette procédure est destinée au personnel informatique ou de sécurité chargé de l'administration des attributs système externes.

Cette procédure décrit comment configurer la source de données pour une **base de données** (Microsoft SQL Server, base de données Oracle, ODBC).

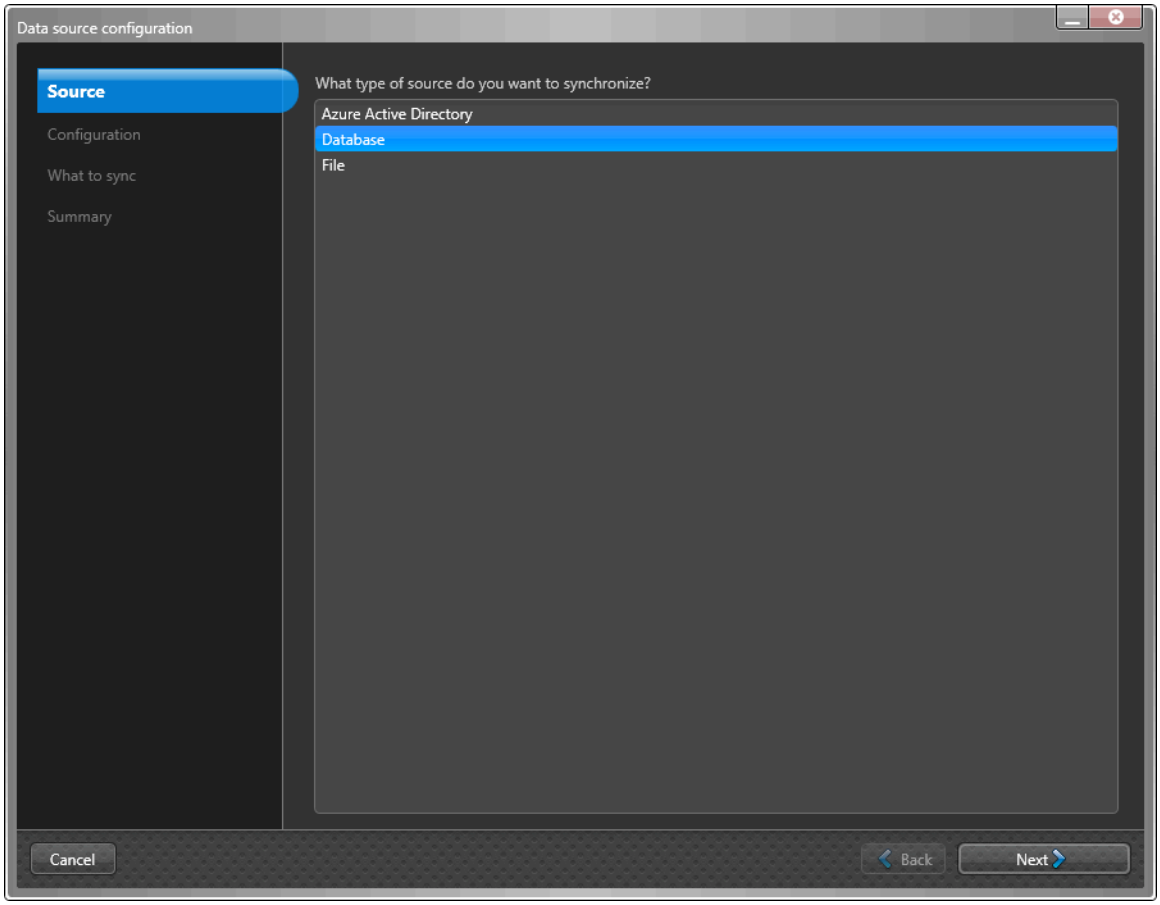
- L'ordre des sources de données est important car la première source de données remplace toujours les champs communs.
- Il n'y a pas de limite au nombre de sources de données. Cependant, plus la source de données est volumineuse, plus les besoins en mémoire augmentent.

Procédure

1 Dans la section *Sources de données* de l'outil de synchronisation One Identity, cliquez sur **Ajouter une source de données** ( ).



2 Dans la section *Source* de la boîte de dialogue *Configuration de la source de données*, cliquez sur **Base de données**, puis sur **Suivant**.

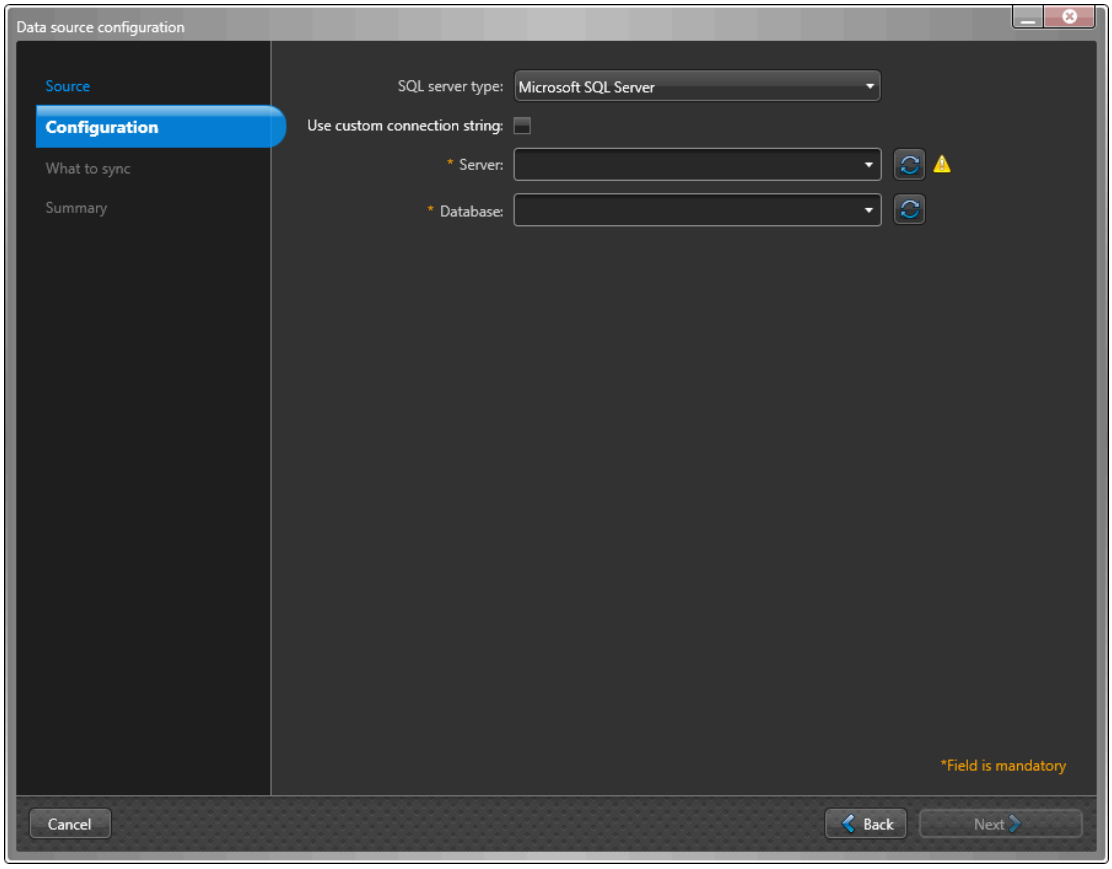


3 Dans la section *Configuration* de la boîte de dialogue *Configuration de la source de données*, configurez les paramètres de la base de données.

a) Sélectionnez un type de serveur SQL :

- Microsoft SQL Server
- Oracle Database (seules les vues sont actuellement prises en charge)
- ODBC

b) Si vous avez sélectionné **Microsoft SQL Server**, configurez les éléments suivants :

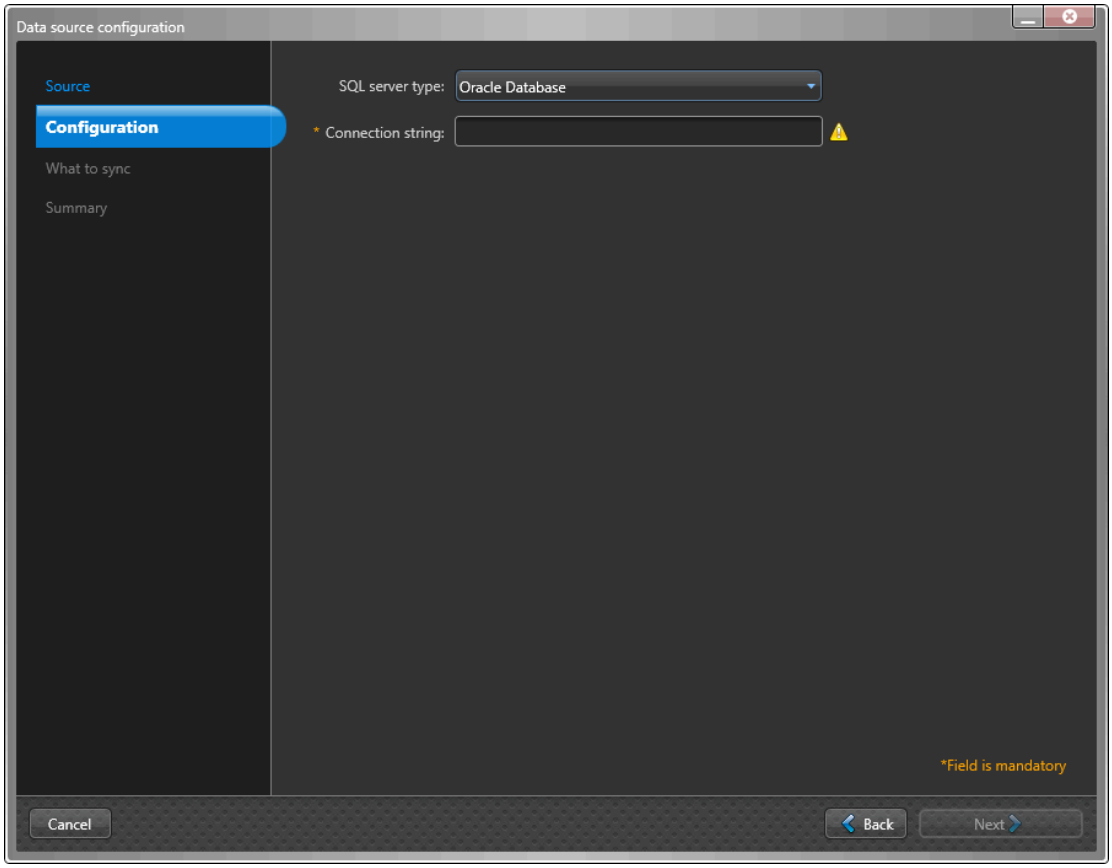


- **Utiliser une chaîne de connexion personnalisée :** Cochez la case si vous souhaitez utiliser une chaîne de connexion personnalisée.

  REMARQUE : Si vous utilisez l'option **Utiliser une chaîne de connexion personnalisée**, les champs **Serveur** et **Base de données** sont supprimés.

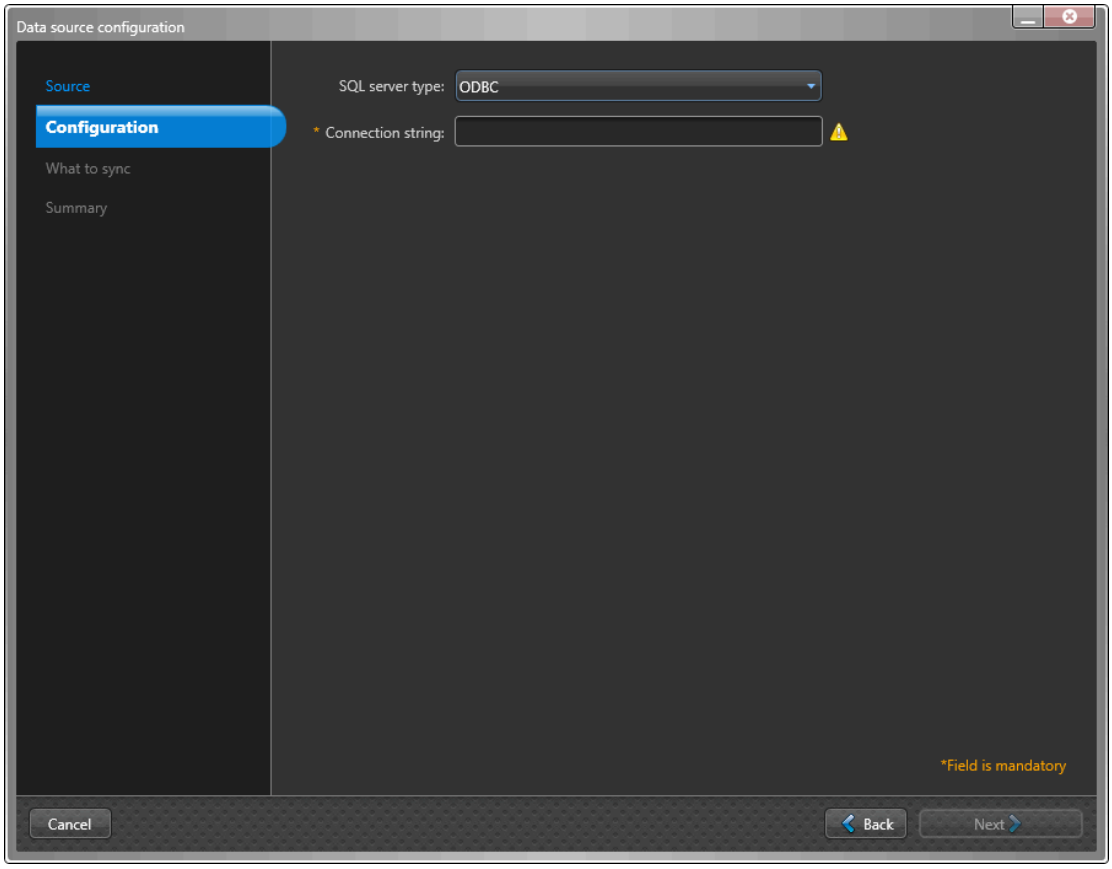
- **Chaîne de connexion :** Saisissez la chaîne de connexion.
- **Security Center :** Saisissez les informations du serveur SQL ou sélectionnez un serveur dans la liste.
- **Base de données :** Saisissez les informations de la base de données ou sélectionnez une base de données dans la liste.

c) Si vous avez sélectionné **Base de données Oracle**, configurez les éléments suivants :



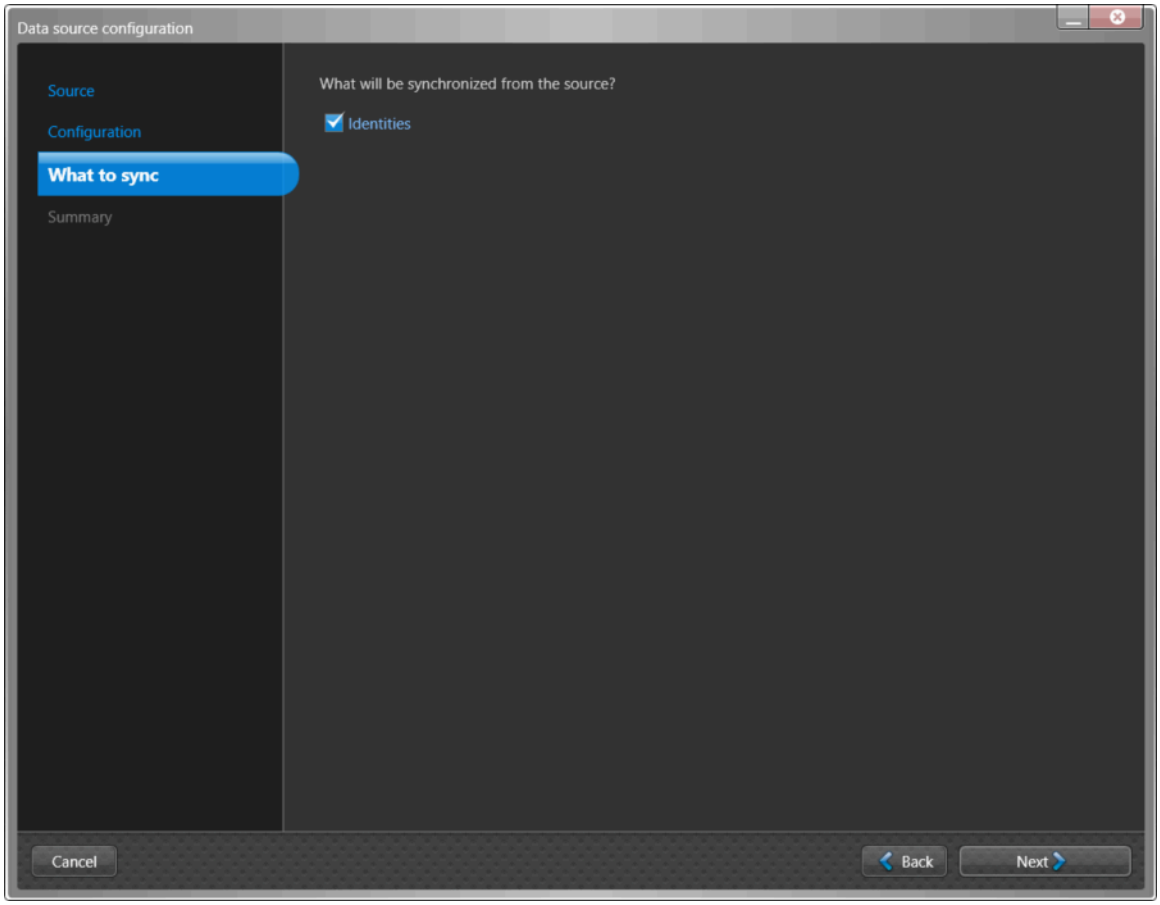
- **Chaîne de connexion :** Saisissez la chaîne de connexion.

d) Si vous avez sélectionné **ODBC**, configurez les éléments suivants :



- **Chaîne de connexion :** Saisissez la chaîne de connexion.

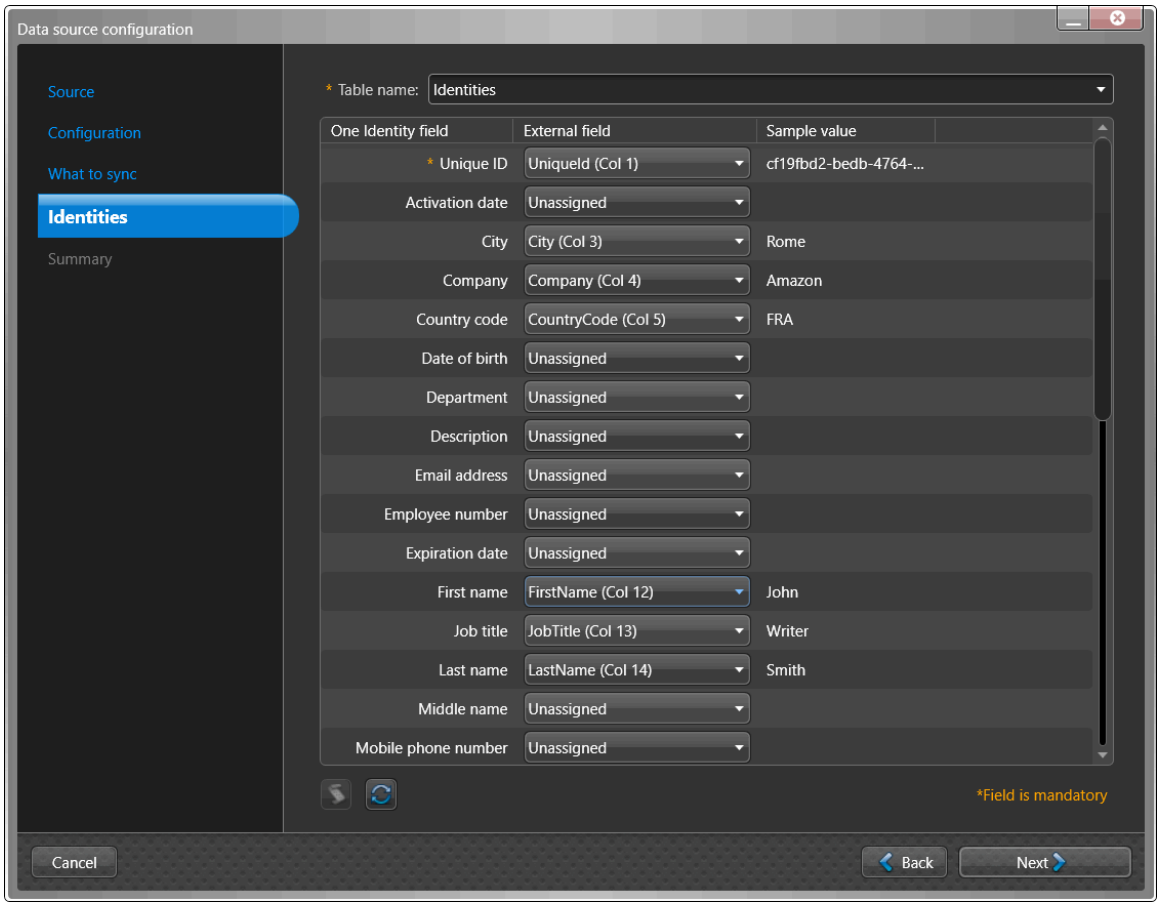
4 Dans la section *Éléments à synchroniser* de la boîte de dialogue *Configuration de la source de données*, sélectionnez **Identités** pour synchroniser avec la source de données du système externe.



5 Si vous avez sélectionné **Identités** comme source de données, dans la section *Éléments à synchroniser*, configurez les paramètres des attributs d'identité.

REMARQUE : Les champs affichés dépendant de la source de données sélectionnée dans la section *Source*.

L'image suivante montre les options qui s'affichent après la sélection d'une source de données **Base de données**.



a) Configurez vos mappages d'attributs de **champ externe**.

- **Champ One Identity :** Affiche les attributs d'identité ClearID. Les champs obligatoires sont indiqués par un astérisque (*).

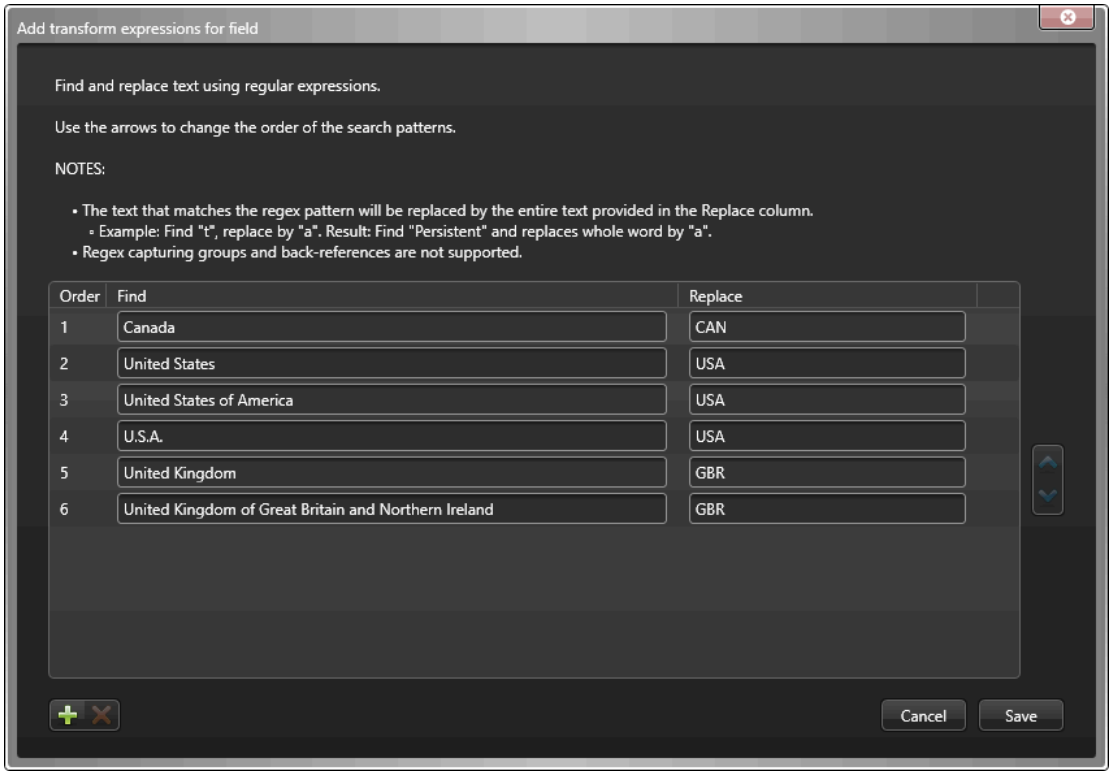
IMPORTANT : L'ID unique est utilisé en interne par One Identity en tant que clé principale d'identification de l'élément. Par exemple, un numéro d'employé ou une adresse e-mail peut être utilisée, tant qu'elle est unique.

- **Champ externe :** Sélectionnez les attributs système dans les colonnes **Champ externe** du système externe que vous souhaitez associer aux attributs d'identité ClearID affichés dans la colonne **Champ One Identity**.
- **Valeur témoin :** Si un **Champ externe** est sélectionné, un exemple des données de champ externe sélectionnées dans votre source de données s'affiche (le cas échéant) dans le texte de la colonne **Valeur échantillon**, à côté de la colonne **Champ externe**.

CONSEIL : Utilisez la colonne Valeur témoin pour valider le format des données d’attribut que vous êtes sur le point d'importer depuis votre système externe dans ClearID.

b) (Facultatif) Cliquez sur **Script** ( ) pour ajouter une expression de transformation afin de rechercher et de remplacer le texte de champ externe à l'aide d'expressions régulières.

Par exemple, vous pouvez rechercher des variantes d'un nom de pays à remplacer par un code de pays correct.



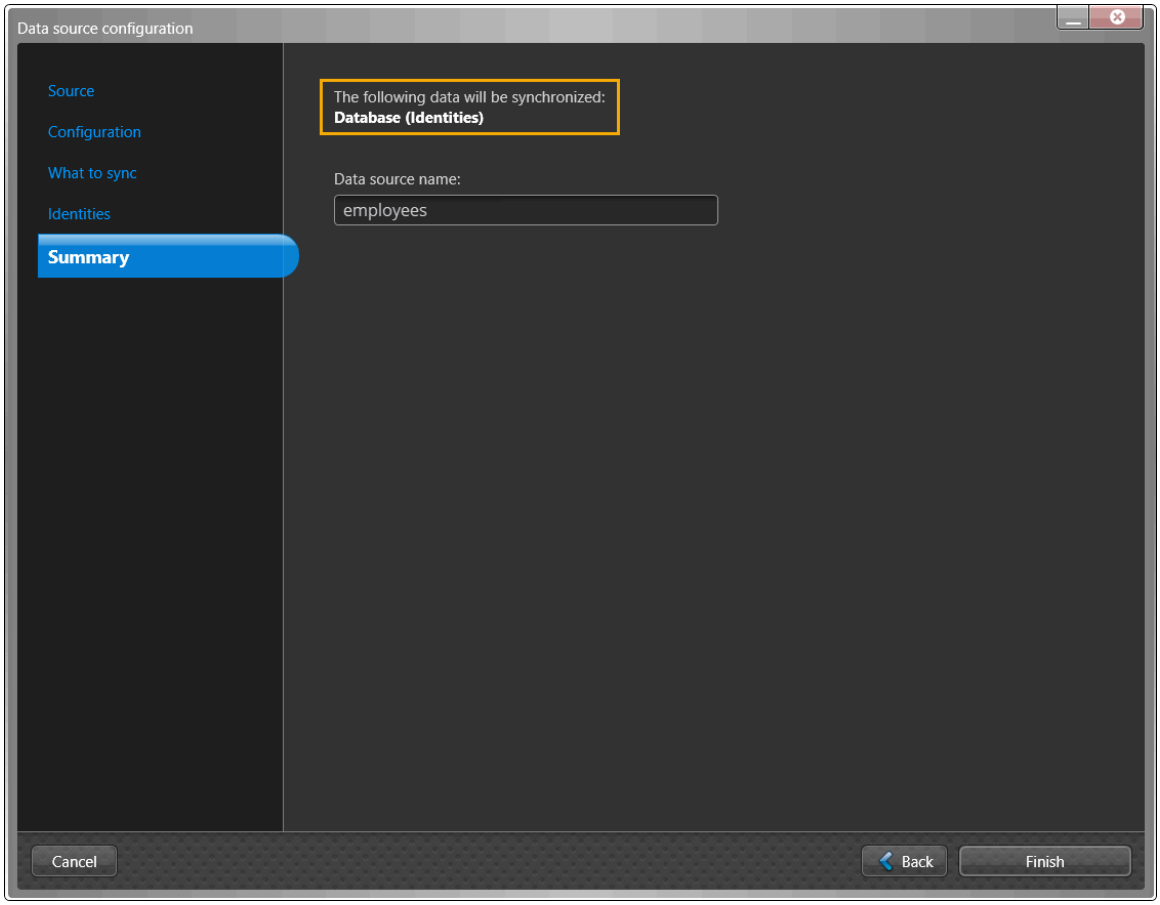
- Une icône de script ( ) est affichée dans la colonne **Exemple de valeur** lorsque le texte du champ est remplacé par une expression régulière.
- Les expressions de transformation sont traitées dans l'ordre spécifié dans la boîte de dialogue *Ajouter des expressions de transformation pour le champ*.

CONSEIL : Si nécessaire, vous pouvez sélectionner la ligne des expressions dont vous n'avez plus besoin et cliquer sur **Supprimer** .

c) (Facultatif) Cliquez sur **Actualiser** ( ) pour mettre à jour les données des champs externes à partir de votre source de données. Cette option d'actualisation est utilisée dans les situations où les données existantes ont été modifiées, de nouvelles lignes de données ont été ajoutées ou de nouvelles colonnes d'attributs ont été ajoutées.

d) Cliquez sur **Suivant**.

6 Dans la section *Résumé*, examinez les données qui seront synchronisées.



REMARQUE : Si plusieurs sources de données sont sélectionnées, seul le premier fichier de source de données s'affiche dans la section *Résumé* pour le champ **Nom de la source de données**. Si vous souhaitez que chacun des fichiers de données soit répertorié dans la section **Sources de données**, vous devez les ajouter individuellement.

a) Si les détails de la synchronisation des données semblent corrects, cliquez sur **Terminer**.

Lorsque vous avez terminé

Configurez vos paramètres de synchronisation.

Rubriques connexes

À propos des champs d'attributs One Identity Synchronization Tool, page 522

Configurer la source de données pour la synchronisation de fichiers

Avant de synchroniser un système externe avec Genetec ClearID[MC], vous devez configurer les sources de données Genetec ClearID[MC] One Identity Synchronization Tool pour la synchronisation de fichiers (CSV).

Avant de commencer

- Familiarisez-vous avec les champs d'attribut One Identity.
- Préparez un fichier CSV contenant les attributs d'identités que vous souhaitez importer et synchroniser.
- Consultez vos informations de licence : La référence CD-IDSYNC-SERVICE-1Y est requise pour l'importation One Identity Synchronization Tool.

IMPORTANT : Vérifiez que vos fichiers CSV ne sont pas en cours d'édition et qu'ils sont fermés, car l'outil de synchronisation verrouille les fichiers pendant le processus de synchronisation.

À savoir

Cette procédure est destinée au personnel informatique ou de sécurité chargé de l'administration des attributs système externes.

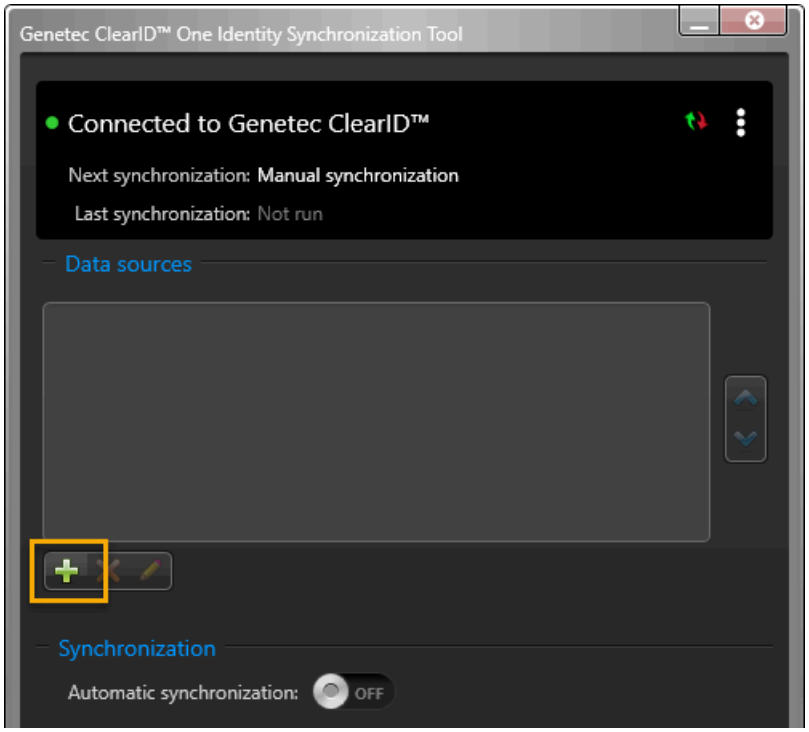
Cette procédure décrit comment configurer la source de données pour un **fichier** (importation CSV).

- L'ordre des sources de données est important car la première source de données remplace toujours les champs communs.
- Une source de données peut inclure plusieurs fichiers CSV contenant des identités.
- Il n'y a pas de limite au nombre de sources de données. Cependant, plus la source de données est volumineuse (pas uniquement les fichiers CSV), plus les besoins en mémoire augmentent.

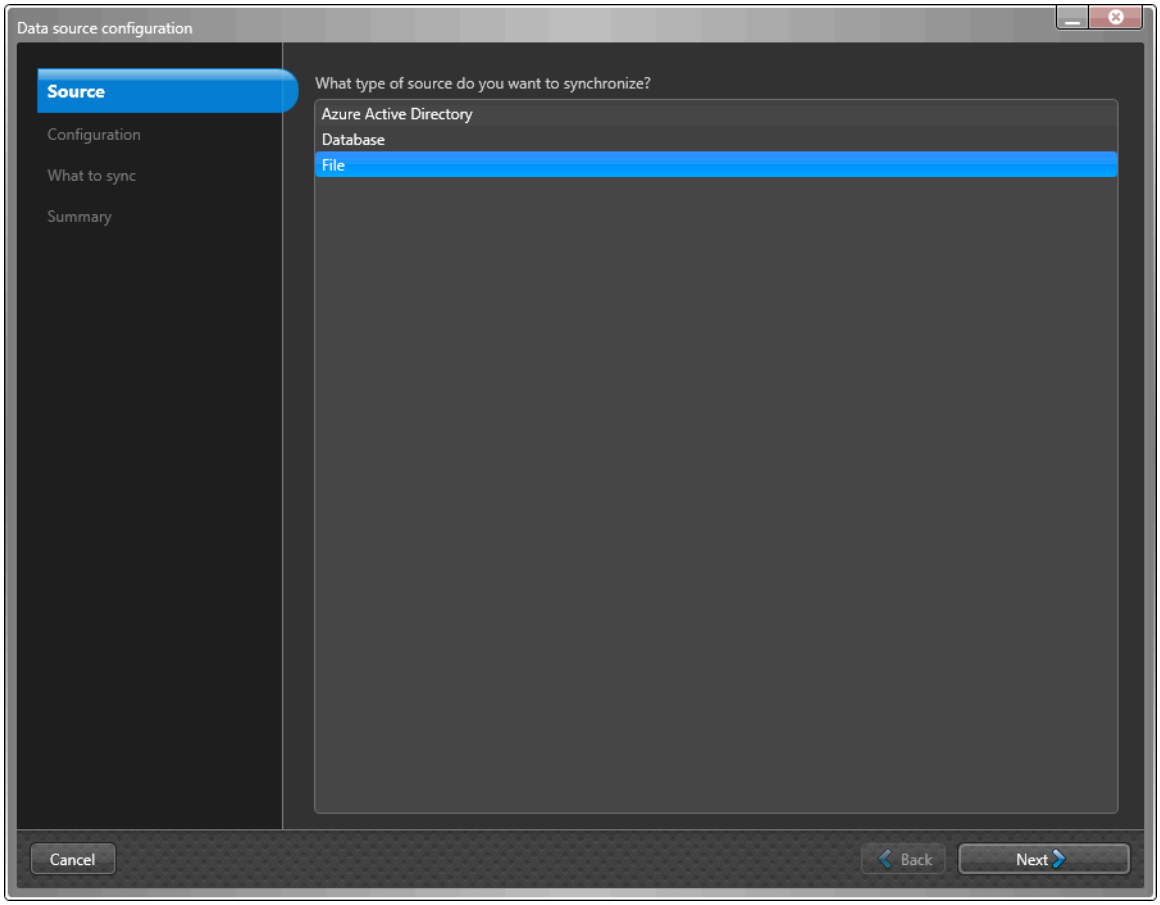
BONNE PRATIQUE : Pour éviter les problèmes d'autorisation lorsque vous utilisez ClearID One Identity Synchronization Tool, enregistrez vos fichiers dans le dossier *C:* or *C:\temp*. N'enregistrez pas les fichiers CSV dans un fichier ou un dossier contrôlé par l'utilisateur (dossier dans *C:\Users* ou sur le *bureau*) ou vous risquez de rencontrer des problèmes d'autorisation d'utilisateur de type Le chemin d'accès au fichier n'est pas valide.

Procédure

1 Dans la section *Sources de données* de l'outil de synchronisation One Identity, cliquez sur **Ajouter une source de données** ( ).

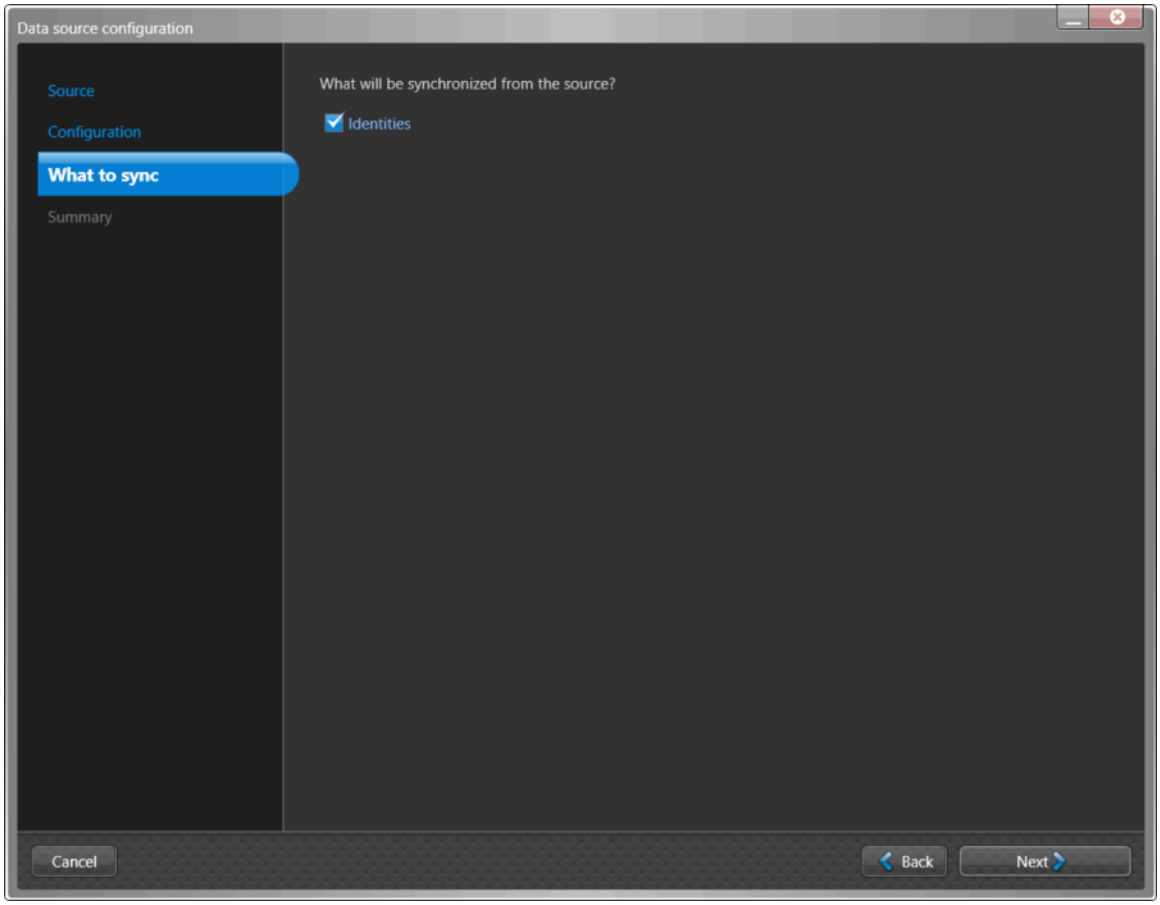


2 Dans la section *Source* de la boîte de dialogue *Configuration de la source de données*, cliquez sur **Fichier**, puis sur **Suivant**.



REMARQUE : Si vous avez sélectionné **Fichier** dans la section *Source*, la section *Configuration* de la boîte de dialogue *Configuration de la source de données* est ignorée car elle n'est pas obligatoire.

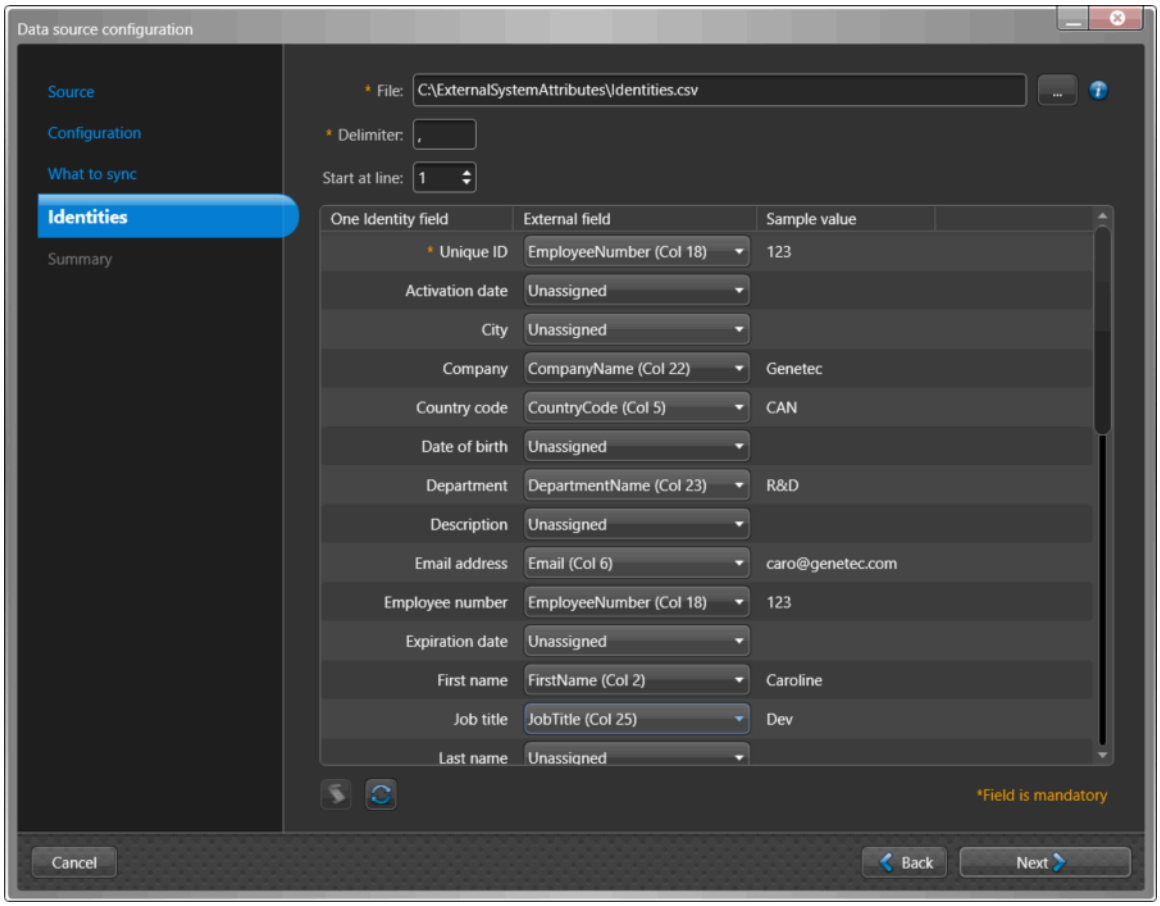
3 Dans la section *Éléments à synchroniser* de la boîte de dialogue *Configuration de la source de données*, sélectionnez **Identités** pour synchroniser avec la source de données du système externe.



4 Si vous avez sélectionné **Identités** comme source de données, dans la section *Éléments à synchroniser*, configurez les paramètres des attributs d'identité.

REMARQUE : Les champs affichés varient en fonction de la source de données sélectionnée dans la section *Source* (étape 2, page 558) précédemment.

L'image suivante montre les options qui s'affichent après la sélection d'une source de données **Fichier** (CSV).



a) Si vous avez sélectionné **Fichier** comme source de données, configurez les paramètres du fichier.

- **Fichier :** Cliquez sur **Plus** ( ) pour sélectionner le fichier CSV contenant vos attributs.

  REMARQUE : Le fichier doit exister sur le serveur sur lequel l'outil de configuration One Identity est installé.
- **Délimiteur :** Saisissez un **Délimiteur**.

  Par exemple, les valeurs d'un fichier CSV sont séparées par des virgules.
- **Démarrer à la ligne :** Sélectionnez une **Ligne de départ**.

Par exemple, les données d'une table sans en-tête peut démarrer à la ligne 0, tandis que celles d'une table avec en-tête démarrera à la ligne 1.

b) Configurez vos mappages d'attributs de **champ externe**.

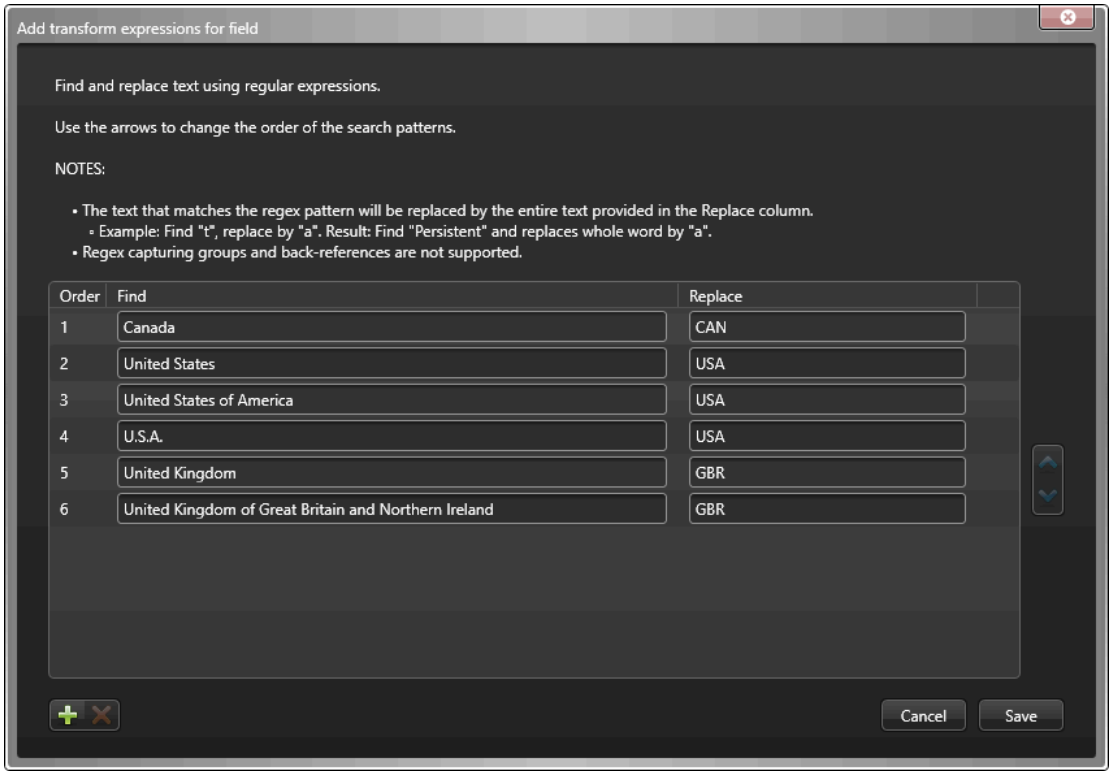
- **Champ One Identity :** Affiche les attributs d'identité ClearID. Les champs obligatoires sont indiqués par un astérisque (*).

IMPORTANT : L'ID unique est utilisé en interne par One Identity en tant que clé principale d'identification de l'élément. Par exemple, un numéro d'employé ou une adresse e-mail peut être utilisée, tant qu'elle est unique.

- **Champ externe :** Sélectionnez les attributs système dans les colonnes **Champ externe** du système externe que vous souhaitez associer aux attributs d'identité ClearID affichés dans la colonne **Champ One Identity**.
- • Si votre fichier CSV contient des titres de colonne, les noms sont affichés.
  - Si votre fichier CSV ne contient pas de titres de colonne, le numéro de la colonne s'affiche.

c) (Facultatif) Cliquez sur **Script** ( ) pour ajouter une expression de transformation afin de rechercher et de remplacer le texte de champ externe à l'aide d'expressions régulières.

