Version 1.6, Octobre 2010

Xerox Secure Access Unified ID System®

Guide d'administration

Traduit par :
Xerox
CTC European Operations
Bessemer Road
Welwyn Garden City
Hertfordshire
AL7 1BU
Royaume-Uni

Table des matières

5 Annexes

1 Consignes de sécurité

Lisez ces consignes de sécurité attentivement afin de manipuler l'équipement en toute sécurité et conformément à la législation en vigueur.

Cet équipement a été conçu et testé pour répondre aux normes de sécurité les plus strictes. Il a fait l'objet d'un contrôle et d'une homologation par un organisme de sécurité et a été déclaré conforme aux normes en vigueur en matière de respect de l'environnement.

Lisez attentivement les instructions ci-après avant d'utiliser cet équipement et consultez-les lorsque nécessaire pour assurer son bon fonctionnement.

AVERTISSEMENT : Toute modification de l'équipement impliquant l'ajout de nouvelles fonctions ou la connexion à des appareils tiers peut annuler la garantie. Pour plus d'informations, prenez contact avec votre revendeur agréé local.

Alimentation électrique

Cet équipement doit être branché sur une alimentation électrique correspondant au type indiqué sur la plaque du produit. En cas de doute concernant l'alimentation électrique, consultez un électricien ou la compagnie d'électricité locale.

AVERTISSEMENT - Sécurité électrique

- Utilisez uniquement l'alimentation électrique fournie avec cet équipement.
- Ne placez pas cet équipement à un endroit où il est possible de marcher ou de trébucher sur son cordon d'alimentation ou sur son alimentation.
- Ne placez rien sur le cordon d'alimentation.
- Lorsque l'une des conditions suivantes se présente, mettez immédiatement l'équipement hors tension et débranchez-le de la prise secteur. Appelez un technicien agréé local pour corriger le problème.
  - Une odeur inhabituelle provient de l'équipement.
  - Le câble d'alimentation est endommagé ou dénudé.
  - Un disjoncteur, un fusible ou tout autre dispositif de sécurité s'est déclenché.
  - L'équipement a été exposé à de l'eau.
  - Une pièce quelconque de l'équipement est endommagée.

Dispositif de déconnexion

Le cordon d'alimentation constitue le dispositif de déconnexion de cet équipement. Pour couper l'alimentation électrique de l'équipement, débranchez le cordon d'alimentation de la prise électrique.

Homologations

Interférences dans les radiocommunications

États-Unis, Canada

Remarque : Cet équipement a été testé et satisfait aux limites s'appliquant aux appareils numériques de classe B, en vertu des dispositions de l'alinéa 15 de la réglementation FCC. Ces limites visent à assurer une protection raisonnable contre les interférences en zone résidentielle. Cet équipement émet et utilise des fréquences radioélectriques et peut provoquer des interférences avec les communications radio s'il n'est pas installé ou utilisé conformément aux instructions. Bien que les interférences ne se manifestent pas dans tous les cas, le risque ne peut être totalement exclu. Si l'utilisateur constate des interférences lors de la réception d'émissions de radio ou de télévision (il lui suffit pour cela d'éteindre et d'allumer successivement l'équipement), il devra prendre les mesures nécessaires pour les éliminer. À cette fin, il devra :

- réorienter ou déplacer l'antenne de réception,
- augmenter la distance entre l'équipement et le poste récepteur,
- brancher l'équipement sur un circuit autre que celui du poste récepteur,
- s'adresser au fournisseur du poste de radio ou de télévision ou à un technicien expérimenté dans ce domaine.

L'utilisation de câbles d'interface blindés est nécessaire pour assurer la conformité avec la réglementation FCC aux États-Unis.

Canada

This Class "B" digital apparatus complies with Canadian ICES-003.

Cet appareil Numérique de la classe "B" est conforme à la norme NMB-003 du Canada.

Europe

Le sigle CE appliqué à cette machine symbolise la déclaration de conformité Xerox avec les réglementations applicables de l'Union européenne aux dates indiquées :

12 décembre 2006 :	Directive 2006/95/EC du Conseil amendée, relative à l'harmonisation des législations des états membres sur les équipements basse tension.
15 décembre 2004 :	Directive 2004/108/EC du Conseil amendée, relative à l'harmonisation des législations des états membres sur la compatibilité électromagnétique.
9 mars 1999 :	Directive 99/5/EC du Conseil, relative aux équipements hertziens et aux équipements terminaux de télécommunications et la reconnaissance mutuelle.

La garantie de conformité complète, avec une description détaillée des directives et normes concernées, peut être obtenue sur simple demande auprès de Xerox Limited.

AVERTISSEMENTS :

- Pour que cet équipement puisse fonctionner à proximité d'une installation industrielle, scientifique et médicale (ISM), les radiations externes de ce dernier doivent être limitées ou des mesures spéciales de réduction de ces radiations doivent être prises.
- Il est impératif d'utiliser des câbles d'interface blindés avec ce produit pour assurer sa conformité à la directive 89/336/EEC.

Homologation RFID

Ce équipement génère 13,56 MHz au moyen d'un système de boucle inductive en tant que système RFID (radio frequency identification system device). Ce système RFID est conforme à l'alinéa 15 de la réglementation FCC, à la norme RSS-210 Industry Canada, à la Directive européenne 99/5/EC et aux lois ou réglementations locales applicables.

Le fonctionnement de cette machine est soumis aux deux conditions suivantes : (1) elle ne doit pas provoquer d'interférences nuisibles, et (2) elle doit accepter les interférences en réception, y compris les interférences qui peuvent entraîner un fonctionnement indésirable.

Toute modification du matériel effectuée sans l'autorisation expresse de Xerox Corporation est de nature à interdire l'usage du matériel.

Recyclage et mise au rebut de l'équipement

S'il vous incombe de gérer la mise au rebut de cet équipement Xerox, il convient de noter que ce dernier contient du plomb, du mercure et d'autres substances dont la mise au rebut peut être réglementée pour des raisons écologiques dans certains pays ou états. La présence de plomb et de mercure est conforme aux réglementations mondiales en vigueur au moment de la mise sur le marché de cet équipement.

Union européenne

Mise au rebut dans le cadre d'un usage commercial

La présence de ce symbole sur cet équipement indique que la mise au rebut de ce dernier doit être conforme à la réglementation nationale en la matière.

Conformément à la législation européenne, les équipements électroniques et électriques usagés destinés au rebut doivent être séparés des ordures ménagères.

Contactez Xerox pour en savoir plus sur la reprise du matériel avant toute mise au rebut.

Amérique du Nord (USA, Canada)

Xerox met en œuvre un programme international de reprise ou réutilisation/recyclage des équipements. Contactez Xerox pour savoir si ce produit Xerox est concerné par ce programme. Pour plus d'informations sur les programmes Xerox relatifs à l'environnement, accédez au site Web suivant http://www.xerox.com/environment

S'il vous incombe de gérer la mise au rebut de votre produit Xerox, notez que ce dernier peut contenir du plomb, du mercure, du perchlorate et d'autres substances dont la mise au rebut peut être réglementée pour des raisons écologiques La présence de ces substances est conforme aux réglementations mondiales en vigueur au moment de la mise sur le marché de cet équipement. Pour de plus amples informations sur le recyclage et la mise au rebut, contactez les autorités locales. Les clients résidant aux États-Unis peuvent consulter le site de Electronic Industries Alliance à l'adresse suivante : http://www.eiae.org

Perchlorate - Ce produit peut présenter un ou plusieurs composants contenant du perchlorate (batteries, par exemple). Le traitement de cette substance peut être soumis à une procédure spéciale ; pour en savoir plus, consultez http://www.dtsc.ca.gov/hazardouswaste/perchlorate

Mise au rebut dans le cadre d'un usage domestique

La présence de ce symbole sur le produit indique que ce dernier ne doit pas être mis au rebut avec les ordures ménagères.

Conformément à la législation européenne, tout équipement électrique et électronique usagé doit faire l'objet d'une collecte séparée.

Les particuliers résidant dans les pays membres de l'Union Européenne ont la possibilité de déposer gratuitement leurs équipements électriques et électroniques usagés dans des centres de ramassage désignés. Pour plus d'informations, prenez contact avec les autorités locales.

Dans certains états membres, un ancien équipement peut être remis sans frais au fournisseur local lors de l'achat d'un équipement neuf. Veuillez contacter le revendeur pour plus d'informations.

Autres pays

Prenez contact avec les autorités locales pour obtenir des informations sur la mise au rebut.

Environnement, hygiène et sécurité

Informations de contact

Pour de plus amples informations sur les consignes de sécurité relatives à ce produit Xerox et à ses consommables, prenez contact avec les Centre Services Xerox suivants :

USA : 1-800 828-6571

Canada : 1-800 828-6571

Europe : +44 1707 353 434

http://www.xerox.com/environment Consignes de sécurité pour les États-Unis (Consignes de sécurité relatives à ce produit pour les États-Unis)

http://www.xerox.com/environment_europe Consignes de sécurité pour l'Europe (Consignes de sécurité relatives à ce produit pour l'Europe)

Liste de contrôle pour l'installation

2

Les Guides d'installation et d'administration de Xerox Secure Access contiennent des instructions pas-à-pas pour l'installation et la configuration du serveur Secure Access et des imprimantes multifonctions. Ce chapitre fournit un tableau présentant l'ordre dans lequel effectuer l'installation en fonction de la configuration du matériel Secure Access, en commençant par le guide d'installation.