Par exemple, vous pouvez rechercher des variantes d'un nom de pays à remplacer par un code de pays correct.



- Une icône de script ( ) est affichée dans la colonne **Exemple de valeur** lorsque le texte du champ est remplacé par une expression régulière.
- Les expressions de transformation sont traitées dans l'ordre spécifié dans la boîte de dialogue *Ajouter des expressions de transformation pour le champ*.

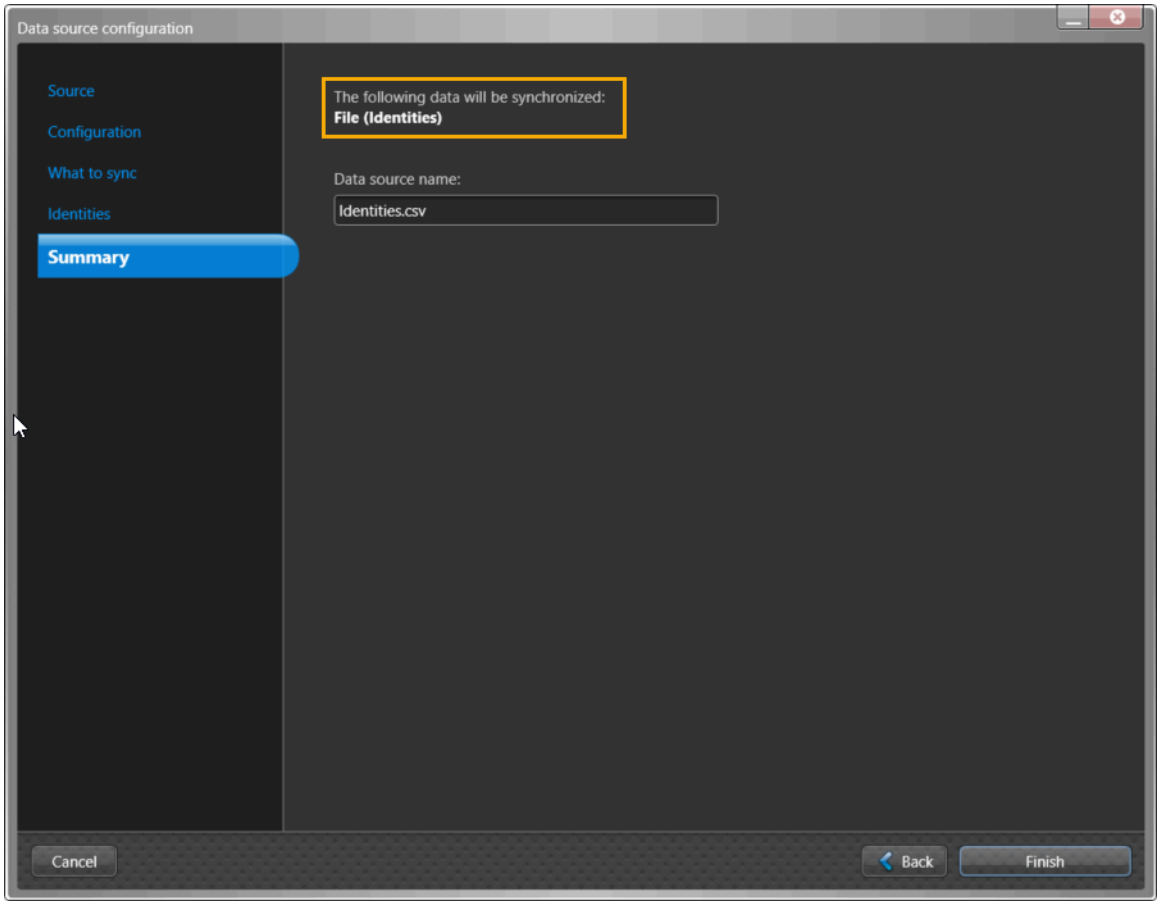
CONSEIL : Si nécessaire, vous pouvez sélectionner la ligne des expressions dont vous n'avez plus besoin et cliquer sur **Supprimer** .

d) (Facultatif) Cliquez sur **Actualiser** ( ) pour mettre à jour les données des champs externes à partir de votre source de données. Cette option d'actualisation est utilisée dans les situations où les données

existantes ont été modifiées, de nouvelles lignes de données ont été ajoutées ou de nouvelles colonnes d'attributs ont été ajoutées.

e) Cliquez sur **Suivant**.

5 Dans la section *Résumé*, examinez les données qui seront synchronisées.



REMARQUE : Si plusieurs sources de données sont sélectionnées, seul le premier fichier de source de données s'affiche dans la section *Résumé* pour le champ **Nom de la source de données**. Si vous souhaitez que chacun des fichiers de données soit répertorié dans la section **Sources de données**, vous devez les ajouter individuellement.

a) Si les détails de la synchronisation des données semblent corrects, cliquez sur **Terminer**.

Lorsque vous avez terminé

Configurez vos paramètres de synchronisation.

Rubriques connexes

À propos des champs d'attributs One Identity Synchronization Tool, page 522

Configurer les réglages de synchronisation

Avant de synchroniser un système externe avec Genetec ClearID[MC], vous devez configurer les réglages de synchronisation de Genetec ClearID[MC] One Identity Synchronization Tool.

Avant de commencer

- Consultez vos informations de licence : La référence CD-IDSYNC-SERVICE-1Y est requise pour l'importation One Identity Synchronization Tool.

IMPORTANT : Vérifiez que vos fichiers ne sont pas en cours d'édition et qu'ils sont fermés, car l'outil de synchronisation verrouille le fichier pendant le processus de synchronisation.

À savoir

Cette procédure est destinée au personnel informatique ou de sécurité chargé de l'administration des attributs système externes.

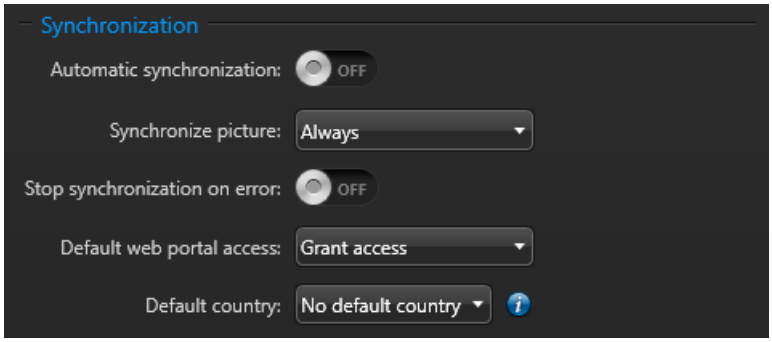
La synchronisation peut être effectuée manuellement à l'aide de l'option **Synchroniser maintenant** ( ) ou automatiquement aux intervalles de **synchronisation automatique** spécifiés dans l'outil de synchronisation One Identity.

La synchronisation des attributs du système externe avec les attributs d'identité ClearID ne fonctionne qu'en mode ENTRANT.

ATTENTION : Toute modification apportée aux identités dans ClearID peut être remplacée lors de la synchronisation suivante du système externe.

Procédure

1 Dans la section **Synchronisation** de l'outil de synchronisation One Identity, configurez vos paramètres de synchronisation.



- **Synchronisation automatique :** Activez la synchronisation automatique si vous souhaitez synchroniser les attributs à des intervalles spécifiques.
  - **Intervalle :** Si la synchronisation automatique est activée, choisissez un intervalle de synchronisation :
    - **Fixe :** Saisissez un intervalle de synchronisation au format suivant : `000j 01h 00m 00s`. Par exemple, tous les sept jours correspond à `007j 00h 00m 00s` et toutes les 12 h à `000j 12h 00m 00s`.
    - **Horaires Cron :** Saisissez un intervalle de synchronisation au format Cron Quartz. Par exemple, `00***?*`.
      Pour plus d'informations, voir quartz-scheduler.org/documentation.

  CONSEIL : Vous pouvez cliquer sur **Synchroniser maintenant** ( ) quels que soient les paramètres d'horaires pour lancer une synchronisation immédiate.
- **Synchroniser la photo :** Indiquez quand vous souhaitez synchroniser les photos d'identité depuis le système externe.
  - **Toujours :** Les photos d'identité sont synchronisées à chaque synchronisation.
  - **Uniquement si manquantes :** Les photos d'identité ne sont synchronisées que si elles sont manquantes lors d'une synchronisation.

  REMARQUE : L'ajout de photos augmente le délai d'importation des attributs.
- **Arrêter la synchronisation lors d'une erreur :** Activez cette option pour arrêter la synchronisation lorsqu'une erreur se produit lors du processus.
- **Accès par défaut au portail Web :** Spécifie l'accès au portail Web pour les utilisateurs synchronisés.

- **Accorder l’accès :** L'accès au portail Web ClearID pour les utilisateurs synchronisés est activé par défaut.
  REMARQUE : Le champ **Nom d'utilisateur** doit correspondre pour fournir l’accès au portail web à une identité ClearID.
  - Il n'y a que deux valeurs possibles pour le mappage **Type d'utilisateur** : **Admin** et **User**. Toute autre valeur saisie est remplacée par défaut par **User**.
  - Si la correspondance n’est pas définie pour l'accès au portail ou si la valeur est vide, le paramètre global **Accès par défaut au portail web** est utilisé.
- **Pas d'accès :** L'accès au portail Web pour les utilisateurs synchronisés est désactivé par défaut.

- **Pays par défaut :** Choisissez l'une des options suivantes :
  - **Aucun pays par défaut :** Si une identité synchronisée ne comprend pas l'attribut de pays, ce dernier est ignoré.
  - **Pays par défaut :** Sélectionnez un pays par défaut. Si une identité synchronisée ne comprend pas l'attribut de pays, l'identité synchronisée utilise le pays par défaut spécifié ici.

2 Cliquez sur **Enregistrer**.

ClearID One Identity Synchronization Tool est à présent configuré pour synchroniser les attributs du système externe en utilisant les réglages de **Sources de données** et de **Synchronisation** spécifiés dans l’outil.

Lorsque vous avez terminé

Une fois la synchronisation effectuée, vérifiez que les nouveaux attributs du système externe ont été synchronisés et contiennent les bons attributs.

Consulter l'état de la synchronisation

Pour vérifier que vos attributs d'identité ont été synchronisés correctement avec Genetec ClearID^{MC}, vous pouvez consulter l’état de la synchronisation de Genetec ClearID^{MC} One Identity Synchronization Tool sur le portail Web ClearID.

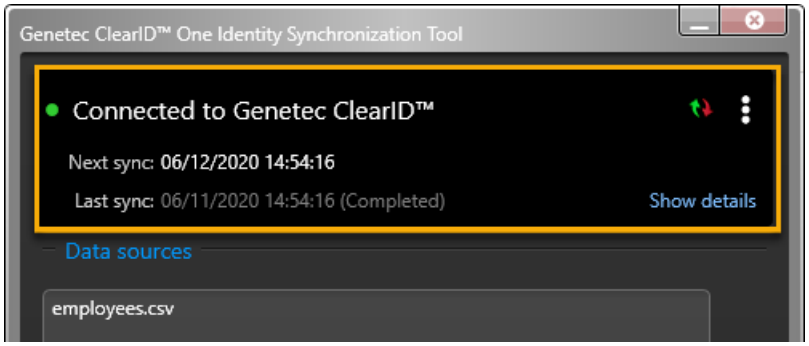
Avant de commencer

- Configurez l'outil de synchronisation One Identity.
- Effectuez une synchronisation manuelle ou automatique à l'aide de l'outil de synchronisation One Identity.

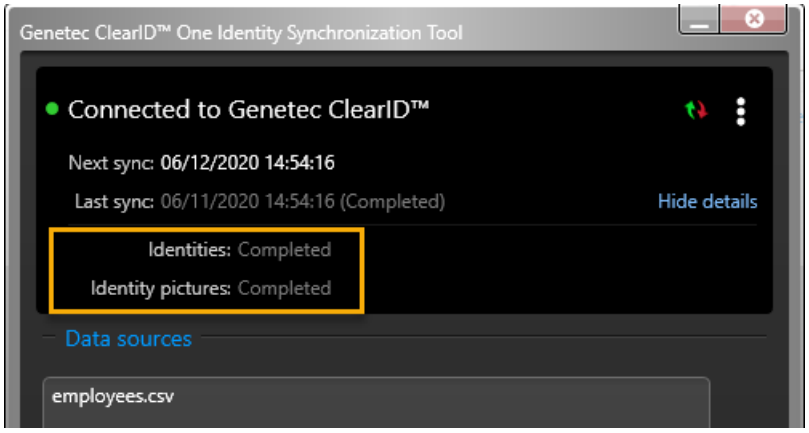
Procédure

Pour consulter l'état de la synchronisation de vos attributs dans l'outil de configuration One Identity :

1 Dans la section de connexion de l'outil de synchronisation One Identity, vérifiez l'état de la synchronisation.



- **Prochaine synchronisation :** Affiche des informations sur la prochaine synchronisation.
  - Si une date est affichée sous la forme **06/16/2020 23:00:00**, il s'agit de la fréquence **Fixe** ou **Horaire Cron** des synchronisations.
  - Si **Synchronisation manuelle** s'affiche, la synchronisation doit être effectuée manuellement.
- **Dernière synchronisation :** Affiche des informations sur la dernière synchronisation.
- **Afficher les détails :** Cliquez sur **Afficher les détails** pour vérifier l'état de la synchronisation des **Identités** et des **Photos d'identité**.



REMARQUE : En cas de problème avec l'une des synchronisations, un message Échec s'affiche à côté de la synchronisation ayant échoué.

2 (Facultatif) Examinez les journaux récapitulatifs.

a) Cliquez sur ⋮ puis cliquez sur **Ouvrir le dossier de journalisation**.

b) Examinez les journaux *récapitulatifs* au format CSV pour identifier les problèmes qui sont potentiellement survenus pendant la synchronisation.

c) Consultez le fichier *Recap.txt* pour un aperçu de la synchronisation.

REMARQUE : Les fichiers journaux récapitulatifs sont enregistrés dans *C:\ProgramData\Genetec \OneIdentity\Logs\Summary*.

Pour consulter l'état de la synchronisation des attributs sur le portail Web ClearID :

1 Sur le portail Web ClearID, vérifiez que les nouveaux attributs provenant du système externe ont bien été synchronisés et qu'ils contiennent les bons attributs.

a) Cliquez sur **Organisation** > **Identités** et vérifiez que vos données d'identité synchronisées sont correctes.

À propos des journaux One Identity Synchronization Tool

Genetec ClearID[MC] One Identity Synchronization Tool crée des journaux qui peuvent être utiles à des fins de dépannage. Les journaux peuvent être utilisés pour vérifier l'état de l'outil de configuration ou du service Windows, ou pour examiner les activités de synchronisation.

ClearID One Identity Synchronization Tool utilise la structure Apache log4net[MC] standard pour la journalisation.

La configuration de la journalisation peut être modifiée à la fois pour le service de synchronisation et pour l'outil de synchronisation.

- Pour modifier la configuration de journalisation de **Genetec.ClearID.OneIdentity.SynchronizationService** (*OneIdentityService.exe*), vous pouvez modifier le fichier *log4net.service.config*.
- Pour modifier la configuration de journalisation de **Genetec.ClearID.OneIdentity.SynchronizationTool** (*OneIdentityConfigurationTool.exe*), vous pouvez modifier le fichier *log4net.ct.config*.

Ces fichiers de configuration des journaux se trouvent dans le dossier d'installation *C:\Program Files (x86)\Genetec ClearID One Identity Synchronization Service*.

Les paramètres par défaut sont les suivants :

- Le niveau de consignation par défaut est WARN.
- La taille du fichier avant roulement est de 10 Mo.
- Le nombre maximum de sauvegardes continues est de 10.

Pour en savoir plus sur les valeurs prises en charge et la manière de les modifier, consultez la documentation Apache log4net.

Consulter les journaux One Identity Synchronization Tool

Vous pouvez utiliser les journaux de Genetec ClearID[MC] One Identity Synchronization Tool pour examiner l'état de l’outil de configuration ou du service Windows, ou pour consulter les activités de synchronisation.

Avant de commencer

- Configurer One Identity Synchronization Tool, page 535
- Configurer les réglages de synchronisation, page 562

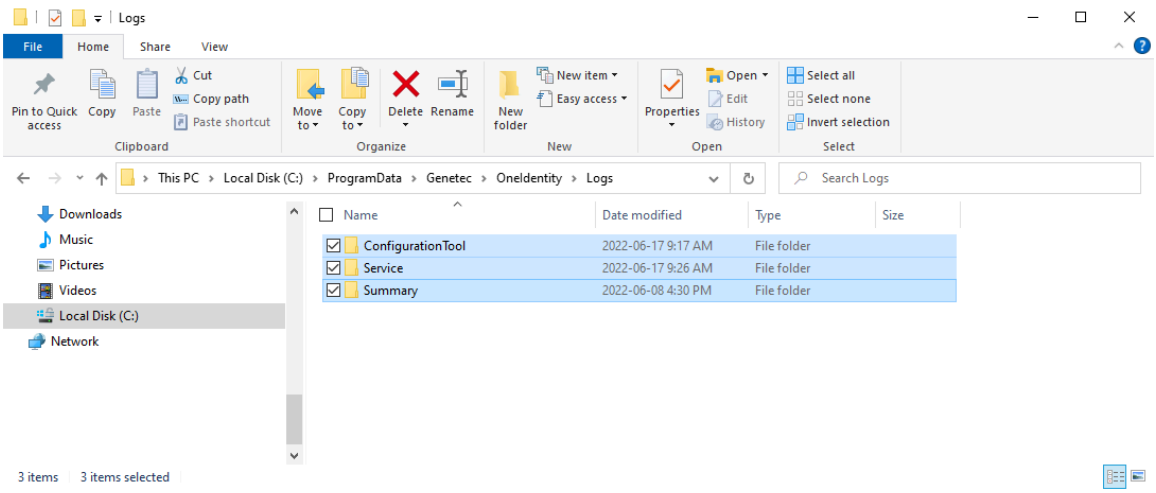
À savoir

Les journaux sont subdivisés en trois dossiers distincts comme suit :

- **Configuration :** Journaux relatifs à l’application *Genetec ClearID[MC] One Identity Synchronization Tool (OneIdentityConfigurationTool.exe)*.
- **Service :** Journaux relatifs à *Genetec.ClearID.OneIdentity.SynchronizationService (OneIdentityService.exe)* .
- **Summary :** Journaux relatifs aux résumés de synchronisation.

Procédure

1 Cliquez sur puis cliquez sur **Ouvrir le dossier de journalisation**.



2 Examinez les journaux *ConfigurationTool* si vous avez des problèmes de connectivité. Par exemple, si l'outil de synchronisation ne parvient pas à se connecter à ClearID ou à Azure AD.

3 Examinez les journaux *Service* si vous avez des problèmes de synchronisation des données. Par exemple, des champs de données manquants, des champs de nom manquants ou des adresses électroniques manquantes.

4 Consultez les journaux du dossier *Summary* pour voir un résumé des activités de synchronisation. Par exemple, quand une synchronisation a commencé ou s'est terminée et ce qui s'est passé pendant la synchronisation.

a) Consultez le fichier *Recap.txt* pour un aperçu de la synchronisation.

REMARQUE : Les fichiers journaux récapitulatifs sont des fichiers au format CSV pour faciliter le tri des informations dans Microsoft® Excel si nécessaire. Ils sont générés automatiquement à la fin de la synchronisation.

- Si la synchronisation échoue complètement, les fichiers journaux récapitulatifs ne sont pas générés.
- S'il n'y a rien à importer, les fichiers journaux récapitulatifs ne sont pas créés.

Mettre à jour des identités existantes à partir de sources de données externes

Lorsque des utilisateurs qui ont déjà été créés ont le même ID externe que des utilisateurs existants, vous pouvez utiliser Genetec ClearID[MC] One Identity Synchronization Tool pour mettre à jour les informations d'identité existantes à partir de la source de données externe.

À savoir

Cette procédure ne concerne que les nouvelles installations du service ClearID One Identity Synchronization Tool lorsque l’environnement Genetec ClearID[MC] contient déjà des identités qui existent également dans la source de données du système externe.

- Lorsqu’un ID externe existe déjà dans ClearID, cette identité est mise à jour avec les valeurs fournies par les sources de données.
- Lorsqu'une identité de la source de données n’existe pas dans One Identity (par exemple, lors de la première synchronisation), le service tente de créer l’identité dans ClearID.
- Lorsque la création échoue parce que l'identité existe déjà, cette identité est alors récupérée et mise à jour.

Procédure

1 Pour reproduire un service nouvellement installé, supprimez les mappages de fichiers sous *%ProgramData%\Genetec\OneIdentity\Configuration*.

2 Configurez une source de données qui contient déjà une ou plusieurs identités déjà présentes dans ClearID.

   Les identités dans les données externes doivent avoir le même ID externe et la même adresse e-mail que les identités dans ClearID.

3 Lancez la synchronisation et attendez qu'elle soit terminée.

Les identités dans ClearID sont actualisées en fonction des correspondances avec la source de données.

Synchroniser les identités par LDAP

Utilisez Genetec ClearID[MC] LDAP Synchronization Agent pour synchroniser les attributs Lightweight Directory Access Protocol (LDAP) Active Directory (AD) avec les attributs d'identité Genetec ClearID[MC]. Ces attributs d'identité dans ClearID peuvent ensuite être utilisés pour affecter des personnes à des rôles et pour automatiser le contrôle d'accès basé sur les rôles.

Procédure

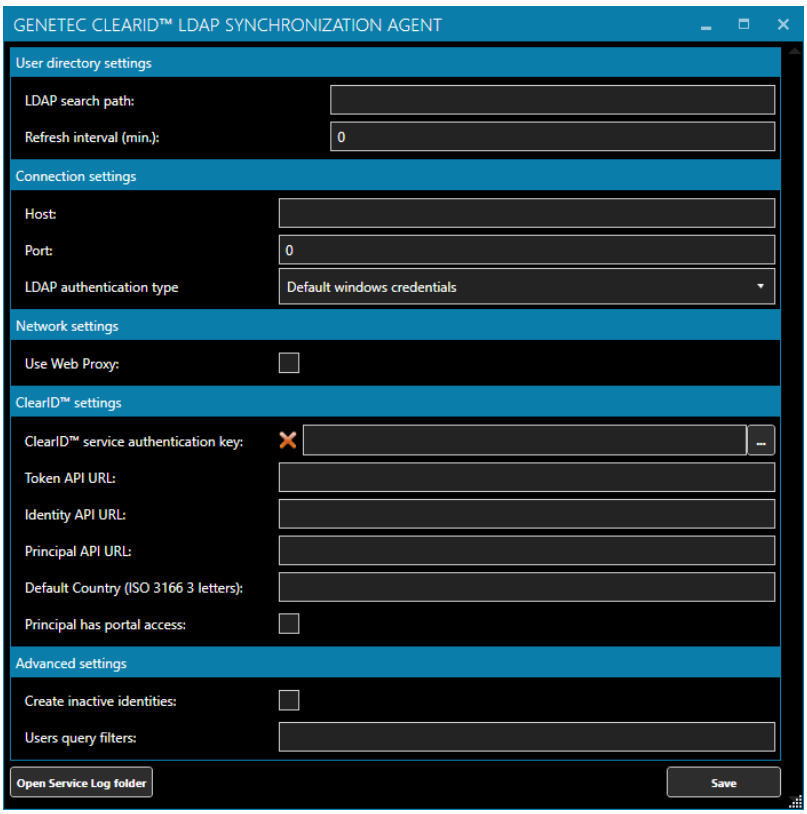
1 En savoir plus sur Genetec ClearID[MC] LDAP Synchronization Agent.

2 En savoir plus sur l’association des attributs LDAP et des attributs ClearID.

3 Configurez ClearID LDAP Synchronization Agent.

À propos de ClearID LDAP Synchronization Agent

Genetec ClearID[MC] LDAP Synchronization Agent est une application Windows servant à synchroniser les attributs Lightweight Directory Access Protocol (LDAP) Active Directory (AD) avec les attributs d'identité Genetec ClearID[MC].



L'application ClearID LDAP Synchronization Agent inclut les composants suivants :

- **Konfigurator** (*Genetec.ClearID.LdapSyncAgentConfiguration.exe*) est l’interface utilisateur de l'application Windows servant à configurer l'agent de synchronisation.
- **Genetec ClearID LDAP Synchronizer** (*Genetec.ClearID.LdapSyncAgent.Service.exe*) est le composant de service Windows de l’application qui effectue la synchronisation des attributs LDAP Active Directory avec les attributs d'identité Genetec ClearID[MC] automatiquement, en arrière-plan et à la fréquence spécifiée dans Synchronization Agent.

L'application ClearID LDAP Synchronization Agent est conçue pour le service informatique ou le personnel de sécurité qui gère l'annuaire Active Directory (AD).

Synchronisation

Dans ClearID, les identités peuvent provenir de différentes sources de données (bases de données, RH, sources externes) et peuvent être synchronisées à l'aide de différents outils (Genetec ClearID[MC] LDAP Synchronization Agent, l’API Genetec ClearID[MC] ou Genetec ClearID[MC] One Identity Synchronization Tool).

La section suivante décrit la synchronisation LDAP Active Directory :

- La synchronisation des attributs LDAP avec les attributs d'identité ClearID ne fonctionne qu’en mode ENTRANT.

  ATTENTION : Toute modification apportée aux identités dans ClearID peut être remplacée lors de la synchronisation Active Directory suivante.
- La synchronisation est effectuée automatiquement en arrière-plan, à une fréquence spécifiée dans ClearID LDAP Synchronization Agent.
  - L’attribut *whenChanged* indique l’heure à laquelle la dernière synchronisation a eu lieu. Cet attribut sert ensuite à rechercher les utilisateurs Active Directory modifiés depuis la dernière synchronisation, afin que seuls ces utilisateurs soient mis à jour lors de la synchronisation suivante.
  - Lors de la première synchronisation, tous les attributs utilisateur Active Directory sont synchronisés.
  - Lors des synchronisations suivantes, seuls les attributs utilisateur qui ont été modifiés depuis la dernière exécution de l’agent sont synchronisés.

Correspondances d'attributs LDAP et d’attributs ClearID

Lorsque vous synchronisez un annuaire Active Directory (AD) avec Genetec ClearID[MC] en passant par ClearID LDAP Agent Configurator, les attributs Lightweight Directory Access Protocol (LDAP) sont associés aux attributs d'identité ClearID.

Correspondances d'attributs LDAP et d’attributs ClearID

Attributs LDAP	Attributs d'identité ClearID
whenChanged **IMPORTANT :** L'attribut *whenChanged* indique l’heure de la dernière synchronisation avec ClearID LDAP Synchronization Agent. Cet attribut sert ensuite à rechercher les utilisateurs Active Directory modifiés depuis la dernière synchronisation, afin que seuls ces utilisateurs soient mis à jour lors de la synchronisation suivante.	Non applicable
userAccountControl	État **REMARQUE :** L’attribut ClearID *État* est réglé sur inactif si l’attribut Active Directory *userAccountControl* est réglé sur désactivé.
givenName	FirstName
sn	LastName
displayName	DisplayName

Attributs LDAP	Attributs d'identité ClearID
jpegPhoto	**REMARQUE :** *jpegPhoto* sert à transférer une photo vers l’identité ClearID.
thumbnailPhoto (si jpegPhoto est vide)	**REMARQUE :** *thumbnailPhoto* est utilisé (si jpegPhoto est vide) pour transférer une photo vers l’identité ClearID.
countryCode	CountryCode
employeeID	EmployeeNumber
employeeNumber (si employeeID est vide)	EmployeeNumber
title	JobTitle
telephoneNumber	PhoneNumberPrimary
phone	PhoneNumberSecondary
Mobile (si phone est vide)	PhoneNumberSecondary
service	DepartmentName
company	CompanyName
userPrincipalName **REMARQUE :** L'attribut userPrincipalName sert de lien entre l’utilisateur AD et l’identité ClearID.	Email, ExternalId
manager	SupervisorName
mail	E-mail

Configurer ClearID LDAP Synchronization Agent

Avant de synchroniser un annuaire Active Directory (AD) avec Genetec ClearID[MC], vous devez configurer Genetec ClearID[MC] LDAP Synchronization Agent.

Avant de commencer

- Téléchargez une clé d'authentification de service.
- Installez ClearID LDAP Synchronization Agent sur un serveur dédié. Il ne doit pas forcément s'agir d’un serveur Security Center.

  REMARQUE : En général, ClearID LDAP Synchronization Agent n’est pas disponible en téléchargement public. Le lien de téléchargement de l’outil de synchronisation est généralement fourni par votre contact de déploiement en cas de besoin.
- Référence : CD-IDSYNC-SERVICE-1Y est requis pour l’importation LDAP.

À savoir

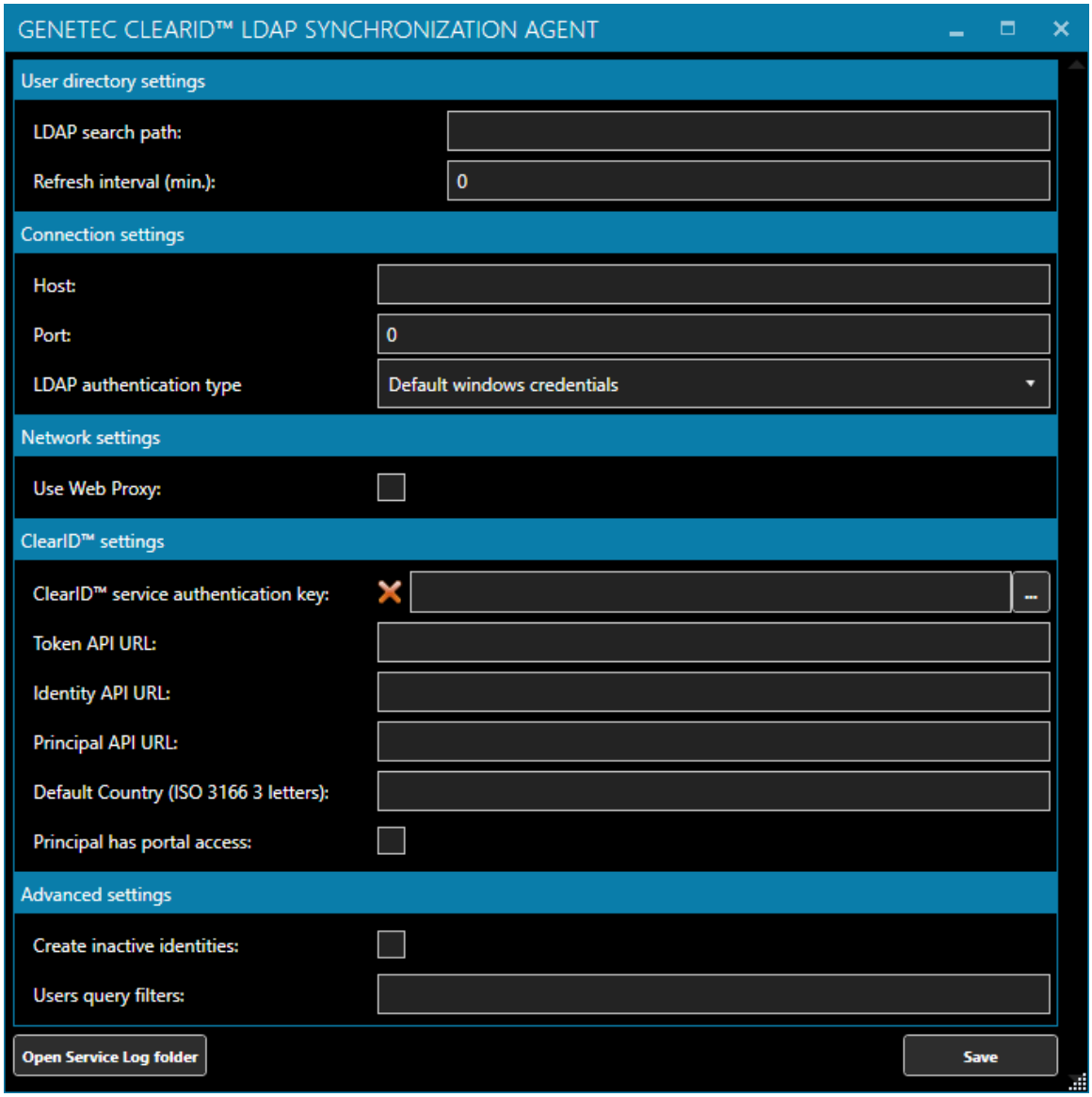
Cette procédure est menée par service informatique ou le personnel de sécurité qui gère l'annuaire Active Directory (AD).

La synchronisation des attributs LDAP avec les attributs d'identité ClearID ne fonctionne qu’en mode ENTRANT.

ATTENTION : Toute modification apportée aux identités dans ClearID peut être remplacée lors de la synchronisation Active Directory suivante.

Procédure

1 Ouvrez ClearID LDAP Synchronization Agent (*Genetec.ClearID.LdapSyncAgentConfiguration.exe*) et configurez les réglages.



2 Dans la section *Réglages de l'annuaire d'utilisateurs*, entrez les informations nécessaires :

La section *Réglages d'annuaire d'utilisateurs* sert à connecter l'annuaire LDAP qui contient les attributs utilisateur.

- **Chemin de recherche LDAP :** Saisissez une unité organisationnelle. Par exemple, `OU=Genetec`. Ce chemin de recherche spécifie l'emplacement, le dossier ou le groupe contenant les attributs utilisateur Active Directory.

REMARQUE : La valeur **distinguishedName** du groupe AD est obligatoire pour le champ Chemin de recherche LDAP.

- **Intervalle d'actualisation (min.) :** Saisissez un intervalle d'actualisation en minutes. Par exemple, 60 pour synchroniser les attributs toutes les heures.

  REMARQUE : Selon la taille de votre organisation et le nombre d'attributs, des synchronisations toutes les *12 h* ou *24 h* (720 ou 1440 min) peuvent être pertinentes.

3 Dans la section *Réglages de connexion*, configurez les réglages de connexion à l’hôte :

La section *Réglages de connexion* sert à se connecter au serveur qui stocke les réglages de l’annuaire d'utilisateurs.

- **Hôte :** Saisissez l'adresse de votre répertoire Active Directory. Par exemple, `Genetec.com`.
- **Port :** Saisissez le port par défaut de votre répertoire Active Directory. Par exemple, `389`.
- **Type d'authentification LDAP :** Sélectionnez un type d'authentification depuis les éléments suivants :
  - **Identifiants Windows par défaut :** Pour une application côté client, cette option utilise les identifiants Windows (*nom d'utilisateur* et *mot de passe*) de l'utilisateur exécutant l'application.
  - **Association simple :** Avec l'option Association simple, les identifiants (*nom d'utilisateur* et *mot de passe*) utilisés pour associer le client LDAP au serveur LDAP sont transmis via le réseau sans chiffrement.
    ATTENTION : Le type d'authentification Association simple n'est pas recommandé pour les serveurs de production LDAP.
  - **Association simple via SSL :**

    BONNE PRATIQUE : Avec l'option Association simple via SSL, les identifiants (*nom d'utilisateur* et *mot de passe*) utilisés pour associer le client LDAP au serveur LDAP sont transmis via le réseau avec chiffrement.
    - **Nom d'utilisateur :** Si l'option **Association simple** ou **Association simple via SSL** a été sélectionnée, saisissez le *nom d'utilisateur* fourni par votre organisation.
    - **Mot de passe :** Si l'option **Association simple** ou **Association simple via SSL** a été sélectionnée, cliquez sur **Définir le mot de passe** et saisissez un `mot de passe`, puis cliquez sur **OK**.
      REMARQUE : Utilisez les bonnes pratiques du secteur pour créer des mots de passe fiables. Tous les mots de passe stockés dans le fichier de configuration sont chiffrés.

4 (Facultatif) Dans la section *Réglages réseau*, configurez les réglages du proxy web :

La section *Réglages réseau* sert à configurer les réglages de proxy.

- **Utiliser un proxy Web :** Cochez la case à cocher **Utiliser un proxy web** pour spécifier qu'un proxy web est requis pour accéder à Internet.

  Cette option est généralement utilisée par les clients situés derrière un pare-feu ou lorsque l'accès réseau à Internet est restreint.

  Un serveur proxy est un serveur qui vérifie et transfère les demandes client entrantes à d'autres serveurs pour une communication ultérieure. Par exemple, lorsqu'un client n'est pas en mesure de répondre aux exigences d'authentification de sécurité du serveur mais doit avoir accès à certains services.
- **URL proxy :** Si la case **Utiliser un proxy Web** est cochée, saisissez l'URL du `proxy` fournie par votre organisation.

  Par exemple, *https://proxy:8080/outgoing*. Ces informations sont généralement fournies par l'équipe d'administration réseau.
- **Authentification proxy :** L'authentification proxy est le processus de validation des identifiants utilisateur permettant d'accéder à un serveur proxy. Cette authentification inclut généralement un *nom d'utilisateur* et peut également comprendre un *mot de passe*.

  Sélectionnez **Identifiants par défaut** ou **Identifiants spécifiques** :
  - **Identifiants par défaut :** Spécifie qu'aucune authentification proxy n'est requise.
  - **Identifiants spécifiques :** Spécifie que l'authentification proxy est requise.

- **Nom d'utilisateur proxy :** Si l'authentification proxy est définie sur **Identifiants spécifiques**, entrez le `nom d'utilisateur` proxy fourni par votre organisation.
- **Mot de passe proxy :** Cliquez sur **Définir le mot de passe** et saisissez un `mot de passe`, puis cliquez sur **OK**.
  REMARQUE : Utilisez les bonnes pratiques du secteur pour créer des mots de passe fiables.
- **Domaine proxy :** Saisissez le `nom de domaine` fourni par votre organisation.

- **État de la connexion proxy :** Les icônes d'état indiquent une connexion proxy valide () ou non valide (). L'état s'affiche uniquement après avoir cliqué sur le bouton **Vérifier**.
- **vérification :** Cliquez sur **Vérifier** pour tester les réglages de connexion de votre serveur de proxy.

5 Dans la section *Réglages ClearID*, configurez les réglages :

La section *Réglages ClearID* sert à se connecter aux services ClearID et à synchroniser les données.

- **Clé d'authentification du service ClearID :** Cliquez sur plus ( ) pour sélectionner la clé d'authentification pour votre intégration API. Cette clé sert à authentifier les communications de l’agent de synchronisation lorsqu’il envoie des requêtes à votre compte ClearID.
  - Indique que l'agent de synchronisation n’est pas connecté à ClearID et qu'une clé privée est nécessaire.
  - Indique que l'agent de synchronisation est connecté à ClearID et que la clé privée a été fournie.

  Les réglages URL API suivants sont automatiquement renseignés lorsque la **clé d'authentification du service ClearID** est sélectionnée :

- **URL de l'API Jeton (lecture seule) :** Le service Jeton fournit un jeton d'authentification pour contacter l'identité et le service principal.
- **URL de l'API Identité (lecture seule) :** Le service Identity sert à accéder à toutes les informations d’identité ClearID.
- **URL de l'API Principal (lecture seule) :** Le service Principal sert à accorder l'accès au portail web aux utilisateurs.
- **Pays par défaut (ISO 3166, 3 lettres) :** Saisissez votre code pays à trois lettres. Par exemple, USA ou CAN.

  REMARQUE : Les codes pays à trois lettres sont basés sur les codes Alpha-3 de la norme de codes pays ISO 3166-1.
- **Le service Principal a accès au portail :** Cochez la case pour autoriser les utilisateurs synchronisés à accéder au portail web ClearID.

6 (Facultatif) Dans la section *Options avancées*, ne remplissez pas ces champs.

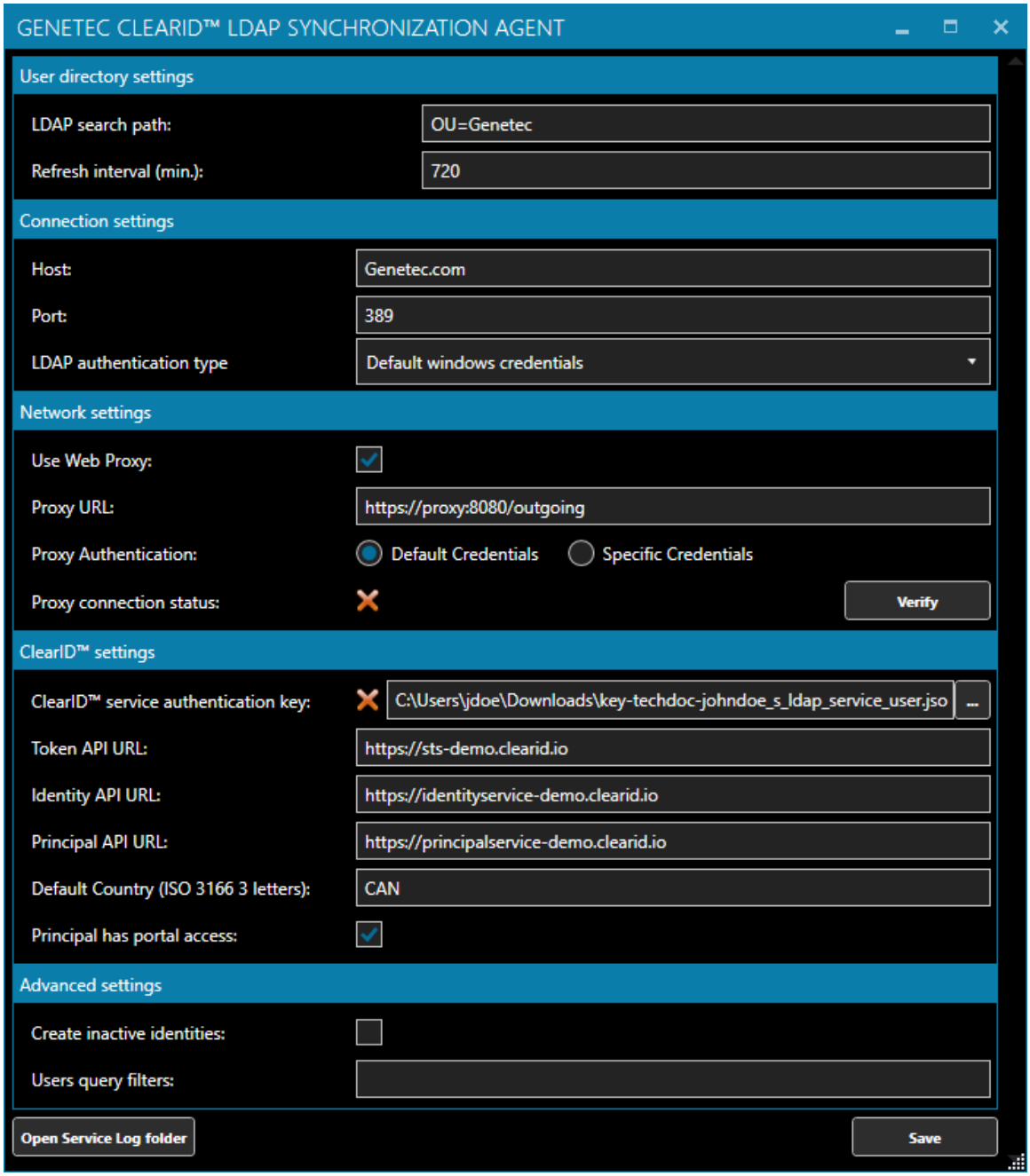
La section *Options avancées* sert à personnaliser le comportement de l'agent de synchronisation.

- **Créer des identités inactives :** Cochez cette case pour créer des identités ClearID inactives pour les utilisateurs inactifs détectés dans Active Directory pendant la synchronisation.

  BONNE PRATIQUE : Cette case est généralement désactivée pour éviter de créer des utilisateurs inactifs.
- **Filtres de demandes utilisateur :** (Facultatif) Entrez les filtres de demande utilisateur spécifiés par votre contact de déploiement.

  IMPORTANT : Utilisez uniquement cette option sur demande de votre contact de déploiement.

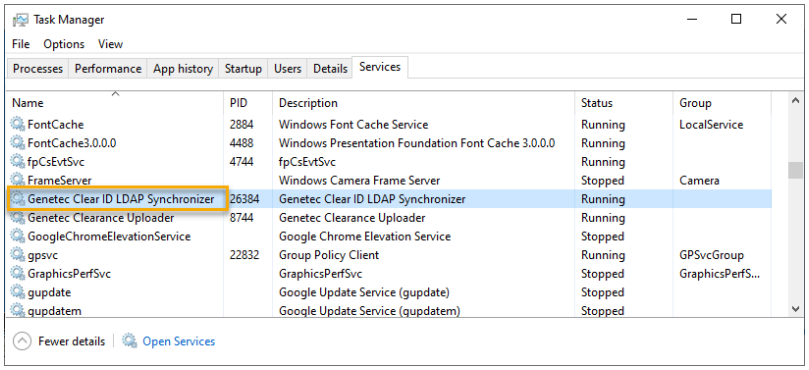
7 Cliquez sur **Enregistrer**.



Le fichier de configuration de l'agent de synchronisation est enregistré dans *C:\ProgramData\Genetec ClearID LDAP Synchronizer\config.json*

CONSEIL : Vous pouvez supprimer ce fichier si vous souhaitez supprimer tous vos paramètres et configurer à nouveau l'agent de synchronisation.

8 Ouvrez le Gestionnaire de tâches Windows et faites un clic droit sur le service Windows **Genetec ClearID LDAP Synchronizer** (*Genetec.ClearID.LdapSyncAgent.Service.exe*).



a) Si vous configurez l'agent pour la première fois, cliquez sur **Démarrer** pour lancer le service afin d'activer les réglages de configuration.

b) Si l'agent est déjà en cours d’exécution, cliquez sur **Redémarrer** pour appliquer les modifications apportées à votre configuration.

Votre agent de synchronisation ClearID est à présent configuré pour synchroniser automatiquement les attributs LDAP Active Directory avec les attributs d'identité ClearID.

Lorsque vous avez terminé

1. Consultez le portail Web ClearID pour vérifier que les nouvelles identités pour les utilisateurs Active Directory ont bien été synchronisées et qu’elles contiennent les bons attributs.
2. (Facultatif) Vous pouvez cliquer sur **Ouvrir le dossier de journalisation** pour consulter les fichiers journaux *ErrorLog.txt* et *Eventlog.txt*.

   REMARQUE : Les informations dans le dossier *Service Log* sont généralement utilisées lorsque vous appelez l’assistance ou lorsque votre contact vous demande d’envoyer les journaux à Genetec Inc.

13

Appareils de gestion des visiteurs

En savoir plus sur l'application mobile ClearID Self-Service Kiosk qui simplifie la gestion et l’inscription des visiteurs.

Cette section aborde les sujets suivants:

- " À propos de ClearID Self-Service Kiosk ", page 578
- " Configurer l’iPad de la borne en libre-service ", page 582
- " Enregistrement par opérateur mobile ", page 594
- " Configurer l'enregistrement par opérateur mobile ", page 597
- " Configurer l'imprimante d'étiquettes de la borne en libre-service (Brother QL-820NWBc, QL-820NWB ou QL-810W) ", page 602
- " Configurer l'imprimante d'étiquettes de la borne en libre-service (Brother TD-4550DNWB) ", page 612
- " Sélectionner une imprimante d'étiquettes de borne en libre-service ", page 622
- " Imprimer un badge de test sur la borne en libre-service ", page 629
- " Réinitialiser l’application mobile Self-Service Kiosk ", page 633
- " Options de la borne en libre-service ", page 635
- "Types de pièces d’identité", page 646

À propos de ClearID Self-Service Kiosk

Genetec ClearID[MC] Self-Service Kiosk est une application mobile qui simplifie la gestion des visiteurs inscrits à l'aide du portail Genetec ClearID[MC] en libre-service. La borne en libre-service est destinée aux centres d'accueil ou aux installations sécurisées où les invités s'enregistrent eux-mêmes.

Les visiteurs peuvent s'inscrire sur la borne en libre-service ClearID à l'aide de plusieurs méthodes :

- Rechercher un visiteur associé à une visite en scannant son code QR d'invitation.
- Rechercher un visiteur associé à une visite en scannant son permis de conduire.
- Rechercher un visiteur associé à une visite en scannant son passeport ou sa carte de citoyen (données MRZ).
- Rechercher un visiteur associé à une visite en scannant sa pièce d'identité (divers types de pièces de plus de 200 pays).
- Rechercher un visiteur associé à une visite par son adresse e-mail.

REMARQUE : Une fois qu'un visiteur est inscrit dans ClearID Self-Service Kiosk, son hôte est informé par e-mail et par SMS (si l'option est activée).

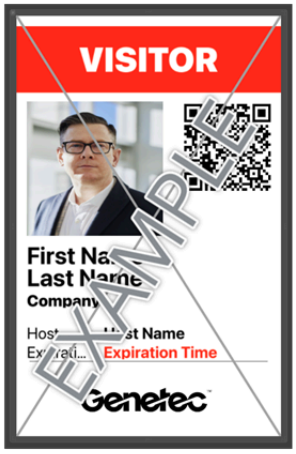
ClearID Self-Service Kiosk vous permet également d'effectuer les tâches suivantes :

- Contrôler les visiteurs durant l'inscription en libre-service ou la préinscription.
- Prendre une photo du visiteur[1].
- Imprimer un badge de visiteur au format sur une imprimante d'étiquettes sans fil (Bluetooth ou Wi-Fi). Le badge intègre une photo et permet d'identifier le visiteur et l'événement auquel il participe.
- Préinscription des visiteurs.
- Logos de sociétés sur la borne ClearID Self-Service Kiosk et sur les badges des visiteurs.
- Messages de bienvenue et d'assistance personnalisés sur la borne ClearID Self-Service Kiosk.

REMARQUE : [1]La photo n'est utilisée que pour l'impression du badge. La photo n'est pas enregistrée ni stockée pour une utilisation ultérieure, afin de protéger les données du visiteur.

Badges de visiteurs

Voici des exemples de badges de visiteurs au format *portrait* et *paysage*.



Dimensions du badge : **10 x 6,1 cm** ou **3,94 x 2,56 pouces**.

Pour télécharger l'application mobile Genetec ClearID[MC] Self-Service Kiosk, rendez-vous sur l'App Store.

Rubriques connexes

Appareils pris en charge, page 78
Types de pièces d'identité, page 646
Fiche technique ClearID Self-Service Kiosk (2 pages)

Inscription sur une borne en libre-service

Utilisez ces informations pour comprendre comment les visiteurs s'inscrivent sur une borne Genetec ClearID[MC] Self-Service Kiosk.

REMARQUE : Les visiteurs peuvent s'inscrire jusqu'à 1 heure avant le début d'un événement de visite.

Scénario 1 : Inscription sur borne en libre-service (badge papier)

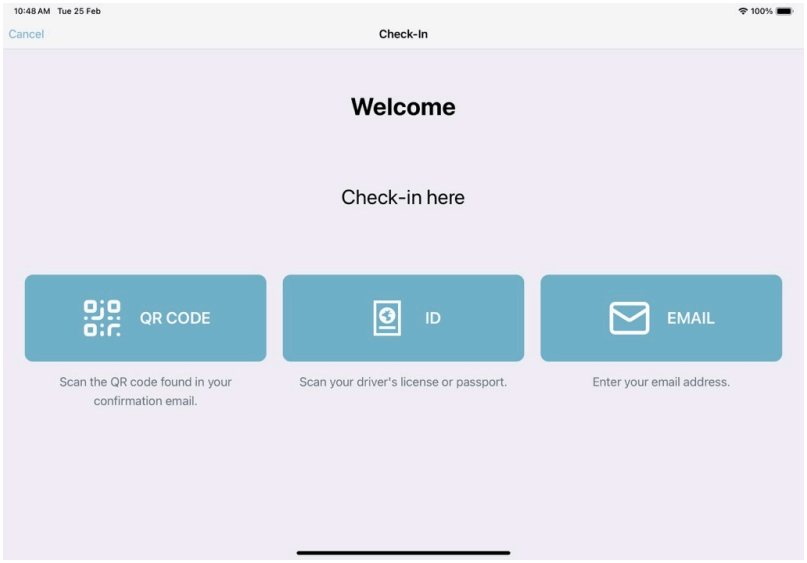
Les visiteurs peuvent s’inscrire facilement sur une borne ClearID Self-Service Kiosk. Ils scannent le code QR reçu par e-mail, prennent une photo et impriment le badge de visiteur qui l’identifie et indique l’événement auquel il participe.

Scénario 2 : Inscription sur borne en libre-service (badge de titulaire de cartes)

À l’aide de Security Center, un agent d'accueil peut attribuer un identifiant à un visiteur Genetec ClearID^{MC}, et le visiteur peut ensuite utiliser son badge pour accéder à certains secteurs du bâtiment lorsqu'il est accompagné par son hôte.

Inscription en libre-service

L'inscription en libre-service est conçue pour les visiteurs qui ont été invités ou qui se sont préinscrits.



Vous pouvez utiliser ClearID Self-Service Kiosk pour vous inscrire vous-même à l'aide d'un code QR, d'une pièce d'identité ou d'un e-mail jusqu’à une heure avant le début d’un événement de visite :

- Si des noms en double sont détectés, vous sélectionnez votre e-mail unique dans la liste.
- Si vous scannez un code QR introuvable, la borne en libre-service passe à la recherche de visiteur par e-mail.
- Si aucun identifiant ou e-mail n'est trouvé, la borne en libre-service passe au processus d'auto-inscription.

REMARQUE : Les options d'inscription affichées sur la page de **Bienvenue** de ClearID Self-Service Kiosk peuvent être personnalisées afin de masquer les options qui ne sont pas pertinentes pour votre site ou vos visiteurs.

Pour en savoir plus, voir l’onglet **Bornes** dans Activer la gestion des visiteurs pour un site , page 257.

Rubriques connexes

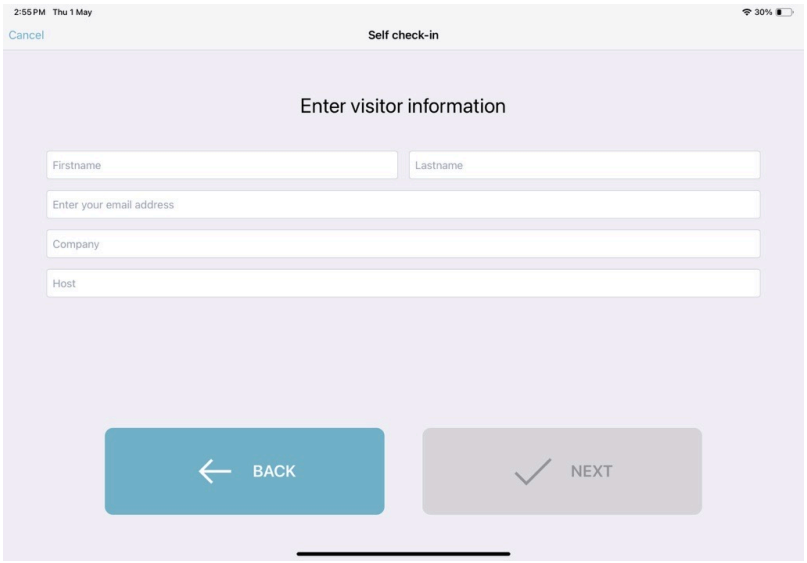
Activer la gestion des visiteurs pour un site, page 257

Auto inscription sur une borne en libre-service

Le processus d'auto-inscription sur Genetec[MC] ClearID Self-Service Kiosk est conçu pour gérer les visites ou visiteurs impromptus, en l'absence d'invitation ou de préinscription.

Le processus d'auto-inscription est déclenché (s'il est activé pour votre compte) lorsqu'un visiteur arrive sur le site sans invitation et qu'il n'est pas trouvé dans le système lors du processus d'inscription en libre-service.

REMARQUE : Les entrées pré-remplies ne peuvent pas être modifiées.



Le processus d'auto-inscription est associé à un site. Les visiteurs sont acceptés automatiquement avec un accès de visiteur de base au site. Par exemple, la porte d'entrée, la réception ou le secteur d'inscription pour assurer une expérience d'inscription fluide.

IMPORTANT : Tout visiteur sur une liste de blocage se voit refuser l'accès si la fonction *liste de surveillance* est activée pour votre compte, et le *responsable de liste de surveillance* est alors notifié. Dans cette situation, le visiteur doit s'adresser au personnel de sécurité ou de l'accueil.

Configurer l'iPad de la borne en libre-service

Avant que les visiteurs puissent utiliser la borne en libre-service pour l'inscription ou la radiation, vous devez ajouter l'iPad Genetec ClearID[MC] Self-Service Kiosk dans Genetec ClearID[MC]. Vous devez ensuite inscrire et activer l'appareil dans l'application mobile ClearID Self-Service Kiosk.

Avant de commencer

- Le Wi-Fi doit être activé sur l'appareil de la borne en libre-service avant l'activation de l'appareil.
- Votre appareil doit exécuter iOS 16.6 ou ultérieur.

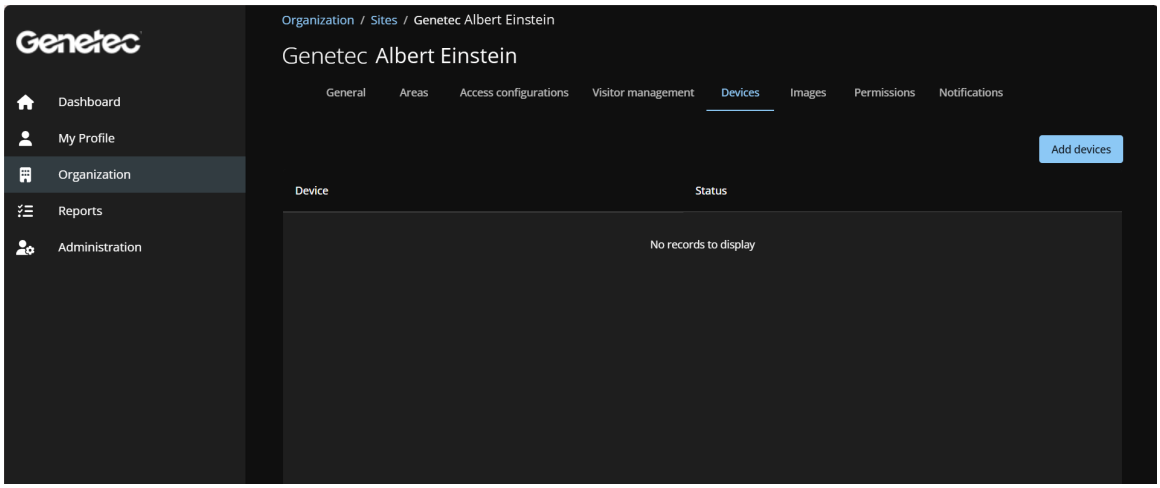
À savoir

- Seul un *administrateur* ou un *propriétaire du site* peut générer un code d'activation d'appareil dans ClearID.
- Vous ne pouvez activer et associer une borne ClearID Self-Service Kiosk qu'à un seul site à la fois.
- L'iPad utilisé pour ClearID Self-Service Kiosk doit être sur le même réseau Wi-Fi que l'imprimante d'étiquettes.

Procédure

1 Dans ClearID, cliquez sur **Organisation** et sélectionnez votre site.

2 Sur la page *Site* , cliquez sur **Appareils**.



a) Cliquez sur **Ajouter des appareils** pour configurer votre borne en libre-serviceClearIDdans ClearID.

b) Dans la boîte de dialogue *Ajouter des appareils*, saisissez un nom pour l'appareil.

CONSEIL : Songez à inclure le site ou le secteur associé dans le nom pour vous aider à identifier votre appareil par la suite.

c) Saisissez le nombre d'appareils que vous souhaitez ajouter, puis cliquez sur **Ajouter**.

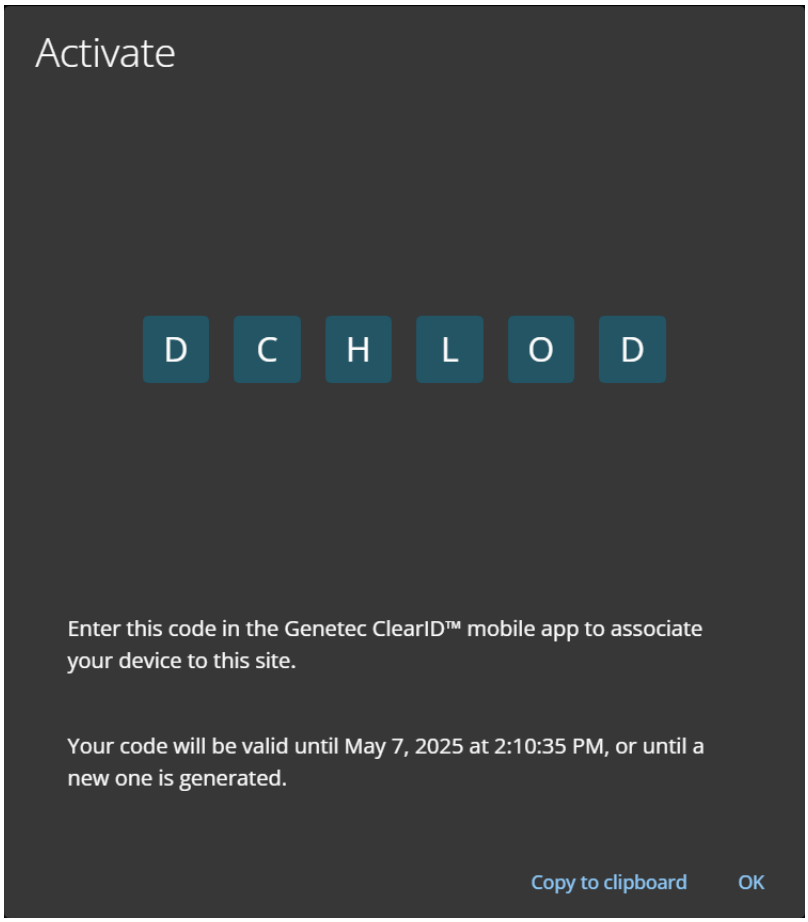
REMARQUE : Vous pouvez configurer jusqu'à 50 appareils avec un seul code d'activation.

3 Téléchargez l'application ClearID Self Service Kiosk sur les appareils iOS que vous souhaitez enregistrer.

4 Activez votre borne dans ClearID :

a) Sélectionnez votre iPhone sur le liste des appareils.

b) Dans le champ **Statut** , cliquez sur **Générer le code d'activation**.



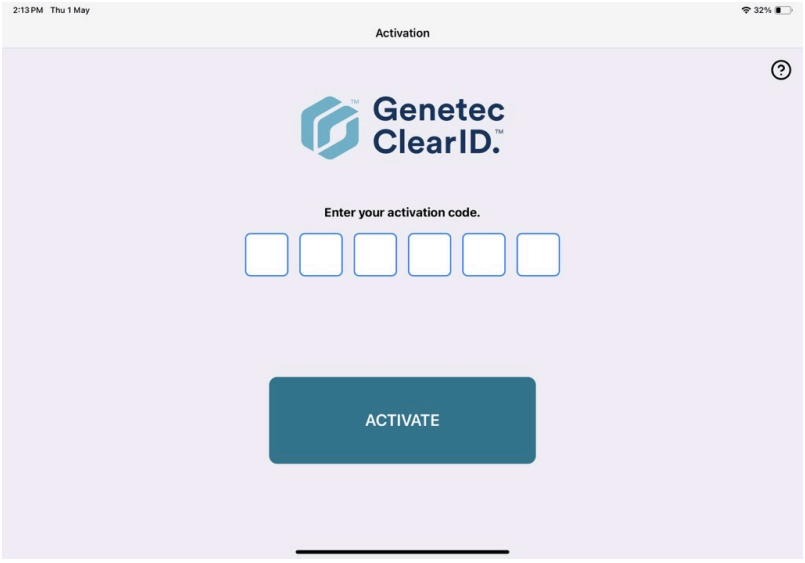
c) Notez le code d'activation pour plus tard.

d) (Facultatif) Copiez-le dans le presse-papier.

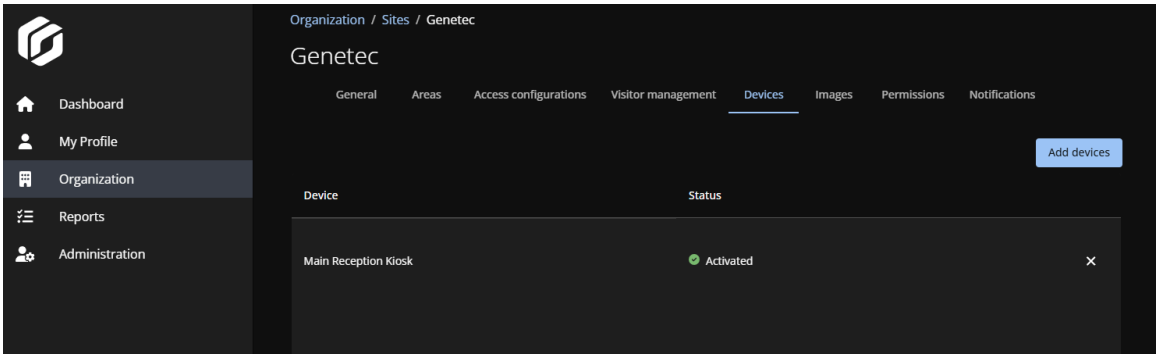
CONSEIL : Utilisez **Copier dans le presse-papiers** si la personne qui enregistre l'appareil d'enregistrement par opérateur mobile ClearID dans le portail ClearID n'est pas celle qui active l'appareil. Une fois que le code est dans le presse-papier, il peut être envoyé par e-mail à la personne qui active l'appareil.

e) Cliquez sur **OK**.

5 Dans l'application mobile ClearID Self-Service Kiosk, saisissez le code d'activation de l'appareil et appuyez sur **Activer**.



Votre borne en libre-service est à présent activée dans ClearID et prête à l'emploi.



Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles.

Lorsque vous avez terminé

- Configurer l'imprimante d'étiquettes de votre borne
- (Facultatif) Personnalisez la bannière pour les e-mails de notification
- (Facultatif) Personnalisez la configuration de votre borne en libre-service
- (Facultatif) Personnalisez le logo de badge de votre borne en libre-service

Rubriques connexes

Appareils pris en charge, page 78
Ports de pare-feu, page 76

Personnaliser la configuration de la borne en libre-service

Configurez les images de votre site et les options de la borne pour personnaliser les choix proposés aux visiteurs sur votre borne Genetec ClearID[MC] Self-Service Kiosk durant le processus d'inscription ou de radiation. Vous pouvez personnaliser les logos de l’entreprise, les thèmes de la borne et des messages de bienvenue ou d'assistance ciblés.

Avant de commencer

Configurer l’iPad de la borne en libre-service, page 582

CONSEIL : Vérifiez que les images d'écran de bienvenue répondent aux exigences spécifiées dans l'infobulle sur la page **Gestion des visiteurs** > **Bornes** du portail web Genetec ClearID[MC].

À savoir

Seul un propriétaire de site ou un administrateur de comptes peut personnaliser les options de configuration de la borne.

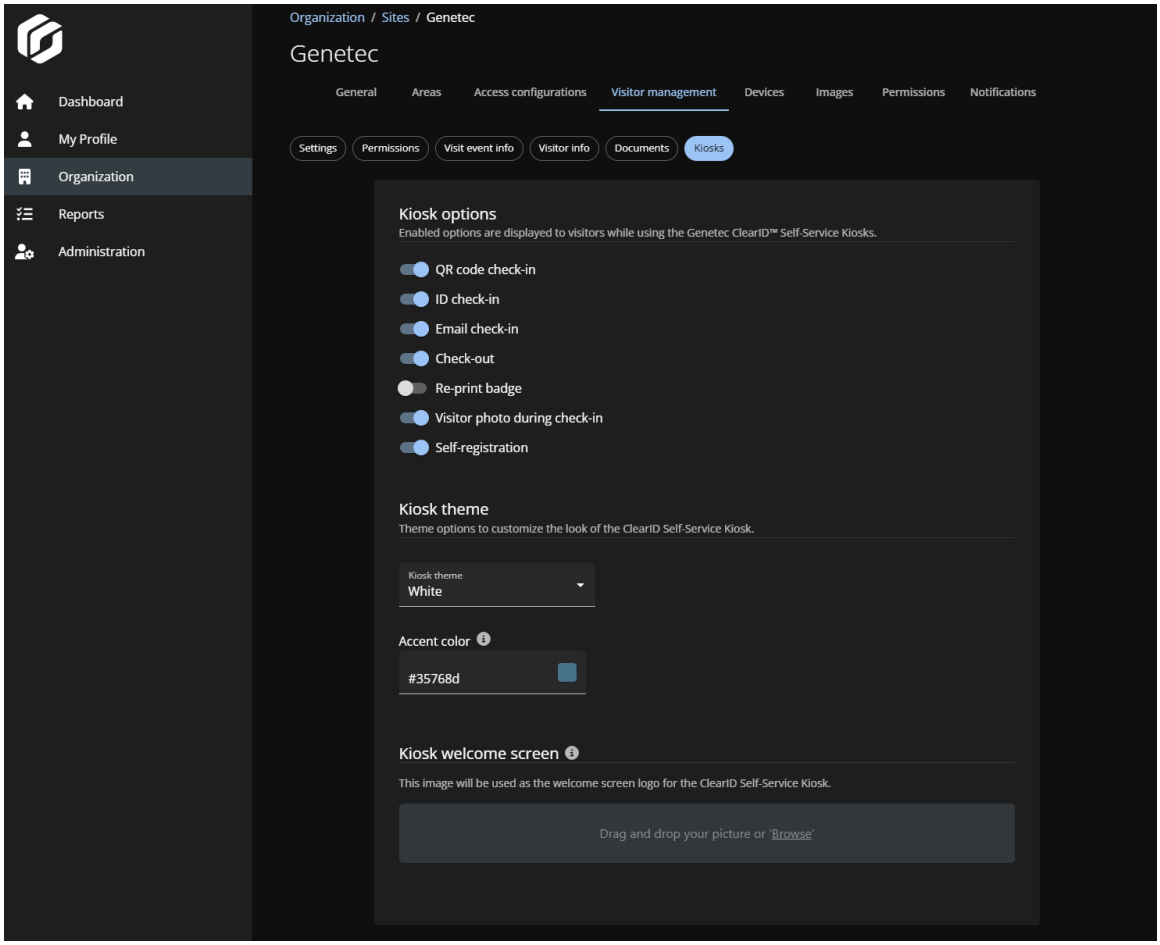
- Les modifications des options personnalisées sont synchronisées avec la borne toutes les 60 secondes.

BONNE PRATIQUE : Pour un résultat optimal, utilisez des images *.PNG* transparentes pour personnaliser votre image d'écran de bienvenue.

Procédure

1 Sur le portail web ClearID,cliquez sur **Organisation** et sélectionnez votre site.

2 Cliquez sur **Gestion des visiteurs** > **Bornes**.



3 Dans l'onglet *Borne*, personnalisez les options de configuration selon vos besoins :

a) (Facultatif) Dans la section *Thème de la borne* , sélectionnez un thème pour personnaliser l'habillage graphique de la borne.

Par exemple, sélectionnez le thème **Blanc** ainsi qu'une **Couleur d'accentuation** qui correspond à la charte graphique de votre organisation.

b) (Facultatif) Dans la section *Écran de bienvenue de la borne*, transférez une image qui doit servir de logo sur l'écran de bienvenue.

Par exemple, le *nom de société* ou un *logo* qui reprend la charte graphique de votre organisation.

Pour des instructions détaillées et pour voir des exemples de personnalisation de la borne, voir Activer la gestion des visiteurs pour un site , page 257.

4 Cliquez sur **Enregistrer**.

Regardez cette vidéo pour en savoir plus. Cliquez sur l'icône Sous-titres (CC) pour activer les sous-titres dans l'une des langues disponibles.

Personnaliser le logo des badges de visiteurs de la borne en libre-service

Vous pouvez personnaliser l'image du logo des badges de visiteurs utilisée sur les badges temporaires ou définitifs imprimés par la borne.

Avant de commencer

Configurer l'iPad de la borne en libre-service, page 582

CONSEIL : Vérifiez que les images de logos de badges répondent aux exigences spécifiées dans l'infobulle sur la page **Images** du portail web Genetec ClearID[MC].

À savoir

Seul un propriétaire de site ou un administrateur de comptes peut personnaliser le logo des badges de visiteurs.

- Les modifications des options personnalisées sont synchronisées avec la borne toutes les 60 secondes.

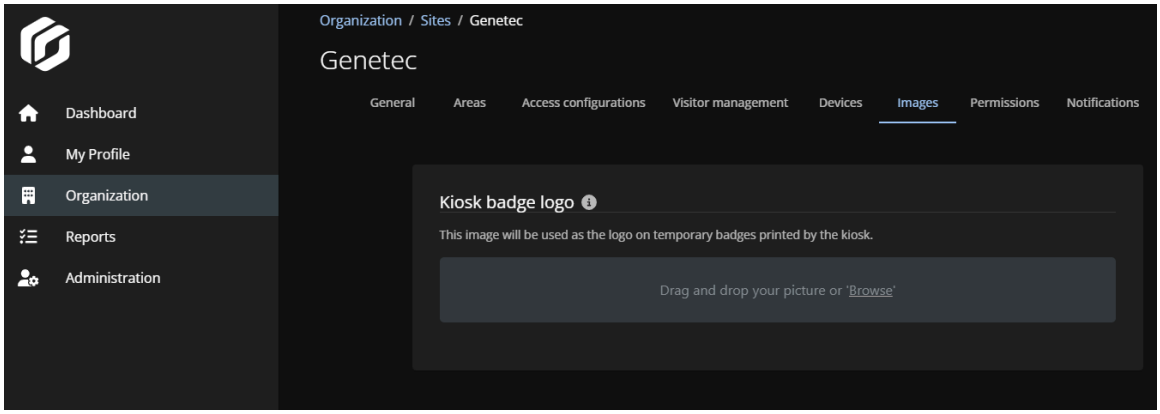
BONNE PRATIQUE : Pour un résultat optimal, utilisez des images *.PNG* transparentes pour personnaliser votre logo de badge.

Procédure

1 Sur le portail Web ClearID, cliquez sur **Organisation** > **Sites**.

2 Recherchez et sélectionnez un site.

3 Cliquez sur **Images**.

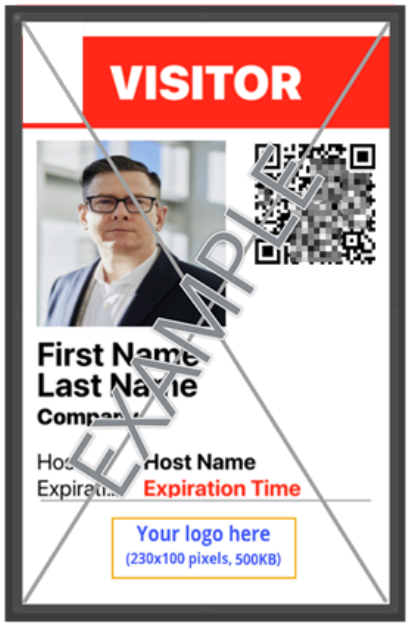


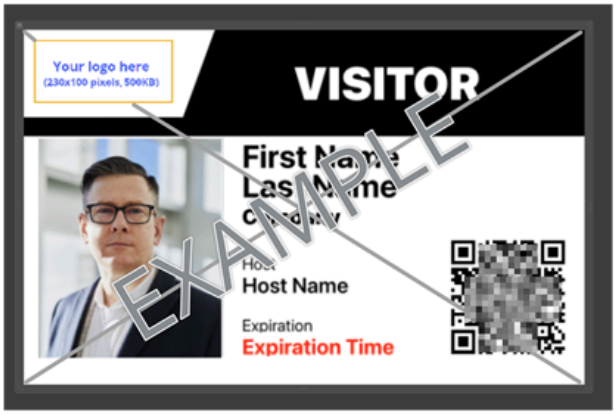
a) Dans la section *Logo de badge de la borne*, faites un glisser-déposer de votre image ou parcourez vos fichiers pour sélectionner une image de **Logo de badge de la borne**.

Cette image est utilisée en tant que logo sur les badges temporaires imprimés par la borne.

b) Cliquez sur **Enregistrer**.

Voici un exemple de logo de badge personnalisé pour la borne.





Ajouter des documents PDF à valider dans le kiosque en libre-service

Pour les sites ayant des conditions requises particulières, les *administrateurs de comptes* et les *propriétaires de sites* peuvent charger des documents, comme des accords de non-divulgation, de décharges et autres, que les visiteurs doivent signer lorsqu'ils s'inscrivent lors de l'utilisation du kiosque en libre-service.

Avant de commencer

Activez la gestion des visiteurs pour les sites.

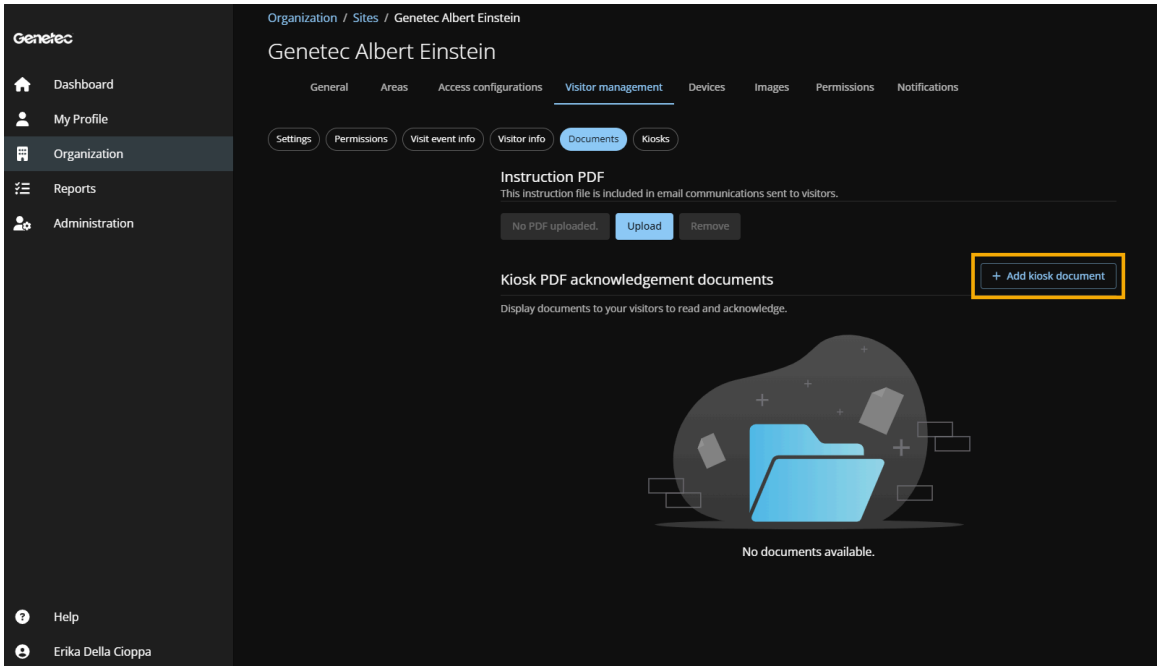
À savoir

- Vous devez être un *administrateur de compte* ou un *propriétaire du site* pour ajouter des documents que les visiteurs doivent accepter dans le kiosque en libre-service.
- Vous pouvez afficher jusqu'à cinq documents sur la borne pendant l'inscription.

Procédure

1 Sur le portail web de Genetec ClearID[MC], cliquez sur **Organisation** > **Site** > **Gestion des visiteurs** > **Documents**.

2 Cliquez sur **Ajouter un document à la borne**.



IMPORTANT : Ces documents doivent être au format PDF.

a) Dans le champ **Nom d'affichage**, donnez un nom au document.

b) Faites glisser un document sur le champ, ou cliquez sur **Parcourir** pour sélectionner un fichier.

3 Configurez les préférences de partage du document selon vos besoins :

a) Cochez la case **Afficher le document sur la borne** pour afficher le document pendant l'inscription du visiteur sur la borne.

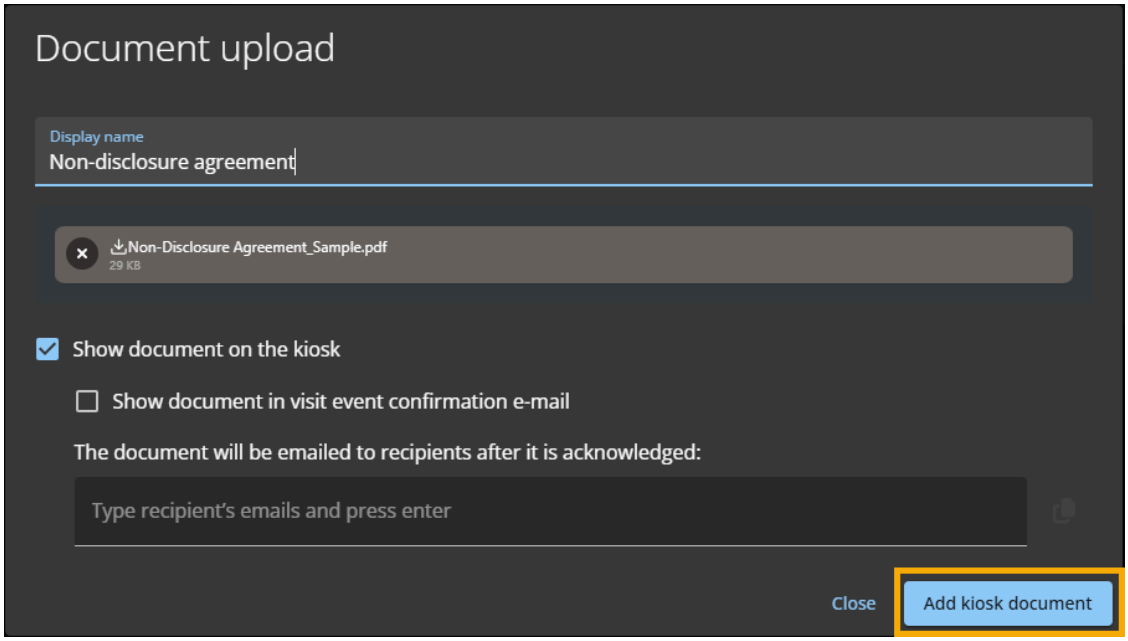
CONSEIL : Lorsque la case est décochée, le document reste disponible en tant que brouillon.

b) Cochez la case **Afficher le document dans l'e-mail de confirmation de visite** pour joindre une copie du document aux e-mails de confirmation envoyés aux visiteurs, afin qu'ils puissent examiner le document avant de venir.

c) Ajoutez la liste des destinataires qui doivent recevoir une copie des documents validés par les visiteurs.

REMARQUE : Cliquez sur pour copier la liste complète des destinataires, par exemple pour ajouter les mêmes destinataires aux autres documents à valider.

4 Cliquez sur **Ajouter un document à la borne** pour enregistrer votre document.



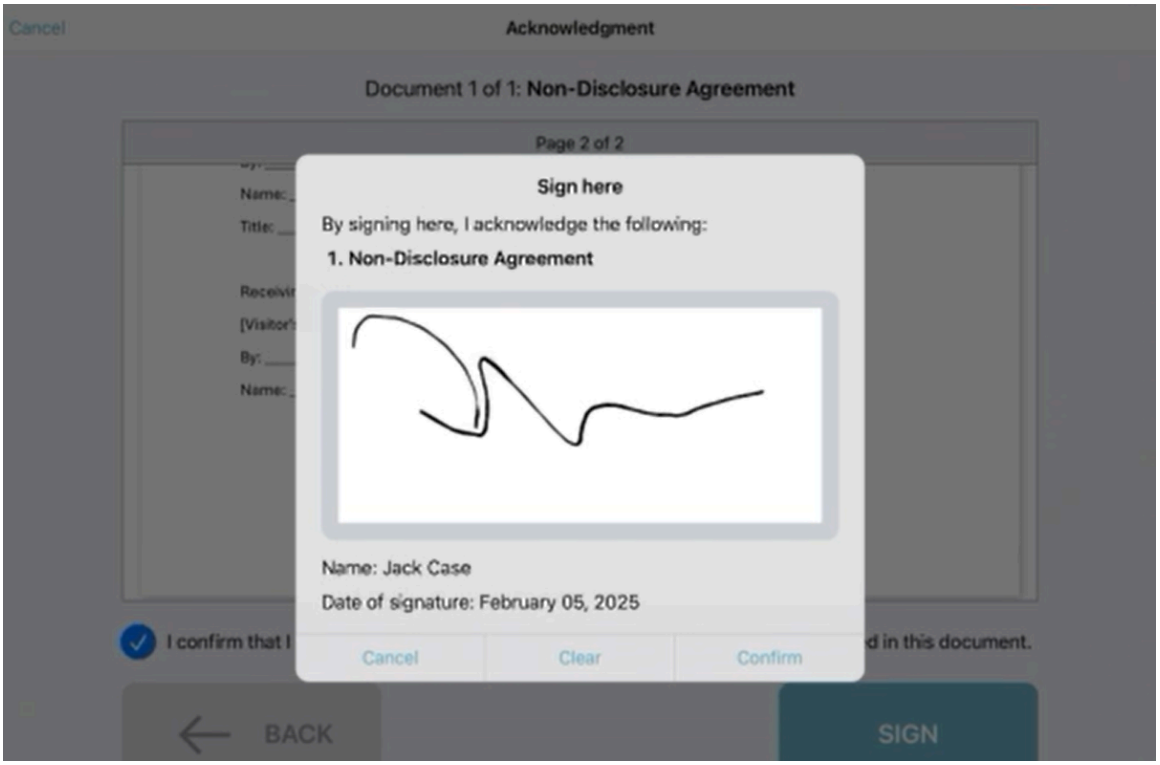
5 Utilisez les icônes pour gérer chaque document transféré :

a) Cliquez sur pour modifier un document existant.

b) Cliquez sur pour télécharger une copie du document.

c) Cliquez sur pour supprimer un document.

Les visiteurs doivent confirmer qu'ils ont lu les documents transférés et les signer pendant l'inscription sur la borne en libre-service.



Activer la réimpression des badges

En tant que *propriétaires de site*, vous pouvez activer la réimpression des badges pour que les visiteurs puissent réimprimer un badge temporaire perdu ou endommagé dans ClearID Self-Service Kiosk.

Avant de commencer

Configurez l'iPad Self-Service Kiosk.

À savoir

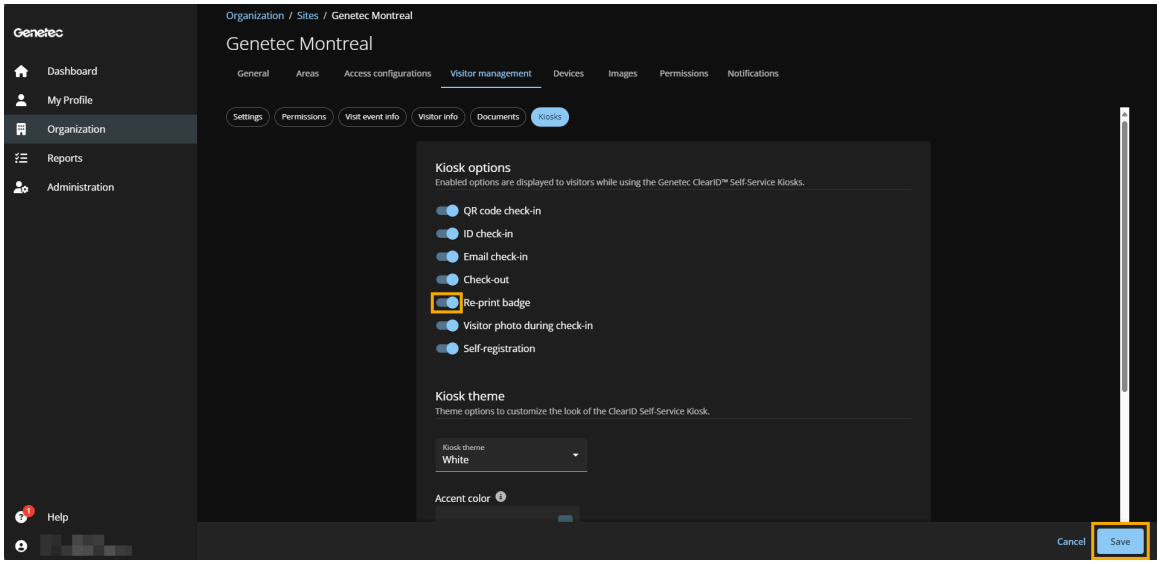
Vous devez être *propriétaire de site* pour activer la réimpression des badges dans ClearID Self-Service Kiosk.

BONNE PRATIQUE : Les codes QR configurés en tant qu'identifiants ne doivent donner accès qu'à des secteurs non sécurisés.

Procédure

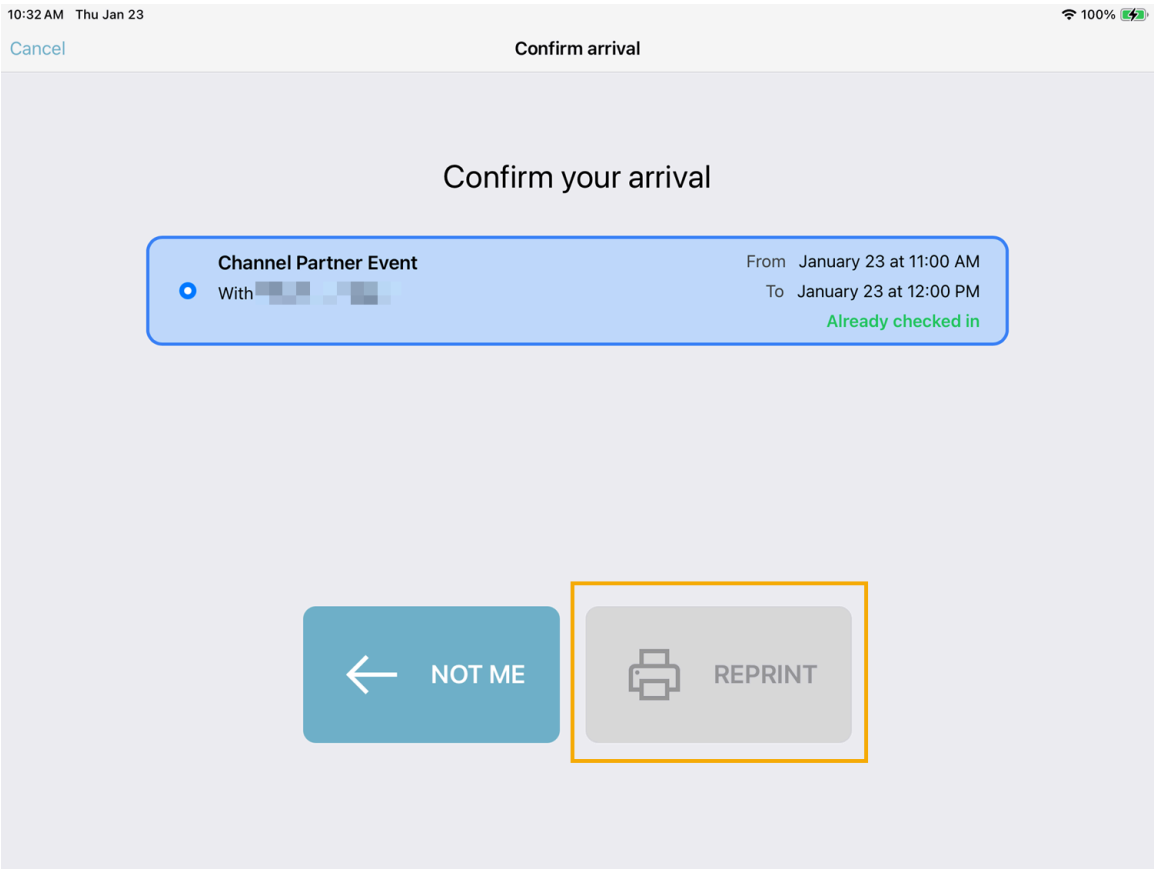
1 Sur le portail web de Genetec ClearID[MC], cliquez sur **Organisation** > **Site** > **Gestion des visiteurs** > **Bornes**.

2 Dans la section *Options de borne*, activez l'option **Réimprimer le badge**.



3 Cliquez sur **Enregistrer**.

Les visiteurs peuvent à présent réimprimer un badge temporaire en accédant aux informations sur leur visite sur une borne en libre-service.



Désactiver la photo du visiteur pendant l'inscription

Sur les sites où la confidentialité des visiteurs est essentielle, les *propriétaires de sites* peuvent désactiver la capture photo durant l'inscription des visiteurs dans ClearID Self-Service Kiosk.

Avant de commencer

Configurez l'iPad Self-Service Kiosk.

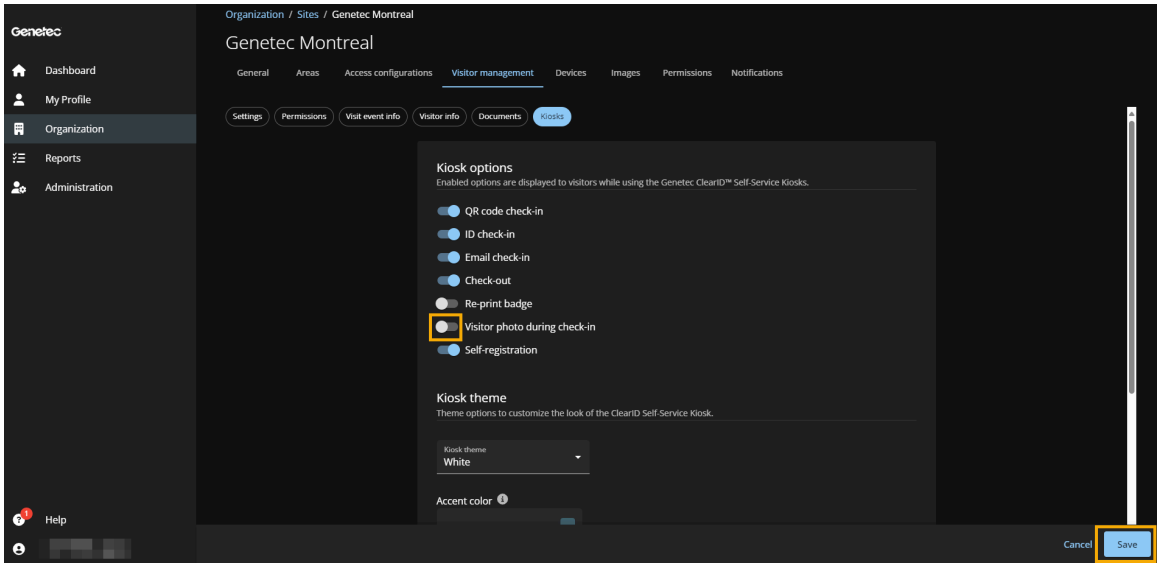
À savoir

Vous devez être *propriétaire de site* pour désactiver la capture photo du visiteur pendant l'inscription avec ClearID Self-Service Kiosk.

Procédure

1 Sur le portail web de Genetec ClearID[MC], cliquez sur **Organisation** > **Site** > **Gestion des visiteurs** > **Bornes**.

2 Dans la section *Options de borne*, désactivez l'option **Photo du visiteur à l'inscription**.



REMARQUE : L'option **Photo du visiteur à l'inscription** est activée par défaut.

3 Cliquez sur **Enregistrer**.

Les visiteurs peuvent à présent s'inscrire sur une borne sans devoir prendre leur photo.

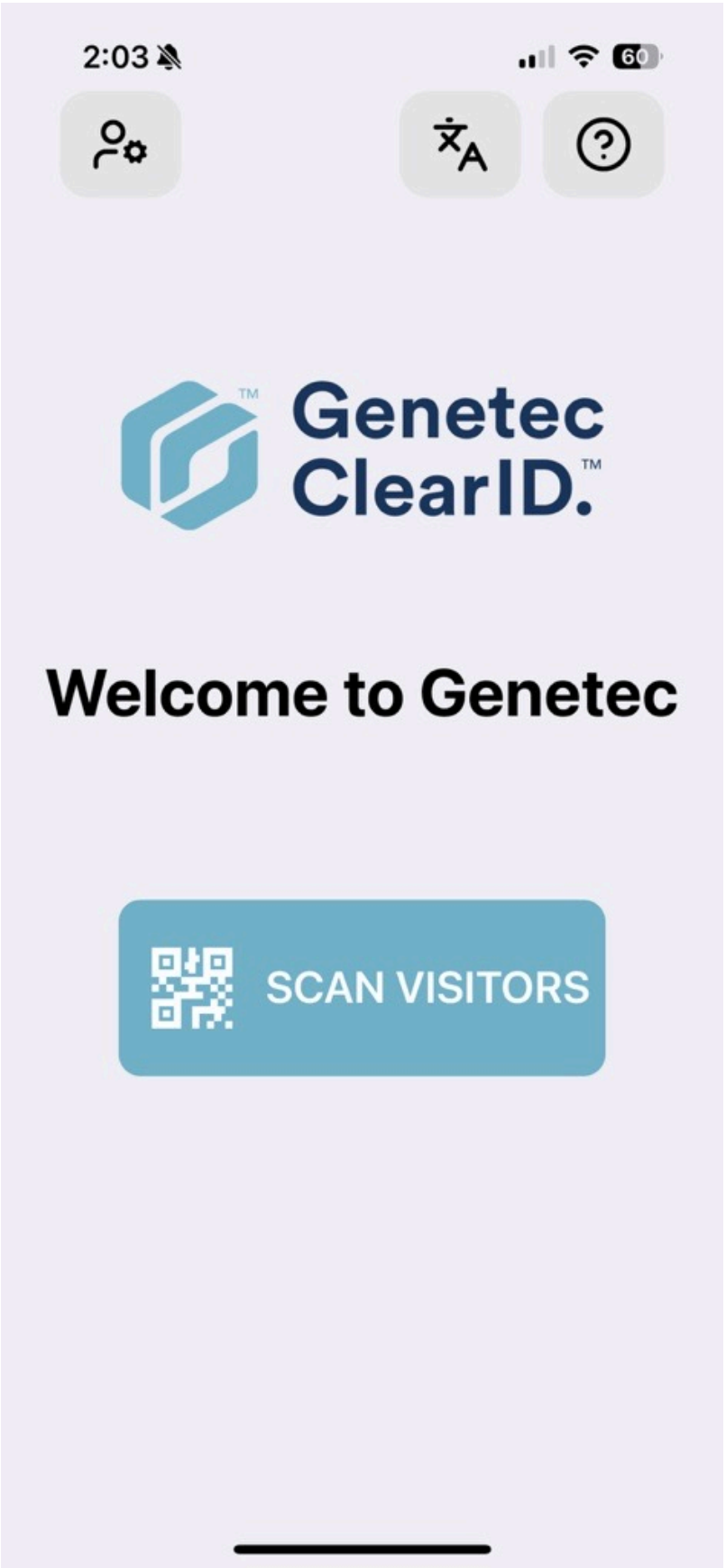
Enregistrement par opérateur mobile

Ces informations vous permettent d'aider à comprendre comment les opérateurs enregistrent les visiteurs à l'entrée et à la sortie des événements à l'aide de l'enregistrement par opérateur mobile.