Étapes **(*) signale les étapes obligatoires**	**Xerox Secure Access avec un lecteur de carte USB**	**Xerox Secure Access avec un périphérique d'authentification et un lecteur de carte USB**
Guide d'installation		
1. Lisez le chapitre 3 Présentation de l'installation	*	*
2. Chapitre 4 Installation du serveur Secure Access : section 1. Préparation du réseau et de la base de données	*	*
3. Chapitre 4 Installation du serveur Secure Access : section 2. Exécution de l'Assistant Installation	*	*
4. Chapitre 5 Configuration du matériel : Étape 1. Configurer l'adresse IP du périphérique d'authentification	À ignorer	*
5. Chapitre 5 Configuration du matériel : Étape 2. Monter le périphérique d'authentification Secure Access	À ignorer	*
6. Chapitre 5 Configuration du matériel : Étape 3. Connecter le matériel	À ignorer	*
7. Chapitre 5 Configuration du matériel : Étape 4. Monter/connecter le lecteur de carte USB Secure Access	*	À ignorer
Guide d'administration		
8. Lisez le chapitre 3 Présentation de Secure Access	*	*
9. Chapitre 4 Procédure de configuration : Étape 1 - Configurer le périphérique multifonctions Xerox de manière à accepter l'authentification réseau par le biais du mécanisme Xerox Secure Access	*	*
10. Chapitre 4 - Ajouter les imprimantes multifonctions à la base de données Secure Access	*	*

Étapes (*) signale les étapes obligatoires	Xerox Secure Access avec un lecteur de carte USB	Xerox Secure Access avec un périphérique d'authentification et un lecteur de carte USB
11. Chapitre 4 - Associer l'imprimante multifonctions à un périphérique d'authentification Secure Access	À ignorer	*
12. Chapitre 4 - Configuration de l'impression Follow-You (facultatif)	*	*
13. Chapitre 4 - Définir les paramètres d'authentification	*	*
14. Chapitre 4 - Importer et synchroniser les comptes utilisateur	*	*
15. Chapitre 4 - Configuration du service personnalisé Release My Documents (Libérer mes documents)	*	*

3 Présentation de Secure Access

Ce chapitre contient les sections suivantes :

Après avoir installé le serveur Xerox Unified ID System™ Secure Access et effectué la configuration physique des périphériques d'authentification ou d'un lecteur de carte USB Secure Access, utilisez ce guide pour ajouter des imprimantes multifonctions à la base de données Secure Access afin de permettre au serveur et aux périphériques d'authentification de communiquer. Utilisez ce guide pour effectuer des tâches de configuration avancée pour la totalité des composants et des fonctionnalités de Secure Access.

Ce chapitre traite les éléments suivants :

- Composants matériels et logiciels de Xerox Secure Access
- Accès au gestionnaire Secure Access afin d'administrer le système

Qu'est-ce que Secure Access ?

Unified ID System ™ permet de contrôler l'accès aux fonctions d'impression, de télécopie, de photocopie et de numérisation des imprimantes multifonctions Xerox. Lorsqu'un utilisateur s'approche d'un périphérique contrôlé par Unified ID System, il doit glisser sa carte ou la passer au-dessus du lecteur de carte de proximité. Le panneau avant de l'imprimante multifonctions ne s'active que lorsque les informations de compte de l'utilisateur sont authentifiées par le serveur Unified ID System.

A l'aide d'un protocole propriétaire (Convenience Authentication Protocol), le périphérique d'authentification Unified ID System contacte le serveur via une connexion réseau Ethernet pour vérifier les informations utilisateur collectées à partir de la carte magnétique ou de proximité. En utilisant un lecteur de carte USB, l'imprimante multifonctions communique directement avec le serveur Secure Access. Si le serveur Unified ID System valide l'utilisateur, le panneau de l'imprimante multifonctions est déverrouillé et peut être utilisé. Si l'utilisateur n'est pas validé, l'imprimante multifonctions demeure verrouillée et l'utilisateur ne peut y effectuer aucune tâche.

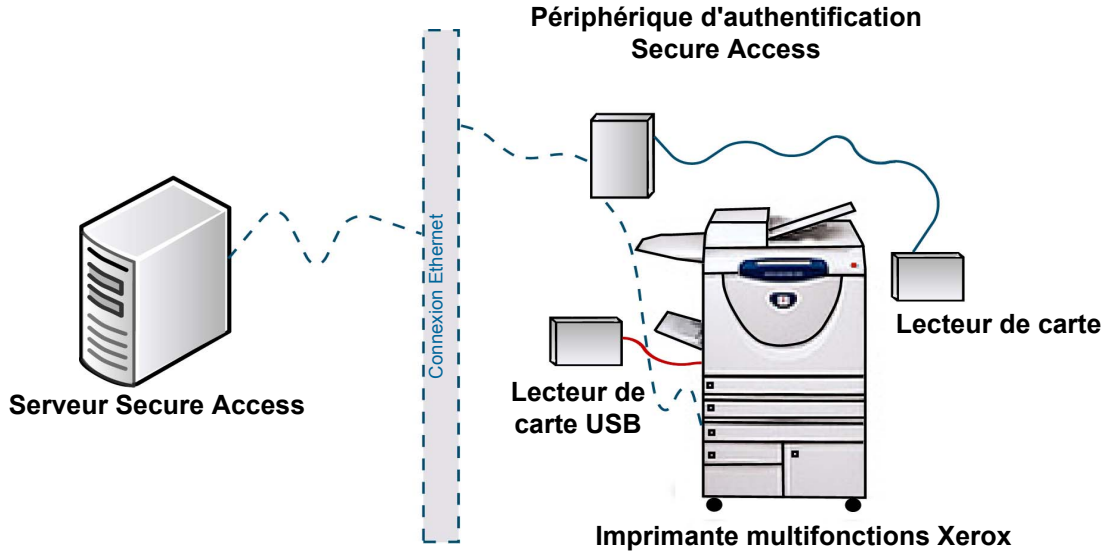


Figure 3-1: Composants de la solution Secure Access

Si l'utilisateur souhaite numériser des documents, le serveur Secure Access fournit l'ID utilisateur réseau à l'imprimante multifonctions compatible ; l'imprimante multifonctions peut alors utiliser l'ID pour implémenter la fonctionnalité d'authentification unique et effectuer une authentification automatique en vue de la numérisation.

Composants de Secure Access

La solution requiert deux composants principaux :

1. Le **périphérique d'authentification Secure Access**, qui comprend un terminal d'authentification et un lecteur de carte externe. Les utilisateurs n'accèdent pas au terminal d'authentification.

   Le lecteur de carte n'est connecté au périphérique d'authentification que via un câble série et n'est pas directement relié à l'imprimante multifonctions. Consultez le *Guide d'installation* pour connaître les instructions de placement et de montage.

Figure 3-2: Composants du périphérique d'authentification Secure Access

ou

1. Un **lecteur de carte USB de serveur**, connecté à l'imprimante multifonctions. Consultez le Guide d'installation pour connaître les instructions de placement et de montage.
2. Le **serveur Secure Access**, qui comprend les composants suivants :
   - Serveur d'authentification central (CAS)
   - Moteur de contrôle de périphérique (DCE)
   - Moteur d'acheminement de document (DRE)
   - Gestionnaire Secure Access (Outils d'administration)

   Remarque : Vous pouvez installer ces composants sur un seul serveur ou les répartir sur plusieurs serveurs. En outre, certains déploiements peuvent nécessiter le recours à plusieurs moteurs DCE ou DRE. Pour des informations détaillées, reportez-vous au *Guide d'installation*.

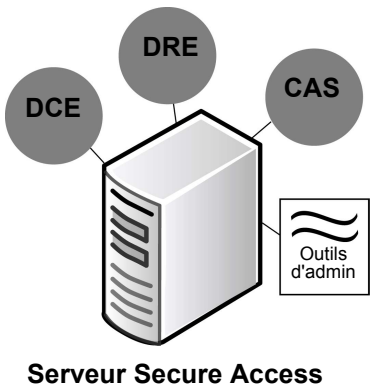


Figure 3-3: Composants du serveur Secure Access

Les composants du serveur central communiquent sur des ports désignés. Chaque composant « écoute » sur un port spécifique les informations ou demandes en provenance des autres composants. Pour obtenir la liste complète des attributions de port par composant, reportez-vous à Affectations des ports à la page 47.

Serveur d'authentification central (CAS)

Le serveur d'authentification central (CAS) héberge la base de données qui contient la totalité des données sur les utilisateurs et sur les périphériques multifonctions.

Chaque installation Secure Access requiert une base de données préinstallée. Le serveur CAS utilise l'instance de base de données pour créer une base de données de comptes qui contient la totalité des informations sur les utilisateurs et sur les périphériques. Pour plus d'informations sur les bases de données prises en charge, reportez-vous à la section Configuration système requise dans le *Guide d'installation*.

Moteur de contrôle de périphérique (DCE)

Le moteur de contrôle de périphérique (DCE) gère toutes les communications avec les périphériques multifonctions. Lorsqu'un utilisateur souhaite utiliser la fonctionnalité de photocopie, de numérisation ou de télécopie sur une imprimante multifonctions, il doit d'abord déclencher le lecteur de carte. Un glissement ou une lecture à proximité initie une demande d'accès.

Le périphérique d'authentification transfère la demande de connexion au moteur DCE, qui contacte à son tour le serveur CAS pour vérifier les données du compte d'utilisateur associées à la carte. Les figures 4 et 5 décrivent ce processus.