REMARQUE : Les visiteurs peuvent s'inscrire jusqu'à 1 heure avant le début d'un événement de visite.

Enregistrement par opérateur mobile

L'enregistrement par opérateur mobile est destinée aux opérateurs chargés d'enregistrer les visiteurs qui ont été invités ou pré-enregistrés. L'enregistrement par opérateur mobile peut être activé sur plusieurs iPhones en même temps, ce qui accélère la vérification lors d'événements importants en évitant les files d'attente aux bornes en libre-service.


2:03
Genetec ClearID.™
Welcome to Genetec
SCAN VISITORS

Les opérateurs tels que les réceptionnistes, les agents de sécurité et les agents peuvent rapidement enregistrer de nombreux visiteurs lors de grands événements. L'application ClearID Self-Service Kiosk sur un iPhone permet aux opérateurs de scanner des codes QR ou de rechercher des visiteurs par nom ou par e-mail.

- Les visiteurs ne peuvent pas s'inscrire eux-mêmes lorsqu'ils sont enregistrés par un opérateur.
- L'enregistrement par opérateur mobile ne scanne pas les identifiants, ne prend pas de photos et n'imprime pas de badges.

Nombre d'enregistrements

Une fois qu'un opérateur scanne le code QR d'un visiteur, toutes les informations sur la visite sont affichées, y compris les options d'enregistrement et de sortie. Grâce à ces options, Genetec ClearID^{MC} suit le nombre de fois où les visiteurs entrent et sortent de votre événement.

Configurer l'enregistrement par opérateur mobile

Avant de pouvoir utiliser l'enregistrement par opérateur mobile pour vérifier les visiteurs lors d'événements importants ou rechercher des informations sur les visiteurs, vous devez ajouter un iPhone à Genetec ClearID[MC]. Vous devez ensuite inscrire et activer l'appareil dans l'application mobile ClearID Self-Service Kiosk.

Avant de commencer

- Les données Wi-Fi ou cellulaires doivent être activées sur l'appareil d'enregistrement par opérateur mobile avant d'activer l'appareil.
- Votre appareil doit exécuter iOS 16.6 ou ultérieur.

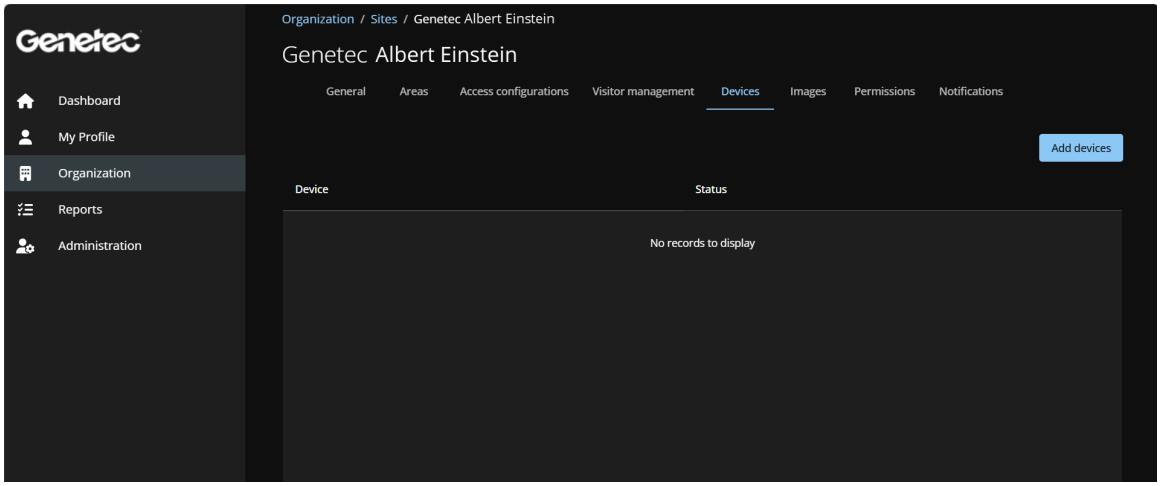
À savoir

- Seul un *administrateur* ou un *propriétaire du site* peut générer un code d'activation d'appareil dans ClearID.
- Vous ne pouvez activer et associer un appareil d'enregistrement par opérateur mobile qu'à un site à la fois.
- Les iPhones héritent du thème et des réglages des iPads du kiosque en libre-service associés au même site.
- Les enregistrements via un iPhone permettent d'éviter de demander aux visiteurs de prendre une photo, d'imprimer un badge ou d'accepter des documents.

Procédure

1 Dans Genetec ClearID, cliquez sur **Organisation** et sélectionnez votre site.

2 Sur la page *Site* , cliquez sur **Appareils**.



a) Cliquer **Ajouter des appareils** pour configurer votre appareil d'enregistrement par opérateur mobile dans ClearID.

b) Dans la boîte de dialogue *Ajouter des appareils*, saisissez un nom pour l'appareil.

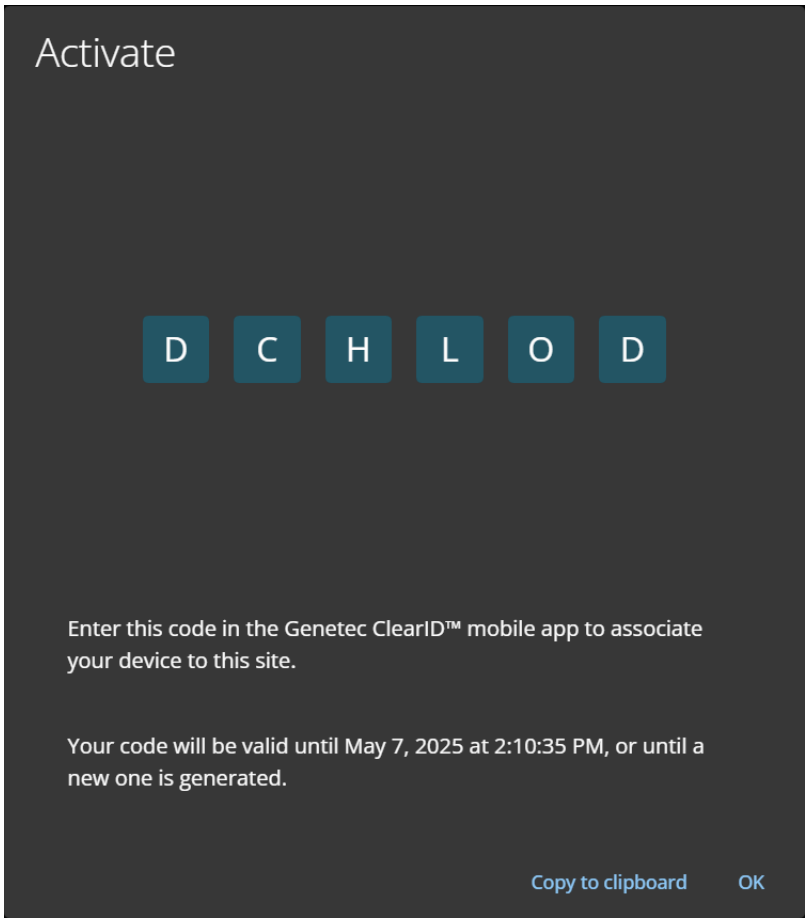
CONSEIL : Songez à inclure le site ou le secteur associé dans le nom pour vous aider à identifier votre appareil par la suite.

c) Saisissez le nombre d'appareils que vous souhaitez ajouter, puis cliquez sur **Ajouter**.

REMARQUE : Vous pouvez configurer jusqu'à 50 appareils avec un seul code d'activation.

3 Téléchargez l'application ClearID Self Service Kiosk sur les appareils iOS que vous souhaitez inscrire.

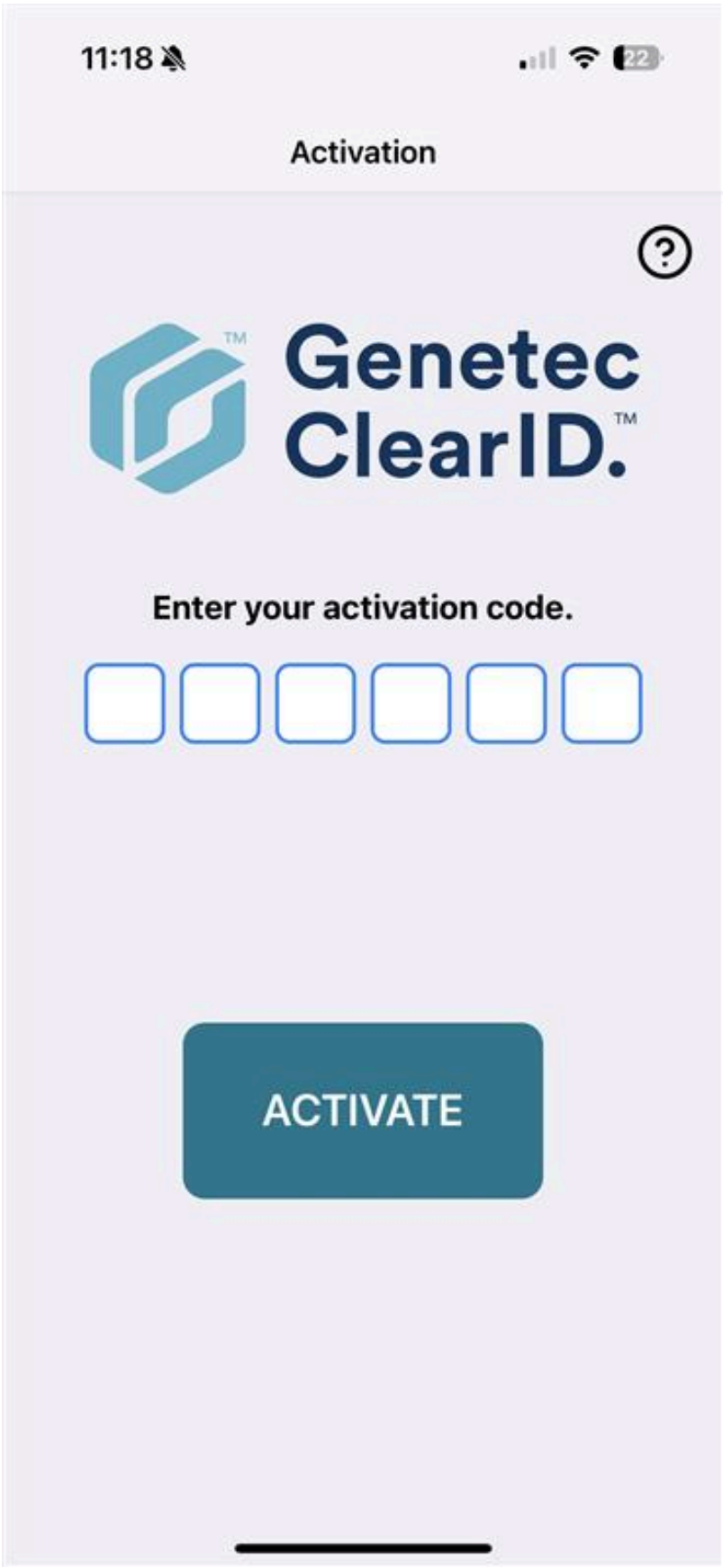
4 Activez votre iPhone dans ClearID :
   a) Sélectionnez votre iPhone sur le liste des appareils.
   b) Dans le champ **Statut** , cliquez sur **Générer le code d'activation**.



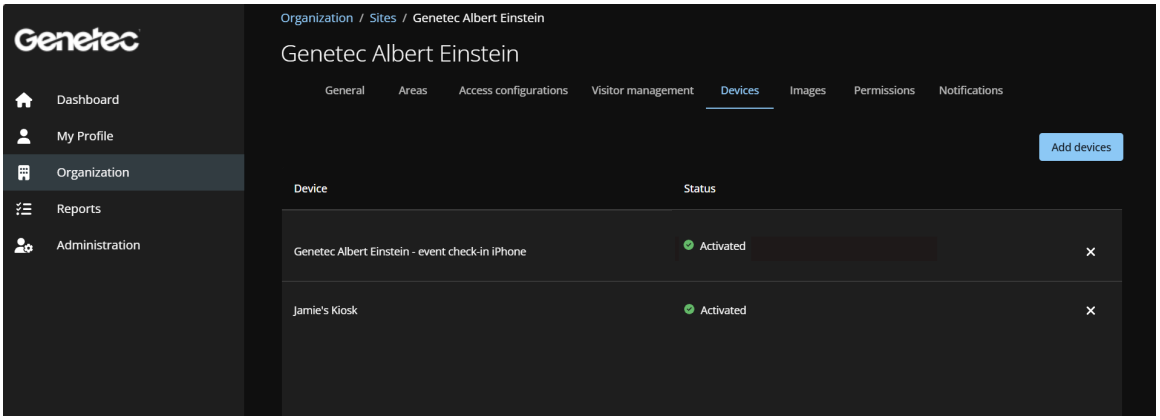
   c) Notez le code d'activation pour plus tard.
   d) (Facultatif) Copiez-le dans le presse-papier.

      CONSEIL : Utilisez **Copier dans le presse-papiers** si la personne qui enregistre l'appareil d'enregistrement par opérateur mobile ClearID dans le portail ClearID n'est pas celle qui active l'appareil. Une fois que le code est dans le presse-papier, il peut être envoyé par e-mail à la personne qui active l'appareil.
   e) Cliquez sur **OK**.

5 Dans l’application iPhone ClearID Self-Service Kiosk, saisissez le code d'activation de votre appareil et appuyez sur **Activer**.


11:18
Activation
Genetec ClearID.™
Enter your activation code.
ACTIVATE

Votre iPhone est désormais activé dans ClearID et prêt à être utilisé en tant qu'appareil d'enregistrement par opérateur mobile.



Configurer l'imprimante d'étiquettes de la borne en libre-service (Brother QL-820NWBc, QL-820NWB ou QL-810W)

Avant que les visiteurs puissent utiliser Genetec ClearID[MC] Self-Service Kiosk pour s'inscrire, vous devez configurer l'imprimante pour pouvoir imprimer les étiquettes au cours du processus d'inscription.

Avant de commencer

Familiarisez-vous avec ce qui suit :

- Guide de configuration rapide Brother QL810W/820NWB (en anglais)
- Guide de l'utilisateur Brother QL-810W/QL-820NWB (en anglais)
- Témoins LED de l'imprimante Brother QL-820NWB

REMARQUE : L'imprimante Brother QL-820NWBc remplace l'imprimante Brother QL-820NWB qui n'est plus commercialisée. Pour en savoir plus sur les différences, voir Nouvelles spécifications Brother QL-820NWBc.

À savoir

BONNE PRATIQUE : N'utilisez qu'une seule imprimante d'étiquettes par borne, et jumelez l'imprimante avec la borne via Bluetooth.

Si vous souhaitez utiliser une imprimante d'étiquettes avec plusieurs bornes ou loin des bornes, utilisez une connexion Wi-Fi ou Ethernet. Par exemple, deux bornes à l'entrée et une imprimante d'étiquettes à l'accueil.

REMARQUE : Une batterie Li-ion rechargeable peut être achetée et utilisée lorsqu'un branchement sur secteur est indisponible.

Procédure

- Choisissez l'une des options suivantes :
  - Configurer le mode Bluetooth (Brother QL-820NWBc ou QL-820NWB)
  - Configurer le mode Wi-Fi (Brother QL-820NWBc, QL-820NWB ou QL-810W)
  - Configurer le mode Ethernet (Brother QL-820NWBc ou QL-820NWB)

Lorsque vous avez terminé

De temps à autre, vous devrez commander des fournitures, remplacer la pile bouton, recharger la batterie (si vous en utilisez une) ou encore nettoyer l'imprimante d'étiquettes.

Pour en savoir plus, voir le *Guide de configuration rapide Brother QL-810W/QL-820NWB* et le *Guide de l'utilisateur Brother QL-810W/QL-820NWB* .

Rubriques connexes

FAQ sur l'imprimante d'étiquettes Brother QL-820NWB

Fournitures pour l'imprimante Brother QL-820NWB

Appareils pris en charge, page 78
Options de la borne en libre-service, page 635

Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Bluetooth (Brother 820NWBc ou QL-820NWB)

Avant que les visiteurs puissent utiliser Genetec ClearID[MC] Self-Service Kiosk pour s'inscrire, vous devez configurer l'imprimante pour pouvoir imprimer les étiquettes au cours du processus d'inscription.

Avant de commencer

Familiarisez-vous avec ce qui suit :

- Guide de configuration rapide Brother QL810W/820NWB (en anglais)
- Guide de l'utilisateur Brother QL-810W/QL-820NWB (en anglais)
- Témoins LED de l'imprimante Brother QL-820NWB

REMARQUE : L'imprimante Brother QL-820NWBc remplace l'imprimante Brother QL-820NWB qui n'est plus commercialisée. Pour en savoir plus sur les différences, voir Nouvelles spécifications Brother QL-820NWBc.

À savoir

Pour utiliser l'imprimante d'étiquettes Brother QL-820NWBc ou QL-820NWB en mode Bluetooth, tenez compte des points suivants :

- Une imprimante d'étiquettes peut être jumelée à une seule borne.
- L'imprimante doit être à moins de 10 mètres de la borne.

REMARQUE : Une batterie Li-ion rechargeable peut être achetée et utilisée lorsqu'un branchement sur secteur est indisponible.

Procédure

1 Branchez l'adaptateur secteur de l'imprimante dans une prise de courant et connectez le câble d'alimentation à l'imprimante d'étiquettes.

Illustration 16 : Imprimante d'étiquettes Brother QL-820NWBc (arrière)

Illustration 17 : Imprimante d'étiquettes Brother QL-820NWB (arrière)

2 Appuyez sur le bouton d'**alimentation** pour allumer l'imprimante.

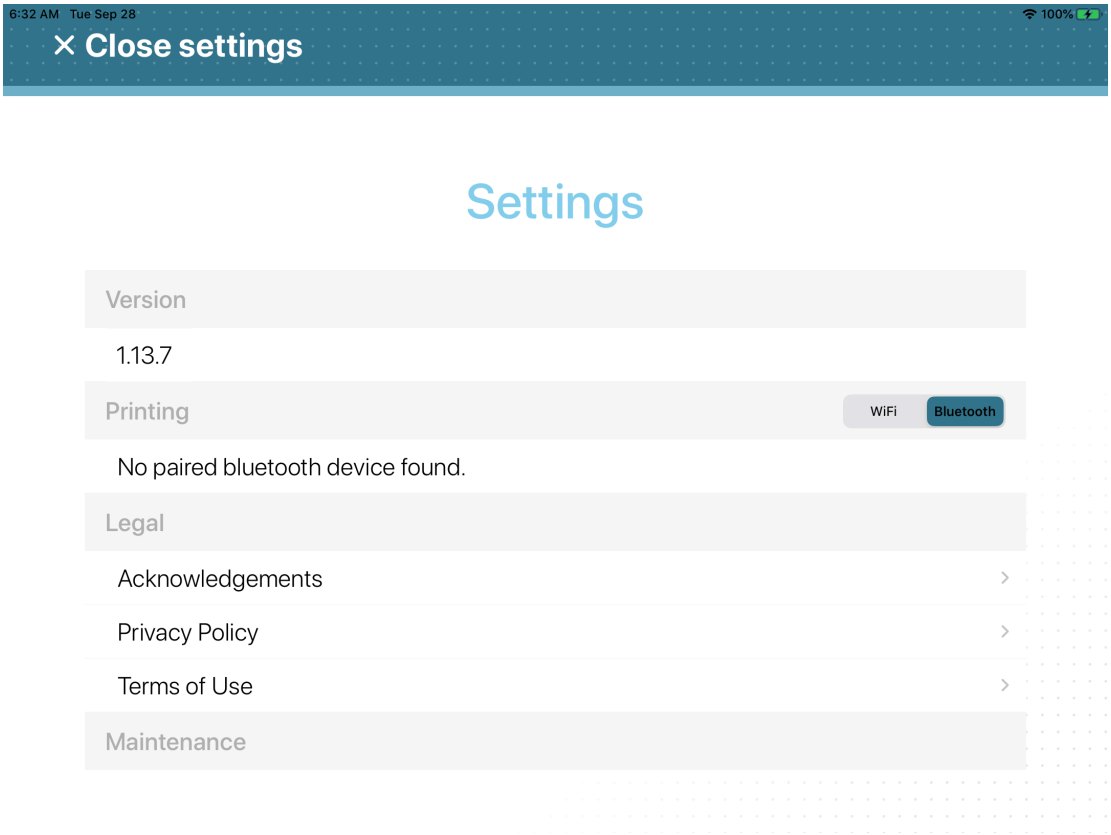
3 (Facultatif) Si vous voyez le menu **Mode modèle** avec la mauvaise taille d'étiquette, désactivez-le.

a) Appuyez sur **Menu**, allez dans **Template Settings** et désactivez le réglage **Template Mode**.

4 Utilisez les touches fléchées pour parcourir le menu de l'imprimante.

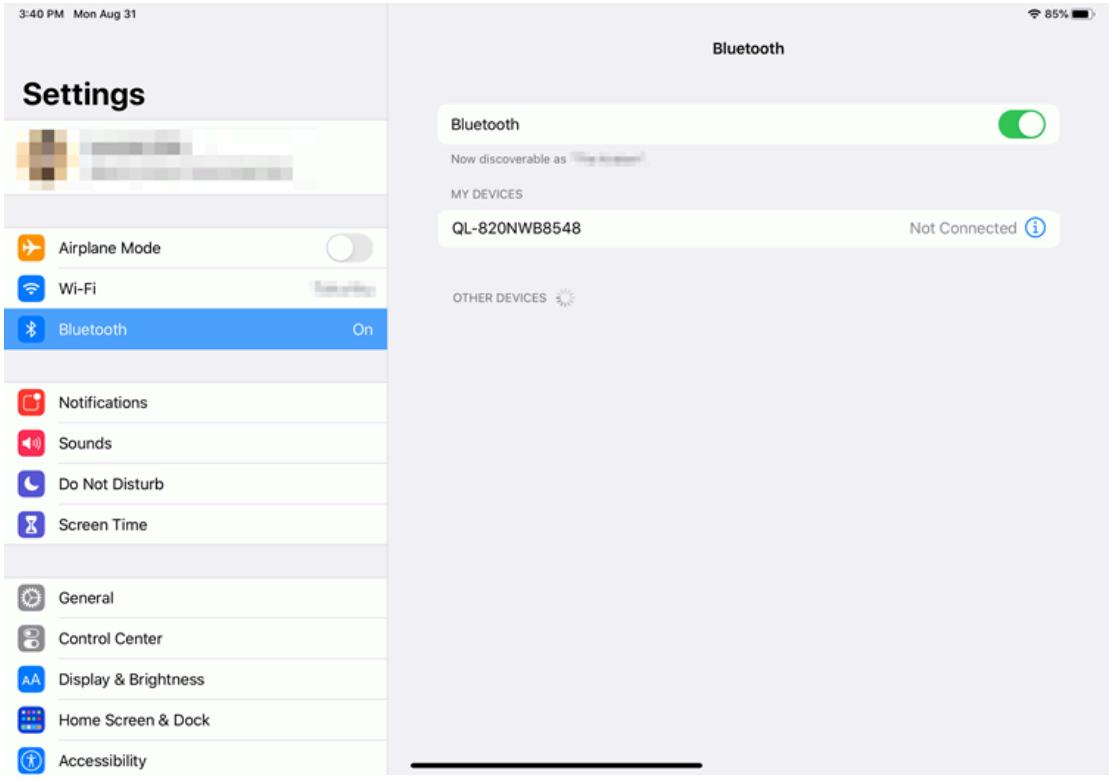
a) Sélectionnez **Bluetooth** > **Bluetooth (On/Off)** > **On** dans le menu des réglages, et appuyez sur **OK**.
b) Sélectionnez **Bluetooth** > **Automatic Reconnection (On/Off)** > **On** dans le menu des réglages, et appuyez sur **OK**.

5 Jumelez votre imprimante d'étiquettes Bluetooth avec votre borne ClearID Self-Service Kiosk.
a) Dans l'application mobile Self-Service Kiosk, touchez **Réglages** ( ).
b) Dans la section *Impression*, activez le bouton **Bluetooth**.



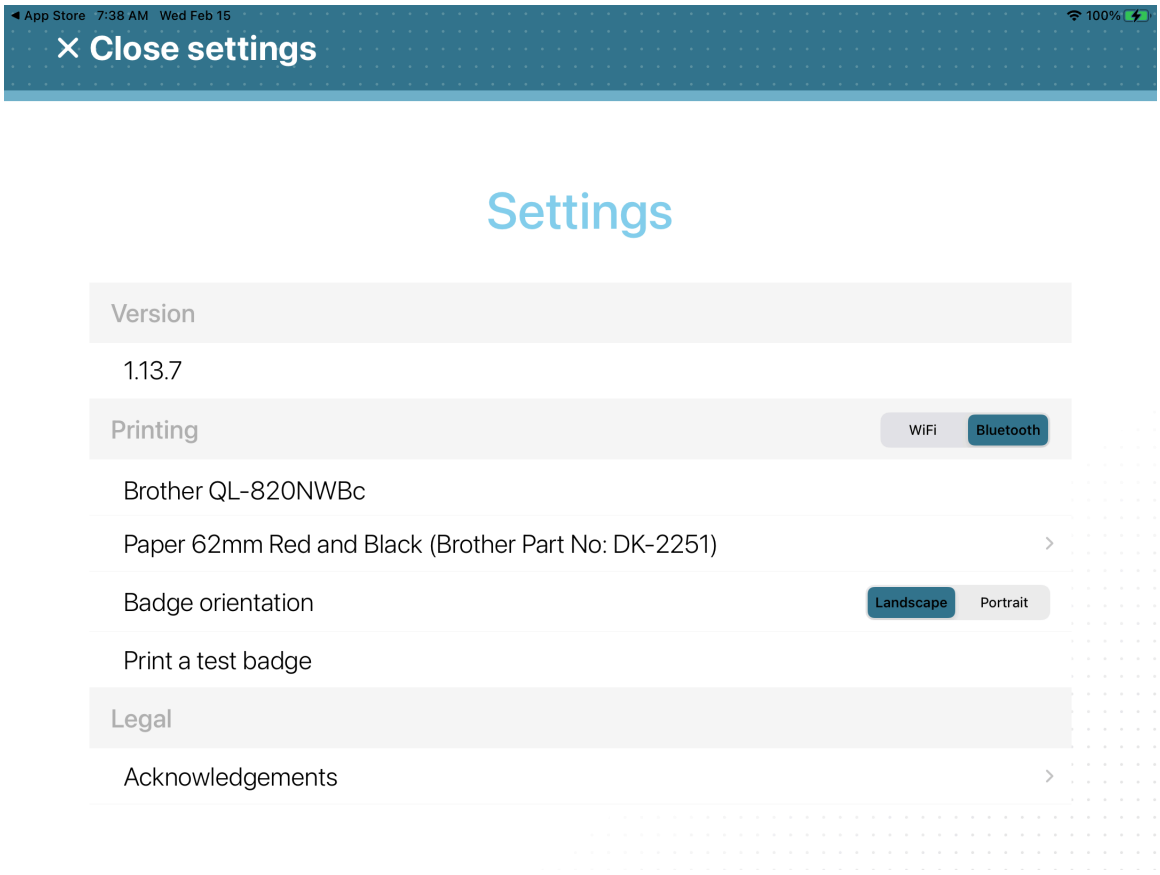
6 Sur votre iPad, accédez à l'icône **Paramètres** Apple, appuyez sur **Paramètres** > **Bluetooth**.

a) (Facultatif) Si **Bluetooth** est désactivé, touchez le commutateur pour activer le Bluetooth.



b) Sélectionnez la bonne imprimante pour associer l'iPad de ClearID Self-Service Kiosk avec votre imprimante.

7 Dans l'application mobile Self-Service Kiosk, touchez **Réglages** ( ).



a) Dans la section *Impression*, vérifiez que votre imprimante Brother QL-820NWBc ou QL-820NWB est affichée.

CONSEIL : Si l'imprimante ne s'affiche pas ou si Bluetooth n'est pas sélectionné, appuyez sur **WiFi**, puis sur **Bluetooth** pour déclencher à nouveau la détection.

Lorsque vous avez terminé

(Facultatif) Imprimez un badge de test.

Rubriques connexes

Ports de pare-feu, page 76

Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Wi-Fi (Brother 820NWBc, QL-820NWB ou QL-810W)

Avant que les visiteurs puissent utiliser Genetec ClearID^{MC} Self-Service Kiosk pour s'inscrire, vous devez configurer l'imprimante pour pouvoir imprimer les étiquettes au cours du processus d'inscription.

Avant de commencer

Familiarisez-vous avec ce qui suit :

- Guide de configuration rapide Brother QL810W/820NWB (en anglais)
- Guide de l’utilisateur Brother QL-810W/QL-820NWB (en anglais)
- Témoins LED de l’imprimante Brother QL-820NWB

REMARQUE : L'imprimante Brother QL-820NWBc remplace l'imprimante Brother QL-820NWB qui n’est plus commercialisée. Pour en savoir plus sur les différences, voir Nouvelles spécifications Brother QL-820NWBc.

À savoir

- Une imprimante d’étiquettes peut être associée à cinq bornes en libre-service.
- L'imprimante doit se trouver sur le même réseau Wi-Fi que l’iPad utilisé pour Genetec ClearID^{MC} Self-Service Kiosk.

  Le réseau Wi-Fi doit être activé et prendre en charge les éléments suivants :

  - Bonjour, requis pour la découverte d'appareils.
  - SNMP, requis pour obtenir l’état de l’imprimante.
  - Port UDP ou TCP 9100, requis pour envoyer les données d'impression.

REMARQUE : Une batterie Li-ion rechargeable peut être achetée et utilisée lorsqu'un branchement sur secteur est indisponible.

Procédure

1 Branchez l'adaptateur secteur de l'imprimante dans une prise de courant et connectez le câble d'alimentation à l'imprimante d'étiquettes.

Illustration 18 : Imprimante d'étiquettes Brother QL-820NWBc (arrière)

Illustration 19 : Imprimante d'étiquettes Brother QL-820NWB (arrière)

2 Appuyez sur le bouton d’**alimentation** pour allumer l’imprimante.

3 (Facultatif) Si vous voyez le menu **Mode modèle** avec la mauvaise taille d'étiquette, désactivez-le.

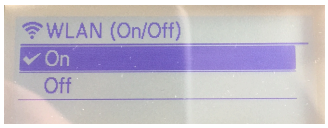
a) Appuyez sur **Menu**, allez dans **Template Settings** et désactivez le réglage **Template Mode**.

4 Appuyez sur la touche **Menu**.

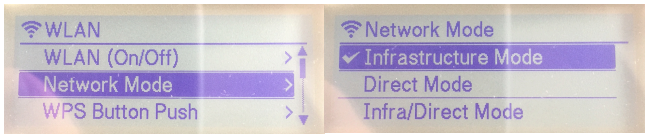
5 Utilisez les touches fléchées pour parcourir le menu de l'imprimante.

6 Faites défiler le menu jusqu'aux paramètres **WLAN (5/7)** et appuyez sur **OK**.

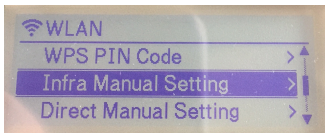
a) Sélectionnez WLAN **On** et appuyez sur **OK** .



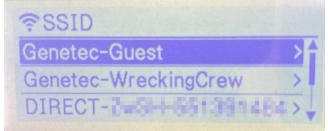
b) Dans le menu *Network Mode*, sélectionnez **Infrastructure Mode** et appuyez sur **OK**.



7 Faites défiler le menu jusqu'à **Infra Manual Setting** et appuyez sur **OK**.



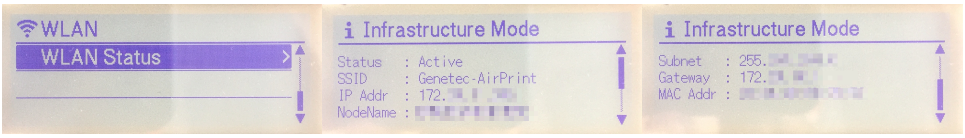
a) Lorsque la recherche est terminée, parcourez la liste des SSID (Service Set Identifier), sélectionnez votre réseau Wi-Fi et appuyez sur **OK**.



REMARQUE : Il s'agit généralement d'un réseau Wi-Fi avec AirPrint.

b) Lorsque vous y êtes invité, entrez le mot de passe Wi-Fi.

8 Accédez à **État WLAN** et appuyez sur **OK** pour vérifier l'état et l'adresse IP de votre réseau Wi-Fi.



CONSEIL : Notez le **SSID** (réseau Wi-Fi) et l'**adresse IP** (l'adresse IP de l'imprimante) pour référence ultérieure.

- Le SSID sert à vérifier que vous êtes sur le même réseau Wi-Fi que l'iPad utilisé pour ClearID Self-Service Kiosk.
- L'adresse IP servira ensuite à vérifier que vous avez sélectionné la bonne imprimante d'étiquettes.

9 Sélectionnez votre imprimante d'étiquettes Wi-Fi.

Lorsque vous avez terminé

(Facultatif) Imprimez un badge de test.

Rubriques connexes

Ports de pare-feu, page 76

Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Ethernet (Brother 820NWBc ou QL-820NWB)

Avant que les visiteurs puissent utiliser Genetec ClearID^{MC} Self-Service Kiosk pour s'inscrire, vous devez configurer l'imprimante pour pouvoir imprimer les étiquettes au cours du processus d'inscription.

Avant de commencer

Familiarisez-vous avec ce qui suit :

- Guide de configuration rapide Brother QL810W/820NWB (en anglais)
- Guide de l'utilisateur Brother QL-810W/QL-820NWB (en anglais)
- Témoins LED de l'imprimante Brother QL-820NWB

REMARQUE : L'imprimante Brother QL-820NWBc remplace l'imprimante Brother QL-820NWB qui n'est plus commercialisée. Pour en savoir plus sur les différences, voir Nouvelles spécifications Brother QL-820NWBc.

À savoir

- Une imprimante d'étiquettes peut être associée à cinq bornes en libre-service.

REMARQUE : Une batterie Li-ion rechargeable peut être achetée et utilisée lorsqu'un branchement sur secteur est indisponible.

Procédure

1 Branchez l'adaptateur secteur de l'imprimante dans une prise de courant et connectez le câble d'alimentation à l'imprimante d'étiquettes.

Illustration 20 : Imprimante d'étiquettes Brother QL-820NWBc (arrière)

Illustration 21 : Imprimante d'étiquettes Brother QL-820NWB (arrière)

2 Vérifiez que l'imprimante est **ÉTEINTE** avant de connecter le câble réseau.

Illustration 22 : Imprimante d'étiquettes Brother QL-820NWBc (arrière)

Illustration 23 : Imprimante d'étiquettes Brother QL-820NWB (arrière)

a) Raccordez un câble réseau au port LAN à l'arrière de l'imprimante.

CONSEIL : Utilisez un câble droit à paires torsadées Category 5 (ou supérieur) pour un réseau Fast Ethernet 100BASE-T ou 10BASE-TX.

3 Appuyez sur le bouton d'**alimentation** pour allumer l'imprimante.

4 (Facultatif) Si vous voyez le menu **Mode modèle** avec la mauvaise taille d'étiquette, désactivez-le.

a) Appuyez sur **Menu**, allez dans **Template Settings** et désactivez le réglage **Template Mode**.

5 Sélectionnez votre imprimante d'étiquettes (Ethernet).

Lorsque vous avez terminé

(Facultatif) Imprimez un badge de test.

Rubriques connexes

Ports de pare-feu, page 76

Configurer l'imprimante d'étiquettes de la borne en libre-service (Brother TD-4550DNWB)

Avant que les visiteurs puissent utiliser Genetec ClearID[MC] Self-Service Kiosk pour s'inscrire, vous devez configurer l'imprimante Brother TD-4550DNWB pour pouvoir imprimer les étiquettes au cours du processus d'inscription.

Avant de commencer

Familiarisez-vous avec ce qui suit :

- Guide de configuration rapide Brother TD-4550DNWB
- Guide de l'utilisateur Brother TD-4550DNWB User Guide
- Guide de l'utilisateur Brother TD-4550DNWB en ligne
- États des témoins LED de l'imprimante Brother TD-4550DNWB

À savoir

BONNE PRATIQUE : N'utilisez qu'une seule imprimante d'étiquettes par borne, et jumelez l'imprimante avec la borne via Bluetooth.
Si vous souhaitez utiliser une imprimante d'étiquettes avec plusieurs bornes ou loin des bornes, utilisez une connexion Wi-Fi ou Ethernet. Par exemple, deux bornes à l'entrée et une imprimante d'étiquettes à l'accueil.

Procédure

- Choisissez l'une des options suivantes :
  - Configurer le mode Bluetooth (Brother TD-4550DNWB)
  - Configurer le mode Wi-Fi (Brother TD-4550DNWB)
  - Configurer le mode Ethernet (Brother TD-4550DNWB)

Lorsque vous avez terminé

De temps à autre, vous devrez commander des fournitures, remplacer la pile bouton ou nettoyer l'imprimante d'étiquettes.

Pour en savoir plus, voir le *Guide de configuration rapide Brother TD-4550DNWB* et le *Guide de l'utilisateur Brother TD-4550DNWB*.

Rubriques connexes

FAQ sur l'imprimante d'étiquettes Brother TD-4550DNWB

Fournitures pour l'imprimante Brother TD-4550DNWB

Appareils pris en charge, page 78

Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Bluetooth (Brother TD-4550DNWB)

Avant que les visiteurs puissent utiliser Genetec ClearID[MC] Self-Service Kiosk pour s'inscrire, vous devez configurer l'imprimante pour pouvoir imprimer les étiquettes au cours du processus d'inscription.

Avant de commencer

Familiarisez-vous avec ce qui suit :

- Guide de configuration rapide Brother TD-4550DNWB
- Guide de l'utilisateur Brother TD-4550DNWB User Guide
- Guide de l'utilisateur Brother TD-4550DNWB en ligne
- États des témoins LED de l'imprimante Brother TD-4550DNWB

À savoir

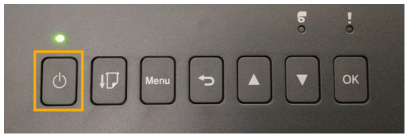
Pour utiliser l'imprimante d'étiquettes Brother TD-4550DNWB en mode Bluetooth, tenez compte des points suivants :

- Une imprimante d'étiquettes peut être jumelée à une seule borne.
- L'imprimante doit être à moins de 10 mètres de la borne.

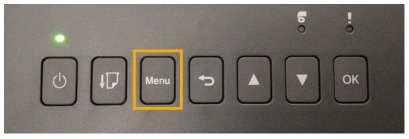
Procédure

1 Branchez l'adaptateur secteur de l'imprimante dans une prise de courant et connectez le câble d'alimentation à l'imprimante d'étiquettes.

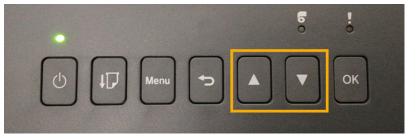
2 Appuyez sur le bouton d'**alimentation** pour allumer l'imprimante.



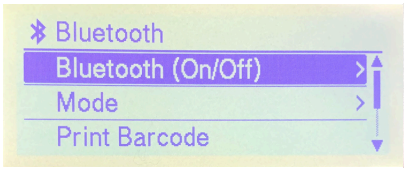
3 Appuyez sur la touche **Menu**.

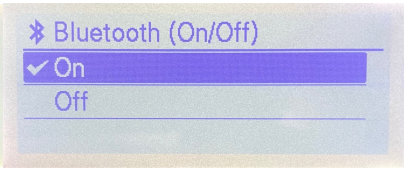


4 Utilisez les touches fléchées pour parcourir le menu de l'imprimante.

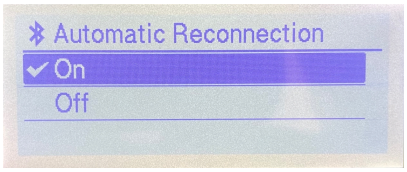


a) Sélectionnez **BLUETOOTH** > **BLUETOOTH (Activé/Désactivé)** > **Activé** dans le menu des paramètres et appuyez sur **OK**.





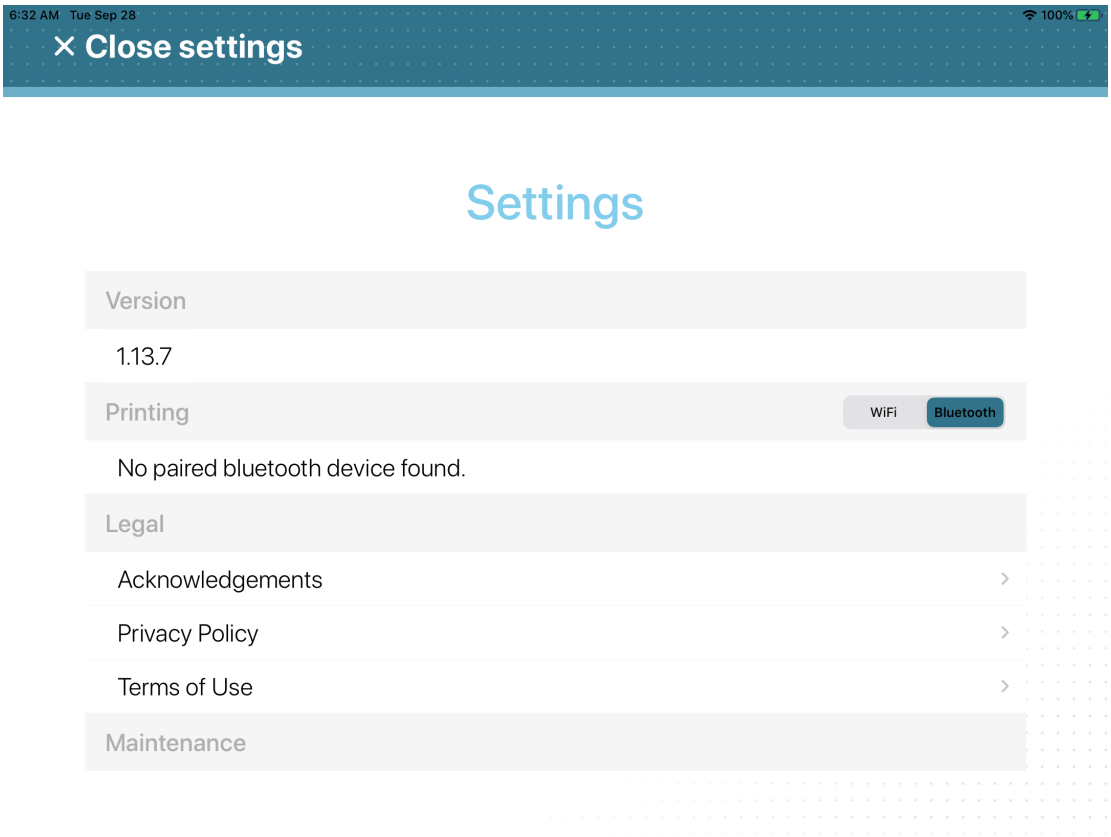
b) Sélectionnez **BLUETOOTH** > **Reconnexion automatique (Activé/Désactivé)** > **Activé** dans le menu des paramètres et appuyez sur **OK**.



5 Jumelez votre imprimante d'étiquettes Bluetooth avec votre borne ClearID Self-Service Kiosk.

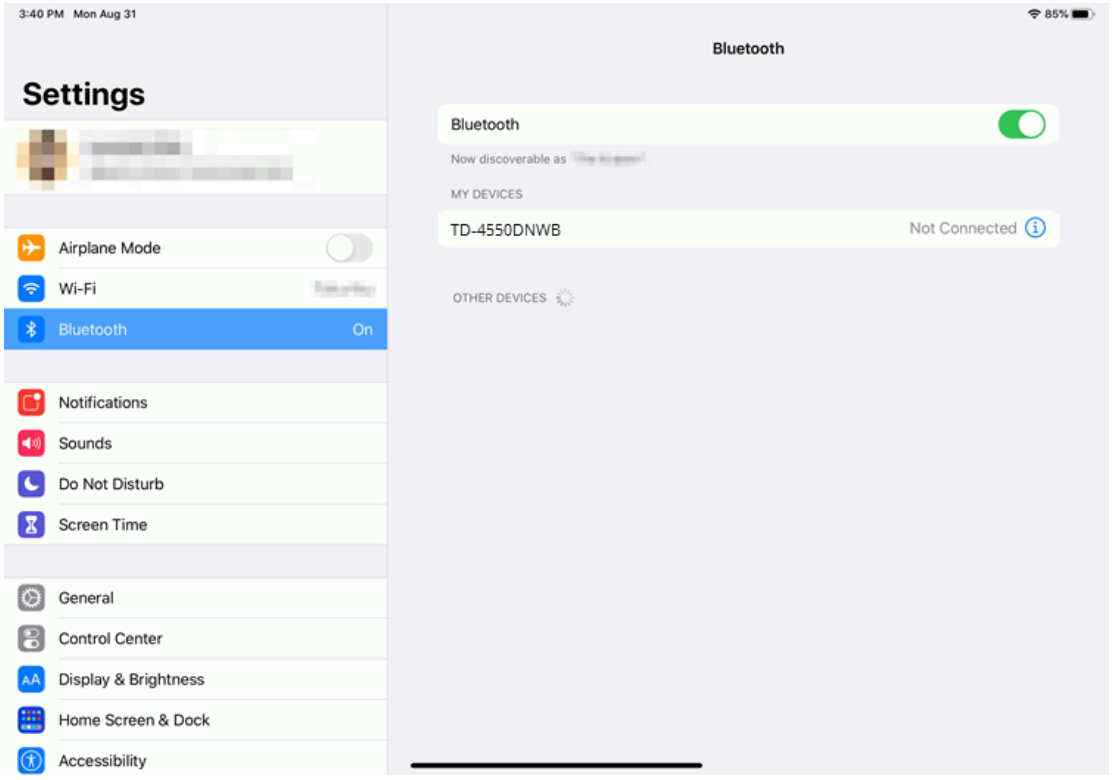
a) Dans l'application mobile Self-Service Kiosk, touchez **Réglages** ( ).

b) Dans la section *Impression*, activez le bouton **Bluetooth**.



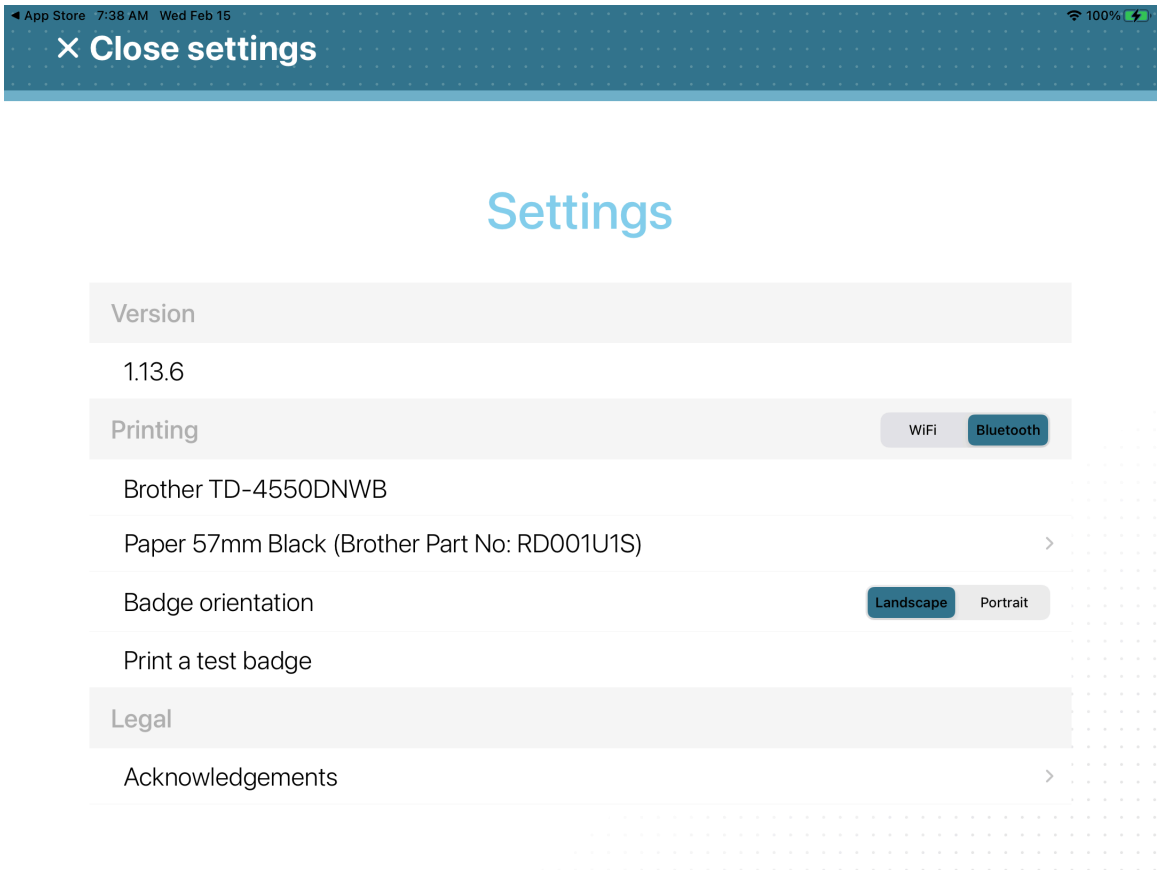
6 Sur votre iPad, accédez à l'icône **Paramètres** Apple, appuyez sur **Paramètres** > **Bluetooth**.

a) (Facultatif) Si **Bluetooth** est désactivé, touchez le commutateur pour activer le Bluetooth.



b) Sélectionnez la bonne imprimante pour associer l'iPad de ClearID Self-Service Kiosk avec votre imprimante.