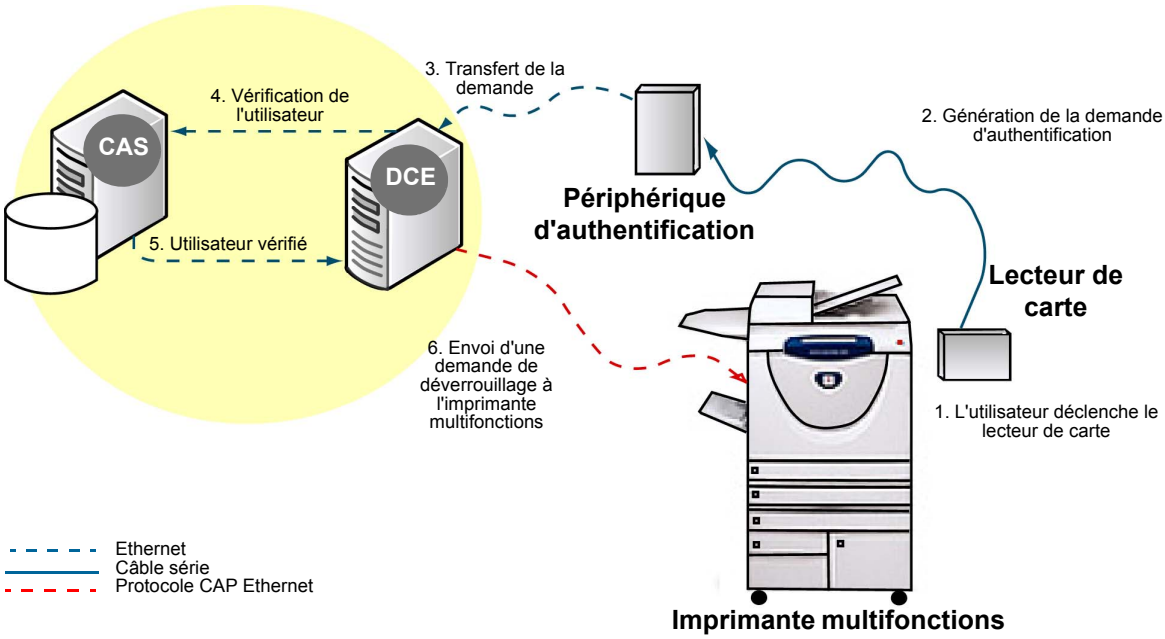


Figure 3-4: Procédure d'authentification de l'utilisateur

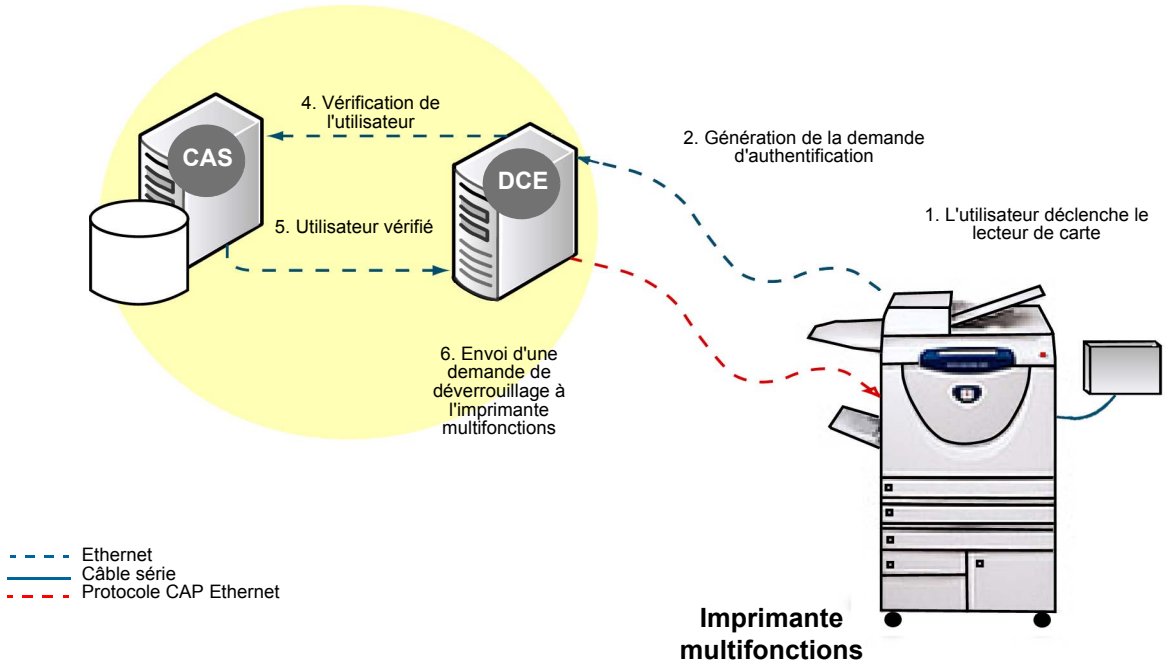


Figure 3-5: Procédure d'authentification de l'utilisateur avec un lecteur de carte USB

Moteur d'acheminement de document (DRE)

Le moteur d'acheminement de document (DRE) est le serveur d'impression. Sa fonction principale est de gérer le flux de documents entre les stations de travail des utilisateurs et les périphériques multifonctions. Voici un scénario typique du fonctionnement du moteur DRE :

1. Un utilisateur génère une demande d'impression sur une imprimante multifonctions enregistrée dans la base de données du gestionnaire Secure Access.
2. Si l'utilisateur imprime dans une file d'attente d'impression qui utilise un port du gestionnaire Secure Access, le moteur DRE conserve le travail sur le serveur d'impression.
3. Lorsque l'utilisateur se connecte à l'imprimante multifonctions, le moteur DRE recherche les travaux en attente pour cette imprimante (et/ou le groupes d'extraction) et libère ceux qui ont été soumis par l'utilisateur connecté.

   Remarque : Si le service personnalisé Release My Documents est installé, les utilisateurs peuvent accéder à l'écran Release My Documents (Libérer mes documents) pour afficher la file d'impression sécurisée, puis libérer au choix un ou plusieurs documents. Reportez-vous à la section Configuration du service personnalisé Release My Documents (Libérer mes documents) à la page 41.

Si aucun port Secure Access n'est installé sur le périphérique, le travail d'impression est imprimé sans validation.

Si vous souhaitez que les travaux d'impression soient conservés dans une file d'attente sécurisée, vous pouvez configurer l'impression Follow-You. Pour activer cette fonctionnalité, vous devez configurer l'imprimante multifonctions de manière à utiliser un port Secure Access plutôt qu'un port standard. Le moniteur de port s'intègre au sous-système d'impression Windows et fonctionne dans le cadre du service spouleur, ce qui lui permet de recevoir des travaux d'impression, puis de les conserver dans une file d'attente virtuelle sécurisée jusqu'à ce qu'un utilisateur validé les libère vers une imprimante multifonctions spécifique.

Lorsque l'impression Follow-You est activée, l'utilisateur doit d'abord s'authentifier sur l'imprimante multifonctions de son choix, comme l'illustre la Figure 3-4: Procédure d'authentification de l'utilisateur à la page 16. Si l'authentification a réussi et que le service personnalisé Release My Documents (Libérer mes documents) a été installé, l'utilisateur peut accéder au panneau avant de l'imprimante multifonctions pour afficher la file d'attente d'impression. L'utilisateur peut libérer tout ou partie des travaux (si la configuration le permet).

Modification des composants du serveur

Si, dans le gestionnaire Secure Access, vous modifiez la configuration de l'un des composants du serveur Secure Access central (serveur CAS, moteur DRE, moteur DCE), par exemple en ajoutant de nouveaux périphériques Secure Access, vous devez patienter pendant au moins trente secondes pour que les changements prennent effet.

Le délai de mise à jour des composants du serveur dépend de la fonctionnalité d'interrogation du serveur CAS. Cela signifie que le délai peut être plus long si le serveur CAS n'est pas disponible pour une raison donnée pendant cette période d'interrogation une fois les modifications apportées au serveur. Le serveur CAS enverra les données de modification aux composants appropriés une fois la connexion restaurée.

Prise en charge du lecteur de données et procédure d'authentification de l'utilisateur

Les fonctions de l'imprimante multifonctions sont verrouillées jusqu'à ce qu'un utilisateur entre des données d'authentification valides. Pour ce faire, l'utilisateur doit passer sa carte de proximité ou carte à puce au-dessus du lecteur de proximité ou glisser sa carte dans un lecteur de piste magnétique.

Une fois les données de l'utilisateur validées par le serveur d'authentification central (CAS), l'imprimante multifonctions est déverrouillée et disponible. Lorsque l'utilisateur a terminé sa tâche, il appuie sur le bouton **Clear All** (Effacer tout) ou **Access** (Accès) du clavier de l'imprimante multifonctions pour se « déconnecter » et verrouiller le périphérique.

Secure Access prend en charge plusieurs types de lecteurs externes : piste magnétique, EM Marin, proximité HID, Hitag, Indala, Mifare et Legic. Tous les lecteurs sont préconfigurés en usine et ne requièrent aucune configuration supplémentaire.

Lecteur de piste magnétique

Secure Access prend en charge les lecteurs externes de piste magnétique. Les utilisateurs peuvent entrer les données de validation en glissant une carte magnétique codée dans le lecteur de carte. Le lecteur de piste magnétique lit pratiquement n'importe quel support de carte magnétique standard sur la piste 2 et accepte les données codées standard ou personnalisées. Les données de la piste 1 sont disponibles avec les lecteurs de piste magnétique USB.

Utilisation d'un lecteur de piste magnétique

Indiquez aux utilisateurs de procéder comme suit pour entrer les données à l'aide d'un lecteur de carte à piste magnétique :

1. Insérez la carte dans la fente de guidage en plaçant la piste magnétique à l'opposé du terminal. Appuyez la carte fermement contre le guide.
2. Faites glisser la carte vers le bas le long de la fente de guidage, puis retirez-la.

   Remarque : Le terminal n'acceptera pas les données si vous faites glisser la carte de biais.

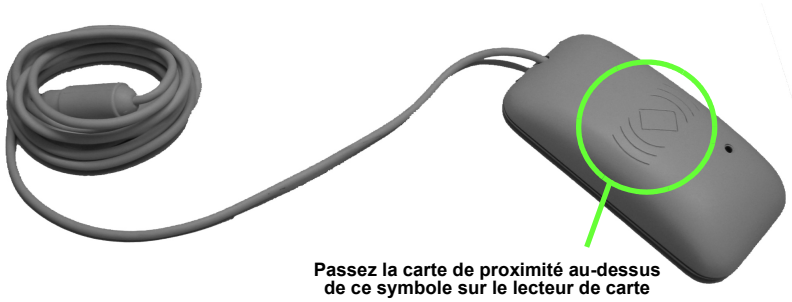
   Si le terminal ne peut pas lire les données, la diode lumineuse est de couleur rouge continue. Réinsérez la carte dans la fente de guidage et passez-la dans le lecteur de nouveau.

Cartes sans contact et cartes de proximité

Secure Access prend en charge les cartes sans contact Legic et Mifare, et les cartes de proximité EM Marin, HID, Hitag et Indala. Les utilisateurs peuvent entrer les données de validation en passant la carte de proximité à moins d'un pouce du lecteur externe.

Utilisation d'une carte à puce ou de proximité

Pour entrer les données à l'aide d'une carte de proximité ou d'une carte à puce, passez la carte à moins de 2,5 cm (1 pouce) du symbole de proximité situé sur la face supérieure du lecteur de carte. Pour savoir où se trouve le lecteur de carte de proximité sur le module du lecteur de données, recherchez le symbole suivant :



Si le glissement est incorrect, la diode lumineuse est de couleur rouge et elle clignote.

Signaux et modes du lecteur de carte

Secure Access affiche ses messages par le biais d'une diode lumineuse sur le module du lecteur de carte.

Sauf mention contraire, la diode lumineuse réagit de la même façon pour les deux types de lecteur de carte. Les signaux suivants peuvent être affichés :

Comportement de la diode lumineuse	Signification
Lumière rouge continue	Le sous-système d'authentification est en mode inactif ; il est prêt mais il n'y a pas de session active.
Lumière verte continue	Le périphérique d'authentification est en mode prêt et une session est active. Cet état s'affiche également si un lecteur de carte USB est utilisé pendant que l'imprimante multifonctions se réamorce, si le contrôleur réseau n'a pas encore été initialisé.

Comportement de la diode lumineuse	Signification
Lumière verte à clignotement lent	Des données sont reçues du lecteur de carte et sont en attente d'authentification pour la session active ou bien des données sont entrées par l'utilisateur (par exemple lors de l'enregistrement automatique de la carte ou après la réponse à l'invite Release All Jobs (Libérer tous les travaux)).
Lumière rouge à clignotement lent	Le sous-système d'authentification ne dispose d'aucune connexion au serveur.
Lumière rouge à clignotement rapide	Carte non valide ; accès refusé.

Le sous-système d'authentification possède deux modes fonctionnels, à savoir le mode inactif ou le mode prêt.

Un sous-système d'authentification prêt à être utilisé est en mode inactif. Lorsqu'un utilisateur glisse une carte à piste magnétique, le périphérique se met en mode prêt. Le périphérique revient au mode inactif lorsqu'un utilisateur termine une transaction ou après une période d'inactivité en mode prêt, telle que configurée sur l'imprimante multifonctions.

Remarque : Le sous-système d'authentification revient au mode inactif si le temporisateur du mode veille de l'imprimante multifonctions s'active.

Lorsque le périphérique est en mode inactif, la diode lumineuse du lecteur de carte est de couleur rouge continue.

En mode prêt, la diode lumineuse du lecteur de carte est de couleur verte continue et l'utilisateur peut commencer à utiliser le périphérique contrôlé pour effectuer une transaction.

Administration de Secure Access

La totalité de l'administration est effectuée dans le gestionnaire Secure Access. Par défaut, le programme d'installation place le gestionnaire Secure Access dans le menu Démarrer.

Vous le trouverez sous **Démarrer > Tous les programmes > Xerox Secure Access > Gestionnaire Secure Access**.

> Remarque : Vous devez disposer des privilèges administrateur sur le serveur Secure Access pour lancer le gestionnaire Secure Access.

Pour pouvoir ouvrir le gestionnaire Secure Access, vous devez sélectionner le serveur CAS à utiliser. Etant donné que le serveur CAS effectue les validations par rapport à une base de données d'authentification unique, vous devez taper le nom exact de la base de données ou le choisir dans la liste.

L'interface du gestionnaire Secure Access comprend cinq zones. Lorsque vous choisissez une tâche parmi les outils, le volet de droite affiche aussitôt les paramètres correspondants disponibles.

Prise en charge linguistique

Lors de l'installation de Secure Access, l'Assistant d'installation vous invite à sélectionner la langue requise pour les composants déployés. Ce paramètre s'applique uniquement à l'interface du gestionnaire Secure Access.

La langue d'affichage sur le panneau avant de l'imprimante multifonctions est déterminée par les paramètres du périphérique. Le serveur Secure Access vérifie la langue sélectionnée sur le périphérique multifonctions chaque fois qu'un utilisateur glisse sa carte. Si une langue autre que l'anglais, le français, l'allemand, l'italien ou l'espagnol est définie sur l'imprimante multifonctions, les invites de Secure Access s'affichent en anglais par défaut.

Configuration et gestion 4

Ce chapitre contient les sections suivantes :

La configuration fait référence à la configuration logicielle requise pour établir une communication entre les imprimantes multifonctions, les périphériques d'authentification et le serveur Secure Access. Veillez à suivre la procédure décrite à la page 24 pour obtenir les meilleurs résultats possibles.

Ce chapitre explique comment :

- effectuer une configuration initiale complète ;
- ajouter les imprimantes multifonctions à la base de données Secure Access ;
- associer un périphérique d'authentification Secure Access à une imprimante multifonctions, lorsque vous n'utilisez pas de lecteur de carte USB ;
- appliquer l'authentification et définir des options d'authentification supplémentaires ;
- importer des comptes utilisateur et les soumettre à une synchronisation Active Directory ;
- surveiller les événements liés à l'authentification.

Procédure de configuration

Vous devez suivre les étapes dans l'ordre dans lequel elles sont présentées ci-après. Sinon, l'installation sera incomplète.

Avant de commencer, vérifiez que vous avez correctement installé le serveur Secure Access. Suivez les instructions indiquées dans le Guide d'installation de Xerox Unified ID System®. Installez le serveur CAS et au moins un moteur DCE et un moteur DRE.

1. **Configurer le périphérique multifonctions Xerox de manière à accepter l'authentification réseau par le biais du mécanisme Xerox Secure Access**

   Cette fonction est assurée par les services Internet CentreWare auxquels vous accédez par un navigateur Internet. Consultez le CD d'administration du système de l'imprimante multifonctions pour obtenir des informations sur l'installation et la configuration de Xerox Secure Access sur le périphérique.

2. **Ajouter les imprimantes multifonctions à la base de données Secure Access**

   Créer une entrée pour chaque imprimante multifonctions dans le gestionnaire Secure Access. Affectez chaque imprimante multifonctions à un serveur d'impression DRE particulier (au besoin).

3. **Configurer l'impression Follow-You**

   Remarque : Cette étape est facultative et ne doit être effectuée que si l'impression Follow-You est requise sur le site.

   Pour configurer l'impression Follow-You, créez des groupes d'extraction qui regroupent des périphériques ayant des caractéristiques communes. Lorsque l'utilisateur envoie un document à une imprimante multifonctions appartenant à un groupe d'extraction, il peut s'authentifier auprès de n'importe quelle imprimante multifonctions du groupe d'extraction et « extraire » le travail de la file d'attente en vue de son impression sur cette imprimante multifonctions.

4. **Définir les paramètres d'authentification**

   Configurez les paramètres qui seront requis par Secure Access pour authentifier les demandes d'accès utilisateur, y compris pour autoriser les invites secondaires et la configuration des données de carte.

5. **Importer et synchroniser les comptes utilisateur**

   Définir les paramètres de synchronisation Active Directory, puis importer les comptes utilisateur existants dans la base de données Secure Access.

6. **Installer le service personnalisé Release My Documents (Libérer mes documents)**

   Pour permettre aux utilisateurs d'afficher la libération d'un ou de plusieurs documents placés dans la file d'attente d'impression sécurisée directement à partir du panneau avant de l'imprimante multifonctions, installez le service personnalisé Release My Documents (Libérer mes documents).

7. **Configurer l'enregistrement automatique des cartes utilisateur**

   Pour permettre aux utilisateurs d'enregistrer eux-mêmes leurs cartes magnétiques.