7 Dans l'application mobile Self-Service Kiosk, touchez **Réglages** ( ).



a) Dans la section *Impression*, vérifiez que votre imprimante Brother TD-4550DNWB est affichée.
CONSEIL : Si l'imprimante ne s'affiche pas ou si Bluetooth n'est pas sélectionné, appuyez sur **WiFi**, puis sur **Bluetooth** pour déclencher à nouveau la détection.

Lorsque vous avez terminé

(Facultatif) Imprimez un badge de test.

Rubriques connexes

Ports de pare-feu, page 76

Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Wi-Fi (Brother TD-4550DNWB)

Avant que les visiteurs puissent utiliser Genetec ClearID^{MC} Self-Service Kiosk pour s'inscrire, vous devez configurer l'imprimante pour pouvoir imprimer les étiquettes au cours du processus d'inscription.

Avant de commencer

Familiarisez-vous avec ce qui suit :

- Guide de configuration rapide Brother TD-4550DNWB
- Guide de l'utilisateur Brother TD-4550DNWB User Guide
- Guide de l'utilisateur Brother TD-4550DNWB en ligne
- États des témoins LED de l'imprimante Brother TD-4550DNWB

À savoir

- Une imprimante d'étiquettes peut être associée à cinq bornes en libre-service.
- L'imprimante doit se trouver sur le même réseau Wi-Fi que l'iPad utilisé pour Genetec ClearID[MC] Self-Service Kiosk.

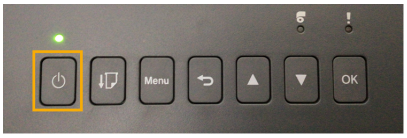
  Le réseau Wi-Fi doit être activé et prendre en charge les éléments suivants :

  - Bonjour, requis pour la découverte d'appareils.
  - SNMP, requis pour obtenir l'état de l'imprimante.
  - Port UDP ou TCP 9100, requis pour envoyer les données d'impression.

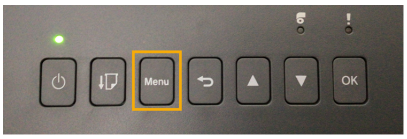
Procédure

1 Branchez l'adaptateur secteur de l'imprimante dans une prise de courant et connectez le câble d'alimentation à l'imprimante d'étiquettes.

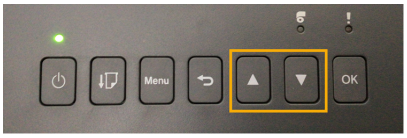
2 Appuyez sur le bouton d'**alimentation** pour allumer l'imprimante.



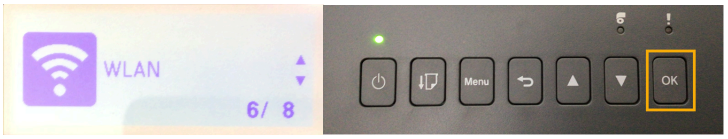
3 Appuyez sur la touche **Menu**.



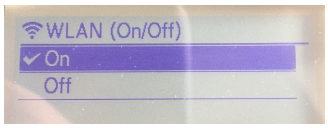
4 Utilisez les touches fléchées pour parcourir le menu de l'imprimante.



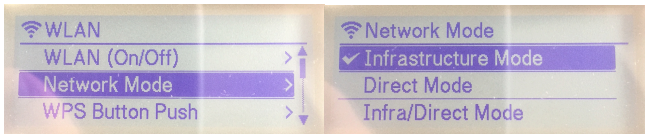
5 Faites défiler le menu jusqu'aux paramètres **WLAN (6/8)** et appuyez sur **OK**.



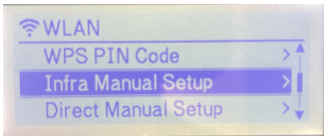
a) Sélectionnez WLAN **WLAN (On/Off)** > **On** et appuyez sur **OK** .



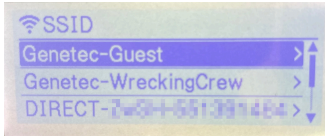
b) Dans le menu *Network Mode*, sélectionnez **Infrastructure Mode** et appuyez sur **OK**.



6 Faites défiler le menu jusqu'à **Infra Manual Setup** et appuyez sur **OK**.



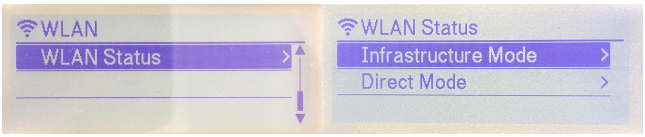
a) Lorsque la recherche est terminée, parcourez la liste des SSID (Service Set Identifier), sélectionnez votre réseau Wi-Fi et appuyez sur **OK**.

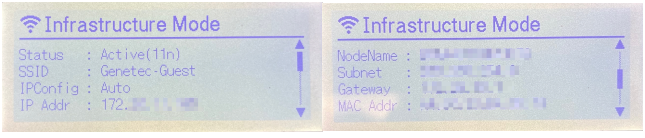


REMARQUE : Il s'agit généralement d'un réseau Wi-Fi avec AirPrint.

b) Lorsque vous y êtes invité, entrez le mot de passe Wi-Fi.

7 Naviguez jusqu'à **WLAN Status** > **Infrastructure Mode** et appuyez sur **OK** pour vérifier l'état et l'adresse IP de votre réseau Wi-Fi.





CONSEIL : Notez le **SSID** (réseau Wi-Fi) et l'**adresse IP** (l'adresse IP de l'imprimante) pour référence ultérieure.

- Le SSID sert à vérifier que vous êtes sur le même réseau Wi-Fi que l'iPad utilisé pour ClearID Self-Service Kiosk.
- L'adresse IP servira ensuite à vérifier que vous avez sélectionné la bonne imprimante d'étiquettes.

8 Sélectionnez votre imprimante d'étiquettes (Wi-Fi).

Lorsque vous avez terminé

(Facultatif) Imprimez un badge de test.

Rubriques connexes

Ports de pare-feu, page 76

Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Ethernet (Brother TD-4550DNWB)

Avant que les visiteurs puissent utiliser Genetec ClearID[MC] Self-Service Kiosk pour s'inscrire, vous devez configurer l'imprimante pour pouvoir imprimer les étiquettes au cours du processus d'inscription.

Avant de commencer

Familiarisez-vous avec ce qui suit :

- Guide de configuration rapide Brother TD-4550DNWB
- Guide de l'utilisateur Brother TD-4550DNWB User Guide
- Guide de l'utilisateur Brother TD-4550DNWB en ligne
- États des témoins LED de l'imprimante Brother TD-4550DNWB

À savoir

- Une imprimante d'étiquettes peut être associée à cinq bornes en libre-service.

IMPORTANT : Ne connectez pas ce produit à une connexion réseau sujette à des surtensions.

Procédure

1 Branchez l'adaptateur secteur de l'imprimante dans une prise de courant et connectez le câble d'alimentation à l'imprimante d'étiquettes.

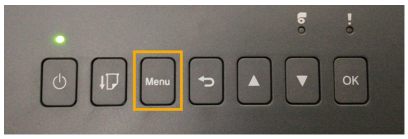
2 Vérifiez que l'imprimante est **ÉTEINTE** avant de connecter le câble réseau.

a) Raccordez un câble réseau au port LAN à l'arrière de l'imprimante.

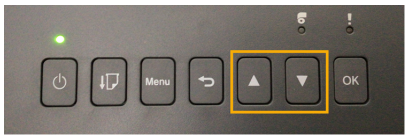
CONSEIL : Utilisez un câble droit à paires torsadées Category 5 (ou supérieur) pour un réseau Fast Ethernet 100BASE-T ou 10BASE-TX.

3 Appuyez sur le bouton d'**alimentation** pour allumer l'imprimante.

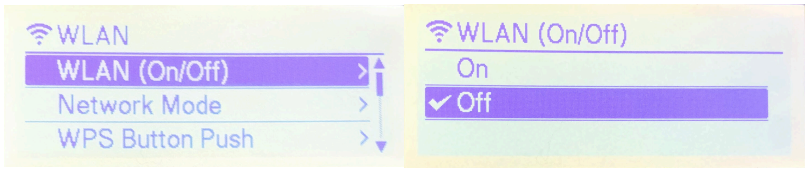
4 Appuyez sur la touche **Menu**.



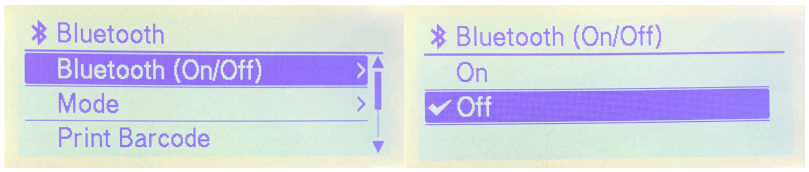
5 Utilisez les touches fléchées pour parcourir le menu de l'imprimante.



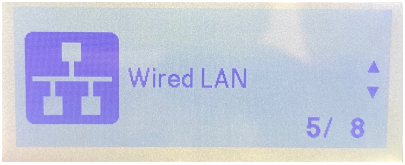
6 Dans le menu **Settings** (Réglages) de l'imprimante, réglez **WLAN** (Wi-Fi) sur OFF.



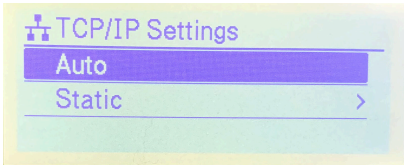
7 Dans le menu **Settings** (Réglages) de l'imprimante, réglez **Bluetooth** sur OFF.



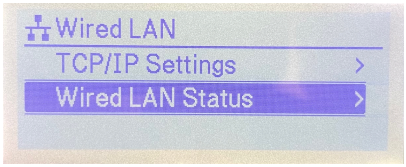
8 Faites défiler le menu jusqu'aux paramètres **LAN (5/8)** et appuyez sur **OK**.



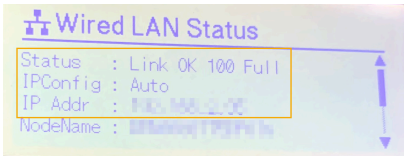
a) Cliquez sur **TCP/IP Settings** et sélectionnez **AUTO**.



b) Cliquez sur **Wired LAN Status** (État du réseau filaire) pour vérifier l'imprimante.



c) Vérifiez les options **Status**, **IPConfig** et **IP Addr** de la connexion.



CONSEIL : Notez l'adresse IP et les autres réglages qui vous serviront plus tard pour sélectionner l'imprimante.

9 Sélectionnez votre imprimante d'étiquettes (Ethernet).

Lorsque vous avez terminé

(Facultatif) Imprimez un badge de test.

Rubriques connexes

Ports de pare-feu, page 76

Sélectionner une imprimante d'étiquettes de borne en libre-service

Avant d'imprimer des badges de visiteurs sur la borne Genetec ClearID[MC] Self-Service Kiosk, vous devez sélectionner une imprimante d'étiquettes.

Avant de commencer

Procédez de l'une des manières suivantes :

- Configurez l'imprimante d'étiquettes Brother QL-820NWBc ou QL-820NWBc de votre borne.
- Configurez l'imprimante d'étiquettes Brother TD-4550DNWB de votre borne.

À savoir

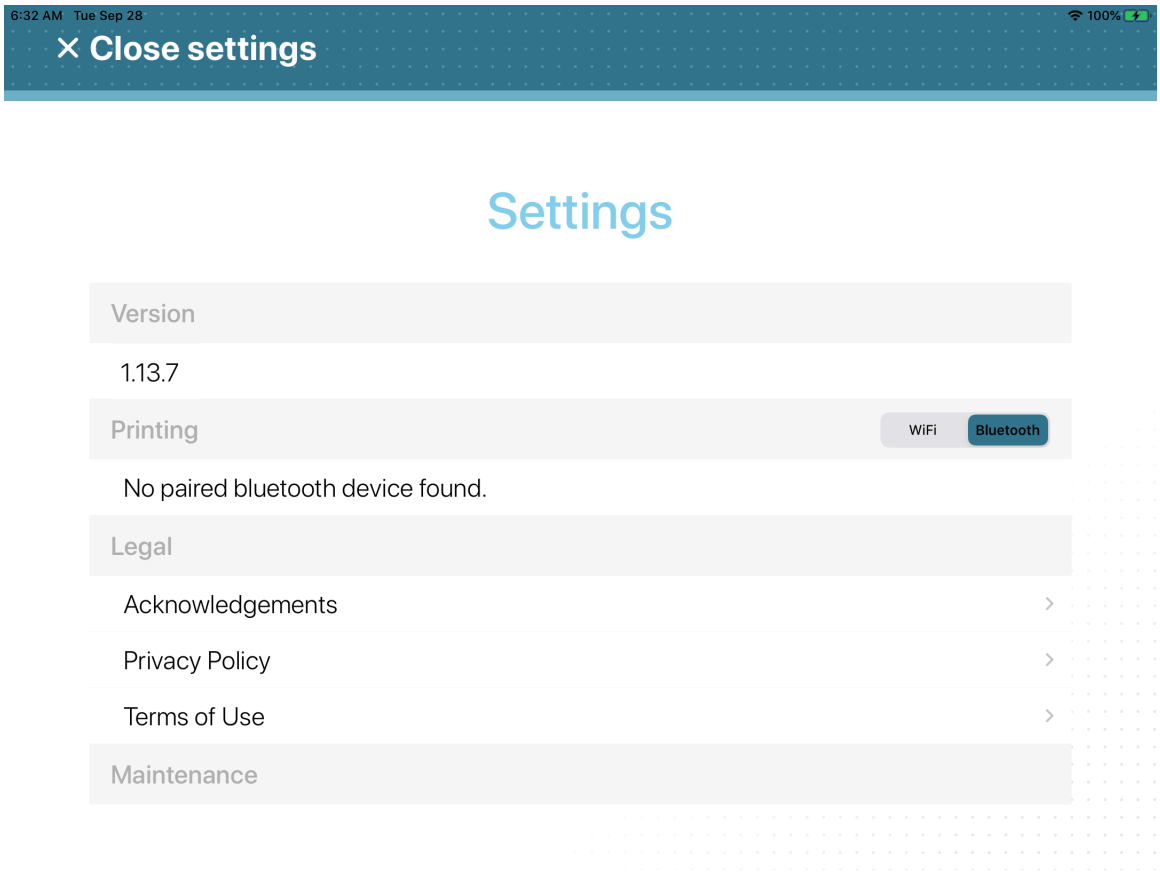
Wi-Fi ou Ethernet seulement : Vérifiez que vous disposez de l’adresse IP de l'imprimante afin de valider votre choix.

Procédure

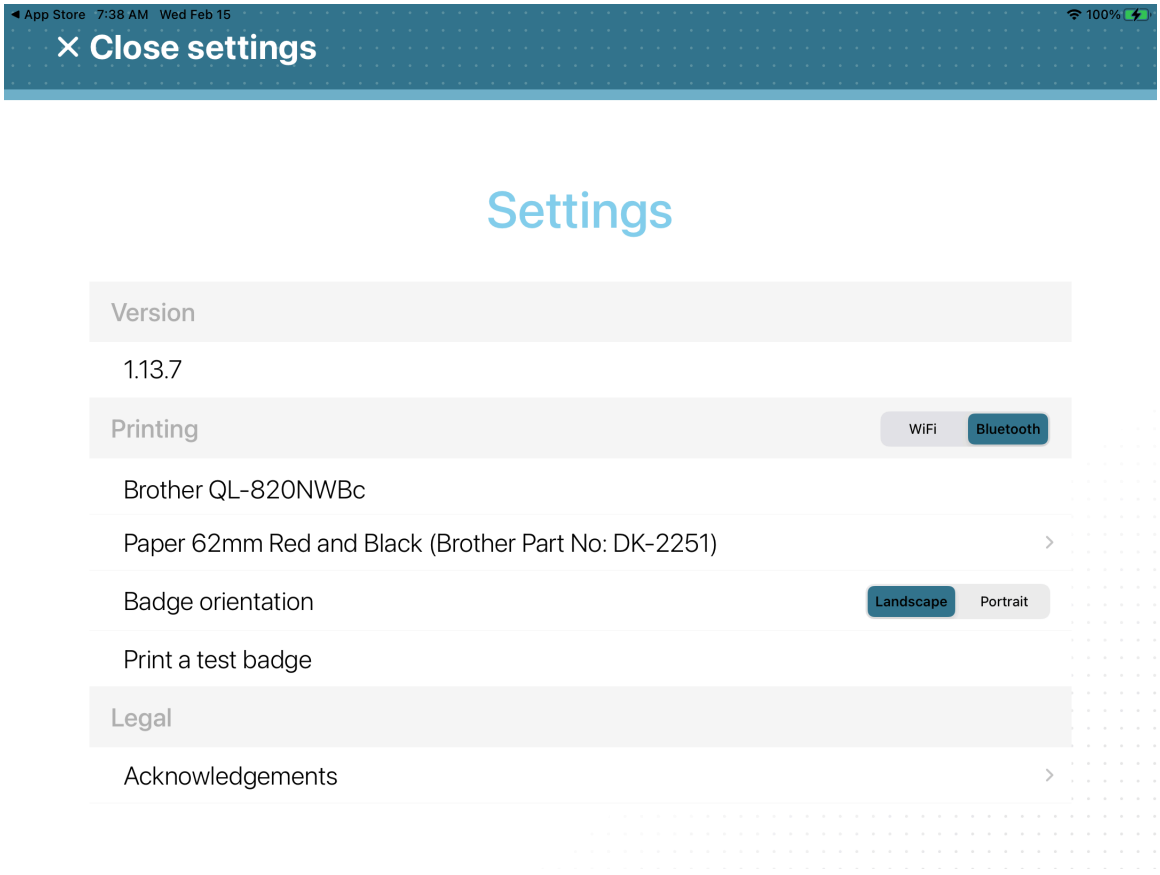
Pour sélectionner une imprimante d'étiquettes Bluetooth d'une borne en libre-service :

1 Dans l’application mobile Self-Service Kiosk, touchez **Réglages** ( ).

2 Sur la page **Réglages**, touchez **Bluetooth** pour sélectionner le mode d'impression.
a) Le cas échéant, authentifiez-vous.



3 Si vous avez sélectionné **Bluetooth**, l'imprimante sélectionnée doit apparaître dans la section **Impression**.



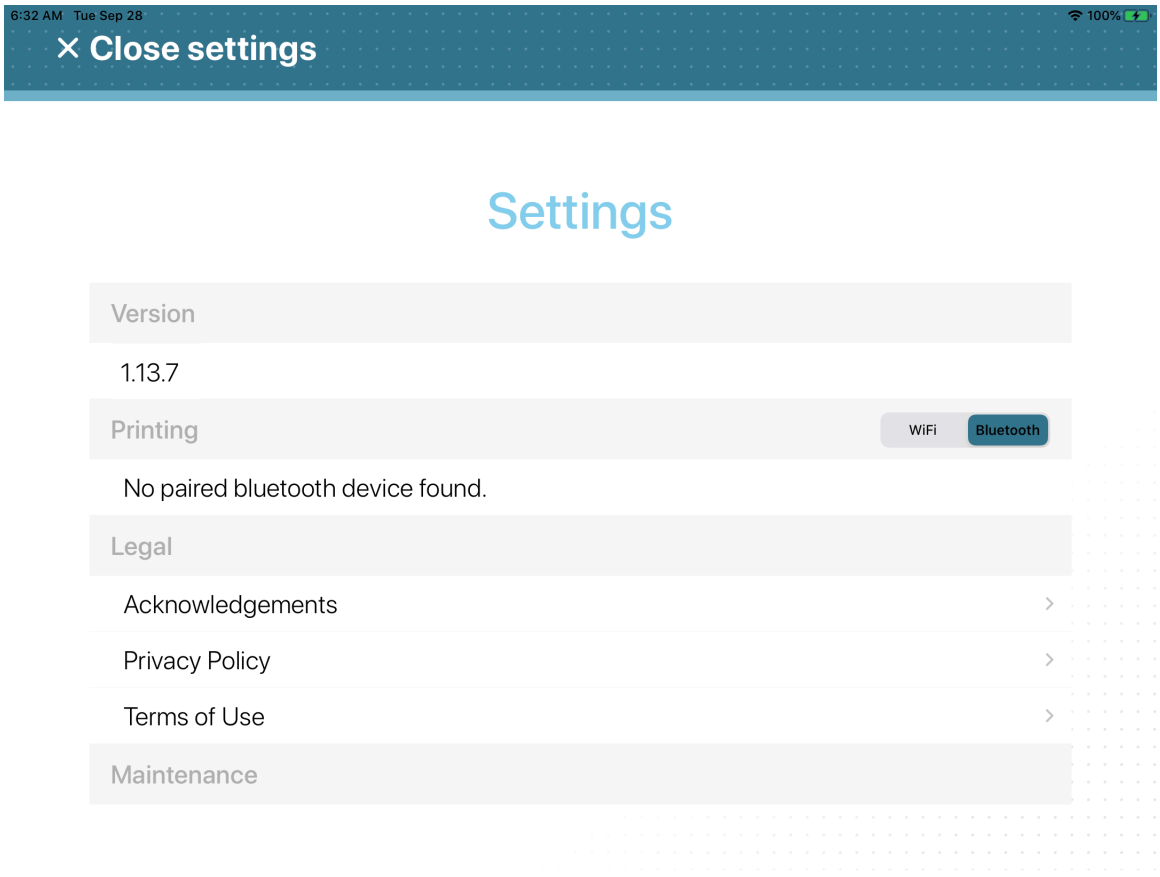
CONSEIL : Mode Bluetooth : Si l'imprimante ne s'affiche pas ou si Bluetooth n'est pas sélectionné, appuyez sur **WiFi**, puis sur **Bluetooth** pour déclencher à nouveau la détection.

4 Touchez **Fermer les réglages** pour terminer le processus de sélection d'imprimante.

Pour sélectionner une imprimante d'étiquettes Wi-Fi d'une borne en libre-service :

1 Dans l'application mobile Self-Service Kiosk, touchez **Réglages** ( ).

2 Sur la page **Réglages**, touchez **Wi-Fi** pour sélectionner le mode d'impression.
a) Le cas échéant, authentifiez-vous.



3 Choisissez l'une des options suivantes :

- **Détecter l'imprimante WiFi**
- **Définir l'imprimante manuellement (adresse IP)**

a) Si vous avez sélectionné **Détecter l'imprimante Wi-Fi**, patientez jusqu'à ce que la liste des **Imprimantes** s'affiche, puis sélectionnez votre imprimante.

Vérifiez que l'adresse IP de l'imprimante sélectionnée correspond à l'adresse notée lors de la configuration de l'imprimante.

CONSEIL : Mode Wi-Fi : si l'imprimante ne s'affiche pas ou si le Wi-Fi n'est pas sélectionné, appuyez sur **Bluetooth**, puis sur **WiFi** pour déclencher à nouveau la détection.

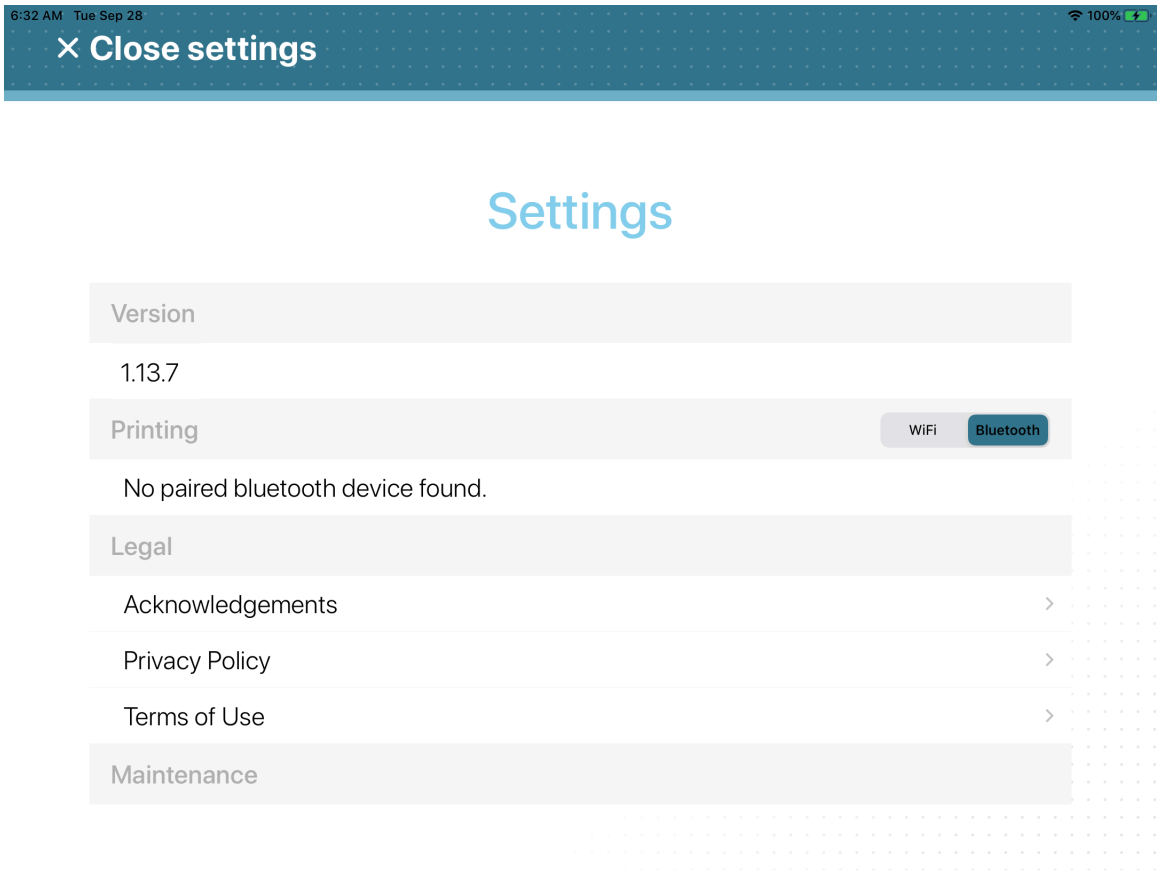
b) Si vous avez sélectionné **Définir l'imprimante manuellement (adresse IP)**, entrez l'adresse IP de l'imprimante et touchez **Enregistrer**.

4 Touchez **Fermer les réglages** pour terminer le processus de sélection d'imprimante.

Pour sélectionner une imprimante d'étiquettes Ethernet d'une borne en libre-service :

1 Dans l'application mobile Self-Service Kiosk, touchez **Réglages** ( ).

2 Sur la page **Réglages**, touchez **Wi-Fi** pour sélectionner le mode d'impression.
a) Le cas échéant, authentifiez-vous.



3 Choisissez l'une des options suivantes :

- **Détecter l'imprimante WiFi**
- **Définir l'imprimante manuellement (adresse IP)**

a) Si vous avez sélectionné **Détecter l'imprimante Wi-Fi**, patientez jusqu'à ce que la liste des **Imprimantes** s'affiche, puis sélectionnez votre imprimante.

Vérifiez que l'adresse IP de l'imprimante sélectionnée correspond à l'adresse notée lors de la configuration de l'imprimante.

CONSEIL : Mode Wi-Fi : si l'imprimante ne s'affiche pas ou si le Wi-Fi n'est pas sélectionné, appuyez sur **Bluetooth**, puis sur **WiFi** pour déclencher à nouveau la détection.

b) Si vous avez sélectionné **Définir l'imprimante manuellement (adresse IP)**, entrez l'adresse IP de l'imprimante et touchez **Enregistrer**.

4 Touchez **Fermer les réglages** pour terminer le processus de sélection d'imprimante.

Lorsque vous avez terminé

Imprimez un badge de test.

Imprimer un badge de test sur la borne en libre-service

Pour vérifier que l'imprimante fonctionne comme prévu, vous pouvez imprimer un badge de test. Cette impression de test peut être lancée lors de la configuration initiale ou après remplacement d'un rouleau d'étiquettes.

Avant de commencer

- Sélectionnez une imprimante d'étiquettes.
- Vérifiez que des étiquettes sont chargées dans l'imprimante.
- Vérifiez que les étiquettes sont alignées correctement.

À savoir

Les imprimantes d'étiquettes Brother QL-820NWBc, QL-820NWB et QL-810W peuvent imprimer des badges en **Noir** ou en **Rouge et noir** :

- 62mm noir (référence Brother : DK-2205)
- 62mm rouge et noir (référence Brother : DK-2251)

L'imprimante Brother TD-4550DNWB n'imprime que des badges en **noir** :

- 57mm noir (référence Brother : RD001U1S)
  IMPORTANT : Les étiquettes pour l'imprimante Brother TD-4550DNWB DOIVENT doivent être orientées correctement pour éviter les problèmes d'impression de badges.

Vous pouvez imprimer les badges au format *Portrait* ou *Paysage*.

Procédure

1 Dans l'application mobile Genetec ClearID^{MC} Self-Service Kiosk, touchez Réglages ( ).

2 Sur la *page des réglages*, touchez **Print a test badge** (Imprimer un badge de test).

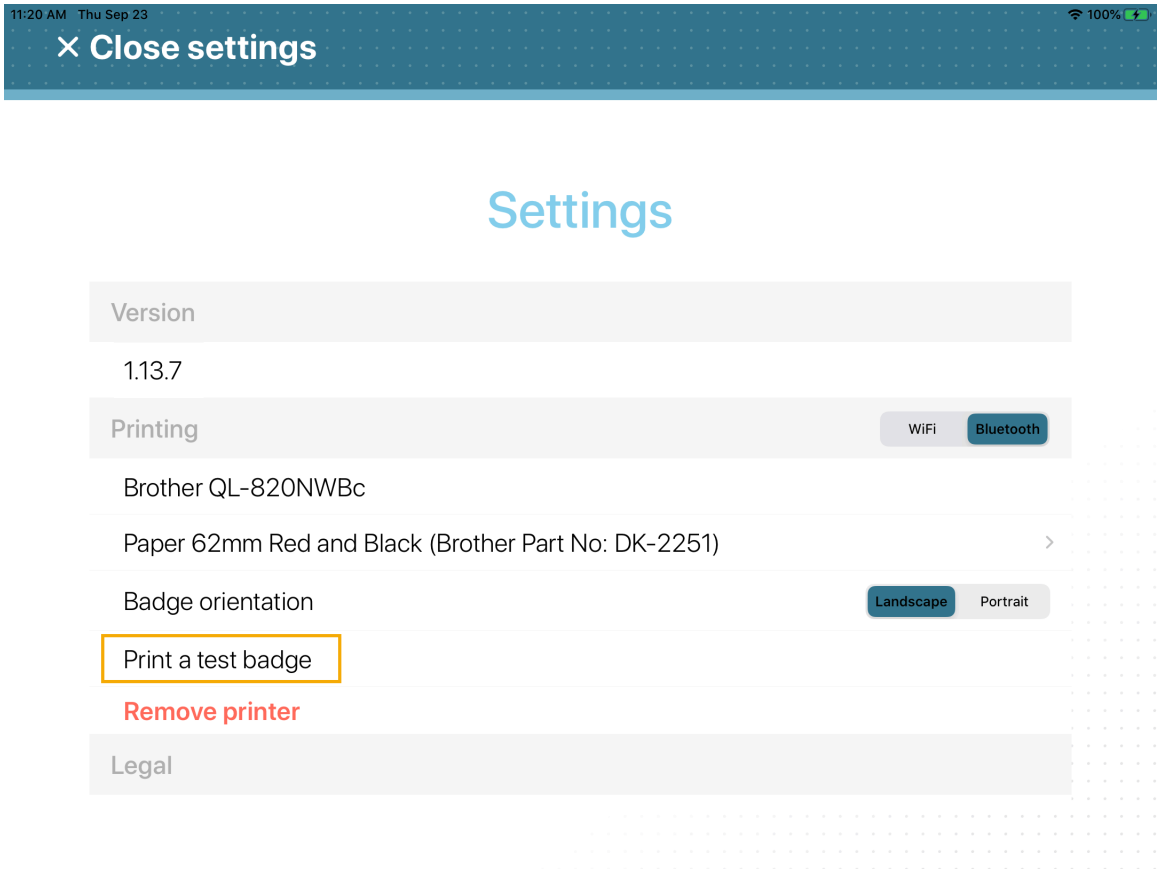


Illustration 24 : Page Réglages - Imprimante Brother QL-820NWBc

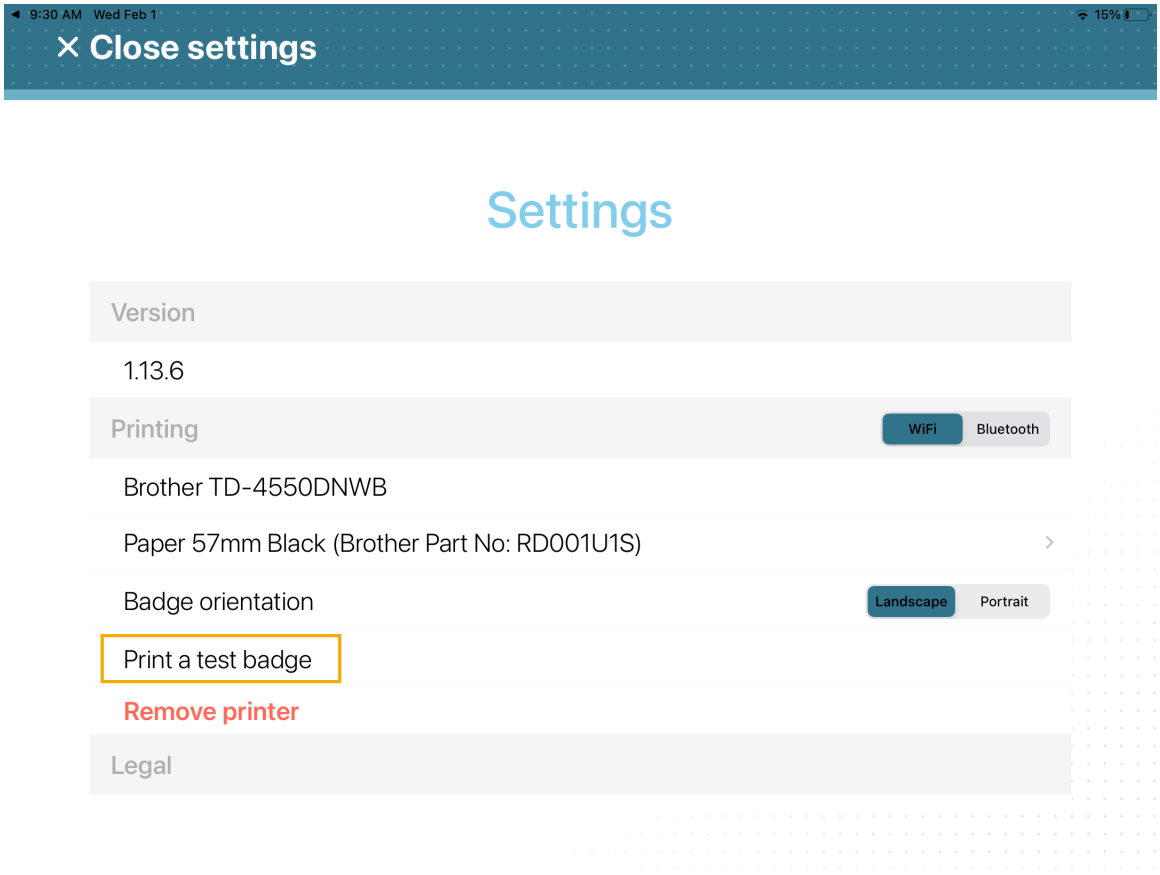
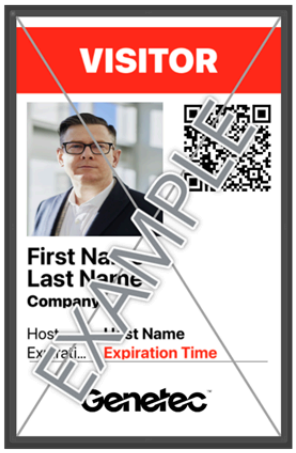


Illustration 25 : Page Réglages - Imprimante Brother TD-4550DNWB

3 Récupérez et examinez votre badge de test.



Dimensions du badge : **10 x 6,1 cm** ou **3,94 x 2,56 pouces**.

REMARQUE : L'imprimante Brother TD-4550DNWB imprime vos badges en noir et blanc.

Vos visiteurs peuvent désormais utiliser la borne ClearID Self-Service Kiosk et imprimer leurs propres badges au cours du processus d'inscription.

Lorsque vous avez terminé

De temps à autre, vous devrez commander des fournitures, remplacer la pile bouton, recharger la batterie (Brother QL-820NWBc ou QL-820NWB seulement) ou encore nettoyer l'imprimante d'étiquettes.

Pour en savoir plus, consultez la documentation tierce fournie avec votre imprimante.

Rubriques connexes

Problèmes d'impression d'étiquettes de la borne en libre-service, page 691

Réinitialiser l’application mobile Self-Service Kiosk

Dans certains cas, vous souhaiterez effectuer une réinitialisation complète de l’application mobile Genetec ClearID[MC] Self-Service Kiosk. Par exemple, si vous rencontrez des problèmes pour sélectionner l'imprimante d'étiquettes, imprimer les étiquettes, afficher les personnes, ou si vous souhaitez déplacer la borne vers un autre site.

Avant de commencer

- Veillez à vous munir de vos informations Apple ID.
- Veillez à vous munir des informations relatives à votre réseau Wi-Fi.

À savoir

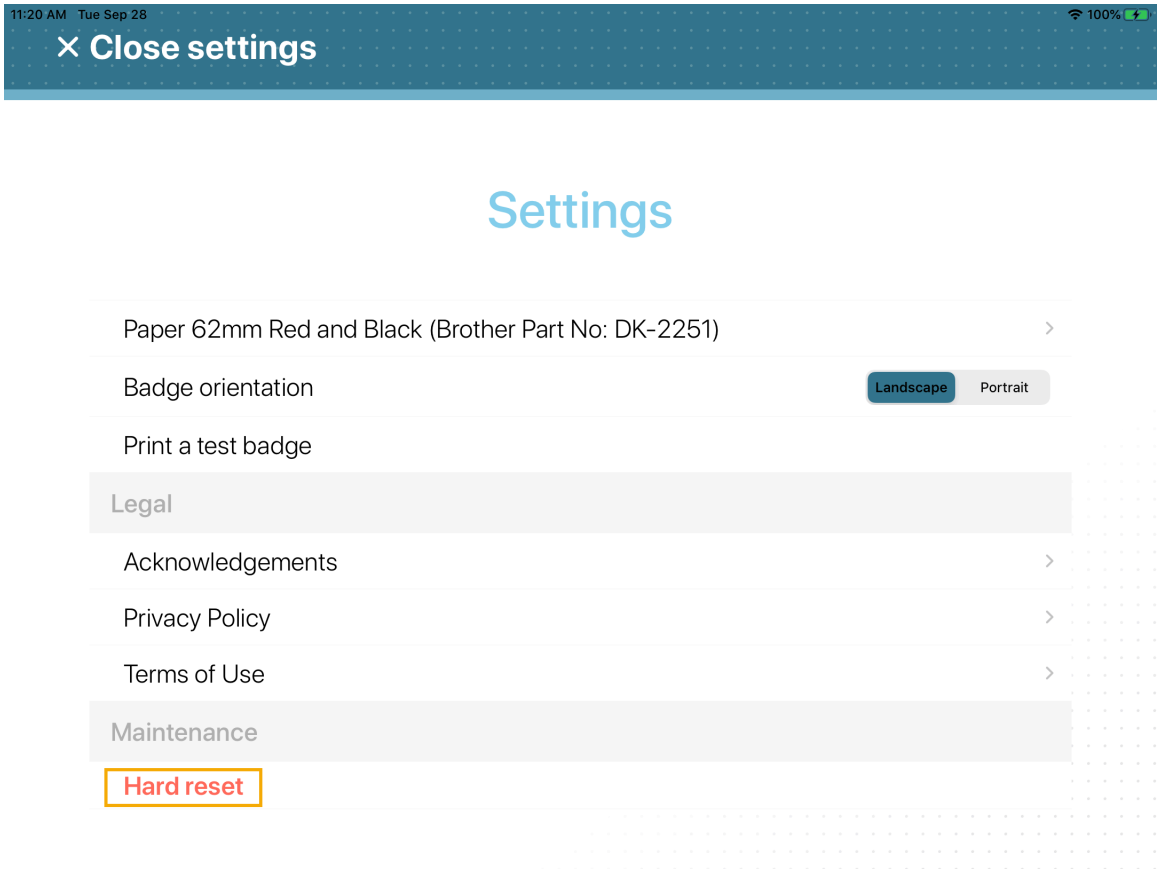
- Seul un *administrateur* ou un *propriétaire du site* peut générer un code d'activation d'appareil dans ClearID.

ATTENTION : La réinitialisation complète supprime toutes les données d'application, les données utilisateurs, ainsi que les informations de visite, d'inscription et de radiation de la borne avant de procéder à la réinitialisation complète de l'application mobile. Si vous continuez, vous devrez réinscrire l’appareil de la borne.

Procédure

1 Dans l’application mobile Self-Service Kiosk, touchez **Réglages** ( ).

2 Faites défiler la page *Réglages* jusqu'en bas, puis touchez **Hard reset** (Réinitialisation complète) dans la section *Maintenance*.



3 Configurez l'iPad de votre borne en libre-service.
4 Configurez l'imprimante d'étiquettes de votre borne en libre-service.
5 Sélectionnez l'imprimante d'étiquettes de votre borne en libre-service.
6 Imprimez un badge de test.

Votre borne en libre-service est prête à l'emploi.

Rubriques connexes

Problèmes d'impression d'étiquettes de la borne en libre-service, page 691

Options de la borne en libre-service

Utilisez les informations suivantes pour prendre connaissance des options disponibles pour la borne Genetec ClearID[MC] Self-Service Kiosk.

Description de l'élément	Partie	
Support table pour borne Apple iPad 10,9 pouces (Wi-Fi) avec Apple Care Kit de borne sur table (imprimante non comprise) **REMARQUE :** En fonction de vos besoins en matière d'inscription, le boîtier de l'iPad de la borne peut être configuré sur ce support au sol pour une utilisation en mode *Portrait* ou *Paysage*.	• CD-KIOSK-TABLETOP-KIT-V2[1]	
Support de borne au sol Apple iPad 10,9 pouces (Wi-Fi) avec Apple Care Kit de borne sur pied (imprimante non comprise) **REMARQUE :** En fonction de vos besoins en matière d'inscription, le boîtier de l'iPad de la borne peut être configuré sur ce support au sol pour une utilisation en mode *Portrait* ou *Paysage*.	• CD-KIOSK-FLOORSTAND-KIT-V2[1]	
Imprimante d'étiquettes pour les visiteurs Imprimante thermique Brother QL-820NWBc : • Réseau (Ethernet), Wi-Fi et Bluetooth • Imprime des étiquettes noires et rouges **REMARQUE :** Seuls les étiquettes Brother DK Roll - 62mm Black (Référence Brother : DK-2205) ou 62mm rouge et noir (référence Brother : DK-2251) sont prises en charge.	Références du kit Brother QL-820NWBc : • CD-KIOSK-PRINTER-AU-KIT • CD-KIOSK-PRINTER-BRA-KIT • CD-KIOSK-PRINTER-EU-KIT • CD-KIOSK-PRINTER-NA-KIT • CD-KIOSK-PRINTER-UK-KIT	
Imprimante d'étiquettes pour les visiteurs Imprimante thermique Brother TD-4550DNWB	**REMARQUE :** Cette imprimante **n'est plus disponible** à l'achat via Genetec[MC]. Nous prenons en charge et vendons désormais	

Description de l'élément	Partie	Élément
• Réseau (Ethernet), Wi-Fi et Bluetooth • Imprime des étiquettes en noir et blanc **REMARQUE :** Seules les étiquettes Brother RD Roll - 57mm Black (Référence Brother : RD001U1S) sont prises en charge.	l'imprimante Brother QL-820NWBc (CD-KIOSK-PRINTER-NA-KIT).	
Abonnement annuel pour une borne (Remises disponibles à partir de 10 bornes)	• CD-KIOSK-LIC-1Y	Licence d'abonnement pour une borne

IMPORTANT : [1] Dans les régions **EMEA**, **APAC** et certaines régions **LATCAR** (lorsque vous commandez le kit CD-KIOSK-FLOORSTAND-KIT-V2 ou le kit CD-KIOSK-TABLETOP-KIT-V2), vous devez inclure le kit **CD-KIOSK-WORLD-ADAPTER-KIT**.

La référence CD-KIOSK-WORLD-ADAPTER-KIT inclut un kit de voyage et des fiches adaptées à différentes prises électriques utilisées dans le monde, notamment dans les régions suivantes : Amérique du Nord, Japon, Chine, Royaume-Uni, Europe continentale, Corée, Australie, Hong Kong et Brésil. Sans ce kit, la fiche n'est pas compatible avec les prises électriques de votre région.

Pour en savoir plus ou pour commander des pièces de bornes, voir Genetec Parts Manager.

Rubriques connexes

Fiche technique ClearID Self-Service Kiosk (2 pages)

Appareils pris en charge, page 78

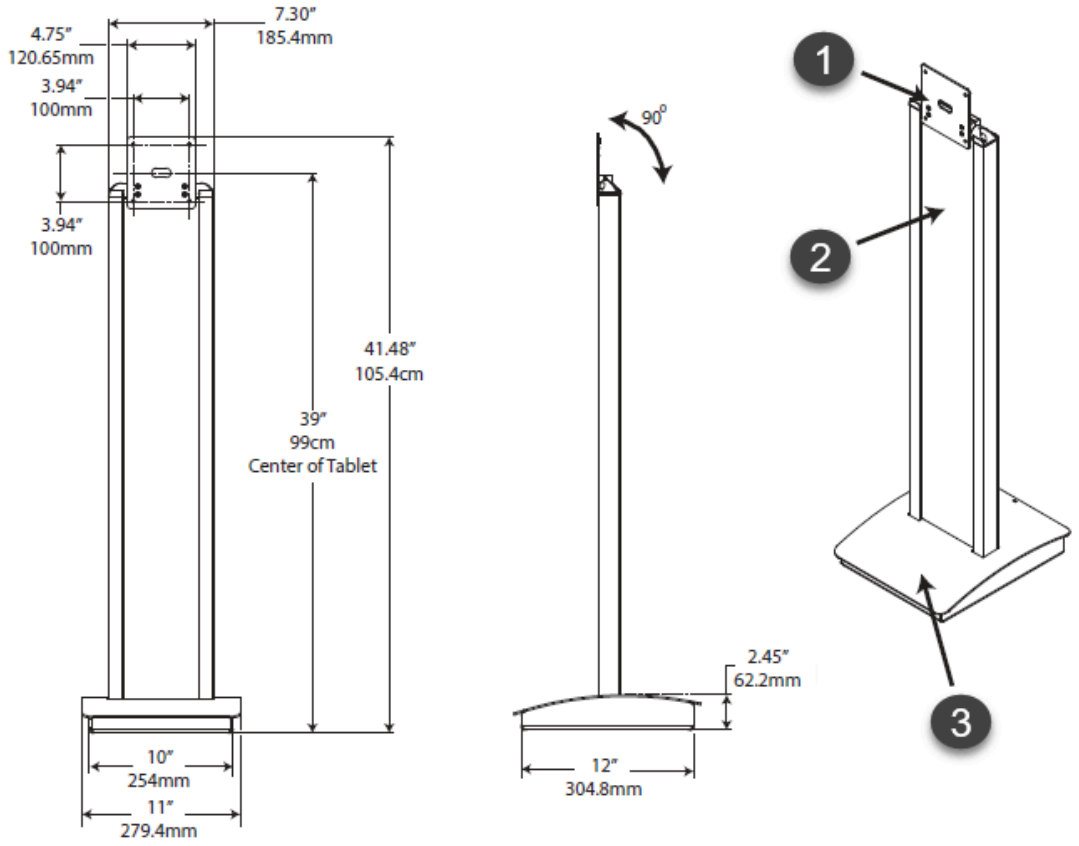
Support de borne au sol

Utilisez les informations suivantes pour prendre connaissance des dimensions, de la fixation et des caractéristiques du support au sol pour la borne Genetec ClearID[MC] Self-Service Kiosk.

REMARQUE : En fonction de vos besoins en matière d'inscription, le boîtier de l'iPad de la borne ClearID Self-Service Kiosk peut être configuré avec ce support au sol pour une utilisation en mode *Portrait* ou *Paysage*.

Dimensions du support sur pied

Le diagramme suivant illustre les dimensions du support sur pied, y compris la hauteur et l'encombrement du support.



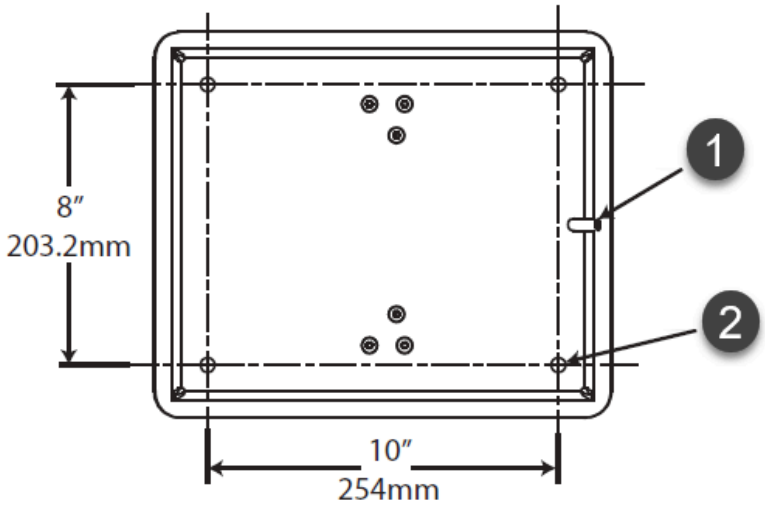
[1] Le support prend en charge tout boîtier de tablette avec un support VESA standard (100mm x 100mm) ou un adaptateur de rotation à 90° degré.

[2] tableau de signalisation amovible (inclus).

[3] Le tableau amovible permet d'accéder à l'alimentation dans l'espace de rangement.

Support au sol

Le schéma suivant présente les dimensions du support au sol ainsi qu'une vue de dessous du support de la borne.



[1] Ouverture pour le câble d'alimentation.

[2] 4x trous de fixation pour de la visserie de 6 mm (non incluse) servant à fixer le support au sol.

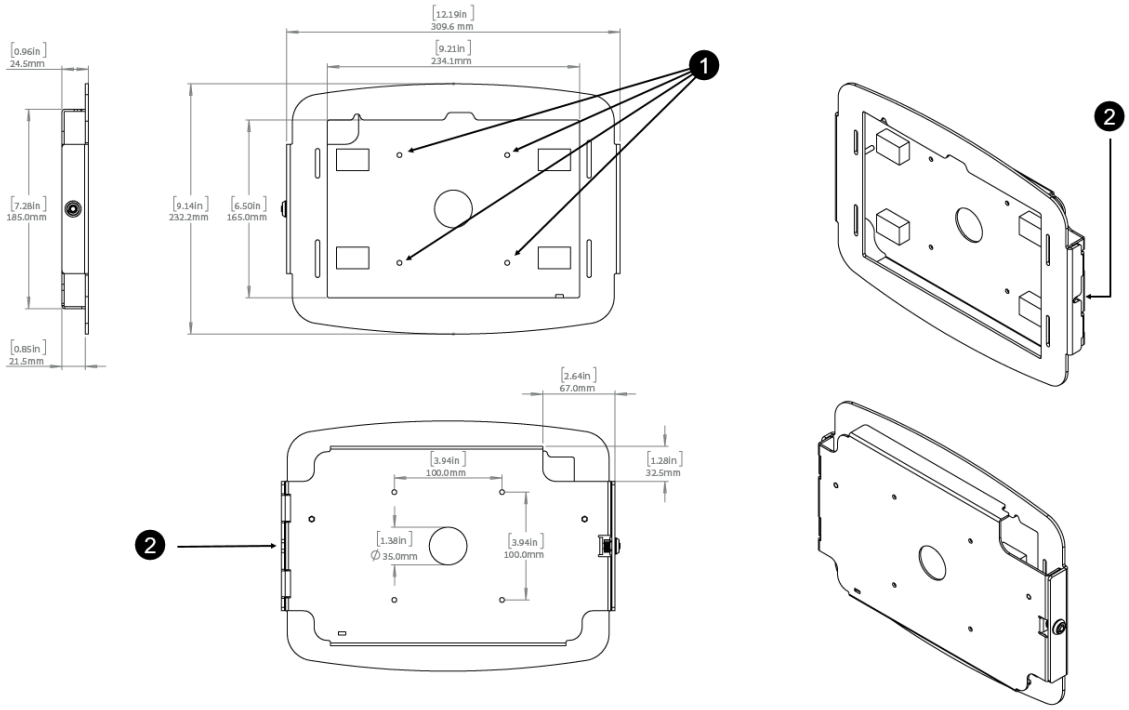
Caractéristiques du support au sol

Le support au sol comprend les caractéristiques suivantes :

- Option de montage sur pied ou au sol.
- Le support est compatible avec tout boîtier pour tablette doté d'une fixation VESA standard (100 x 100 mm).
- L'alimentation de la tablette peut être stockée dans la base.
- Le câble d'alimentation de la tablette peut être dissimulé dans les montants.
- La surface de fixation du boîtier peut pivoter de 90 degrés. Cette rotation signifie que le boîtier de l'iPad peut être orienté sur ce support de sol pour une utilisation en mode *Portrait* ou *Paysage*.

Boîtier d'iPad

Le schéma suivant montre les dimensions du boîtier pour iPad du support au sol.



[1] 4x trous pour fixer le boîtier de l'iPad au support au sol.

[2] Ouverture pour le câble d'alimentation.

Rubriques connexes

Options de la borne en libre-service, page 635
À propos de ClearID Self-Service Kiosk, page 578
Fiche technique ClearID Self-Service Kiosk (2 pages)

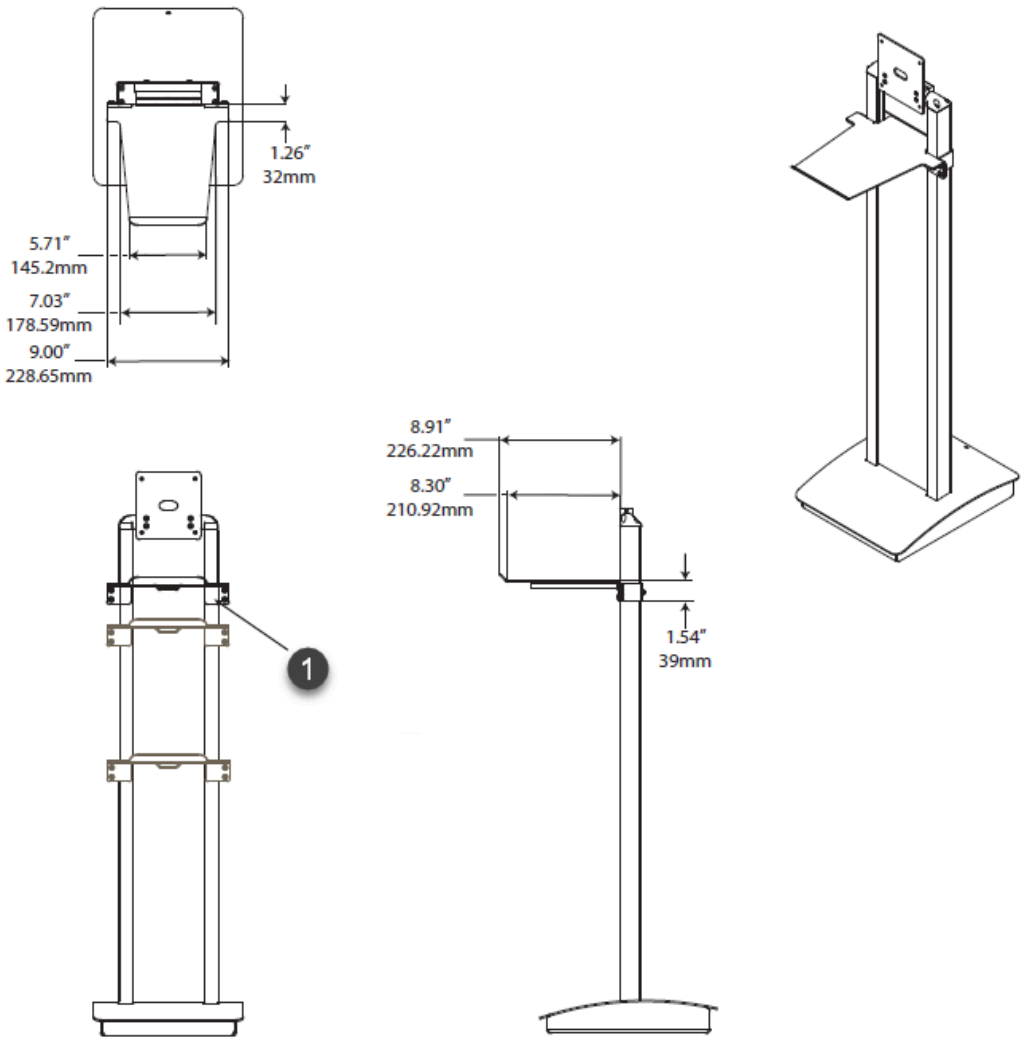
Étagère pour imprimante pour le support de borne au sol

Utilisez les informations suivantes pour prendre connaissance des dimensions et caractéristiques de l’étagère pour imprimante conçue pour le support au sol pour la borne Genetec ClearID[MC] Self-Service Kiosk.

REMARQUE : Selon la taille et le modèle de l’imprimante que vous utilisez, vous devrez parfois raccourcir ou modifier le tableau central (tableau graphique) du support au sol pour faire passer les câbles.

Dimensions de l’étagère pour imprimante

Le diagramme suivant montre les dimensions de l’étagère pour imprimante.



[1] Étagère d'imprimante réglable en hauteur.

Caractéristiques de l’étagère pour imprimante

L'étagère pour imprimante intègre les caractéristiques suivantes :

- Montage sur pied
- Réglable en hauteur
- Adaptable à plusieurs imprimantes

Rubriques connexes

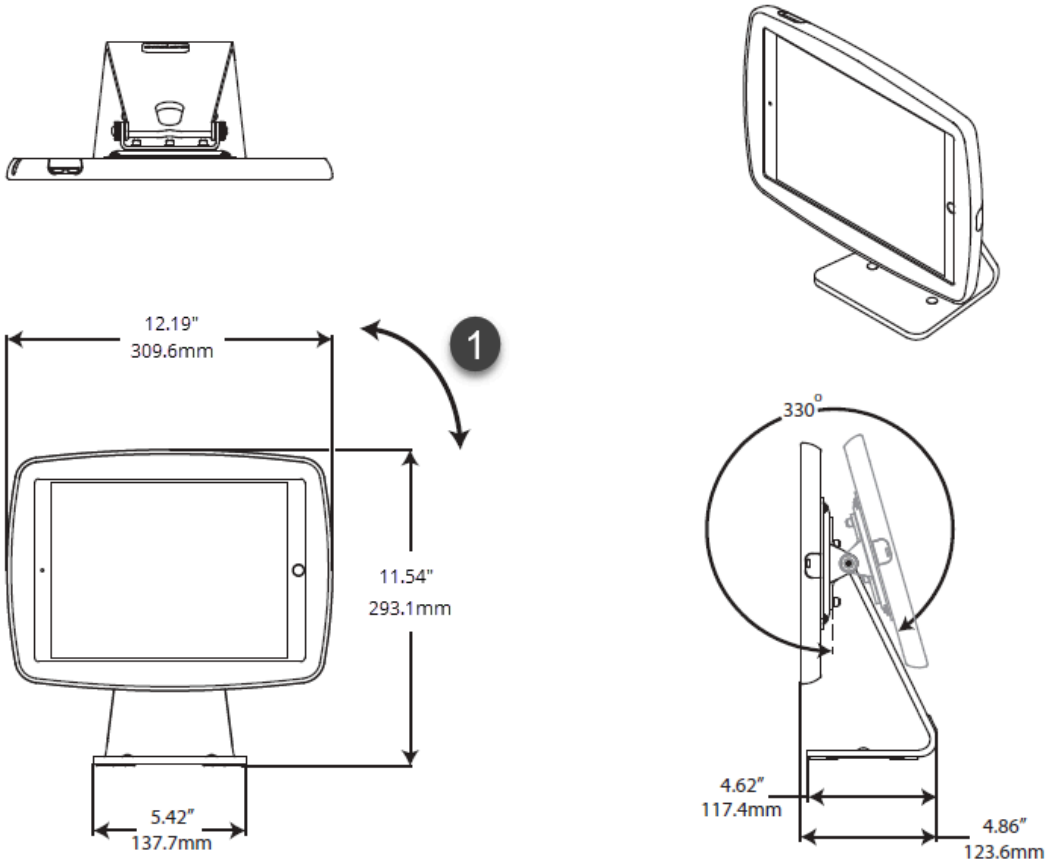
Options de la borne en libre-service, page 635
À propos de ClearID Self-Service Kiosk, page 578
Fiche technique ClearID Self-Service Kiosk (2 pages)

Support de table pour borne

Utilisez les informations suivantes pour prendre connaissance des dimensions, de la fixation et des caractéristiques du support de table pour la borne Genetec ClearID[MC] Self-Service Kiosk.

Dimensions du support de table

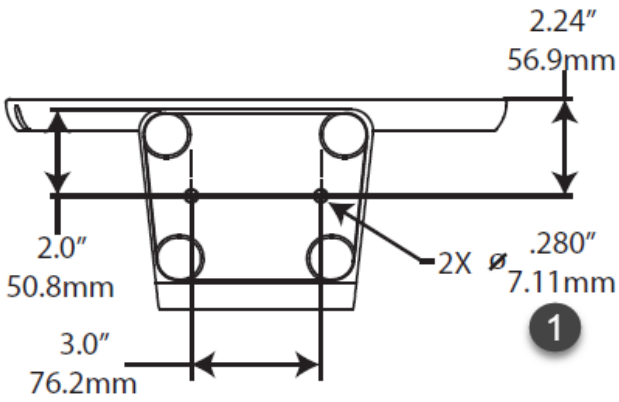
Le diagramme suivant illustre les dimensions du support de table, y compris la hauteur et l'encombrement du support.



[1] Rotation de 90° (orientation en mode portrait ou paysage).

Montage du support de table

Le diagramme suivant illustre les dimensions du support de table.



[1] 2x Trous de fixation pour de la visserie de 6 mm (non fournie).

Caractéristiques du support de table

Le support de table comprend les caractéristiques suivantes :

- Rotation de 90° (orientation en mode portrait ou paysage).
- Fonction de tablette rabattable.
- Option de fixation au comptoir.

Rubriques connexes

Options de la borne en libre-service, page 635
À propos de ClearID Self-Service Kiosk, page 578
Fiche technique ClearID Self-Service Kiosk (2 pages)

Types de pièces d’identité

Utilisez les informations suivantes pour mieux comprendre les différents types de pièces d'identité pris en charge par Genetec ClearID[MC] Self-Service Kiosk.

Vous pouvez utiliser une liste exhaustive de types d’ID au moment de l’inscription sur une borne ClearID Self-Service Kiosk.

REMARQUE : Le traitement des pièces d'identité est effectué intégralement en local sur l’iPad de la borne ClearID Self-Service Kiosk. Ce traitement en local à l’inscription permet d'assurer que les données d'identification ou les photos ne sont jamais envoyées dans le nuage, à des fins de sécurité maximale ou de conformité.

Pièces d'identité prises en charge (Asie)

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Afghanistan	Carte d'identité	کارت هویت الکترونیکی	Recto, verso	Latin
Afghanistan	Passeport papier[BÊTA]	پاسپورت	Page de données biométriques	Latin
Arménie	Carte d'identité	Նույնականացման քարտ	Recto, verso	Latin
Azerbaïdjan	Carte d'identité	Şəxsiyyət vəsiqəsi	Recto, verso	Latin
Azerbaïdjan	Passeport en polycarbonate[BÊTA]	Pasport	Page de données biométriques	Latin
Bangladesh	Permis de conduire[BÊTA]	মটোর ড্রাইভিং লাইসন্সে	Recto, verso	Latin
Bangladesh	Carte d'identité	জাতীয় পরিচয় পত্র	Recto, verso	Latin
Bangladesh	Passeport papier	পাসপোর্ট	Page de données biométriques	Latin
Brunei	Carte d'identité	Kad Pengenalan (Kuning)	Recto, verso	Latin
Brunei	Pièce d'identité militaire[BÊTA]	Kad Pengenalan Tentera (ABDB)	Recto, verso	Latin
Brunei	Permis de séjour[BÊTA]	Kad Pengenalan (Ungu)	Recto, verso	Latin
Brunei	Permis de séjour temporaire[BÊTA]	Kad Pengenalan (Hijau)	Recto, verso	Latin
Cambodge	Permis de conduire[BÊTA]	##########	Recto	Latin
Cambodge	Carte d'identité	##########	Recto	Latin
Cambodge	Passeport en polycarbonate	##########	Page de données biométriques	Latin
Chine	Carte d'identité	中华人民共和国居民身份证	Recto, verso	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Chine	Passeport papier	中华人民共和国护照	Page de données biométriques	Latin
Hong Kong	Carte d'identité	香港 身份證	Recto	Latin
Hong Kong	Passeport en polycarbonate[BÊTA]	護照	Page de données biométriques	Latin
Inde	Carte d'identité[BÊTA]	Carte Aadhaar, आधार कार्ड	Recto, verso	Latin
Inde	PAN Card	स्थायी खाता संख्या कार्ड	Recto	Latin
Inde	Passeport papier		Page de données biométriques	Latin
Inde	Carte d'électeur	भारतीय मतदाता पहचान पत्र	Recto, vertical	Latin
Inde, Gujarat	Permis de conduire[BÊTA]	ड्राइवंगि लाइेंसस	Recto	Latin
Inde, Karnataka	Permis de conduire	ड्राइवंगि लाइेंसस	Recto	Latin
Inde, Kerala	Permis de conduire[BÊTA]	ड्राइवंगि लाइेंसस	Recto, verso	Latin
Inde, Madhya Pradesh	Permis de conduire[BÊTA]	ड्राइवंगि लाइेंसस	Recto	Latin
Inde, Maharashtra	Permis de conduire	ड्राइवंगि लाइेंसस	Recto	Latin
Inde, Punjab	Permis de conduire[BÊTA]	ड्राइवंगि लाइेंसस	Recto	Latin
Inde, Tamil Nadu	Permis de conduire[BÊTA]	ड्राइवंगि लाइेंसस	Recto, verso	Latin
Indonesia	Permis de conduire	Sourate Izin Mengemudi (SIM)	Recto	Latin
Indonesia	Carte d'identité	Kartu Tanda Penduduk (KTP)	Recto	Latin
Indonesia	Passeport papier	Paspor	Page de données biométriques	Latin
Japon	Permis de conduire[BÊTA]	運転免許	Recto	Latin
Japon	My Number Card	マイナンバーカード	Recto	Latin
Japon	Passeport papier	旅券	Page de données biométriques	Latin
Japon	Permis de séjour[BÊTA]	在留カード	Recto	Latin
Kazakhstan	Carte d'identité	Жеке куәлік, Удостоверение личности	Recto, verso	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Kirghizistan	Carte d'identité	идентификациялык карта,идентификационная карта	Recto, verso	Latin
Malaisie	Permis de conduire	Lesen Memandu	Recto	Latin
Malaisie	MyKAS		Recto, verso	Latin
Malaisie	MyKad		Recto, verso	Latin
Malaisie	MyKid		Recto, verso	Latin
Malaisie	MyPR		Recto, verso	Latin
Malaisie	MyPolis[BETA]		Recto, verso	Latin
Malaisie	MyTentera		Recto, verso	Latin
Malaisie	Refugee ID	UNHCR Card	Recto	Latin
Malaisie	Passeport en polycarbonate	Pasport	Page de données biométriques	Latin
Malaisie	i-Kad		Recto	Latin
Maldives	Carte d'identité	############## ###### #### ##########	Recto, verso	Latin
Myanmar	Permis de conduire	##################	Recto, verso	Latin
Népal	Passeport papier	राहदानी	Page de données biométriques	Latin
Pakistan	ID consulaire	Carte d'identité nationale pour les Pakistanais d'outre-mer (NICOP)	Recto, verso	Latin
Pakistan	Carte d'identité	Computerized National Identity Card (CNIC), Smart National Identity Card (SNIC)	Recto, verso	Latin
Pakistan	Passeport papier		Page de données biométriques	Latin
Pakistan, Punjab	Permis de conduire		Recto	Latin
Philippines	Permis de conduire		Recto	Latin
Philippines	Carte d'identité	PhilSys ID, PhilID	Recto, verso	Latin
Philippines	Multipurpose ID	ID polyvalent unifié	Recto	Latin
Philippines	Passeport papier		Page de données biométriques	Latin
Philippines	Professional ID	Licence PRC	Recto	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Philippines	Social Security Card	SSS ID	Recto	Latin
Philippines	Numéro d'identification fiscale[BÊTA]	TIN ID card	Recto	Latin
Philippines	Carte d'électeur[BÊTA]		Recto	Latin
Singapour	Permis de conduire		Recto, verso	Latin
Singapour	Badge d'employé		Recto	Latin
Singapour	Fin Card		Recto	Latin
Singapour	Carte d'identité	NRIC (rose)	Recto, verso	Latin
Singapour	ID de résident	NRIC (bleu)	Recto, verso	Latin
Singapour	Passeport en polycarbonate		Page de données biométriques	Latin
Singapour	S Pass		Recto, verso	Latin
Singapour	Permis de travail		Recto, verso	Latin
Corée du Sud	Permis de conduire	자동차운전면허증	Recto	Latin
Corée du Sud	Carte d'identité[BÊTA]	주민등록증	Recto	Latin
Corée du Sud	Passeport papier[BÊTA]	여권	Page de données biométriques	Latin
Sri Lanka	Permis de conduire	####### #######	Recto	Latin
Sri Lanka	Carte d'identité	##### ##########, தேசிய அடையாள அட்டை	Recto, verso, vertical	Latin
Sri Lanka	Passeport papier	#### #######, கடவுச்சீட்டு	Page de données biométriques	Latin
Taïwan	Carte d'identité[BÊTA]	中華民國 國民 身分 證	Recto	Latin
Taïwan	Permis de séjour temporaire[BÊTA]	中華民國居留證 (ARC)	Recto	Latin
Latin	Latin	Latin	Latin	Latin
Thaïlande	Pièce d'identité d'étranger	บัตรประจำตัวคนซึ่งไม่มีสัญชาติไทย (บัตรสีชมพู)	Recto	Latin
Thaïlande	Permis de conduire[BÊTA]	ใบอนุญาตขับรถ	Recto, verso	Latin
Thaïlande	Carte d'identité	บัตร ประจำ ตัว ประชาชน	Recto, verso	Latin
Thaïlande	Passeport en polycarbonate	หนังสือเดินทาง	Page de données biométriques	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Vietnam	Permis de conduire[BÊTA]	Giấy phép lái xe	Recto	Latin
Vietnam	Carte d'identité[BÊTA]	Căn cước công dân, Giấy chứng minh nhân dân	Recto, verso	Latin

Pièces d'identité prises en charge (Europe)

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Albanie	Permis de conduire	Leje drejtimi	Recto	Latin
Albanie	Permis de conduire	Karta e drejtuesit të mjetit	Recto	Latin
Albanie	Carte d'identité	Letërnjoftim	Recto, verso	Latin
Albanie	Permis professionnel	Certifikatë aftësimi profesionale	Recto	Latin
Albanie	Passeport en polycarbonate	Pasaportë	Page de données biométriques	Latin
L'Autriche	Permis de conduire	Führerschein	Recto	Latin
L'Autriche	Carte d'identité	Personalausweis	Recto, verso	Latin
L'Autriche	Passeport papier	Reisepass	Page de données biométriques	Latin
L'Autriche	Permis de séjour[BÊTA]	Aufenthaltstitel	Recto, verso	Latin
Belarus	Permis de conduire	ВАДЗІЦЕЛЬСКАЕ ПАСВЕДЧАННЕ, ВОДИТЕЛЬСКОЕ УДОСТОВЕРЕНИЕ	Recto	Latin
Belarus	Passeport papier	Пашпарт, Паспорт	Page de données biométriques	Latin
Belgique	Permis de conduire	Rijbewijs, Permis de conduire, Führerschein	Recto	Latin
Belgique	Carte d'identité	Identiteitskaart, Carte d'identité, Personalausweis	Recto, verso	Latin
Belgique	Pièce d'identité de mineur	Kids-ID	Recto, verso	Latin
Belgique	Passeport papier	Paspoort, Passeport, Reisepass	Page de données biométriques	Latin
Belgique	Permis de séjour	Verblijfstitel, Titre de Sejour	Recto, verso	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Belgique	ID de résident	Document de Seojur, Verblijfsdocument, Aufenthaltsdokument, E Kaart, Carte E, E Karte; E+ Kaart, Carte E+, E+ Karte; F Kaart, Carte F, F Karte; F+ Kaart, Carte F+, F+ Karte	Recto, verso	Latin
Belgique	Passeport en polycarbonate[BÊTA]	Paspoort, Passeport, Reisepass	Page de données biométriques	Latin
Bosnie Herzégovine	Permis de conduire	Vozačka dozvola	Recto	Latin
Bosnie Herzégovine	Carte d'identité	Lična karta, Osobna iskaznica	Recto, verso	Cyrillique, Latin
Bosnie Herzégovine	Passeport en polycarbonate	Pasoš, Пасош, Putovnica	Page de données biométriques	Latin
Bulgarie	Permis de conduire	Свидетелство за управление на МПС	Recto	Cyrillique, Latin
Bulgarie	Carte d'identité	Лична карта	Recto, verso	Cyrillique, Latin
Bulgarie	Passeport papier	Паспорт	Page de données biométriques	Latin
Croatie	Permis de conduire	Vozačka dozvola	Recto	Latin
Croatie	Carte d'identité	Osobna iskaznica	Recto, verso	Latin
Croatie	Permis de séjour[BÊTA]	Boravišna iskaznica, Dozvola boravka	Recto, verso	Latin
Croatie	Passeport en polycarbonate	Putovnica	Page de données biométriques	Latin
Chypre	Permis de conduire	Sürüş ruhsati, Αάδεια οδήγησης	Recto	Latin
Chypre	Carte d'identité	Kimlik kartı, Δελτίο Ταυτότητας	Recto, verso	Latin
Chypre	Passeport papier	Pasaport, Διαβατήριο	Page de données biométriques	Latin
Chypre	Permis de séjour	ΑΔΕΙΑ ΔΙΑΜΟΝΗΣ	Recto, verso	Latin
Tchéquie	Permis de conduire	Řidičský průkaz	Recto	Latin
Tchéquie	Carte d'identité	Občanský průkaz	Recto, verso	Latin
Tchéquie	Permis de séjour	Povolení k pobytu	Recto, verso	Latin
Tchéquie	Passeport en polycarbonate	Cestovní pas	Page de données biométriques	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Danemark	Permis de conduire	Kørekort	Recto	Latin
Danemark	Permis de séjour[BÊTA]	Opholdstilladelse, Opholdskort	Recto, verso	Latin
Danemark	Passeport en polycarbonate	Pas	Page de données biométriques	Latin
Estonie	Permis de conduire	Juhiluba	Recto	Latin
Estonie	Carte d'identité	Isikutunnistus	Recto, verso	Latin
Estonie	Passeport papier	Pass	Page de données biométriques	Latin
Estonie	Permis de séjour[BÊTA]	Elamisluba	Recto, verso	Latin
Finlande	Pièce d'identité d'étranger	Ulkomaalaisen henkilökortti, Identitetskort för utlänning	Recto, verso	Latin
Finlande	Permis de conduire	Ajokortti, Körkort	Recto	Latin
Finlande	Carte d'identité	Henkilökortti, Identitetskort	Recto, verso	Latin
Finlande	Permis de séjour	Oleskelulupa, Uppehållstillstånd	Recto, verso	Latin
Finlande	Passeport en polycarbonate	Passi, Pass	Page de données biométriques	Latin
France	Permis de conduire	Permis de conduire	Recto	Latin
France	Carte d'identité	Carte d'identité	Recto, verso	Latin
France	Passeport papier[BÊTA]	Passeport	Page de données biométriques	Latin
France	Permis de séjour[BÊTA]	Titre de séjour	Recto, verso	Latin
Georgie	Permis de conduire	მართვის მოწმობა	Recto	Latin
Georgie	Carte d'identité	მოქალაქის პირადობის მოწმობა	Recto, verso	Latin
Georgie	Passeport papier[BÊTA]	პასპორტი	Page de données biométriques	Latin
Allemagne	Permis de conduire	Führerschein	Recto	Latin
Allemagne	Carte d'identité	Personalausweis	Recto, verso	Latin
Allemagne	Passeport de mineur	Kinderreisepass	Page de données biométriques	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Allemagne	Passeport papier	Reisepass	Page de données biométriques	Latin
Allemagne	Permis de séjour	Aufenthaltstitel	Recto, verso	Latin
Allemagne	Passeport en polycarbonate	Reisepass	Page de données biométriques	Latin
Grèce	Permis de conduire	Αάδεια οδήγησης	Recto	Latin
Grèce	Carte d'identité	ΔΕΛΤΙΟ ΤΑΥΤΟΤΗΤΑΣ	Recto, verso	Latin
Grèce	Passeport papier	Διαβατήριο	Page de données biométriques	Latin
Grèce	Permis de séjour	ΑΔΕΙΑ ΔΙΑΜΟΝΗΣ	Recto, verso	Latin
Hongrie	Carte d'adresse[BÊTA]	Lakcímkártya, Lakcímigazolvány	Recto, verso	Latin
Hongrie	Permis de conduire	Vezetői engedély	Recto	Latin
Hongrie	Carte d'identité	Személyazonosító igazolvány	Recto, verso	Latin
Hongrie	Passeport papier	Útlevél	Page de données biométriques	Latin
Hongrie	Permis de séjour[BÊTA]	Tartózkodási engedély	Recto, verso	Latin
Islande	Permis de conduire[BÊTA]	Ökuskírteini	Recto	Latin
Islande	Passeport papier[BÊTA]	Vegabréf	Page de données biométriques	Latin
Irlande	Permis de conduire	Ceadúnas tiomána	Recto	Latin
Irlande	Carte passeport	Cárta Pas	Recto, verso	Latin
Irlande	Carte des services publics	Cárta Seirbhísí Poiblí	Recto, verso	Latin
Irlande	Permis de séjour[BÊTA]		Recto, verso	Latin
Irlande	Passeport en polycarbonate	Pas	Page de données biométriques	Latin
Italie	Permis de conduire	Patente di guida	Recto	Latin
Italie	Carte d'identité	Carta d'identità	Recto, verso	Latin
Italie	Passeport papier[BÊTA]	Passaporto	Page de données biométriques	Latin
Italie	Permis de séjour	Permesso di soggiorno	Recto, verso	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Kosovo	Permis de conduire	Patentë shoferi, возачка дозвола	Recto	Latin
Kosovo	Carte d'identité	Letërnjoftim, Лична карта	Recto, verso	Latin
Kosovo	Passeport papier	Pasaportë, Пасош	Page de données biométriques	Latin
Lettonie	Pièce d'identité d'étranger	Nepilsoņa personas apliecība	Recto, verso	Latin
Lettonie	Permis de conduire	Vadītāja apliecība	Recto	Latin
Lettonie	Carte d'identité	Personas apliecība	Recto, verso	Latin
Lettonie	Permis de séjour[BÊTA]	Uzturēšanās atļauja	Recto, verso	Latin
Lettonie	Passeport étranger en polycarbonate	Nepilsoņa pase	Page de données biométriques	Latin
Lettonie	Passeport en polycarbonate	Pase	Page de données biométriques	Latin
Liechtenstein	Carte d'identité	Identitätskarte	Recto, verso	Latin
Lithuania	Permis de conduire	Vairuotojo pažymėjimai	Recto	Latin
Lithuania	Carte d'identité	Asmens tapatybės kortelė	Recto, verso	Latin
Lithuania	Permis de séjour[BÊTA]	Leidimas gyventi	Recto, verso	Latin
Lithuania	Passeport en polycarbonate	Pasas	Page de données biométriques	Latin
Luxembourg	Permis de conduire	Permis de conduire	Recto	Latin
Luxembourg	Carte d'identité	Carte d'Identité, Personalausweis	Recto, verso	Latin
Luxembourg	Permis de séjour	Titre de séjour	Recto, verso	Latin
Luxembourg	Passeport en polycarbonate	Pass, Passeport	Page de données biométriques	Latin
Malte	Permis de conduire	Liċenzja tas-Sewqan	Recto	Latin
Malte	Carte d'identité	Karta tal-Identità	Recto, verso	Latin
Malte	Permis de séjour	Permess ta' residenza, Residence documentation	Recto, verso	Latin
Moldavie	Carte d'identité[BÊTA]	Buletin de Identitate	Recto, verso	Latin
Moldavie	Passeport papier[BÊTA]	Paşaport	Page de données biométriques	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Monténégro	Permis de conduire	Vozačka dozvola, Возачка дозвола	Recto	Latin
Monténégro	Carte d'identité	Lična karta, Лична карта	Recto, verso	Latin
Monténégro	Passeport en polycarbonate	Pasoš, Пасош	Page de données biométriques	Latin
Pays-Bas	Permis de conduire	Rijebewijs	Recto, verso	Latin
Pays-Bas	Carte d'identité	Identiteitskaart (ID-kaart)	Recto, verso	Latin
Pays-Bas	Permis de séjour	Verblijfstitel, Verblijfskaart	Recto, verso	Latin
Pays-Bas	Passeport en polycarbonate	Paspoort	Page de données biométriques	Latin
Macédoine du Nord	Permis de conduire	возачка дозвола, Patentë shoferi	Recto	Cyrillique, Latin
Macédoine du Nord	Carte d'identité	лична карта, Letërnjoftim	Recto, verso	Cyrillique, Latin
Macédoine du Nord	Passeport en polycarbonate	Пасош, Pasaportë	Page de données biométriques	Latin
Norvège	Permis de conduire	Førerkort, Førarkort	Recto	Latin
Norvège	Carte d'identité		Recto, verso	Latin
Norvège	Permis de séjour	Oppholdstillatelse, Opphaldsløyve	Recto, verso	Latin
Norvège	Passeport en polycarbonate	Pass	Page de données biométriques	Latin
Pologne	Permis de conduire	Prawo jazdy	Recto	Latin
Pologne	Carte d'identité	Osobistie Dowód	Recto, verso	Latin
Pologne	Passeport papier	Paszport	Page de données biométriques	Latin
Pologne	Permis de séjour[BÊTA]	Karta pobytu	Recto, verso	Latin
Pologne	Passeport en polycarbonate	Paszport	Page de données biométriques	Latin
Portugal	Permis de conduire	Carta de Condução	Recto	Latin
Portugal	Carte d'identité	Cartão de Cidadão (CC)	Recto, verso	Latin
Portugal	Passeport papier	Passaporte	Page de données biométriques	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Portugal	Permis de séjour[BÊTA]	Título de Residência, Cartão de Residência	Recto, verso	Latin
Roumanie	Permis de conduire	Permis de conducere	Recto	Latin
Roumanie	Carte d'identité	Carte de identité	Recto	Latin
Roumanie	Passeport en polycarbonate	Pasaport, Paşaport	Page de données biométriques	Latin
Russie	Permis de conduire	Водительское удостоверение	Recto	Latin
Russie	Passeport en polycarbonate	(Заграничный) Паспорт	Page de données biométriques	Latin
Serbie	Permis de conduire	Возачка дозвола, Vozačka dozvola	Recto	Latin
Serbie	Carte d'identité	Лична карта, Lična karta	Recto, verso	Cyrillique, Latin
Serbie	Passeport en polycarbonate	Пасош, Pasoš	Page de données biométriques	Latin
Slovaquie	Permis de conduire	Vodičský preukaz	Recto	Latin
Slovaquie	Carte d'identité	Občiansky preukaz	Recto, verso	Latin
Slovaquie	Permis de séjour	Povolenie na pobyt, Pobytový preukaz občana EÚ, Pobytový preukaz rodinného príslušníka občana EÚ	Recto, verso	Latin
Slovaquie	Passeport en polycarbonate	Cestovný pas	Page de données biométriques	Latin
Slovénie	Permis de conduire	Vozniško dovoljenje	Recto	Latin
Slovénie	Carte d'identité	Osebna izkaznica	Recto, verso	Latin
Slovénie	Permis de séjour	Dovoljenje za prebivanje	Recto, verso	Latin
Slovénie	Passeport en polycarbonate	Potni list	Page de données biométriques	Latin
Espagne	Pièce d'identité d'étranger	Tarjeta de Identidad de Extranjero (TIE)	Recto, verso	Latin
Espagne	Permis de conduire	Permiso de Conducción	Recto	Latin
Espagne	Carte d'identité	Documento Nacional de Identidad (DNI)	Recto, verso	Latin
Espagne	Passeport papier	Pasaporte	Page de données biométriques	Latin
Espagne	Permis de séjour	Permiso de residencia	Recto, verso	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Suède	Permis de conduire	Körkort	Recto	Latin
Suède	Carte d'identité	Nationellt identitetskort	Recto, verso	Latin
Suède	Permis de séjour	Uppehållstillstånd, Uppehållskort	Recto, verso	Latin
Suède	Passeport en polycarbonate	Pass	Page de données biométriques	Latin
Suède	Social Security Card	Identitetskort, Skatteverkets id-kort	Recto	Latin
Suisse	Permis de conduire	Führerausweis, Permis de conduire, Licenza di condurre, Permiss da manischar	Recto	Latin
Suisse	Carte d'identité	Identitätskarte, Carte d'identité, Carta d'identitéità, Carta d'identitéitad	Recto, verso	Latin
Suisse	Passeport papier	Pass, Passeport, Passaporto,Passaport	Page de données biométriques	Latin
Suisse	Permis de séjour	Aufenthaltstitel, Titre de séjour, Permesso di soggiorno, Permissiun da dimora	Recto, verso	Latin
Royaume-Uni	Permis de conduire	Trwydded yrru	Recto	Latin
Royaume-Uni	Passeport papier		Page de données biométriques	Latin
Royaume-Uni	Carte de preuve de majorité	CitizenCard	Recto	Latin
Royaume-Uni	Permis de séjour		Recto, verso	Latin
Royaume-Uni	Passeport en polycarbonate		Page de données biométriques	Latin
Ukraine	Permis de conduire	Посвідчення водія,Водительское удостоверение	Recto	Cyrillique, Latin
Ukraine	Carte d'identité	Паспорт громадянина України	Recto, verso	Cyrillique, Latin
Ukraine	Permis de séjour	Посвідка на постійне проживання (ППП)	Recto, verso	Cyrillique, Latin
Ukraine	Passeport en polycarbonate	Паспорт	Page de données biométriques	Latin
Ukraine	Permis de séjour temporaire	Посвідка на тимчасове проживання	Recto, verso	Cyrillique, Latin

Pièces d'identité prises en charge (Amérique latine et Caraïbes)

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Antigua-et-Barbuda	Permis de conduire[BÊTA]		Recto	Latin
Argentine	Pièce d'identité d'étranger	DNI para extranjeros	Recto, verso	Latin
Argentine	Permis de conduire[BÊTA]	Licencia de Conducir	Recto	Latin
Argentine	Carte d'identité	Documento Nacional de Identidad (DNI)	Recto, verso	Latin
Argentine	Passeport papier	Pasaporte	Page de données biométriques	Latin
Bahamas	Permis de conduire		Recto	Latin
Bahamas	Carte d'identité[BÊTA]	NIB Smart Card	Recto	Latin
Barbade	Carte d'identité[BÊTA]		Recto, verso	Latin
Bolivie	Permis de conduire	Licencia para conducir	Recto	Latin
Bolivie	Carte d'identité	Cédula de identidad	Recto, verso	Latin
Bolivie	Pièce d'identité de mineur	Cédula de identidad para menores	Recto, verso	Latin
Brésil	Passeport consulaire[BÊTA]	Passaporte	Page de données biométriques	Latin
Brésil	Permis de conduire	Carteira Nacional de Habilitação (CNH)	Recto, verso	Latin
Brésil	Carte d'identité[BÊTA]	Cédula de identidade	Recto, verso	Latin
Brésil	Passeport papier[BÊTA]	Passaporte	Page de données biométriques	Latin
Brésil, Rio de Janeiro	Carte d'identité	Cédula de identidade	Recto, verso	Latin
Brésil, Rio Grande do Sul	Carte d'identité[BÊTA]	Cédula de identidade	Recto, verso	Latin
Brésil, Sao Paulo	Carte d'identité	Cédula de identidade	Recto, verso	Latin
Îles Caïman	Permis de conduire[BÊTA]	Permis de conduire	Recto	Latin
Chili	Pièce d'identité d'étranger	Cédula de identidad para extranjeros	Recto, verso	Latin
Chili	Permis de conduire	Licencia de conducir	Recto	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Chili	Carte d'identité	Cédula de Identidad	Recto, verso	Latin
Chili	Passeport en polycarbonate	Pasaporte	Page de données biométriques	Latin
Colombie	Pièce d'identité d'étranger	Cédula de Extranjería (CE)	Recto, verso	Latin
Colombie	Permis de conduire	Licencia de Conducción	Recto, verso	Latin
Colombie	Carte d'identité	Cédula Digital Colombiana, Cédula de Ciudadanía (CC)	Recto, verso	Latin
Colombie	Pièce d'identité de mineur	Tarjeta de identidad Biométrica (Azul)	Recto, verso	Latin
Colombie	Passeport en polycarbonate	Pasaporte	Page de données biométriques	Latin
Costa Rica	Permis de conduire[BÊTA]	Licencia de conducir	Recto	Latin
Costa Rica	Carte d'identité	Cédula de identidad	Recto, verso	Latin
Cuba	Carte d'identité[BÊTA]	Carné de Identidad	Recto, verso	Latin
Cuba	Passeport papier	Pasaporte	Page de données biométriques	Latin
République dominicaine	Permis de conduire[BÊTA]	Licencia de conducir	Recto, verso	Latin
République dominicaine	Carte d'identité	Cédula de Identidad y Electoral (CIE)	Recto, verso	Latin
République dominicaine	Passeport papier	Pasaporte	Page de données biométriques	Latin
Équateur	Permis de conduire	Licencia de conducir	Recto	Latin
Équateur	Carte d'identité	Cédula de Identidad, Cédula de Identidad Electrónica	Recto, verso	Latin
El Salvador	Permis de conduire[BÊTA]	Licencia de conducir	Recto, verso	Latin
El Salvador	Carte d'identité	Documento Único de Identidad (DUI)	Recto, verso	Latin
Guatemala	ID consulaire	Tarjeta de Identificación Consular (TICG)	Recto, verso	Latin
Guatemala	Permis de conduire	Licencia de conducir	Recto, verso	Latin
Guatemala	Carte d'identité	Documento Personal de Identificación (DPI)	Recto, verso	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Guatemala	Passeport papier	Pasaporte	Page de données biométriques	Latin
Haïti	Permis de conduire	Permis de conduire	Recto	Latin
Haïti	Carte d'identité	Carte d'identification nationale (CIN), Kat Idantifikasyon Nasyonal	Recto, verso	Latin
Haïti	Passeport papier	Passeport, Paspò	Page de données biométriques	Latin
Honduras	Permis de conduire[BÊTA]	Licencia de conducir	Recto, verso	Latin
Honduras	Carte d'identité[BÊTA]	Tarjeta de identidad	Recto, verso	Latin
Honduras	Passeport papier[BÊTA]	Pasaporte	Page de données biométriques	Latin
Jamaïque	Permis de conduire	Motor vehicle license, MV license	Recto, verso	Latin
Mexique	Identifiant consulaire[BÊTA]	Matrícula consular	Recto, verso	Latin
Mexique	Passeport papier[BÊTA]	Pasaporte	Page de données biométriques	Latin
Mexique	Permis professionnel[BÊTA]	Licencia Federal de Conductor	Recto	Latin
Mexique	Pièce d'identité professionnelle[BETA]	Cédula Profesional	Recto, verso, vertical	Latin
Mexique	Permis de séjour[BÊTA]	Tarjeta de Residencia Temporal y Residencia Permanente	Recto, verso	Latin
Mexique	Passeport en polycarbonate	Pasaporte	Page de données biométriques	Latin
Mexique	Carte d'électeur	Crédence para votar	Recto, verso	Latin
Mexique, Aguascalientes	Permis de conduire	Licencia de Conducir	Recto, verso, vertical	Latin
Mexique, Basse-Californie	Permis de conduire	Licencia de Conducir	Recto, verso, vertical	Latin
Mexique, Basse-Californie du Sud	Permis de conduire[BÊTA]	Licencia de Conducir	Recto, verso	Latin
Mexique, Campeche	Permis de conduire[BÊTA]	Licencia de Conducir	Recto, verso	Latin
Mexique, Chiapas	Permis de conduire	Licencia de Conducir	Recto, verso	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Mexique, Chihuahua	Permis de conduire	Licencia de Conducir	Recto, verso	Latin
Mexique, Mexico	Permis de conduire	Licencia de Conducir	Recto, vertical	Latin
Mexique, Coahuila	Permis de conduire	Licencia de Conducir	Recto, verso	Latin
Mexique, Colima	Permis de conduire	Licencia de Conducir	Recto, verso	Latin
Mexique, Durango	Permis de conduire	Licencia de Conducir	Recto	Latin
Mexique, Guanajuato	Permis de conduire	Licencia de Conducir	Recto, verso	Latin
Mexique, Guerrero Cocula	Permis de conduire[BÊTA]	Licencia de Conducir	Recto, verso	
Mexique, Guerrero Juchitan	Permis de conduire[BÊTA]	Licencia de Conducir	Recto, verso	Latin
Mexique, Hidalgo	Permis de conduire	Licencia de Conducir	Recto, verso, vertical	Latin
Mexique, Jalisco	Permis de conduire	Licencia de Conducir	Recto	Latin
Mexique, Mexico	Permis de conduire	Licencia de Conducir	Recto, verso	Latin
Mexique, Michoacan	Permis de conduire	Licencia de Conducir	Recto, verso	Latin
Mexique, Morelos	Permis de conduire	Licencia de Conducir	Recto	Latin
Mexique, Nayarit	Permis de conduire[BÊTA]	Licencia de Conducir	Recto, verso	Latin
Mexique, Nuevo León	Permis de conduire	Licencia de Conducir	Recto, verso	Latin
Mexique, Oaxaca	Permis de conduire	Licencia de Conducir	Recto, verso	Latin
Mexique, Puebla	Permis de conduire[BÊTA]	Licencia de Conducir	Recto, verso	Latin
Mexique, Quintana Roo Cozumel	Permis de conduire[BÊTA]	Licencia de Conducir	Recto, verso	Latin
Mexique, Quintana Roo Solidaridad	Permis de conduire	Licencia de Conducir	Recto, verso, vertical	Latin
Mexique, San Luis Potosi	Permis de conduire	Licencia de Conducir	Recto	Latin
Mexique, Sinaloa	Permis de conduire[BÊTA]	Licencia de Conducir	Recto	Latin
Mexique, Sonora	Permis de conduire[BÊTA]	Licencia de Conducir	Recto, verso	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Mexique, Tabasco	Permis de conduire[BÊTA]	Licencia de Conducir	Recto, verso	Latin
Mexique, Tamaulipas	Permis de conduire	Licencia de Conducir	Recto, verso, vertical	Latin
Mexique, Tlaxcala	Permis de conduire	Licencia de Conducir	Recto, verso	Latin
Mexique, Veracruz	Permis de conduire[BÊTA]	Licencia de Conducir	Recto, verso	Latin
Mexique, Yucatan	Permis de conduire[BÊTA]	Licencia de Conducir	Recto, verso	Latin
Mexique, Zacatecas	Permis de conduire	Licencia de Conducir	Recto, verso	Latin
Nicaragua	Carte d'identité	Cédula de Identidad Ciudadana	Recto, verso	Latin
Panama	Permis de conduire	Licencia de Conducir	Recto	Latin
Panama	Carte d'identité	Cédula de Identidad	Recto	Latin
Panama	Permis de séjour	Carné de Residente Permanente	Recto	Latin
Panama	Permis de séjour temporaire	Carné de Residencia Provisional	Recto, verso	Latin
Le Paraguay	Permis de conduire	Licencia de Conducir	Recto, verso	Latin
Le Paraguay	Carte d'identité	Cédula de Identidad Civil	Recto, verso	Latin
Pérou	Permis de conduire	Licencia de conducir	Recto, verso	Latin
Pérou	Carte d'identité	Documento Nacional de Identidad (DNI)	Recto, verso	Latin
Pérou	Pièce d'identité de mineur[BÊTA]	Documento Nacional de Identidad (DNI) para menores	Recto, verso	Latin
Pérou	Passeport papier	Pasaporte	Page de données biométriques	Latin
Porto Rico	Permis de conduire	Licencia de Conducir	Recto	Latin
Porto Rico	Carte d'électeur[BÊTA]	Tarjeta de Identificación Electoral (TIE), Electoral Identification Card	Recto	Latin
Sainte-Lucie	Carte d'identité[BÊTA]		Recto, verso	Latin
Trinité-et-Tobago	Permis de conduire		Recto	Latin
Trinité-et-Tobago	Carte d'identité		Recto, verso	Latin
Uruguay	Carte d'identité	Cédula de Identidad	Recto, verso	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Venezuela	Permis de conduire	Licencia para conducir	Recto	Latin
Venezuela	Carte d'identité	Cédula de Identidad	Recto	Latin
Venezuela	Passeport en polycarbonate	Pasaporte	Page de données biométriques	Latin