Ajout des imprimantes multifonctions à la base de données Secure Access

Chaque imprimante multifonctions doit être enregistrée dans la base de données Secure Access. Vous devez affecter un nom unique à chaque imprimante multifonctions et vous avez besoin de l'adresse IP réseau de chaque périphérique.

Afin que l'administration soit simplifiée, cette étape est divisée en deux sous-étapes : Entrer les paramètres de périphérique et Associer l'imprimante multifonctions à un périphérique d'authentification Secure Access.

Entrer les paramètres de périphérique

1. Dans le gestionnaire Secure Access, cliquez sur **Devices** (Périphériques).
2. À partir des paramètres (Settings), cliquez sur **Add...** (Ajouter) dans la liste des périphériques.
3. Dans la boîte de dialogue Physical Device Summary (Récapitulatif des périphériques physiques) qui apparaît, tapez les informations requises, décrites dans le tableau ci-après.

   Remarque : Le fabricant et le modèle sont automatiquement insérés lorsque le périphérique contacte le moteur DRE pour la première fois. La prochaine fois que vous ouvrirez cette boîte de dialogue, ces informations y figureront.

Paramètre	Description
Name (Nom)	Tapez un nom unique pour cette imprimante multifonctions. Vous utiliserez ce nom pour identifier le périphérique dans le gestionnaire Secure Access.
Hostname/IP address (Nom d'hôte/Adresse IP)	Tapez l'adresse IP ou le nom d'hôte. Vérifiez que vous pouvez résoudre le nom d'hôte si vous ne connaissez pas l'adresse IP.
Description	Entrez une description qui permet aux autres administrateurs d'identifier le périphérique, généralement en fonction de l'emplacement. Par exemple, « deuxième étage, RH ».
Périphérique d'authentification	Sélectionnez le périphérique d'authentification Secure Access (à partir de son adresse MAC) qui contrôlera l'accès à cette imprimante multifonctions. Remarque : Si vous utilisez un lecteur de carte USB Secure Access, vous n'associez pas de périphérique d'authentification et vous devez laisser dans ce champ la valeur <USB Reader> (Lecteur USB).

Paramètre	Description
Compatibilité Secure Access	• **Imprimante multifonctions gérant Secure Access :** indiquez si votre imprimante multifonctions utilise un lecteur de carte USB ou si vous utilisez une imprimante multifonctions Xerox prenant en charge Secure Access. Saisissez également l'**ID administrateur** et le **mot de passe** associés à cette imprimante multifonctions. • **Autre type de périphérique multifonctions ou d'imprimante :** sélectionnez si le périphérique d'authentification est utilisé pour l'impression Follow-You avec un périphérique multifonctions ou une imprimante ne prenant pas en charge Secure Access.
Serveur	Saisissez le nom du serveur sur lequel a été installé le moteur DCE et qui contrôlera le périphérique multifonctions ou l'imprimante en question.
Initialiser le périphérique Secure Access	Le périphérique Secure Access est automatiquement initialisé lors de sa première configuration. Si vous avez changé d'imprimante multifonctions, initialisez le périphérique Secure Access en cliquant sur ce bouton. Une fenêtre indépendante apparaît pour confirmer la réussite de l'initialisation. Remarque : Vous pouvez cliquer sur ce bouton pour installer le service personnalisé Release My Documents (Libérer mes documents). Pour plus d'informations, voir Configuration du service personnalisé Release My Documents (Libérer mes documents) à la page 41.
Behavior (Comportement)	Si vous utilisez le moniteur de port Secure Access pour activer l'impression Follow-You, vous pouvez sélectionner l'une des deux options de libération suivantes : • **At assigned control terminal** (Sur le terminal de contrôle affecté) : l'utilisateur doit glisser sa carte dans l'imprimante multifonctions pour libérer les documents envoyés à ce périphérique. • **Release documents from pull group** (Libérer les documents à partir d'un groupe d'extraction) : après l'authentification, l'utilisateur peut suivre les instructions affichées sur le panneau avant pour sélectionner les documents en attente à partir d'un groupe d'extraction spécifique. Pour plus d'informations, voir Configuration de l'impression Follow-You à la page 32. Si vous utilisez les moniteurs de port Windows, ces paramètres sont sans effet.

4. Cliquez sur **OK** pour enregistrer les paramètres.

   Remarque : Si Secure Access détecte que le périphérique est activé pour les services personnalisés et que vous avez effectué des modifications dans la boîte de dialogue Périphériques, une fenêtre contextuelle s'affiche :

   - Si l'extension Release My Documents (Libérer mes documents) n'est pas installée sur le périphérique, l'invite « Voulez-vous activer l'impression Follow-You ? » s'affiche.
   - Si l'extension Release My Documents (Libérer mes documents) est installée sur le périphérique, l'invite demande « Voulez-vous conserver l'activation de l'impression Follow-You ? ».

Associer l'imprimante multifonctions à un périphérique d'authentification Secure Access

Remarque : Si vous utilisez un lecteur de carte USB Secure Access, vous pouvez ignorer cette étape.

Lorsque vous mettez sous tension un périphérique d'authentification connecté au réseau, le moteur DCE enregistre le périphérique. Le périphérique apparaît dans le gestionnaire Secure Access en tant que périphérique d'authentification Secure Access non assigné. Vous devez associer chaque imprimante multifonctions à un périphérique d'authentification Secure Access spécifique. Utilisez le feuillet détachable (voir le Guide d'installation) que vous avez rempli lors de la configuration matérielle afin de mapper chaque périphérique d'authentification avec l'imprimante multifonctions appropriée.

1. Dans le gestionnaire Secure Access, cliquez sur **Devices** (Périphériques), puis sélectionnez l'imprimante multifonctions à configurer.
2. Dans la boîte de dialogue Physical Device Summary (Récapitulatif des périphériques physiques), ouvrez la liste déroulante Hardware Address (Adresse matérielle).
3. A l'aide du feuillet détachable, recherchez l'adresse MAC adéquate du périphérique d'authentification qui contrôlera l'accès à cette imprimante multifonctions spécifique.
4. Cliquez sur **OK** pour enregistrer les modifications.

Définition des paramètres d'authentification

Avant d'importer les comptes utilisateur, vous devez configurer le serveur d'authentification central pour valider les comptes par rapport aux codes confidentiels des comptes principaux et secondaires. Les informations sur le code confidentiel permettent d'établir une connexion entre un compte d'utilisateur Secure Access et les informations enregistrées dans une carte magnétique.

Le code confidentiel principal est la séquence numérique qui identifie l'utilisateur de manière unique et correspond généralement au numéro de carte. Pour entrer le code confidentiel principal, l'utilisateur glisse simplement sa carte.

Si vous souhaitez un niveau de sécurité supplémentaire, vous pouvez activer des codes confidentiels secondaires. Ainsi, l'utilisateur doit d'abord glisser sa carte, puis entrer un « mot de passe » supplémentaire sur le panneau avant de l'imprimante multifonctions. C'est seulement lorsque les données de la carte magnétique et le mot de passe du code confidentiel secondaire sont authentifiés que l'utilisateur a accès à l'imprimante multifonctions.

1. Dans le gestionnaire Secure Access, sélectionnez **Configuration > Authentication Device Settings** (Paramètres du périphérique d'authentification).
2. Dans la section **Authentication mechanisms** (Mécanismes d'authentification), sélectionnez un ou plusieurs mécanismes d'authentification :
   - Laissez la case **Secure Access PINs** (Codes confidentiels Secure Access) activée uniquement si vous souhaitez connecter un compte d'impression Secure Access avec des informations d'ouverture de session.
   - Activez la case **External user ID and password** (ID utilisateur et mot de passe externes) uniquement si vous utilisez des cartes magnétiques pour vérifier toutes les informations utilisateur hors de Secure Access.
   - Activez la case **Secure Access PIN with external password** (Code confidentiel Secure Access avec mot de passe externe) si les utilisateurs doivent glisser leurs cartes pour l'identification, mais également entrer leur mot de passe de compte d'utilisateur de domaine Secure Access. Secure Access recherche le nom de compte correspondant dans la base de données, puis vérifie le compte par rapport à l'autorité externe sélectionnée pour l'ouverture de session réseau.

   Remarque : Si vous sélectionnez un mécanisme d'authentification externe, le champ **Enable secondary prompt** (Activer l'invite secondaire) est automatiquement activé. L'authentification externe ne peut avoir lieu si les informations sur le code confidentiel secondaire ne sont pas indiquées.
3. Dans la section **External authorities** (Autorités externes), ne sélectionnez une ou plusieurs autorités externes que si vous avez sélectionné une méthode d'authentification correspondante :
   - Sélectionnez **Windows** pour valider les comptes par rapport à un domaine Windows par défaut. Tapez le nom de domaine dans le champ **Default domain** (Domaine par défaut).
   - Sélectionnez **NetWare** pour valider les comptes par rapport à un contexte NetWare par défaut. Tapez le nom dans le champ **Default context** (Contexte par défaut).

   Remarque : Vous devez installer le client Novell NetWare pour Windows sur le serveur d'authentification central si vous envisagez de procéder à la validation par rapport à un contexte NetWare.

- Sélectionnez **LDAP** pour valider les comptes par rapport à un serveur LDAP par défaut. Tapez le nom du serveur LDAP, puis choisissez un type LDAP dans la liste. Sélectionnez Force SSL encryption (Forcer le chiffrement SSL) si vous souhaitez utiliser le chiffrement Secure Socket Layer.