Pièces d'identité prises en charge (Moyen-Orient et Afrique)

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Algérie	Permis de conduire	رخصة القيادة	Recto, verso	Latin
Algérie	Carte d'identité	Carte nationale d'identité, بطاقة الهوية الوطني	Recto, verso	Latin
Algérie	Passeport papier	جواز السفر, Passeport	Page de données biométriques	Latin
Bahreïn	Carte d'identité	بطاقة الهوية, CPR Card	Recto, verso	Latin
Botswana	Carte d'identité	Omang	Recto, verso	Latin
Burkina Faso	Carte d'identité	Carte Nationale d'Identité Burkinabè (CNIB)	Recto, verso	Latin
Cameroun	Carte d'identité	Carte Nationale d'Identité (CNI)	Recto, verso	Latin
République démocratique du Congo	Permis de conduire[BÊTA]	Permis de conduire (CONADEP)	Recto, verso	Latin
Egypte	Permis de conduire[BÊTA]	رخصة القيادة	Recto, verso	Latin
Egypte	Carte d'identité	بطاقة تحقيق الشخصية	Recto, verso	Arabe, Latin
Egypte	Passeport papier[BÊTA]	جواز سفر	Page de données biométriques	Latin
Eswatini	Passeport papier		Page de données biométriques	Latin
Ghana	Permis de conduire		Recto	Latin
Ghana	Carte d'identité	Ghana Card	Recto, verso	Latin
Ghana	Passeport papier		Page de données biométriques	Latin
Iran	Passeport papier[BÊTA]	گذرنامه	Page de données biométriques	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Iraq	Carte d'identité	بطاقة الوطنية, بطاقة الهوية	Recto, verso	Latin
Iraq	Passeport papier[BÊTA]	جواز سفر, پاسپورت	Page de données biométriques	Latin
Israël	Permis de conduire	רישיון נהיגה	Recto	Latin
Israël	Carte d'identité	Tehudat Zehut, بطاقة هوية, תעודת זהות	Recto, verso	Latin
Israël	Passeport papier[BÊTA]	דרכון	Page de données biométriques	Latin
Côte d'Ivoire	Permis de conduire	Permis de conduire	Recto	Latin
Côte d'Ivoire	Carte d'identité	Carte Nationale d'Identité (CNI)	Recto, verso	Latin
Jordanie	Permis de conduire[BÊTA]	رخصة القيادة	Recto	Latin
Jordanie	Carte d'identité	بطاقة شخصية	Recto, verso	Arabe, Latin
Jordanie	Passeport papier[BÊTA]	جواز سفر	Page de données biométriques	Latin
Kenya	Carte d'identité	Kitambulisho	Recto, verso	Latin
Kenya	Passeport en polycarbonate	Passport, Pasi	Page de données biométriques	Latin
Koweït	Permis de conduire	رخصة القيادة	Recto, verso	Latin
Koweït	Carte d'identité	بطاقة المدنية	Recto, verso	Latin
Koweït	ID de résident	بطاقة المدنية	Recto, verso	Latin
Liban	Carte d'identité	بطاقة الهوية	Recto, verso	Latin
Libye	Passeport en polycarbonate	جواز سفر	Page de données biométriques	Latin
Ile Maurice	Carte d'identité		Recto, verso	Latin
Maroc	Permis de conduire	Permis de conduire, رخصة القيادة	Recto, verso	Latin
Maroc	Carte d'identité	Carte nationale d'identité, بطاقة التعريف الوطنية	Recto, verso	Latin
Maroc	Passeport papier[BÊTA]	Passeport, جواز سفر	Page de données biométriques	Latin
Mozambique	Permis de conduire[BÊTA]	Carta de Condução	Recto	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Mozambique	Carte d'identité	Bilhete de Identidade (BI)	Recto, verso	Latin
Nigeria	Permis de conduire		Recto, verso	Latin
Nigeria	Carte d'identité	e-ID card	Recto, verso	Latin
Nigeria	Passeport papier		Page de données biométriques	Latin
Nigeria	Passeport en polycarbonate[BÊTA]		Page de données biométriques	Latin
Nigeria	Carte d'électeur	Permanent Voter Card (PVC)	Recto, verso	Latin
Oman	Permis de conduire[BÊTA]	رخصة قيادة مركبة	Recto, verso	Latin
Oman	Carte d'identité	بطاقة الهوية	Recto, verso	Latin
Oman	ID de résident	بطاقة مقيم	Recto, verso	Latin
Qatar	Permis de conduire	رخصة القيادة	Recto	Latin
Qatar	Carte d'identité[BÊTA]	بطاقة إثبات شخصية	Recto	Latin
Qatar	Passeport papier	جواز سفر	Page de données biométriques	Latin
Qatar	Permis de séjour	تصريح الإقامة	Recto, verso	Latin
Rwanda	Carte d'identité	Indangamuntu	Recto	Latin
Arabie Saoudite	Permis de conduire	رخصة قيادة	Recto	Latin
Arabie Saoudite	Carte d'identité	بطاقة الأحوال المدنية	Recto, verso	Latin
Arabie Saoudite	Passeport papier	جواز سفر	Page de données biométriques	Latin
Arabie Saoudite	ID de résident	Iqama, هوية المقيم	Recto	Latin
Sénégal	Carte d'identité	Carte d'identité biométrique CEDEAO, Carte nationale d'identité	Recto, verso	Latin
Afrique du Sud	Permis de conduire	Bestuurslisensie	Recto	Latin
Afrique du Sud	Carte d'identité	Smart ID card	Recto, verso	Latin
Afrique du Sud	Carte d'identité[BÊTA]	Livret d'identité à code-barres vert	Recto, vertical	Latin
Afrique du Sud	Passeport en polycarbonate	Passeport	Page de données biométriques	Latin
Soudan	Passeport en polycarbonate	جواز سفر	Page de données biométriques	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Syrie	Passeport papier	جواز سفر	Page de données biométriques	Latin
Tanzanie	Permis de conduire	Leseni ya udereva	Recto	Latin
Tanzanie	Carte d'identité[BÊTA]	Kitambulisho cha Taifa, NIDA	Recto, verso	Latin
Tanzanie	Carte d'électeur[BÊTA]	Kadi ya mpiga kura, Voter Card	Recto	Latin
Togo	Carte d'identité	Permis de conduire	Recto, verso	Latin
Tunisie	Permis de conduire	رخصة قيادة	Recto	Latin
Tunisie	Carte d'identité	بطاقة التعريف الوطنية	Recto	Latin
Tunisie	Passeport papier	جواز سفر	Page de données biométriques	Latin
Turquie	Permis de conduire	Sürücü belgesi	Recto	Latin
Turquie	Carte d'identité	Kimlik Kartı	Recto, verso	Latin
Turquie	Passeport papier	Pasaport	Page de données biométriques	Latin
Turquie	Permis de séjour[BÊTA]	İkamet İzni	Recto, verso	Latin
Turquie	Passeport en polycarbonate	Pasaport	Page de données biométriques	Latin
Émirats arabes unis	Permis de conduire	رخصة القيادة	Recto, verso	Latin
Émirats arabes unis	Carte d'identité	بطاقة الهوية	Recto, verso	Arabe, Latin
Émirats arabes unis	Passeport papier	جواز سفر	Page de données biométriques	Arabe, Latin
Émirats arabes unis	ID de résident	بطاقة الهوية الوطنية	Recto, verso	Arabe, Latin
Ouganda	Permis de conduire		Recto	Latin
Ouganda	Carte d'identité		Recto, verso	Latin
Zimbabwe	Carte d'identité	National registration card (NRC)	Recto, verso	Latin
Zimbabwe	Passeport papier		Page de données biométriques	Latin

Pièces d'identité prises en charge (Amérique du Nord)

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Bermudes	Permis de conduire[BÊTA]		Recto	Latin
Canada	Certificat de citoyenneté[BÊTA]	Canada citizenship card, Carte de citoyenneté canadienne	Recto, verso	Latin
Canada	Passeport papier	Passport, Passeport	Page de données biométriques	Latin
Canada	Permis de séjour	Permanent residence (PR) card, Carte de résident permanent	Recto, verso	Latin
Canada	Carte de sécurité sociale[BÊTA]	Social insurance card (SIN card), Carte d'assurance sociale (Carte de NAS)	Recto	Latin
Canada	Pièce d'identité tribale	Certificate of Indian Status, Certificat de statut Indien	Recto, verso	Latin
Canada	Permis de port d'armes	Possesion and Aquisition License (PAL), Permis de possession et d'acquisition	Recto	Latin
Canada, Alberta	Permis de conduire		Recto, verso	Latin
Canada, Alberta	Carte d'identité		Recto, verso	Latin
Canada, Colombie-Britannique	Permis de conduire		Recto, verso	Latin
Canada, Colombie-Britannique	Permis de conduire, carte de services publics (combinés)		Recto, verso	Latin
Canada, Colombie-Britannique	Carte d'identité		Recto, verso	Latin
Canada, Colombie-Britannique	Minors Public Services Card		Recto, verso	Latin
Canada, Colombie-Britannique	Carte des services publics		Recto, verso	Latin
Canada, Manitoba	Permis de conduire		Recto, verso	Latin
Canada, Manitoba	Carte d'identité		Recto, verso	Latin
Canada, Nouveau-Brunswick	Permis de conduire	Permis de conduire	Recto, verso	Latin
Canada, Terre-Neuve et Labrador	Permis de conduire		Recto, verso	Latin
Canada, Nouvelle Écosse	Permis de conduire		Recto, verso	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Canada, Nouvelle Écosse	Carte d'identité[BÊTA]		Recto, verso	Latin
Canada, Nouvelle Écosse	Permis de conduire		Recto, verso	Latin
Canada, Nouvelle Écosse	Carte d'identité[BÊTA]		Recto, verso	Latin
Canada, Ontario	Permis de conduire		Recto, verso	Latin
Canada, Ontario	Carte d'identité	Carte photo	Recto, verso	Latin
Canada, Québec	Permis de conduire	Permis de conduire	Recto, verso	Latin
Canada, Saskatchewan	Permis de conduire		Recto, verso	Latin
Canada, Saskatchewan	Carte d'identité[BÊTA]		Recto, verso	Latin
Canada, Yukon	Permis de conduire	Permis de conduire	Recto, verso	Latin
USA	Border Crossing Card	BCC	Recto, verso	Latin
USA	Global Entry Card		Recto, verso	Latin
USA	Green Card	Carte de résident permanent	Recto, verso	Latin
USA	Pièce d'identité militaire	Common Access Card (CAC)	Recto, verso, vertical	Latin
USA	Nexus Card[BETA]		Recto, verso	Latin
USA	Passeport papier		Page de données biométriques	Latin
USA	Carte passeport		Recto, verso	Latin
USA	Passeport en polycarbonate		Page de données biométriques	Latin
USA	Carte de sécurité sociale[BÊTA]		Recto	Latin
USA	Carte d'ancien combattant	VIC	Recto	Latin
USA	Permis de travail	Employment authorization document, EAD Card	Recto, verso	Latin
USA, Alabama	Permis de conduire		Recto, verso, vertical	Latin
USA, Alabama	Carte d'identité		Recto, verso, vertical	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
USA, Alaska	Permis de conduire		Recto, verso	Latin
USA, Alaska	Carte d'identité		Recto, verso	Latin
USA, Arizona	Permis de conduire		Recto, verso, vertical	Latin
USA, Arizona	Carte d'identité		Recto, verso, vertical	Latin
USA, Arkansas	Permis de conduire		Recto, verso, vertical	Latin
USA, Arkansas	Carte d'identité		Recto, verso, vertical	Latin
USA, Californie	Permis de conduire		Recto, verso, vertical	Latin
USA, Californie	Carte d'identité		Recto, verso, vertical	Latin
USA, Colorado	Permis de conduire		Recto, verso, vertical	Latin
USA, Colorado	Carte d'identité		Recto, verso	Latin
USA, Connecticut	Permis de conduire		Recto, verso, vertical	Latin
USA, Connecticut	Carte d'identité		Recto, verso	Latin
USA, Delaware	Permis de conduire		Recto, verso, vertical	Latin
USA, District of Columbia	Permis de conduire		Recto, verso, vertical	Latin
USA, District of Columbia	Carte d'identité		Recto, verso, vertical	Latin
USA, Floride	Permis de conduire		Recto, verso, vertical	Latin
USA, Floride	Carte d'identité		Recto, verso, vertical	Latin
USA, Georgie	Permis de conduire		Recto, verso, vertical	Latin
USA, Georgie	Carte d'identité		Recto, verso, vertical	Latin
USA, Hawaii	Permis de conduire		Recto, verso, vertical	Latin
USA, Hawaii	Carte d'identité		Recto, verso	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
USA, Idaho	Permis de conduire		Recto, verso, vertical	Latin
USA, Idaho	Carte d'identité		Recto, verso	Latin
USA, Illinois	Permis de conduire		Recto, verso, vertical	Latin
USA, Illinois	Carte d'identité		Recto, verso, vertical	Latin
USA, Indiana	Permis de conduire		Recto, verso	Latin
USA, Indiana	Carte d'identité		Recto, verso	Latin
USA, Iowa	Permis de conduire		Recto, verso, vertical	Latin
USA, Iowa	Carte d'identité		Recto, verso, vertical	Latin
USA, Kansas	Permis de conduire		Recto, verso, vertical	Latin
USA, Kansas	Carte d'identité		Recto, verso, vertical	Latin
USA, Kentucky	Permis de conduire		Recto, verso, vertical	Latin
USA, Kentucky	Carte d'identité		Recto, verso, vertical	Latin
USA, Louisiane	Permis de conduire		Recto, verso	Latin
USA, Maine	Permis de conduire		Recto, verso, vertical	Latin
USA, Maine	Carte d'identité		Recto, verso	Latin
USA, Maryland	Permis de conduire		Recto, verso, vertical	Latin
USA, Maryland	Carte d'identité		Recto, verso, vertical	Latin
USA, Massachusetts	Permis de conduire		Recto, verso, vertical	Latin
USA, Massachusetts	Carte d'identité		Recto, verso, vertical	Latin
USA, Michigan	Permis de conduire		Recto, verso, vertical	Latin
USA, Michigan	Carte d'identité		Recto, verso, vertical	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
USA, Minnesota	Permis de conduire		Recto, verso, vertical	Latin
USA, Minnesota	Carte d'identité		Recto, verso, vertical	Latin
USA, Missouri	Permis de conduire		Recto, verso, vertical	Latin
USA, Missouri	Carte d'identité		Recto, verso, vertical	Latin
USA, Montana	Permis de conduire		Recto, verso	Latin
USA, Montana	Carte d'identité		Recto, verso	Latin
USA, Nebraska	Permis de conduire		Recto, verso, vertical	Latin
USA, Nebraska	Carte d'identité		Recto, verso	Latin
USA, Nevada	Permis de conduire		Recto, verso, vertical	Latin
USA, Nevada	Carte d'identité		Recto, verso, vertical	Latin
USA, New Hampshire	Permis de conduire		Recto, verso, vertical	Latin
USA, New Hampshire	Carte d'identité[BÊTA]		Recto, verso	Latin
USA, New Jersey	Permis de conduire		Recto, verso, vertical	Latin
USA, New Jersey	Carte d'identité		Recto, verso, vertical	Latin
USA, Nouveau Mexique	Permis de conduire		Recto, verso, vertical	Latin
USA, Nouveau Mexique	Carte d'identité		Recto, verso	Latin
USA, New York	Permis de conduire		Recto, verso, vertical	Latin
USA, New York	Carte d'identité		Recto, verso, vertical	Latin
USA, New York City	Carte d'identité		Recto, verso	Latin
USA, Caroline du Nord	Permis de conduire		Recto, verso, vertical	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
USA, Caroline du Nord	Carte d'identité		Recto, verso, vertical	Latin
USA, Dakota du Nord	Permis de conduire		Recto, verso, vertical	Latin
USA, Dakota du Nord	Carte d'identité[BÊTA]		Recto, verso	Latin
USA, Ohio	Permis de conduire		Recto, verso, vertical	Latin
USA, Ohio	Carte d'identité		Recto, verso, vertical	Latin
USA, Oklahoma	Permis de conduire		Recto, verso, vertical	Latin
USA, Oklahoma	Carte d'identité		Recto, verso, vertical	Latin
USA, Oregon	Permis de conduire		Recto, verso, vertical	Latin
USA, Oregon	Carte d'identité		Recto, verso	Latin
USA, Pennsylvanie	Permis de conduire		Recto, verso, vertical	Latin
USA, Pennsylvanie	Carte d'identité		Recto, verso, vertical	Latin
USA, Rhode Island	Permis de conduire		Recto, verso, vertical	Latin
USA, Rhode Island	Carte d'identité		Recto, verso	Latin
USA, Caroline du Sud	Permis de conduire		Recto, verso, vertical	Latin
USA, Caroline du Sud	Carte d'identité		Recto, verso, vertical	Latin
USA, Dakota du Sud	Permis de conduire		Recto, verso, vertical	Latin
USA, Dakota du Sud	Carte d'identité[BÊTA]		Recto, verso	Latin
USA Tennessee	Permis de conduire		Recto, verso, vertical	Latin
USA Tennessee	Carte d'identité		Recto, verso, vertical	Latin
USA, Texas	Permis de conduire		Recto, verso, vertical	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
USA, Texas	Carte d'identité		Recto, verso, vertical	Latin
USA, Texas	Permis de port d'armes	License to Carry a Handgun (LTC)	Recto	Latin
USA, Utah	Permis de conduire		Recto, verso, vertical	Latin
USA, Utah	Carte d'identité		Recto, verso, vertical	Latin
USA, Vermont	Permis de conduire		Recto, verso	Latin
USA, Virginie	Permis de conduire		Recto, verso, vertical	Latin
USA, Virginie	Carte d'identité		Recto, verso	Latin
USA, Washington	Permis de conduire		Recto, verso, vertical	Latin
USA, Washington	Carte d'identité		Recto, verso, vertical	Latin
USA, Virginie-Occidentale	Permis de conduire		Recto, verso	Latin
USA, Wisconsin	Permis de conduire		Recto, verso, vertical	Latin
USA, Wisconsin	Carte d'identité		Recto, verso	Latin
USA, Wyoming	Permis de conduire		Recto, verso	Latin
USA, Wyoming	Carte d'identité		Recto, verso	Latin

Pièces d'identité prises en charge (Océanie)

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Australie	Passeport papier		Page de données biométriques	Latin
Australie, Territoire de la capitale australienne	Permis de conduire		Recto	Latin
Australie, Nouvelle-Galles-du-Sud	Permis de conduire		Recto	Latin
Australie, Nouvelle-Galles-du-Sud	Carte d'identité		Recto	Latin

Pays ou région	Type de document	Nom de document localisé	Côté et orientation pris en charge	Alphabets pris en charge
Australie, Territoire du Nord	Permis de conduire[BÊTA]		Recto, verso	Latin
Australie, Territoire du Nord	Carte de preuve de majorité	NT Evidence of age card	Recto, verso	Latin
Australie, Queensland	Permis de conduire		Recto, verso	Latin
Australie, Australie-Méridionale	Permis de conduire		Recto, verso	Latin
Australie, Australie-Méridionale	Carte de preuve de majorité		Recto	Latin
Australie, Tasmanie	Permis de conduire		Recto, verso	Latin
Australie, Victoria	Permis de conduire		Recto, verso	Latin
Australie, Victoria	Carte de preuve de majorité		Recto	Latin
Australie, Australie-Occidentale	Permis de conduire		Recto, verso	Latin
Nouvelle-Zélande	Permis de conduire		Recto	Latin
Nouvelle-Zélande	Passeport en polycarbonate	Uruwhenua	Page de données biométriques	Latin

Rubriques connexes

À propos de ClearID Self-Service Kiosk, page 578

14

Dépannage

Résolvez les problèmes courants.

Cette section aborde les sujets suivants:

- "Module externe installé mais manquant dans Security Desk et Config Tool", page 676
- "Le rôle module externe ne trouve pas de fichier avec certificat", page 677
- "Les champs personnalisés ne sont pas affichés dans Security Desk", page 678
- "Aucun compte actif trouvé pour l'utilisateur", page 681
- "Notification de visite par e-mail non reçue par les visiteurs", page 682
- "Les champs Hôtes de visiteurs sont vides dans Security Desk.", page 683
- " Problèmes de connectivité (One Identity Synchronization Tool) ", page 685
- " Problèmes de synchronisation des données (One Identity Synchronization Tool) ", page 686
- " Problèmes de la borne en libre-service ", page 688
- " Problèmes d'impression d'étiquettes de la borne en libre-service ", page 691

Module externe installé mais manquant dans Security Desk et Config Tool

Si l'onglet **Propriétés** du module externe est manquant, ce dernier n'est pas installé sur votre machine locale. Le module externe doit être installé sur un serveur Genetec[MC] (principal ou secondaire).

Pour vous aider à résoudre ce problème, reportez-vous aux causes possibles et leurs solutions respectives.

Symptômes possibles :

- Dans Config Tool, vous pouvez voir le module externe dans la tâche **Modules externes**, et vous pouvez ajouter un nouveau rôle module externe, mais le nouveau rôle est manquant dans l'onglet **Propriétés**.
- Dans Security Desk, le module externe n'apparaît pas sur la page *Options*.

Description de la cause : le module externe n'est pas installé sur l'ordinateur local, la licence (le certificat) est non valable ou vous n'avez pas les privilèges utilisateur requis.

Solution 1 : **installez le module externe en local sur votre ordinateur.**

Solution 2 : vérifiez que le module externe est installé sur un serveur Genetec[MC] et que le rôle a été créé et configuré correctement.

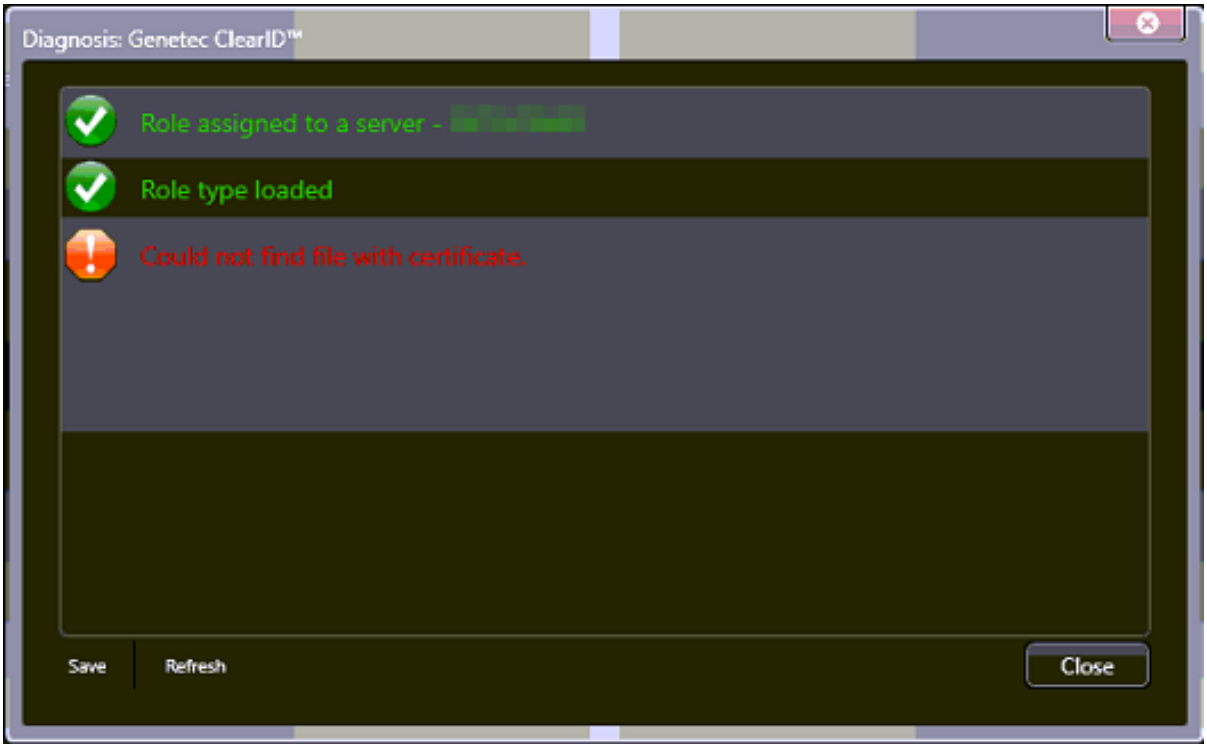
Solution 3 : vérifiez que le module externe est installé sur votre ordinateur Security Center : sur la page d'accueil de Security Desk ou Config Tool, cliquez sur **À propos** > **Composants installés** et cherchez l'entrée *Genetec.Iams.SCPlugin.Client* dans la liste.

Solution 4 : vérifiez que votre système dispose d'une licence (un certificat) pour le module externe : sur la page d'accueil de Security Desk ou Config Tool, cliquez sur **À propos** > **Certificats**, cherchez le nom du module externe dans la liste, puis vérifiez que les autorisations d'accès sont réglées sur **Illimité** ou sur une valeur correspondant au nombre de licences.

Le rôle module externe ne trouve pas de fichier avec certificat

À l'ajout du rôle module externe Genetec ClearID[MC], le rôle refuse de démarrer et affiche le message d'erreur Fichier avec certificat introuvable.

Dans Config Tool, dans la section *Rôles* de la tâche *Système*, le message d'erreur suivant est affiché dans la boîte de dialogue Diagnostic.



Cause

La licence CD-SC-PLUGIN est manquante sur ce système (GSC n'a pas la référence de licence pour ClearID).

Solution

Vérifiez que le rôle module externe est configuré correctement avec la bonne référence de licence.

1. Dans Config Tool, cliquez sur **À propos** > **Certificats** et recherchez `ClearID`.
2. Si le certificat ClearID est introuvable, ajoutez la référence CD-SC-PLUGIN à la licence, appliquez la licence au système, puis redémarrez le système.

Les champs personnalisés ne sont pas affichés dans Security Desk

Si les champs personnalisés ne sont pas affichés dans Security Desk, vérifiez les privilèges utilisateur et que l'utilisateur ou le groupe d'utilisateurs pertinent est configuré pour le champ personnalisé.

Pour résoudre le problème, découvrez les causes possibles et leurs solutions respectives.

Privilèges utilisateur incorrects

Description de la cause : aucun champ personnalisé n'est affiché, car l'utilisateur ne dispose pas des privilèges requis.

Solution : ajoutez les privilèges requis.

1. Sur la page d'accueil de Config Tool, ouvrez la tâche *Gestion des utilisateurs*.
2. Sélectionnez l'utilisateur pertinent, puis cliquez sur l'onglet **Privilèges**.
3. Définissez les privilèges suivants sur **Autoriser** :
   - **Privilèges d'application** > **Security Desk**
   - **Privilèges d'application** > **Config Tool**
   - **Privilèges administratifs** > **Gestion du système** > **Afficher les propriétés de rôle**
   - **Privilèges administratifs** > **Gestion du système** > **Afficher les propriétés de serveur**
   - **Privilèges des tâches** > **Administration** > **Modules externes**
4. (Facultatif) Définissez les privilèges de champ personnalisé dont vous avez besoin sur **Autoriser**.
   - **Privilèges administratifs** > **Gestion du contrôle d'accès** > **Afficher les propriétés du groupe de titulaires de carte** > **Modifier les propriétés du groupe de titulaires de carte** > **Modifier les champs personnalisés**
   - **Privilèges administratifs** > **Gestion du contrôle d'accès** > **Afficher les propriétés du titulaire de carte** > **Modifier les propriétés du titulaire de carte** > **Modifier les champs personnalisés**
   - **Privilèges administratifs** > **Gestion du contrôle d'accès** > **Afficher les propriétés des identifiants** > **Modifier les propriétés des identifiants** > **Modifier les champs personnalisés**
   - **Privilèges administratifs** > **Gestion du contrôle d'accès** > **Afficher les propriétés des visiteurs** > **Modifier les propriétés des visiteurs** > **Modifier les champs personnalisés**
   - **Privilèges administratifs** > **Gestion du système** > **Afficher les paramètres généraux** > **Modifier les définitions de champs personnalisés**
5.

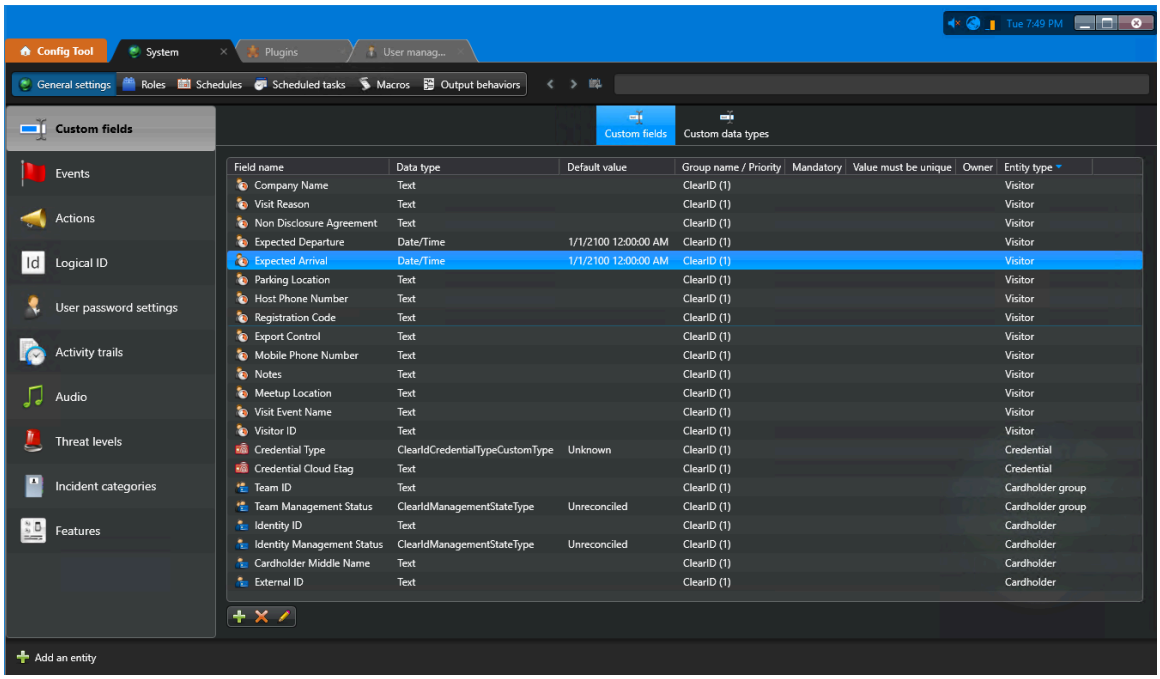
Champ personnalisé non configuré pour l'utilisateur ou le groupe d'utilisateurs

Description de la cause : l'affichage du champ personnalisé n'a pas été configuré pour l'utilisateur ou le groupe d'utilisateurs.

Solution : configurez l'affichage du champ personnalisé pour l'utilisateur ou le groupe d'utilisateurs.

1. Sur la page d'accueil de Config Tool, ouvrez la tâche *Système*.
2. Cliquez sur **Paramètres généraux** > **Champs personnalisés**.

3. Sélectionnez le champ personnalisé que l'utilisateur ne parvient pas à afficher. Par exemple, **Arrivée prévue**.



4. Cliquez sur **Modifier l'élément** ( ) pour modifier les paramètres du champ personnalisés.
5. Dans la section *Sécurité* de la boîte de dialogue *Modifier le champ personnalisé*, cliquez sur **Ajouter un élément** ( ).

6. Sélectionnez un utilisateur ou un groupe d'utilisateurs dans la liste et cliquez sur **OK**.

   Dans l'exemple suivant, nous avons configuré le champ personnalisé *Arrivée prévue* afin qu'il soit visible pour le groupe d'utilisateurs *Réceptionnistes Genetec*.

7. Cliquez sur **Enregistrer et fermer**, puis sur **Appliquer**.

Rubriques connexes

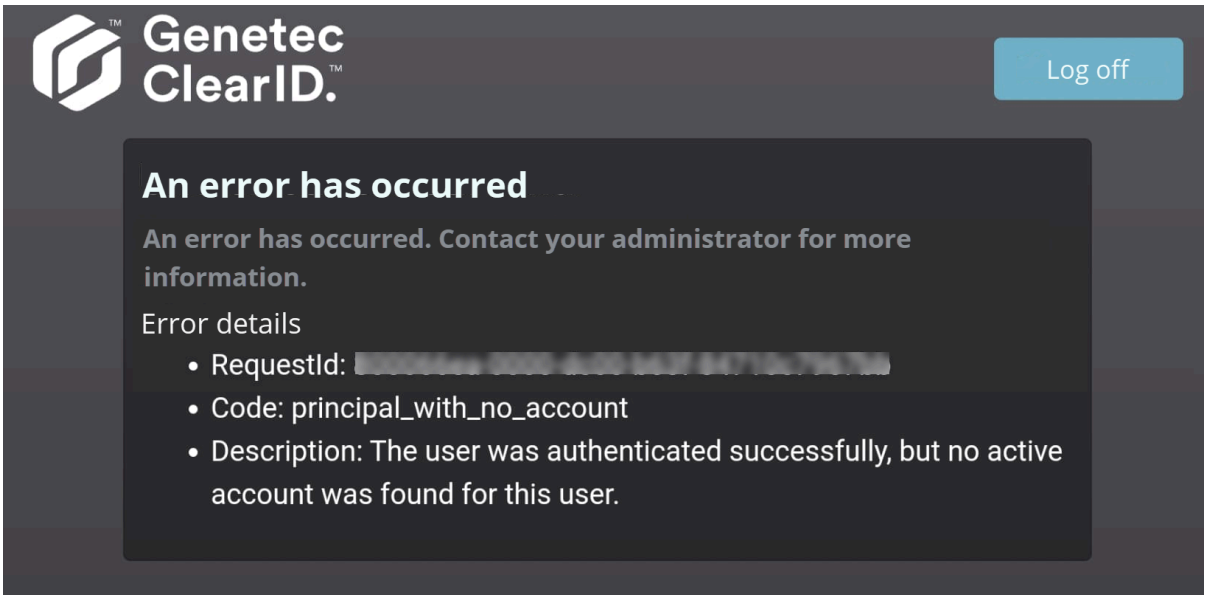
Accorder des privilèges utilisateur, page 101
À propos des champs personnalisés, page 103

Aucun compte actif trouvé pour l’utilisateur

Si aucun compte actif n’a été trouvé pour l’utilisateur lors de la connexion par authentification unique (SSO), utilisez une autre identité, ou accordez l'accès au portail Web Genetec ClearID[MC].

Cause

Utilisateur authentifié avec succès, mais aucun compte actif trouvé pour l’utilisateur.



L’identité associée à l’e-mail utilisé pour se connecter n’a pas accès au portail Web.

Solution

Accordez l’accès au portail Web à l’utilisateur.

Notification de visite par e-mail non reçue par les visiteurs

Si les visiteurs ne reçoivent pas les notifications par e-mail, vérifiez que la demande de visite d'un événement ou d'un secteur a été approuvée.

Pour résoudre le problème, découvrez les causes possibles et leurs solutions respectives.

Cause

Les e-mails de notification ne sont pas reçus parce que la demande de visite d'un événement ou d'un secteur n’a pas été approuvée.

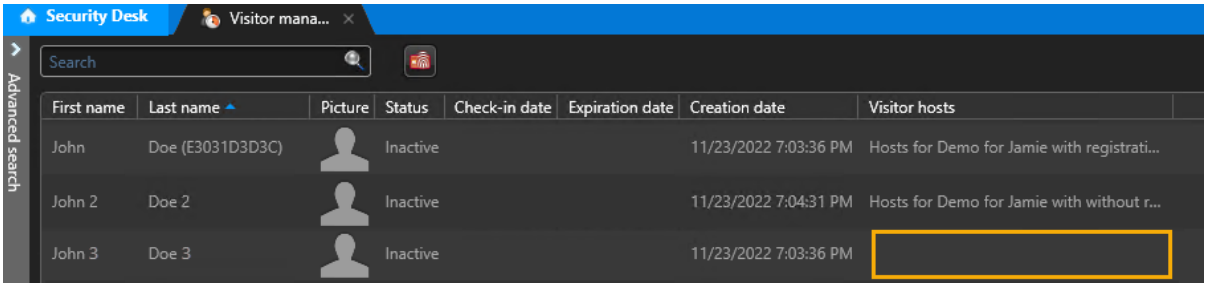
Solution

Consultez les demandes de visite d'un événement ou d'un secteur pour identifier la demande en attente d’approbation :

1. Approuvez les demandes d'accès à un secteur.
2. Approuvez les événements de visite.

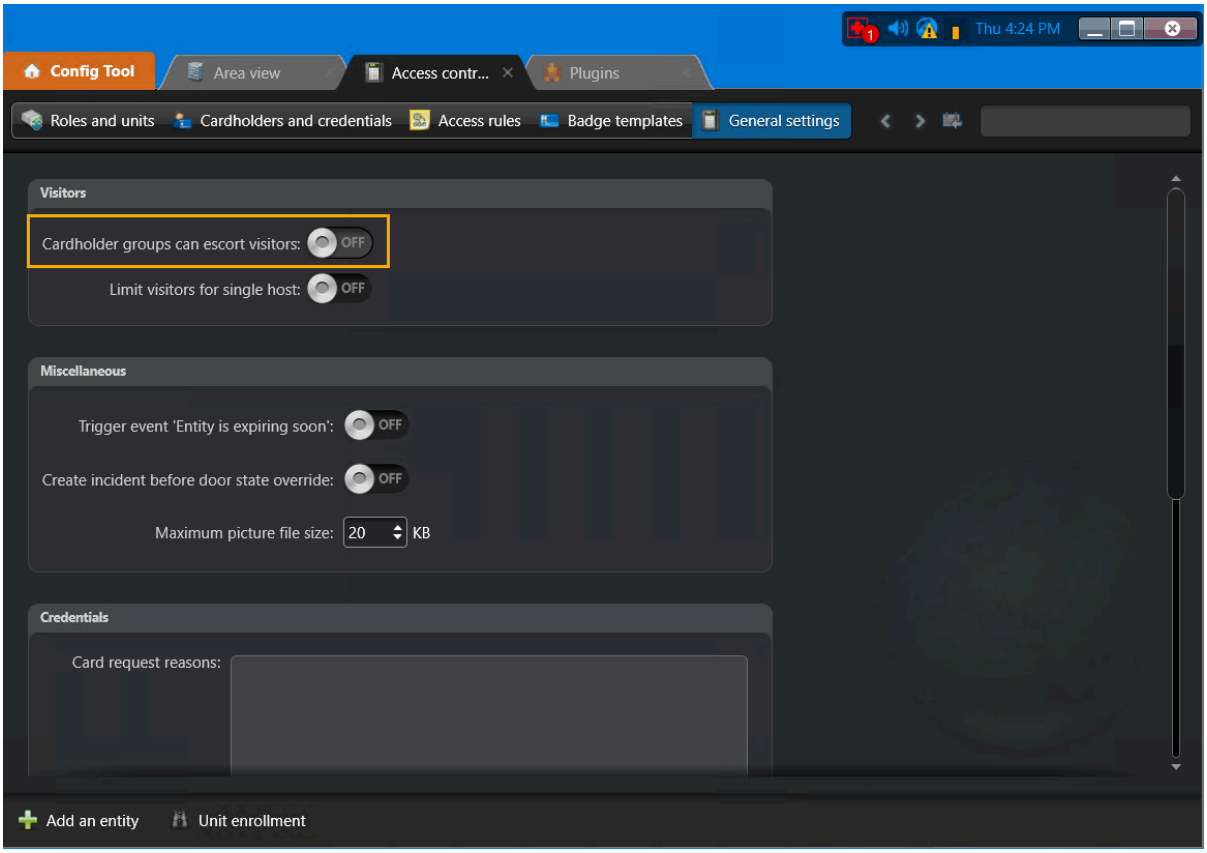
Les champs Hôtes de visiteurs sont vides dans Security Desk.

Si les champs **Hôtes de visiteurs** dans Security Desk sont vides, cela peut indiquer que le réglage **Les titulaires de cartes peuvent escorter les visiteurs** n'est pas configuré correctement pour Genetec ClearID[MC].



Cause

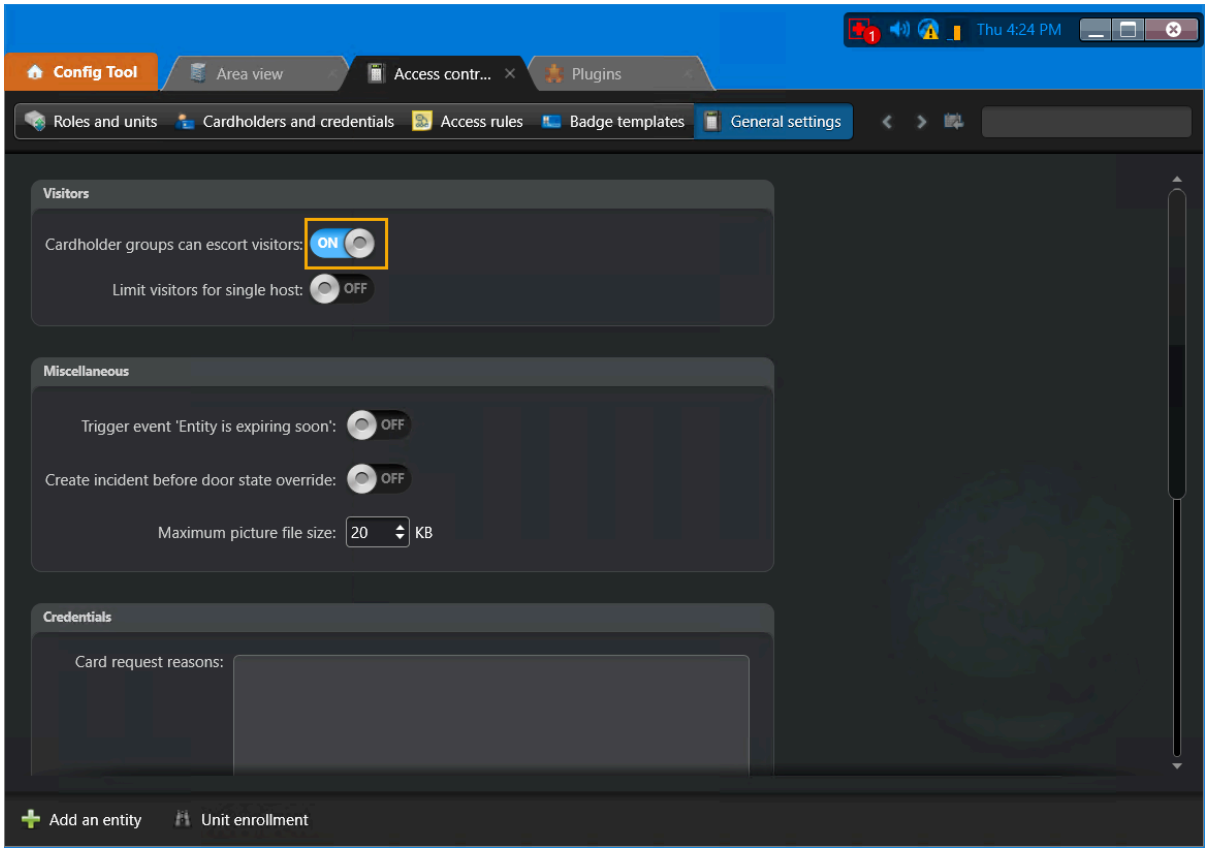
Dans la section *Visiteurs* de la tâche *Contrôle d'accès*, le réglage **Les groupes titulaires de cartes peuvent escorter les visiteurs** dans Config Tool est peut-être désactivé.



Solution

Dans la section *Visiteurs* de la tâche *Contrôle d'accès*, vérifiez que le paramètre **Groupes de titulaires de carte pouvant escorter les visiteurs** est activé (ON).

1. Sur la page d'accueil de Config Tool, ouvrez la tâche *Contrôle d'accès*.
2. Cliquez sur **Paramètres généraux**.
3. Cliquez ou faites glisser l'option **Les groupes de titulaires de carte peuvent escorter les visiteurs** sur la position **ON**.



4. (Facultatif) Dans ClearID, créez une demande de visite pour vérifier que l'option fonctionne comme prévu.
5. (Facultatif) Dans Security Desk, vérifiez que le champ **Hôtes de visiteurs** contient des informations sur les hôtes.

Problèmes de connectivité (One Identity Synchronization Tool)

Si vous rencontrez des problèmes de connectivité à l'utilisation de Genetec ClearID[MC] One Identity Synchronization Tool, examinez votre intégration API ou les réglages de connexion de l'application à Azure AD.

Pour résoudre le problème, découvrez les causes possibles et leurs solutions respectives.

Connexion impossible à Genetec ClearID[MC].

Description : L'outil de synchronisation ne parvient pas à se connecter à ClearID.

Solution : Consultez les journaux One Identity *ConfigurationTool*.

1. Cliquez sur , puis cliquez sur **Ouvrir le dossier de journalisation**.

   CONSEIL : Vous pouvez également ouvrir les journaux *ConfigurationTool* manuellement à l'emplacement suivant :

   %ProgramData%\Genetec\OneIdentity\Logs\ConfigurationTool

2. Recherchez des messages associés aux problèmes de connexion à ClearID dans les journaux *ConfigurationTool* de One Identity.
3. Vérifiez votre connexion d'intégration API.
   a. Cliquez sur **Administration** > **Automatisation** et sélectionnez votre intégration API.
   b. Vérifiez que votre clé d'intégration API et les détails de votre ID client soient corrects.
4. Vérifiez vos paramètres de connexion.

Impossible de se connecter à Azure AD

Description : L'outil de synchronisation ne parvient pas à se connecter à Azure Active Directory.

Solution : Consultez les journaux One Identity *ConfigurationTool*.

1. Cliquez sur , puis cliquez sur **Ouvrir le dossier de journalisation**.

   CONSEIL : Vous pouvez également ouvrir les journaux *ConfigurationTool* manuellement à l'emplacement suivant :

   %ProgramData%\Genetec\OneIdentity\Logs\ConfigurationTool

2. Recherchez des messages d'erreur liés aux problèmes de connectivité Azure AD dans les journaux One Identity *ConfigurationTool*.
3. Vérifiez vos informations de connexion à l'application Azure AD.

Rubriques connexes

Synchroniser les identités avec One Identity, page 518

Problèmes de synchronisation des données (One Identity Synchronization Tool)

Si vous rencontrez des problèmes de connectivité à l'utilisation de Genetec ClearID[MC] One Identity Synchronization Tool, consultez les journaux pour plus de détails. Pour résoudre le problème, découvrez les causes possibles et leurs solutions respectives.

Champs de données manquants

Description : des champs de données sont manquants.

Solution : consultez les journaux du *service* One Identity.

1. Cliquez sur , puis cliquez sur **Ouvrir le dossier de journalisation**.

   CONSEIL : Vous pouvez également ouvrir les journaux *ConfigurationTool* manuellement à l'emplacement suivant :

   ```
   %ProgramData%\Genetec\OneIdentity\Logs\Service
   ```

2. Recherchez des messages d'erreur liés aux champs de données manquants dans les journaux du *service* One Identity.

   Pour plus d'informations sur les champs d'attribut, consultez Champs d'attribut de l'outil de synchronisation One Identity.

3. Vérifiez vos autorisations d'API Azure AD.

Champs de nom manquants (prénom, nom)

Description : des champs de nom (prénom ou nom) sont manquants.

Solution : consultez les journaux du *service* One Identity.

1. Cliquez sur , puis cliquez sur **Ouvrir le dossier de journalisation**.

   CONSEIL : Vous pouvez également ouvrir les journaux *ConfigurationTool* manuellement à l'emplacement suivant :

   ```
   %ProgramData%\Genetec\OneIdentity\Logs\Service
   ```

2. Recherchez des messages d'erreur liés aux champs de nom dans les journaux du *service* One Identity.

   Pour plus d'informations sur les champs d'attribut, consultez Champs d'attribut de l'outil de synchronisation One Identity.

3. Vérifiez vos autorisations d'API Azure AD.

Adresses e-mail manquantes

Description : des champs d'adresse e-mail sont manquants.

Solution : consultez les journaux du *service* One Identity.

1. Cliquez sur , puis cliquez sur **Ouvrir le dossier de journalisation**.

   CONSEIL : Vous pouvez également ouvrir les journaux *ConfigurationTool* manuellement à l'emplacement suivant :

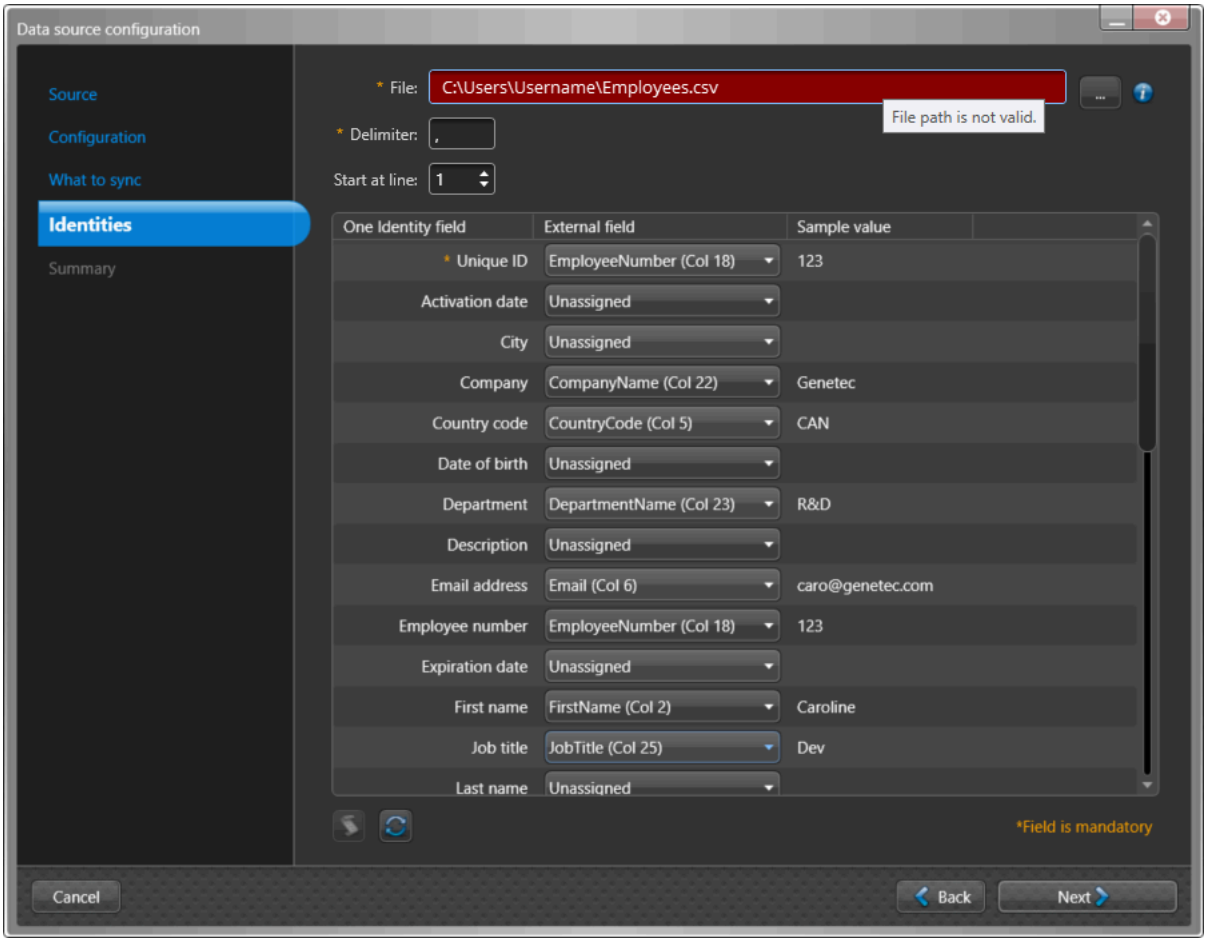
   ```
   %ProgramData%\Genetec\OneIdentity\Logs\Service
   ```

2. Recherchez des messages d'erreur liés aux champs d'adresse e-mail dans les journaux du *service* One Identity.

   Pour plus d'informations sur les champs d'attribut, consultez Champs d'attribut de l'outil de synchronisation One Identity.
3. Vérifiez vos autorisations d'API Azure AD.

Le chemin d'accès au fichier n'est pas valide

Description : Problèmes d'autorisation d'utilisateur lors de l'utilisation de fichiers CSV comme source de données pour des **Identités**, car le chemin d'accès au fichier n'est pas valable.



Solution :

BONNE PRATIQUE : Pour éviter les problèmes d'autorisation lorsque vous utilisez ClearID One Identity Synchronization Tool, enregistrez vos fichiers dans le dossier *C:* or *C:\temp*. N'enregistrez pas vos fichiers CSV dans un fichier ou un dossier contrôlé par l'utilisateur (dossier dans *C:\Users* ou sur le *bureau*) ou vous risquez de rencontrer des problèmes d'autorisation d'utilisateur de type Le chemin d'accès au fichier n'est pas valide.

Rubriques connexes

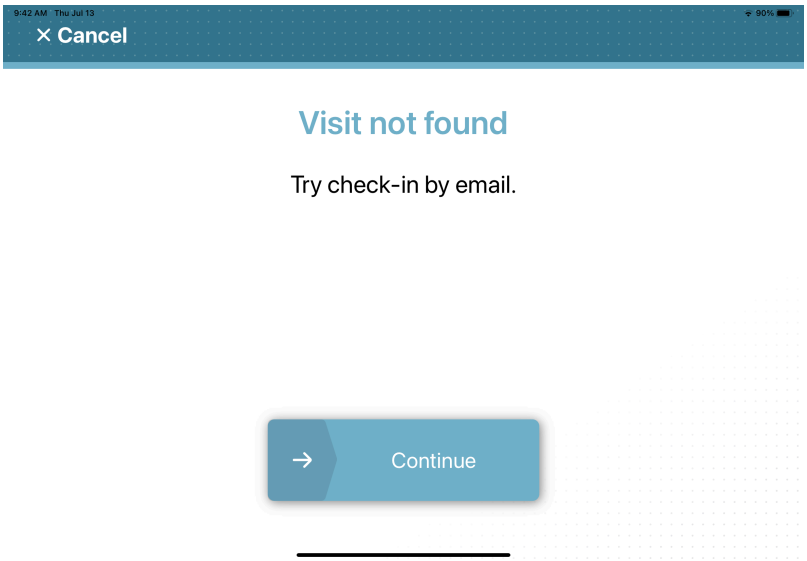
Synchroniser les identités avec One Identity, page 518

Problèmes de la borne en libre-service

Si la fonction d'inscription de Genetec ClearID[MC] Self-Service Kiosk ou si la borne ne fonctionne pas comme prévu, vous pouvez tenter des mesures de dépannage supplémentaires.

Invitation de visiteur ou événement de visite introuvable

Description : Vous ne voyez pas votre invitation de visiteur lors de l'inscription



L'erreur *visite introuvable* peut survenir pour différentes raisons :

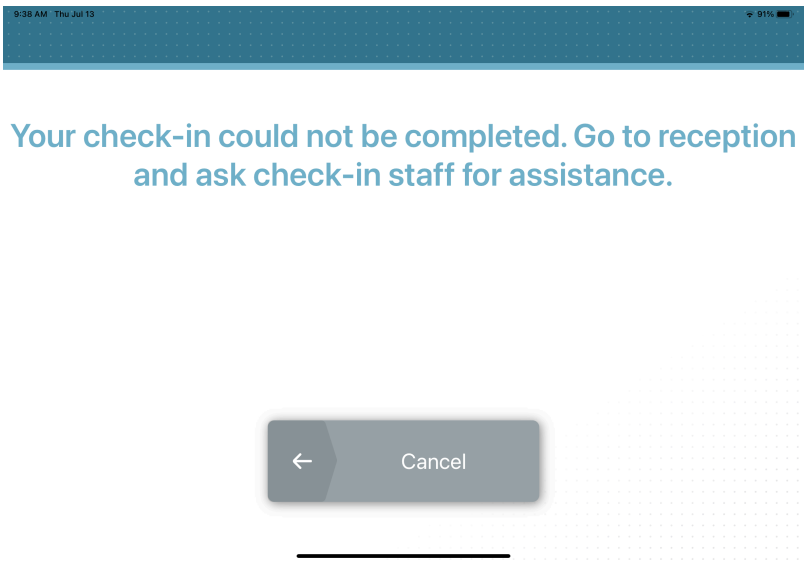
- Il est trop tôt pour l'inscription des visiteurs (plus d'une heure avant le début de l'événement).
- Il est trop tard pour l'inscription des visiteurs (plus d'une heure après la fin de l'événement).
- Le visiteur est absent de la liste des invitations.
- Le nom du visiteur dans l'invitation contient une erreur ou une coquille.

Solution :

- Vérifiez l'heure de début et de fin de l'événement de visite. Les visiteurs peuvent s'inscrire jusqu'à 1 heure avant le début ou la fin d'un événement de visite.
- Vérifiez le nom des visiteurs dans la liste de l'événement de visite. Recherchez les visiteurs qui ne figurent pas dans la liste ou des erreurs dans les informations sur les visiteurs.

Impossible de terminer l'inscription

Description : Vous n'avez pas pu terminer votre inscription.



Solution : Vérifiez les réglages de site et de secteurs. L'inscription automatique peut échouer pour l'une ou plusieurs des raisons suivantes :

1. La gestion des visiteurs n'est pas activée pour le site.
   a. Dans Genetec ClearID[MC], cliquez sur **Organisation** > **Sites**.
   b. Sélectionnez votre site et cliquez sur **Gestion des visiteurs**.
   c. Sélectionnez **Activer la gestion des visiteurs pour ce site**.
   d. Cliquez sur **Enregistrer**.
2. Les autorisations de gestion des visiteurs pour le site n'ont pas été configurées.
   a. Dans ClearID, cliquez sur **Organisation** > **Sites**.
   b. Sélectionnez votre site et cliquez sur **Gestion des visiteurs** > **Autorisations**.
   c. Vérifiez les autorisations d'identités
   d. Modifiez les autorisations selon vos besoins et cliquez sur **Enregistrer**.

      Par exemple, ajoutez des autorisations de rôle ou autorisez toutes les identités à inviter des visiteurs.
3. La gestion des visiteurs est activée pour le site, mais aucun secteur n'est spécifié, ou il n'y a pas de secteur par défaut.
   a. Dans ClearID, vérifiez que la gestion des visiteurs est activée pour le secteur. (**Secteurs** > **Sélectionner un secteur** > **Gestion des visiteurs**).
   b. Vérifiez que l'option **Ajouter automatiquement ce secteur lors de la création de demandes de visite** est activée.
4. La gestion des visiteurs est activée pour le site et au moins un secteur par défaut est présent sous ce site. Toutefois, l'hôte n'a pas l'autorisation d'inviter des visiteurs à ce site.
   a. Voir l'étape 2.
5. L'approbation obligatoire est activée pour le site. Le processus d'approbation d'événement de visite doit être réglé sur **Aucune approbation nécessaire**.
   a. Dans ClearID, cliquez sur **Organisation** > **Sites** et sélectionnez votre site.
   b. Cliquez sur **Gestion des visiteurs**, puis dans la section *Avancé*, vérifiez que l'option **Processus d'approbation d'événement de visiteur** est réglée sur **Aucune approbation nécessaire**.

Erreurs de caméras

Description : La borne en libre-service peut parfois rencontrer les problèmes de caméra suivants :

- Impossible d'initialiser la caméra avant.
- Une erreur est survenue pendant la configuration de la caméra. Veuillez réessayer.

Solution : Vérifiez les points suivants :

1. Sur l'iPad, touchez **Réglages**, naviguez jusqu'à l'application **Self-Service Kiosk**, puis touchez **Caméra** pour activer la caméra.
2. Sur l'iPad, touchez **Réglages** > **Confidentialité et sécurité**, puis vérifiez que **Self-Service Kiosk** a accès à la caméra.

CONSEIL : Ces réglages ne seront pas forcément visibles sur votre iPad si vous n'avez pas encore utilisé la fonction Scanner un code QR. Dans ce cas, vous pouvez essayer de procéder de la manière suivante : Touchez **S'inscrire** > **Code QR**, puis touchez **Annuler**, et réessayez les étapes précédentes.

Problèmes d'impression d'étiquettes de la borne en libre-service

Si l'imprimante d'étiquettes de Genetec ClearID[MC] Self-Service Kiosk ne fonctionne pas correctement, vous pouvez vérifier la configuration ou le matériel, ou effectuer d'autres tâches de dépannage.

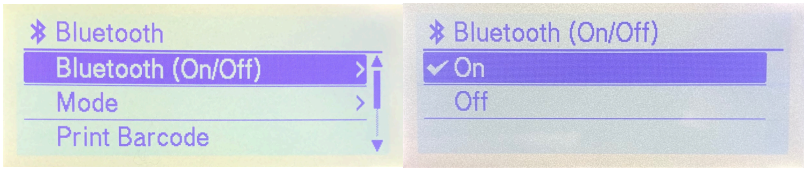
Pour vous aider à résoudre les problèmes d'impression d'étiquettes de la borne en libre-service, reportez-vous aux causes possibles et leurs solutions respectives.

Aucune imprimante d'étiquette Bluetooth détectée

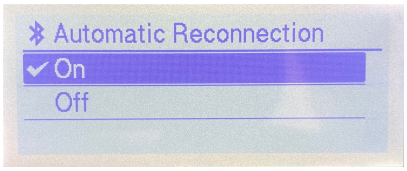
Description : Aucune imprimante d'étiquette Bluetooth n'a été détectée. Il peut s'agir d'un problème de configuration ou d'un problème matériel.

Solution :

1. Vérifiez que l'imprimante est allumée et prête à l'emploi.
2. Vérifiez que Bluetooth est activé sur l'imprimante d'étiquettes.
   a. Dans le menu **Réglages**, sélectionnez **Bluetooth** > **Bluetooth (On/Off)** > **On** et appuyez sur **OK**.



   b. Dans le menu **Réglages**, sélectionnez **Bluetooth** > **Automatic Reconnection (On/Off)** > **On** et appuyez sur **OK**.



3. Vérifiez que le Bluetooth est activé dans l'application mobile ClearID Self-Service Kiosk.
4. Vérifiez que Bluetooth est activé sur l'iPad.
5. Vérifiez que l'imprimante est jumelée avec ClearID Self-Service Kiosk.
6. (Facultatif) Effectuez une réinitialisation matérielle de l'iPad de la borne en libre-service.
   a. Configurez l'iPad de votre borne en libre-service.
   b. Procédez de l'une des manières suivantes :
      - Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Bluetooth (Brother 820NWBc ou QL-820NWB) , page 603.
      - Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Bluetooth (Brother TD-4550DNWB) , page 613.
   c. Sélectionnez une imprimante d'étiquettes.
   d. Imprimez un badge de test.

Aucune imprimante d'étiquette Wi-Fi détectée

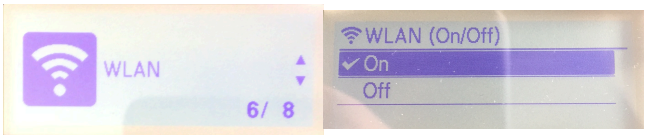
Description : Aucune imprimante d'étiquettes n'a été détectée sur le réseau Wi-Fi. Il peut s'agir d'un problème de configuration ou d'un problème matériel.

Solution :

1. Vérifiez que l'imprimante est allumée et prête à l'emploi.
2. Vérifiez que le réseau Wi-Fi est disponible.

   Le réseau Wi-Fi doit être activé et prendre en charge les éléments suivants :

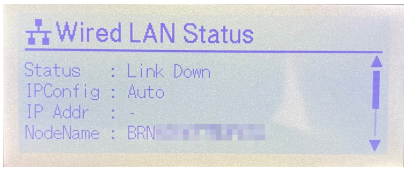
   - Bonjour, requis pour la découverte d'appareils.
   - SNMP, requis pour obtenir l'état de l'imprimante.
   - Port UDP ou TCP 9100, requis pour envoyer les données d'impression.
3. Vérifiez que le Wi-Fi est activé sur l'imprimante d'étiquettes.
   a. Dans le menu **Réglages**, sélectionnez **WLAN** > **WLAN (On/Off)** > **On** et appuyez sur **OK**.



4. Vérifiez que le Wi-Fi est activé sur l'iPad.
5. Vérifiez que l'iPad de la borne en libre-service et l'imprimante d'étiquettes sont connectés au même réseau Wi-Fi.
6. (Facultatif) Effectuez une réinitialisation matérielle de l'iPad de la borne en libre-service.
   a. Configurez l'iPad de votre borne en libre-service.
   b. Procédez de l'une des manières suivantes :
      - Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Wi-Fi (Brother 820NWBc, QL-820NWB ou QL-810W) , page 606.
      - Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Wi-Fi (Brother TD-4550DNWB) , page 616.
   c. Sélectionnez une imprimante d'étiquettes.
   d. Imprimez un badge de test.

Aucune imprimante d'étiquette Ethernet détectée

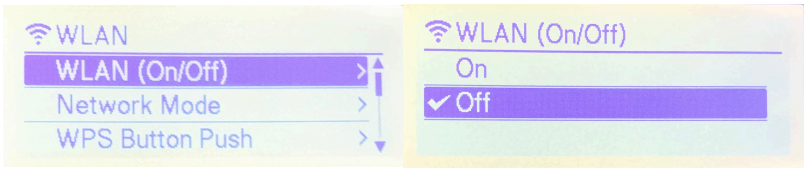
Description : L'imprimante d'étiquettes affiche l'état **Wired LAN Status** Link Down (Réseau filaire, déconnecté).



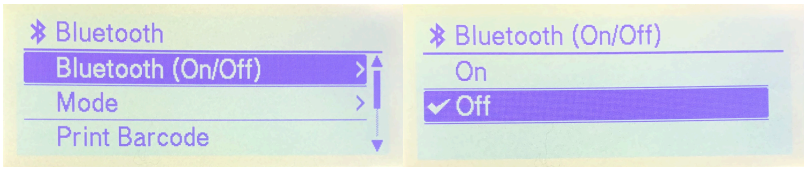
Solution :

1. Vérifiez que l'imprimante est allumée et prête à l'emploi.

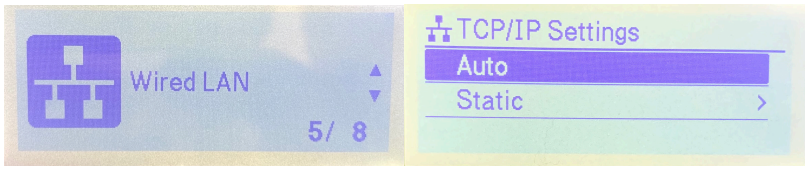
2. Vérifiez que la fonction Wi-Fi de l'imprimante d'étiquettes est désactivée.
   a. Dans le menu **Settings** (Réglages) de l'imprimante, réglez **WLAN** (Wi-Fi) sur OFF.



3. Vérifiez que la fonction Bluetooth de l'imprimante d'étiquettes est désactivée.
   a. Dans le menu **Réglages**, sélectionnez **Bluetooth** > **Bluetooth (On/Off)** > **Off** et appuyez sur **OK**.



4. Vérifiez que le réseau Ethernet est disponible.
5. Vérifiez que l'Ethernet est activé sur l'imprimante d'étiquettes.
   a. Dans le menu **Réglages**, sélectionnez **Wired LAN** > **TCP/IP Settings** > **Auto** et appuyez sur **OK**.



6. Vérifiez que l'imprimante est connectée à un port LAN et pas WAN (sur le routeur ou sur le réseau de votre organisation).
7. Vérifiez que vous utilisez le bon type de câble Ethernet.

   BONNE PRATIQUE : Utilisez un câble droit à paires torsadées Category 5 (ou supérieur) pour un réseau Fast Ethernet 100BASE-T ou 10BASE-TX.
8. (Facultatif) Effectuez une réinitialisation matérielle de l'iPad de la borne en libre-service.
   a. Configurez l'iPad de votre borne en libre-service.
   b. Procédez de l'une des manières suivantes :
      - Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Ethernet (Brother 820NWBc ou QL-820NWB) , page 609.
      - Configurer l'imprimante d'étiquettes de la borne en libre-service en mode Ethernet (Brother TD-4550DNWB) , page 619.
   c. Sélectionnez une imprimante d'étiquettes.
   d. Imprimez un badge de test.

Impression : Une erreur d'impression est survenue. Il n'y a pas de papier dans l'imprimante.

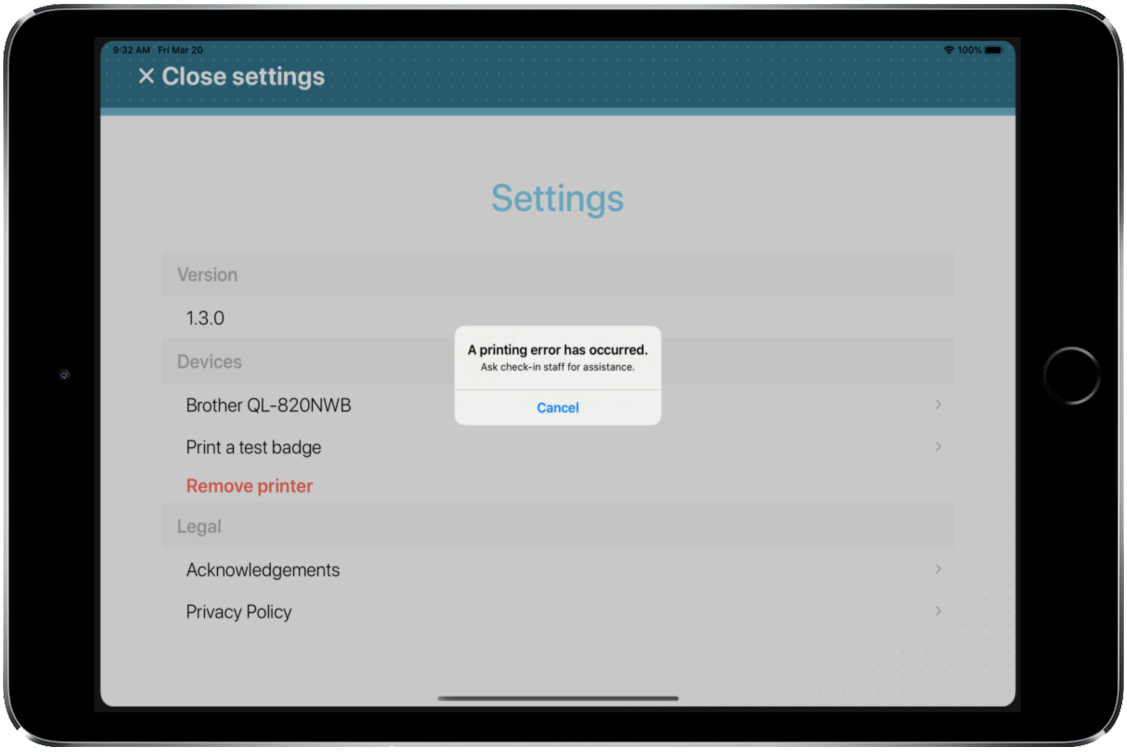
Description : L'imprimante d'étiquettes est à court d'étiquettes ou un bourrage est survenu.

Solution :

1. Vérifiez que le rouleau d'étiquettes n’est pas fini et remplacez-le si nécessaire.
   - Brother QL-820NWBc ou QL-820NWB : DK Roll - 62mm noir (référence Brother : DK-2205) ou 62mm rouge et noir (référence Brother : DK-2251)
   - Brother TD-4550DNWB : RD Roll - 57mm noir (référence Brother : RD001U1S)
2. Vérifiez si l'imprimante ne présente pas un problème de bourrage ou d'alimentation des étiquettes.

Brother QL-820NWBc ou QL-820NWB : Une erreur d'impression est survenue

Description : L'imprimante d'étiquettes Brother QL-820NWBc ou QL-820NWB a rencontré une erreur d'impression inconnue.



Solution :

1. Consultez Label Printer Led Status indicators (Témoins LED d'état) dans la FAQ pour des explications possibles.
2. Voir la section Connexion à un appareil mobile pour d'autres explications possibles.
3. Consultez la section FAQ et dépannage de l’Impression pour des explications possibles.

Brother QL-820NWBc ou QL-820NWB : L'imprimante s'éteint inopinément

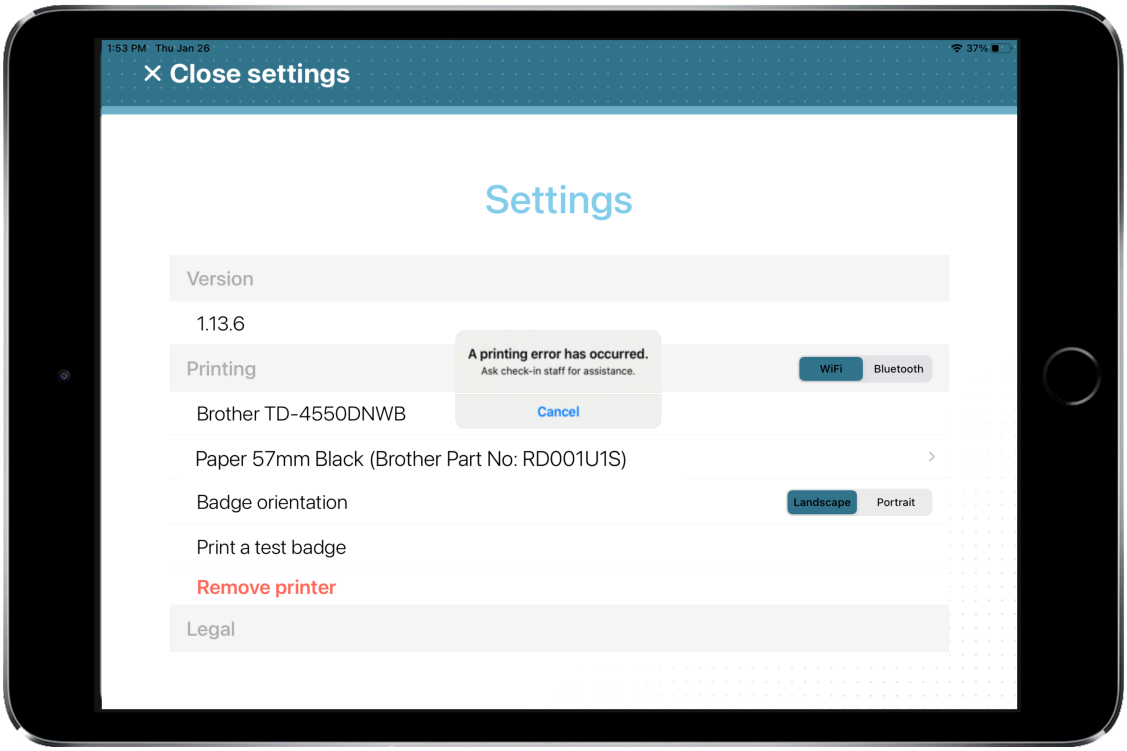
Description : L'imprimante s'éteint automatiquement à la même heure tous les jours.

Solution : Modifiez les réglages depuis le menu de l’imprimante.

1. Appuyez sur la touche **Menu**.
2. Sélectionnez **Settings** à l'aide des boutons ▲ ▼, puis appuyez sur le bouton **OK**.
3. Sélectionnez **Auto Power Off** à l'aide des boutons ▲ ▼, puis appuyez sur le bouton **OK**.
4. Sélectionnez **Adapter** à l'aide des boutons ▲ ▼, puis appuyez sur le bouton **OK**.
5. Sélectionnez **Off** à l'aide des boutons ▲ ▼, puis appuyez sur le bouton **OK**.
6. (Facultatif) Réglez également l'heure sur **Off** pour [**Li-ion battery**], à la suite des étapes ci-dessus.

Brother TD-4550DNWB : Une erreur d'impression est survenue

Description : L'imprimante d'étiquettes Brother TD-4550DNWB a rencontré une erreur d'impression inconnue.



Solution :

1. Consultez Label Printer Led Status indicators (Témoins LED d'état) dans la FAQ pour des explications possibles.
2. Voir la section Connexion à un appareil mobile pour d'autres explications possibles.
3. Consultez la section FAQ et dépannage de l'Impression pour des explications possibles.

Brother TD-4550DNWB : L'impression du badge n'arrive jamais

Description : Lors de l'impression de badges, ceux-ci sont envoyés à l'imprimante mais ne sont jamais imprimés.

Solution :

1. Vérifiez que vous n'êtes pas dans un menu de configuration et de réglage en regardant l'écran LCD.

   REMARQUE : Laisser l'imprimante dans un menu de configuration ou de réglage peut entraîner la suspension des impressions.
2. Si l'imprimante est restée dans un menu de configuration ou de réglage, appuyez sur la touche **Menu** ou utilisez les commandes de l'imprimante pour revenir à l'écran d'accueil.

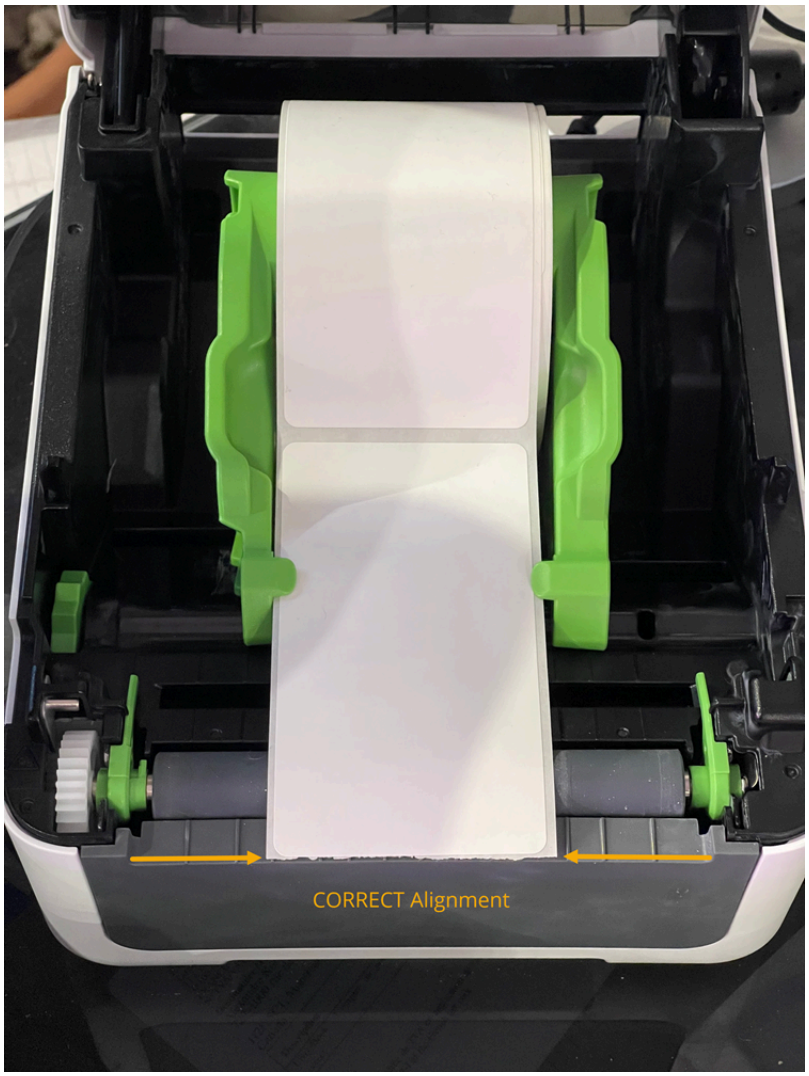
   L'impression des badges devrait alors reprendre normalement.

Brother TD-4550DNWB : Les badges ne sont pas imprimés correctement

Description : L'imprimante imprime une étiquette incomplète, ou avec un problème d'orientation. Par exemple, l'imprimante imprime un badge incomplet ou le badge chevauche deux étiquettes.

Solution :

1. Avant d'imprimer des badges, vérifiez l’alignement et l'orientation des étiquettes.



IMPORTANT : La première étiquette doit être alignée avec le bord avant de l’imprimante pour assurer une impression conforme. Vérifiez qu'aucune étiquette ne dépasse du bord avant de l’imprimante avant de lancer l’impression. L’imprimante ne détecte les bords des étiquettes automatiquement qu’après l’impression de la première étiquette. Dès lors, si la première étiquette est mal alignée, des problèmes d'impression peuvent survenir.

Pour en savoir plus sur la façon de charger les étiquettes ou sur la position du capteur pour différents types d'étiquettes, voir les sections Load the RD roll (Charger le rouleau RD) et Check the sensor position (Vérifier la position du capteur) dans la documentation Brother en ligne.

Rubriques connexes

Réinitialiser l’application mobile Self-Service Kiosk, page 633
Ports de pare-feu, page 76

15

Ressources complémentaires

Besoin d'assistance technique ou d'informations sur le produit? Consultez ces ressources.

Cette section aborde les sujets suivants:

- "Assistance technique", page 698

Assistance technique

Le centre d'assistance technique de Genetec[MC] (GTAC) s'engage à fournir le meilleur service d'assistance technique possible à ses clients du monde entier. En tant que client de Genetec Inc., vous avez accès au TechDoc Hub, où vous pouvez trouver des informations et chercher des réponses à vos questions sur les produits.

- **Genetec TechDoc Hub :** Recherchez des articles, manuels et vidéos répondant à vos questions ou vous aidant à résoudre les problèmes techniques.

  Avant de contacter GTAC ou d'ouvrir un dossier de support, il est recommandé de rechercher dans TechDoc Hub les correctifs potentiels, solutions de contournement ou problèmes connus.

  Pour accéder à TechDoc Hub, connectez-vous au Portail Genetec et cliquez sur TechDoc Hub. Vous ne trouvez pas ce que vous cherchez ? Envoyez un e-mail à l'adresse documentation@genetec.com.
- **Centre d'assistance technique de Genetec (GTAC) :** La procédure pour contacter GTAC est décrite dans la Description de Genetec Advantage.

Formation technique

Que ce soit en classe professionnelle ou depuis votre bureau, nos formateurs qualifiés peuvent vous guider dans la conception, l'installation, le fonctionnement et le dépannage du système. Des services de formation technique sont proposés pour tous les produits et pour différents niveaux d'expérience, et peuvent en outre être personnalisés pour répondre à vos besoins ou objectifs particuliers. Pour en savoir plus, voir http://www.genetec.com/support/training/training-calendar.

Licences

- Pour l'activation ou la réinitialisation des licences, contactez GTAC sur https://portal.genetec.com/support.
- Pour des problèmes de contenu de licences ou de références ou concernant une commande, contactez le service clientèle de Genetec à l'adresse customerservice@genetec.com, ou appelez le 1-866-684-8006 (option 3).
- Pour obtenir une licence de démo ou pour des questions sur les tarifs, contactez le service commercial de Genetec à l'adresse sales@genetec.com, ou appelez le 1-866-684-8006 (option 2).

Problèmes et pannes des produits matériels

Contactez GTAC sur https://portal.genetec.com/support pour tout problème lié aux appareils Genetec ou au matériel acheté auprès de Genetec Inc.

Glossaire

abonnement

Dans Genetec ClearID[MC], un abonnement est une licence renouvelable qui attribue un ensemble de privilèges à un compte Genetec ClearID[MC] durant une période prédéfinie. Il comprend la connexion au portail, la configuration de plusieurs postes de travail et utilisateurs Security Center et l'utilisation d'un ensemble de fonctionnalités, telles que définies par la licence d'abonnement.

antiretour

L'antiretour correspond à une restriction d'accès à un secteur sécurisé empêchant un titulaire de cartes de pénétrer dans un secteur qu'il n'a pas encore quitté, ou inversement.

Approbateur de secteur

Dans Genetec ClearID[MC] un approbateur de secteur est une identité qui a un pouvoir d'approbation sur un secteur. L'approbateur peut approuver ou refuser les demandes d'accès à un secteur. Il est également responsable de l’approbation des examens d'accès de secteurs.

attributs

Dans Genetec ClearID[MC], les attributs sont les traits ou les caractéristiques qui forment une identité. Parmi les exemples d'attributs figurent le service, l'emplacement, le rôle, l'ancienneté, le niveau de rémunération, les certifications de formation et l'habilitation de sécurité.

authentification proxy

L'authentification proxy est le processus de validation des identifiants utilisateur permettant d'accéder à un serveur proxy. Cette authentification inclut généralement un nom d'utilisateur et peut également comprendre un mot de passe.

certificat d'identité

Un certificat d'identité est un *certificat numérique* qui permet d'authentifier une partie à une autre dans une communication sécurisée sur un réseau public. Les certificats d'identité sont généralement émis par une autorité approuvée par les deux parties, appelée *autorité de certificat (AC)*.

champ personnalisé

Un champ personnalisé est une propriété définie par l’utilisateur et associée à un type d'entité. Les champs personnalisés sont pratiques pour stocker des informations complémentaires.

Comptage d’individus

La tâche *Comptage d’individus* est une tâche d'exploitation qui suit en temps réel le nombre de titulaires de cartes au sein des secteurs sécurisés de votre système.

contrôle d'accès (accès physique)

Le contrôle d'accès (accès physique) correspond à la gestion de l'accès aux actifs physiques, tels que les portes et les groupes de portes.

Délégation

Dans Genetec ClearID[MC], la délégation est le processus consistant à transférer des tâches Genetec ClearID[MC] de propriétaires de sites, propriétaires de secteurs, approbateurs de secteurs, responsables de rôles et approbateurs d'événements de visite à quelqu’un d'autre au sein de votre organisation. Par exemple, à l'occasion de vacances prévues, de congés sabbatiques, etc.

Droits d'accès de titulaire de cartes

La tâche *Droits d'accès de titulaire de cartes* est une tâche de maintenance qui répertorie les titulaires de cartes et groupes de titulaires de cartes qui sont autorisés ou non à accéder à des secteurs, portes ou ascenseurs particuliers.

Genetec ClearID[MC]

Genetec ClearID[MC] est un moyen plus intelligent de gérer les accès physiques à l'aide d'une solution en libre-service pour Synergis[MC].

Genetec ClearID[MC] API

L'API Genetec ClearID[MC] est une interface de programmation que les développeurs peuvent utiliser pour aider leurs clients et partenaires à intégrer des logiciels supplémentaires ou des fonctions personnalisées.

Genetec ClearID[MC] LDAP Synchronization Agent

Genetec ClearID[MC] LDAP Synchronization Agent est une application Windows servant à synchroniser les attributs Lightweight Directory Access Protocol (LDAP) Active Directory (AD) avec les attributs d'identité Genetec ClearID[MC].

Genetec ClearID[MC] One Identity Synchronization Tool

Genetec ClearID[MC] One Identity Synchronization Tool est un service Windows qui permet d'importer des informations d'identités à partir d'un système externe dans Genetec ClearID[MC].

Genetec ClearID[MC] Self-Service Kiosk

Genetec ClearID[MC] Self-Service Kiosk est une application mobile qui simplifie la gestion des visiteurs inscrits à l'aide du portail Genetec ClearID[MC] en libre-service. La borne en libre-service est destinée aux centres d'accueil ou aux installations sécurisées où les invités s'enregistrent eux-mêmes.

Gestion des visiteurs

La tâche *Gestion des visiteurs* est une tâche d'exploitation qui permet d'inscrire, de radier et de modifier les visiteurs, et de gérer leurs identifiants, y compris les cartes temporaires.

groupe de titulaires de cartes

Un groupe de titulaires de cartes est une entité qui détermine les droits d'accès communs d'un groupe de titulaires de cartes.

horaire

Un horaire est une entité qui définit des contraintes horaires qui peuvent être appliquées à de nombreuses situations au sein du système. Chaque contrainte horaire est décrite par une plage de dates (quotidien, hebdomadaire, mensuel, annuel ou à dates spécifiques) et par une plage horaire (toute la journée, plage fixe, journée ou nuit).

identifiant

Entité qui représente une carte de proximité, un modèle biométrique ou un code PIN exigé pour accéder à un secteur sécurisé. Un identifiant ne peut être affecté qu'à un titulaire à la fois.

identité

Dans Genetec ClearID[MC], une identité représente une personne et détermine ce qu'elle peut faire sur une variété de plates-formes, de systèmes de sécurité, de systèmes d'entreprise et de fonctions. Chaque identité a un ou plusieurs badges de contrôle d'accès (identifiants) et est associée à un titulaire de cartes dans Synergis[MC]. Par exemple, les identifiants peuvent être un utilisateur Windows (Active Directory), un employé (ressources humaines et paie), un vendeur (outils CRM ou de création de devis) et un titulaire de cartes (sécurité physique).

liste de surveillance globale

Dans Genetec ClearID[MC], une liste de surveillance globale est une liste de surveillance appliquée à tous les sites de votre système.

processus

Dans Genetec ClearID[MC], un processus est une procédure constituée de plusieurs étapes, dont l'autorisation de différentes parties prenantes. Par exemple, les demandes d'accès ou de visite sur site.

processus de demande d'accès

Un processus de demande d'accès est une série d'activités effectuées par le système ou par des personnes habilitées au cours du cycle de vie d'une demande d'accès. Les activités peuvent modifier l'état et les

propriétés des demandes d'accès, affecter d'autres entités du système, ou attendre qu'une condition soit réunie.

processus de demande d'identité

Un processus de demande d'identité est une série d'activités effectuées par le système ou par des personnes habilitées au cours du cycle de vie d'une demande d'identité. Ces activités peuvent créer une identité individuelle ou plusieurs identités en important un fichier CSV, et ajouter chaque nouvelle identité à un rôle afin d'hériter des accès pertinents sur une période donnée.

processus de demande de visite

Un processus de demande de visite est une série d'activités effectuées par le système ou par des personnes habilitées au cours du cycle de vie d'une demande de visite. Les activités peuvent modifier l'état et les propriétés des demandes de visite, affecter d'autres entités du système, ou attendre que certaines conditions soient réunies.

processus de liste de surveillance

Un processus de liste de surveillance est une série d'activités effectuées par le système ou par des personnes habilitées au cours du cycle de vie d'une demande de visite si les listes de surveillance sont activées. Les activités peuvent modifier l'état et les propriétés des listes de surveillance, affecter d'autres entités du système, ou attendre que certaines conditions soient réunies.

propriétaire de rôle

Dans Genetec ClearID[MC], un propriétaire de rôle est responsable de l'affectation de responsables de rôles et de la configuration des stratégies basées sur les rôles.

Propriétaire de secteur

Dans Genetec ClearID[MC] un propriétaire de secteur est une identité qui a un pouvoir sur un secteur. Le propriétaire peut définir la stratégie liée à un secteur et affecter des approbateurs de secteur.

propriétaire de site

Dans Genetec ClearID[MC], un propriétaire de site est une identité qui a autorité sur les secteurs associés à un site particulier. Le propriétaire de site peut attribuer ou modifier des propriétaires de secteurs et peut configurer des paramètres de secteur spécifiques exclusifs aux propriétaires de site. Il est également chargé des analyses d'accès au site.

rapport d'activité de rôle

Dans Genetec ClearID[MC], le rapport d'activité de rôle est un historique de toutes les activités associées aux rôles. Le rapport contient des informations d'horodatage, de type d'activité, sur les personnes ayant effectué l'activité, ainsi qu'une section détails qui contient des informations de motif.

rapport d'activité de site

Dans Genetec ClearID[MC], le rapport d'activité de site est un historique des activités ou des événements associés à un site particulier. Le rapport contient des informations d'horodatage, de type d'activité, de secteur, sur les personnes ayant effectué l'activité, ainsi qu'une section détails qui contient des informations de motif.

Rapport de demandes d'accès

Dans Genetec ClearID[MC], un rapport de demandes d'accès renvoie une liste de demandes d'accès à un site particulier. Le rapport inclut des informations sur la date de la demande d'accès, le secteur demandé, l'état, le demandeur, le destinataire de la demande et la période d'accès.

Rapport Demandes d'identités

Dans Genetec ClearID[MC], le rapport de demandes d'identités renvoie une liste de demandes d'identités pour votre compte ClearID. Le rapport contient des informations sur la date de la demande d'identité, le demandeur, le nom, le modèle d'identité, l'état et les évaluateurs.

Rapport de visiteurs

Dans Genetec ClearID[MC], un rapport de visiteurs est une liste de toutes les visites prévues ou en cours, ou des visites effectuées dans le passé sur un site particulier. Le rapport inclut des informations sur le nom du

visiteur, le demandeur de l'événement, le nom de l'événement, l'arrivée prévue, l'inscription, la radiation et l'état de la liste de surveillance.

rapport d'activité d'utilisateurs

Dans Genetec ClearID[MC], le rapport d'activité d'utilisateurs est un historique de toutes les activités associées aux utilisateurs. Le rapport contient des informations d'horodatage, de type d'activité, sur les personnes ayant effectué l'activité, ainsi qu'une section détails qui contient des informations de motif.

rapport d'examen d'accès

Dans Genetec ClearID[MC], un rapport d'examens d'accès renvoie une liste d'examens d'accès. Le rapport contient des informations sur les examens d'accès de secteurs, de rôles ou d'identités, ainsi que l'état d'examen actuel (non démarré, démarré, en cours, terminé ou expiré).

rapport propriétaires de sites et de secteurs

Dans Genetec ClearID[MC], le rapport Propriétaires de sites et de secteurs est une liste qui fournit une vue d'ensemble de toutes les identités et de leurs autorisations. Seules les identités qui sont des propriétaires de sites, approbateurs de secteurs, propriétaires de secteurs ou responsables de listes de surveillance sont affichées dans ce rapport. Le rapport contient des informations sur les sites, secteurs, identités, autorisations, délégations, l'état des identités et les accès au portail web.

Rapport Subordonnés

Dans Genetec ClearID[MC], le rapport Subordonnés renvoie une liste d'identités d'employés qui rendent des comptes à un superviseur. Le rapport contient des informations sur les subordonnés, les subordonnés délégués, les intitulés de poste, les sociétés et l'état du contrôle d'accès.

règle d'accès

Une entité règle d'accès définit une liste de titulaires de cartes qui se voient accorder ou refuser l'accès en fonction d'un horaire. Les règles d'accès s'appliquent aux secteurs sécurisés et aux portes d'entrée et de sortie, ou aux secteurs de détection d'intrusion pour l'armement et le désarmement.

règle d'escorte de visiteur

Restriction d'accès à un secteur sécurisé qui requiert l'accompagnement des visiteurs par un titulaire de cartes durant leur visite. Pour que le passage par un point d'accès soit accordé, le visiteur et son hôte attitré (un titulaire de cartes) doivent tous les deux présenter leurs identifiants dans un délai donné.

règle de provisionnement

Dans Genetec ClearID[MC], une règle de provisionnement est un critère logique servant à accorder ou révoquer l'accès en ajoutant ou supprimant des identités d'un rôle ou d'un secteur particulier.

responsable de liste de surveillance

Dans Genetec ClearID[MC], un responsable de liste de surveillance est une identité qui gère des listes de surveillance. Un responsable de liste de surveillance peut créer ou modifier des listes et leur ajouter des personnes ou des sociétés. Il configure également les listes pour déterminer si elles s'appliquent localement ou globalement.

responsable de rôle

Dans Genetec ClearID[MC], un responsable de rôle est une identité qui a autorité sur les personnes affectées à un rôle. Un responsable de rôle peut ajouter des personnes à un rôle et en supprimer. Il est également chargé de l'approbation des analyses d'accès.

rôle

Dans Genetec ClearID[MC], un rôle est un groupe de personnes dotées des mêmes accès. Une personne peut se voir attribuer plusieurs rôles. Les rôles sont associés aux groupes de titulaires de cartes dans Synergis[MC]. Un responsable de rôle contrôle les accès aux groupes.

secteur

Dans Security Center, une entité secteur représente un concept ou un lieu physique (pièce, étage, bâtiment, site, etc.) utilisé pour le regroupement logique d'autres entités du système.

secteur

Dans Genetec ClearID[MC], un secteur est une entité logique qui définit la relation entre les propriétaires de secteurs et les portes Synergis[MC]. Les secteurs sont gérés par le propriétaire du secteur.

Security Center

Security Center est une plate-forme réellement unifiée qui marie vidéosurveillance, contrôle d'accès, reconnaissance automatique de plaques d'immatriculation, détection d'intrusion et communications au sein d'une même solution intuitive et modulaire. En tirant parti d'une approche unifiée de la sécurité, votre organisation devient plus efficace, prend de meilleures décisions et réagit aux situations et aux menaces avec une plus grande confiance.

serveur proxy

Un serveur proxy est un serveur qui vérifie et transfère les demandes client entrantes à d'autres serveurs pour une communication ultérieure. Par exemple, lorsqu'un client n'est pas en mesure de répondre aux exigences d'authentification de sécurité du serveur mais doit avoir accès à certains services.

site

Dans Genetec ClearID[MC], un site est une entité logique. Les sites incluent un ou plusieurs secteurs. Chaque site et chaque zone peuvent avoir un propriétaire différent.

subordonnés

Dans Genetec ClearID[MC], les subordonnés correspondent aux employés (identités) qui répondent à un superviseur.

Synchroniseur de titulaires de cartes globaux

Le rôle Synchroniseur de titulaires de cartes globaux (STCG) assure la synchronisation bidirectionnelle des titulaires de cartes partagés et des entités associées entre le système local (client de partage) qui l'héberge et le système central (hôte de partage).

Synergis[MC]

Security Center Synergis[MC] est le système de contrôle d'accès (SCA) sur IP qui renforce la sécurité physique de votre organisation ainsi que votre capacité à réagir aux menaces. Synergis[MC] prend en charge un éventail croissant de matériel de contrôle de portes et de verrous électroniques. Avec Synergis[MC], vous pouvez exploiter vos équipements de réseau et de sécurité existants.

Synergis[MC] Cloud Link

Synergis[MC] Cloud Link est l'appareil de contrôle d'accès intelligent compatible PoE qui prend en charge divers modules d'interface tiers sur IP et RS-485.

titulaire de cartes

Une entité titulaire de cartes représente un individu autorisé à pénétrer et à quitter des secteurs sécurisés en fonction de ses identifiants (généralement des cartes d'accès), et dont les activités peuvent être surveillées.

watchlist

Dans Genetec ClearID[MC], les listes de surveillance des visiteurs peuvent être utilisées pour filtrer les visiteurs au niveau individuel ou de l'entreprise. Vous pouvez configurer la liste de surveillance pour effectuer des actions d'autorisation, de blocage ou de notification au niveau d'un site ou au niveau mondial.