4. Dans la zone **Card setup** (Configuration de la carte), procédez comme suit :
   a. Entrez les positions initiale et finale des données dans les champs respectifs. Les données extraites de ces positions font office de code confidentiel principal.
   b. Cliquez sur **<None>** (Aucun) en regard de **HID decoding** (Décodage HID) si vous utilisez un lecteur de carte de proximité HID. Les périphériques d'authentification doivent être configurés de manière à renvoyer les informations de la carte dans un format standard.

   Pour plus d'informations sur la façon d'entrer les paramètres de décodage, voir HID decoding (Décodage HID) à la page 30.
   c. Sélectionnez **Auto-register primary PINs** (Enregistrement automatique des codes confidentiels principaux) pour autoriser les utilisateurs à enregistrer une carte magnétique pour une utilisation future. Pour plus d'informations, voir Enregistrement automatique des cartes magnétiques à la page 31.
5. Dans la zone des **invites du périphérique Secure Access**, entrez le texte qui apparaîtra par défaut sur le panneau avant de l'imprimante multifonctions :
   a. Entrez le titre (**Title**) qui apparaîtra dans toutes les invites.
   b. Entrez le texte de l'invite de connexion (**Login prompt**) qui apparaîtra pour inviter l'utilisateur à se connecter. Par exemple, « Veuillez glisser votre carte pour vous connecter ».
   c. Sélectionnez l'option **Enable secondary prompt** (Activer l'invite secondaire) pour afficher sur le panneau avant de l'imprimante multifonctions Xerox une invite indiquant à l'utilisateur d'entrer un code confidentiel (ou mot de passe) secondaire.
   d. Sélectionnez l'option **Enable release all jobs prompt** (Activer l'invite de la libération de tous les travaux) pour afficher sur le panneau avant de l'imprimante multifonctions Xerox une invite demandant à l'utilisateur s'il souhaite libérer tous les travaux en attente d'impression.
6. Dans la section **SNMP**, entrez vos **noms de communauté Get** et **Set**.

   Remarque : Si vous modifiez les noms par défaut dans Secure Access, vous devez également les modifier sur tous les périphériques physiques, afin que la communication SNMP fonctionne. Consultez la documentation de l'imprimante multifonctions pour plus d'informations sur la modification de ces paramètres.
7. Entrez le numéro d'identification de compte JBA (**JBA Account ID**) si vous souhaitez utiliser Secure Access avec une application de gestion de comptes JBA tierce.
8. Définissez le délai d'expiration des travaux (**Job Expiry**) (**en heures**) au terme duquel tous les travaux en attente d'impression expireront et seront supprimés de la file d'attente. La durée par défaut est 1 heure.

9. Si vous utilisez sur votre réseau des noms de communauté SNMP qui ne sont pas attribués par défaut (« public » pour l'accès en lecture et « privé » pour l'accès en écriture), précisez ces noms de communauté dans les champs correspondants de la boîte de dialogue. Notez que tous les périphériques doivent porter les mêmes noms de communauté.

   Remarque : Si vous ne saisissez pas les noms de communauté, le serveur Secure Access ne détectera pas automatiquement les types de périphériques lors de la création de nouveaux ports. Toutefois, vous pourrez toujours créer ces ports manuellement en indiquant les informations de connexion.

10. Cliquez sur **OK** pour enregistrer les paramètres.

HID decoding (Décodage HID)

Pour configurer l'encodage HID, procédez comme suit :

1. Dans le gestionnaire Secure Access, sélectionnez **Configuration** > **Authentication Device Settings** (Paramètres du périphérique d'authentification).
2. Cliquez sur **<None>** (Aucun) en regard de **HID decoding** (Décodage HID) dans la section Card Setup (Configuration de la carte).
3. Dans la boîte de dialogue **HID decoding** (Décodage HID), procédez comme suit :
   - Si vous connaissez le codage, entrez les informations de codage de carte HID suivantes. Sinon, contactez votre fournisseur HID pour déterminer le type de codage utilisé sur vos cartes de proximité.
   - Si vous n'avez pas besoin d'extraire les informations sur le code de facilité, activez uniquement la case **ID code** (Code ID). Si vous devez extraire le code de facilité et le code ID, activez les deux options.

   a. Dans le champ **Facility Start** (Début facilité), entrez la position initiale du code de facilité dans le flux binaire brut (base 0, de la gauche vers la droite, inclus).
   b. Dans le champ **Facility End** (Fin facilité), entrez la position finale du code de facilité dans le flux binaire brut (base 0, de la gauche vers la droite, inclus).
   c. Dans le champ **Facility Width** (Largeur facilité), entrez le nombre de chiffres décimaux pour la partie facilité de la valeur que doit générer le périphérique d'authentification. Le cas échéant, les nombres seront complétés à gauche par des zéros. Si votre site ou carte HID n'utilise pas de code de facilité ou que celui-ci n'a pas besoin d'être renvoyé en tant qu'élément de la valeur de la carte, entrez une largeur de 0 pour désactiver l'extraction du numéro de facilité.
   d. Dans le champ **ID Start** (Début ID), entrez la position initiale du code ID dans le flux binaire brut (base 0, de la gauche vers la droite, inclus).
   e. Dans le champ **ID End** (Fin ID), entrez la position finale du code ID dans le flux binaire brut (base 0, de la gauche vers la droite, inclus).
   f. Dans le champ **ID Width** (Largeur ID), entrez le nombre de chiffres décimaux pour la partie du code ID de la valeur que doit générer le périphérique d'authentification. Le cas échéant, les nombres seront complétés à gauche par des zéros. Le périphérique d'authentification renverra une valeur unique pour chaque glissement de carte, c'est-à-dire le code de facilité décodé suivi de l'ID décodé.
   g. Cliquez sur **OK** pour enregistrer les paramètres.

Enregistrement automatique des cartes magnétiques

Si vous souhaitez que les utilisateurs puissent enregistrer automatiquement leurs cartes magnétiques, vous devez activer cette option dans Secure Access.

1. Dans le gestionnaire Secure Access, sélectionnez **Configuration > Authentication Device Settings** (Paramètres du périphérique d'authentification).
2. Sélectionnez **Auto-register primary PINs** (Enregistrement automatique des codes confidentiels principaux) dans la section **Card Setup** (Configuration de la carte).
3. Cliquez sur **OK** pour enregistrer les modifications.

Lorsqu'un utilisateur glisse une carte non enregistrée, il est invité à se connecter à l'imprimante multifonctions à l'aide d'informations de connexion valides (ID et mot de passe utilisateur). Les informations de connexion de l'utilisateur doivent exister préalablement sur le serveur CAS pour que l'enregistrement automatique soit possible.

Une fois que l'utilisateur a enregistré sa carte, lorsqu'il glissera sa carte la prochaine fois, les informations de son compte seront associées automatiquement à sa carte et il pourra se connecter sans avoir à entrer manuellement ses informations de connexion. Si l'option correspondante a été configurée, l'utilisateur peut être invité à entrer un code confidentiel secondaire.

Remarque : Si l'option **Secure Access PIN with external password** (Code confidentiel Secure Access avec mot de passe externe) est sélectionnée lors de la configuration de l'enregistrement automatique de la carte, le code confidentiel Secure Access est remplacé par les données de la carte magnétique une fois la carte authentifiée et enregistrée. Le code confidentiel Secure Access n'est plus une information de connexion valide.

Configuration de l'impression Follow-You

L'impression Follow-You permet à un utilisateur d'envoyer un travail d'impression à une imprimante multifonctions spécifique, mais de s'authentifier sur une autre imprimante multifonctions afin de visualiser une liste de travaux conservés dans une file d'attente sécurisée. L'utilisateur peut alors « extraire » le travail d'impression sur l'imprimante multifonctions où il s'est authentifié, même s'il ne s'agit pas du périphérique initialement sélectionné pour cette tâche.

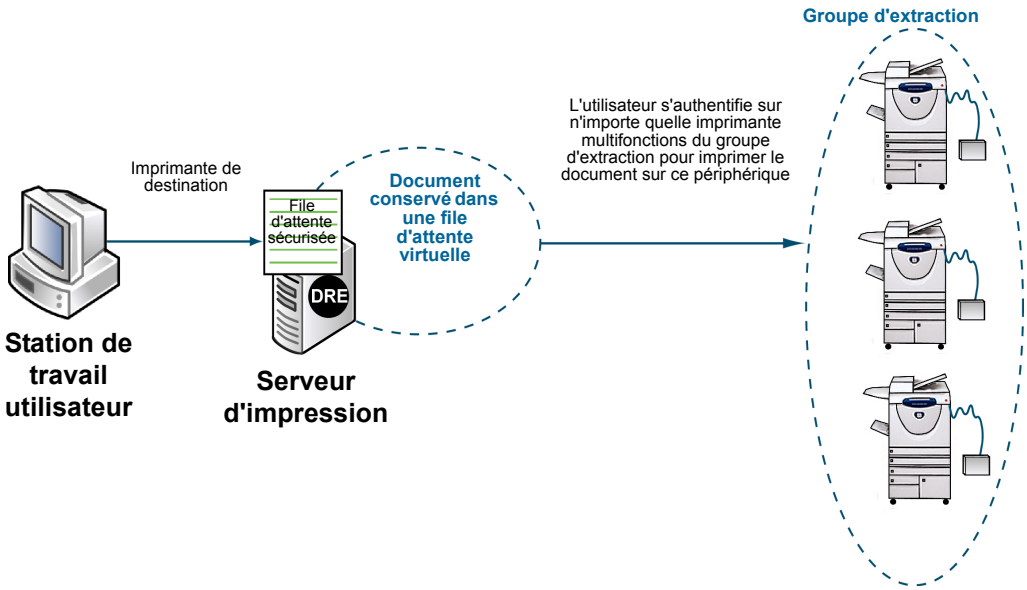


Figure 4-1: Procédure utilisateur pour l'impression Follow-You

La configuration de l'impression Follow-You comprend deux étapes :

1. Utilisez le moniteur de port Secure Access pour activer la configuration entre le serveur d'impression et toutes les imprimantes multifonctions contrôlées. Vous pouvez convertir les ports Windows existants en ports Secure Access. Le moniteur de port intercepte tous les documents envoyés aux périphériques appartenant à un groupe d'extraction et les conserve dans la file d'attente sécurisée jusqu'à ce qu'ils soient libérés par l'utilisateur authentifié. La section Convertir des ports pour utiliser le moniteur de port Secure Access à la page 33 indique la procédure à suivre.
2. Créez les groupes d'extraction dans le gestionnaire Secure Access. Reportez-vous à la section Créer des groupes d'extraction à la page 34.

Si vous voulez permettre à l'utilisateur de consulter ses travaux d'impression en attente dans la file sécurisée directement à partir du panneau avant de l'imprimante multifonctions, mettez à jour cette dernière de manière à inclure le service personnalisé Release My Documents (Libérer mes documents). La section Configuration du service personnalisé Release My Documents (Libérer mes documents) à la page 41 indique la procédure à suivre.

Convertir des ports pour utiliser le moniteur de port Secure Access

Secure Access utilise des ports spécialisés pour activer l'impression Follow-You. Chaque périphérique appartenant à un groupe d'extraction doit utiliser un moniteur de port Secure Access. Si des périphériques existants sont déjà configurés de manière à utiliser des ports Windows, vous pouvez facilement convertir les ports.

1. Vérifiez que les périphériques à convertir sont sous tension, connectés au réseau et configurés pour l'impression.
2. A l'aide du **Poste de travail**, recherchez l'emplacement où vous avez installé Secure Access.
3. Ouvrez le dossier **Tools** (Outils), puis double-cliquez sur **SAPrinterConversionWizard.exe**.
4. Dans l'écran de bienvenue de l'Assistant de conversion d'imprimante, cliquez sur Next (Suivant).
5. Sélectionnez l'emplacement du serveur d'impression (**Print server location**).

   Si le serveur d'impression (moteur DRE) réside sur l'ordinateur local, sélectionnez l'option **Local machine** (Ordinateur local), sinon sélectionnez l'option **Remote server** (Serveur distant).
6. Sélectionnez l'option **Convert printers to use the Secure Access Port Monitor** (Convertir les imprimantes pour utiliser le moniteur de port Secure Access), puis cliquez sur **Next** (Suivant).
7. Sélectionnez ou désélectionnez des imprimantes dans la liste **Convert printers** (Convertir les imprimantes), puis cliquez sur **Next** (Suivant).
8. Cliquez sur **Finish** (Terminer) pour achever la conversion.

Créer une file d'attente d'impression avec un port Secure Access

Suivant votre matériel d'impression, il se peut que vous ayez besoin de plusieurs ports utilisant le moniteur de port Secure Access sur un serveur d'impression. Vous pouvez configurer une nouvelle définition d'imprimante utilisant le moniteur de port Secure Access.

1. A l'aide de l'interface Windows standard, ouvrez l'Assistant Windows **Ajout d'imprimante**.
2. Suivez les invites pour ajouter une imprimante locale et créer un nouveau port.
3. Lorsque vous y êtes invité, sélectionnez **Port Secure Access** comme type de port à créer, puis cliquez sur Suivant. L'Assistant Add Printer Port Secure Access (Ajouter un port d'imprimante Secure Access) s'affiche et vous êtes invité à vérifier que le périphérique d'impression est sous tension, connecté au réseau et correctement configuré.
4. Cliquez sur **Next** (Suivant) et sélectionnez l'option **Physical printer** (Imprimante physique) comme **Device Type** (Type de périphérique) dans la liste déroulante.
5. Spécifiez un nom d'imprimante (**Printer name**) ou une adresse IP (**IP address**).
6. L'Assistant fournit un nom de port (**Port name**) basé sur le nom de l'imprimante ou sur l'adresse IP. Si vous le souhaitez, vous pouvez modifier ce nom manuellement.
7. Cliquez sur **Next** (Suivant) pour poursuivre la définition des options de configuration du port. L'écran Port Configuration (Configuration du port) apparaît. Le message **Detected device information** (Informations sur le périphérique détecté) apparaît automatiquement si l'Assistant peut collecter ces données à partir de l'imprimante.
8. Indiquez si vous souhaitez utiliser des paramètres standard ou personnalisés pour ce port.

Si vous sélectionnez l'option **Use custom settings** (Utiliser des paramètres personnalisés) :

a. Si vous sélectionnez l'option **Raw port communication** (Communication de port RAW), identifiez le numéro de port TCP et indiquez si le moniteur de port doit maintenir la connexion ouverte.
b. Si vous sélectionnez l'option **LPR**, spécifiez le nom de la file d'attente (**Queue**) sur le périphérique physique (par exemple, PORT1).
c. Si vous sélectionnez l'option **Specific device** (Périphérique spécifique), sélectionnez le fabricant (**Manufacturer**) et le modèle (**Model**) appropriés dans les listes déroulantes. En fonction des choix effectués, le périphérique utilise les paramètres de communication par défaut appropriés.

9. Cliquez sur **Next** (Suivant) et spécifiez le nom du périphérique physique (**Physical device name**). Il s'agit du nom du périphérique tel qu'il apparaît dans Secure Access.
10. Examinez les détails de l'enregistrement de ces nouveaux port et périphérique, puis cliquez sur **Finish** (Terminer) pour fermer l'Assistant Add Secure Access Printer Port (Ajouter un port d'imprimante Secure Access) ou sur **Back** (Précédent) pour modifier les paramètres de votre choix. Si vous fermez l'Assistant Add Secure Access Printer Port (Ajouter un port d'imprimante), vous revenez à l'Assistant Ajout d'imprimante Windows.
11. Exécutez les étapes restantes de l'Assistant Ajout d'imprimante. Lorsque vous y êtes invité, sélectionnez **Oui** pour imprimer une page de test.
12. Confirmez les détails d'imprimante Windows, puis cliquez sur **Terminer** pour quitter l'Assistant ou sur **Précédent** si vous souhaitez modifier des paramètres.

Créer des groupes d'extraction

Les groupes d'extraction que vous créez doivent refléter les besoins de votre organisation. Par exemple, vous pouvez regrouper les périphériques compatibles en fonction de leur emplacement physique, du service, du fabricant, et ainsi de suite. Vous pouvez également créer des groupes d'extraction qui comprennent une sélection de périphériques relevant d'un seul serveur d'impression.

Le pilote de périphérique sélectionné dans le groupe d'extraction doit être compatible avec l'ensemble des périphériques associés à ce groupe. Si vous souhaitez qu'un travail d'impression généré pour une imprimante multifonctions donnée soit imprimé sur une autre imprimante multifonctions, assurez-vous que l'autre imprimante peut comprendre toutes les commandes d'impression incluses dans le flux de données provenant du pilote.

1. Dans le gestionnaire Secure Access, cliquez sur la ou les imprimantes multifonctions à affecter au même groupe d'extraction.
2. Dans la boîte de dialogue Physical Device Summary (Récapitulatif des périphériques physiques), sélectionnez l'option **Release documents from pull group** (Libérer les documents à partir d'un groupe d'extraction). Tapez le nom explicite de votre choix pour le groupe d'extraction, puis cliquez sur **OK** pour appliquer la modification.

   Remarque : Vous ne devez taper le nom du groupe d'extraction que lorsque vous l'utilisez pour la première fois. Ensuite, il apparaîtra automatiquement dans la liste.
3. Répétez les étapes 1 et 2 pour sélectionner des périphériques et créer d'autres groupes d'extraction.

Importation et synchronisation de comptes utilisateur

Pour activer l'authentification, vous devez créer des comptes utilisateur qui correspondent aux attributs utilisés lors du glissement des cartes. Lorsqu'un utilisateur glisse sa carte, le périphérique d'authentification transfère la demande d'accès au moteur DCE, qui transfère à son tour les détails du glissement de la carte au serveur CAS. Si le serveur CAS trouve un compte d'utilisateur dont les attributs correspondent à ceux figurant sur la carte, l'imprimante multifonctions est déverrouillée et l'utilisateur peut libérer le travail de télécopie, de numérisation, de photocopie ou d'impression.

Secure Access met à votre disposition trois méthodes pour importer les comptes utilisateur :

- Utiliser Active Directory pour importer (et éventuellement synchroniser) les comptes
- Importer les comptes utilisateur depuis un fichier CSV
- Créer les comptes manuellement dans le gestionnaire Secure Access

Utiliser le serveur ADS pour importer des utilisateurs existants

Si vous disposez d'un serveur Active Directory, vous pouvez sélectionner les informations de compte à importer, puis procéder à la synchronisation. La synchronisation réduit au minimum le temps système consacré à l'administration et permet d'automatiser les mises à jour des comptes.

La réalisation de la procédure détaillée ci-après amène une tâche à s'exécuter en arrière-plan. Dans le gestionnaire Secure Access, cliquez sur l'outil Users (Utilisateurs) pour voir le résultat de la tâche ; la liste des utilisateurs se remplit automatiquement une fois la tâche achevée.

> Remarque : Les services Secure Access doivent être démarrés par un compte de domaine ayant accès à l'annuaire Active Directory de contact. Vérifiez que vous avez ouvert une session en tant qu'administrateur de domaine. Si les services sont démarrés sous le compte administratif local, la synchronisation Active Directory échouera.

Il est important de sélectionner les options dans l'ordre adéquat dans la boîte de dialogue Active Directory Synchronization (Synchronisation Active Directory) ; par conséquent, suivez attentivement les étapes indiquées ci-après.

1. Dans le gestionnaire Secure Access, cliquez sur **Configuration > Active Directory Synchronization** (Synchronisation Active Directory).
2. Dans la zone **Domain controllers** (Contrôleurs de domaine), cliquez sur **Add** (Ajouter). Un contrôleur de domaine est un serveur qui permet d'accéder à l'annuaire Active Directory des ordinateurs membres. Tapez le nom du contrôleur (Controller name) dans le champ.
3. Dans la zone **Containers** (Conteneurs), cliquez sur **Add** (Ajouter). Un conteneur est un dossier, dans l'arborescence Active Directory, qui contient des utilisateurs, des groupes ou des ordinateurs.

> ⚠ **ATTENTION :** Vérifiez que les conteneurs d'unité d'organisation que vous choisissez ne comprennent que des données de compte d'utilisateur. Si les unités d'organisation contiennent d'autres données (telles que des informations système ou de contact), vous obtiendrez des résultats inattendus. Vous pouvez être amené à créer des conteneurs d'unité d'organisation spécifiques à utiliser uniquement à des fins d'importation et de synchronisation.

4. Ajustez l'intervalle de synchronisation (**Synchronization interval**) pour modifier la fréquence avec laquelle Secure Access synchronise sa base de données avec l'annuaire Active Directory spécifié. La valeur de l'intervalle de synchronisation doit être d'au moins 15 minutes.
5. Sélectionnez ou désélectionnez les options **Active Directory updates to be applied** (Mises à jour Active Directory à appliquer)—**Adds** (Ajouts), **Deletes** (Suppressions) ou **Changes** (Modifications)—pour spécifier les comptes Active Directory que Secure Access devra recevoir et appliquer à la base de données des comptes lors des prochaines synchronisations.

   Vous pouvez importer des utilisateurs ajoutés ou modifiés ou supprimer des comptes inactifs de la base de données Secure Access. Conservez les valeurs par défaut de ces paramètres afin que les comptes soient mis à jour et constamment synchronisés avec le serveur Active Directory.
6. Les attributs **Assign Values from Active Directory** (Affecter des valeurs à partir d'Active Directory) vous permettent de gagner du temps en affectant des attributs spécifiques à tous les utilisateurs appartenant au conteneur sélectionné. Notez que vous devez entrer le nom d'attribut Active Directory et pas l'étiquette du champ. Bien que vous puissiez mettre à jour les comptes utilisateur individuels ultérieurement, choisissez ces attributs avant de procéder à l'importation afin d'accélérer la création des comptes.

   Les attributs **Primary PIN** (Code confidentiel principal) et **Secondary PIN** (Code confidentiel secondaire) mappent les valeurs de code confidentiel numériques trouvées sur le serveur Active Directory avec les champs Primary PIN (Code confidentiel principal) et Secondary PIN (Code confidentiel secondaire) de Secure Access. Si vous souhaitez importer ces champs, cochez la valeur Secondary PIN (Code confidentiel secondaire), que l'utilisateur pourra entrer sur le panneau avant de l'imprimante multifonctions (une invite secondaire est similaire à un mot de passe qui ajoute une autre couche de sécurité) si l'invite secondaire est activée dans **Configuration > User Authentication Device Settings** (Paramètres du périphérique d'authentification utilisateur). Pour les champs PIN1 (code confidentiel 1) (généralement le numéro de carte) et PIN2 (code confidentiel 2), tapez le nom d'attribut utilisé sur le serveur Active Directory.

   Les attributs **Primary PIN** (Code confidentiel principal) et **Secondary PIN** (Code confidentiel secondaire) peuvent également mapper des adresses de messagerie.
7. Cliquez sur **Import** (Importer) pour commencer immédiatement la tâche d'importation pour la première fois. La tâche d'importation s'exécute en arrière-plan et peut prendre plusieurs minutes, suivant la taille de l'annuaire Active Directory que vous importez.
8. Vous pouvez cliquer sur **OK** pour quitter la boîte de dialogue. L'exécution de la tâche se poursuivra, même si la boîte de dialogue est fermée.
9. Après plusieurs minutes, actualisez le gestionnaire Secure Access, puis consultez la liste des utilisateurs pour vérifier que l'importation des comptes a réussi. Par ailleurs, ouvrez les propriétés d'un compte d'utilisateur et vérifiez que les paramètres sont corrects.

Ajouter des utilisateurs à partir de l'importation d'un fichier plat

L'utilitaire **SACmd.exe** vous permet d'ajouter, de supprimer, de modifier et d'interroger des comptes d'utilisateur à partir d'un fichier plat.

Remarque : Cette méthode constitue une importation unique, dont les données ne sont pas synchronisées.

Secure Access installe cet utilitaire par défaut sur le serveur d'authentification dans le répertoire : **Program Files > Xerox >Secure Access > Tools**.

L'utilitaire de ligne de commande accepte les commandes dans le format suivant :

```
SACmd  -s(serveur) (action) (ID_obj)| [(options)]
Example : -sTestServer add user1 "Pierre Jean" pierrej@ici.com pin1 pin2
```

Exécution de la commande avec un fichier de commandes :

```
SACmd  -s(serveur) -f(fichier_commandes)
```

SACmd Processus de fichier de commandes

SACmd dispose d'un mode de traitement par lots et accepte un fichier CSV comme fichier de commandes, à raison d'un fichier par serveur. L'opération de traitement par lots autorise toutes les actions de commande, à l'exception de la commande d'interrogation.

Remarque : Copiez le fichier .csv dans le dossier **Secure Access > Tools**.

```
[Secure Acces\chemin_fichier_Tools]\SACmd –s(serveur) –f
nom_fichier_commandes.csv
```

Format de fichier CSV : `(action), (ID_obj)|All,  [(détails)]`

Les paramètres de ligne de commande entre parenthèses ( ) sont obligatoires, tandis que ceux entre crochets [ ] sont facultatifs. Utilisez le tableau ci-après pour renseigner les paramètres.

Paramètre	Variables
Serveur	Spécifiez le nom ou l'adresse IP du serveur CAS.
Action	Spécifiez l'action à exécuter sur le compte. Utilisez l'une des actions suivantes : • add - Ajouter un utilisateur • delete - Supprimer un utilisateur • query - Interroger la base de données. • modify - Modifier un attribut d'objet
ID_obj	Applique (action) uniquement à l'ID objet spécifié. Placez entre guillemets les ID objet comprenant un espace, par exemple Pierre Jean.
Options de la commande Action	Spécifiez des valeurs supplémentaires. Utilisez des guillemets pour délimiter les valeurs vides ou les valeurs détaillées contenant des espaces. Spécifiez les quantités avec un point en guise de séparateur décimal. Pour l'action modify, placez “!” pour les champs requis à ne pas modifier. (ID_utilisateur): ID d'utilisateur (nom_utilisateur): Nom d'utilisateur (adresse_électronique): Adresse électronique de l'utilisateur

Add

Add permet d'ajouter des comptes d'utilisateur. Tous les champs requis doivent être renseignés, jusqu'au dernier champ inclus.

Ajouter un utilisateur :

```
add(ID_utilisateur) [(nom_utilisateur) (adresse_électronique)
(code_confidentiel_principal) (code_confidentiel_secondaire)]
```

Exemple :

```
SACmd -SMonServeur add PierreJ "Pierre Jean" "pierrej@ici.com" 123
Motdepasse
```

Supprimer

Delete permet de supprimer des comptes d'utilisateur.

Supprimer un utilisateur :

```
delete (ID_utilisateur)
```

Exemple :

```
SACmd -SMonServeur delete PierreJ
```

Modify

Modify permet à l'utilisateur de modifier le paramètre de base de données utilisateur. Tous les champs requis doivent être renseignés, jusqu'au dernier champ inclus.

Modifier un utilisateur :

```
modify (ID_utilisateur) [(nom_utilisateur) (adresse_électronique)
(code_confidentiel_principal) (code_confidentiel_secondaire)]
```

Exemple : Mettre à jour l'adresse électronique de l'utilisateur pierrej et conserver les autres informations.

```
SACmd -SMonServeur modify pierrej! pierrej@nouvelendroit.com
```

Créer des comptes manuellement

Vous pouvez utiliser le gestionnaire Secure Access pour ajouter des comptes utilisateur individuels selon vos besoins.

1. Sélectionnez Users (Utilisateurs), puis cliquez avec le bouton droit dans le volet Settings (Paramètres) et choisissez l'option **Add User** (Ajouter un utilisateur) dans le menu.

2. Dans la boîte de dialogue User Properties (Propriétés de l'utilisateur), entrez les informations requises, décrites dans le tableau ci-après.

Champ	Description
User ID (ID utilisateur)	ID enregistré dans la base de données pour le suivi du compte.
Full Name (Nom complet)	Nom complet de l'utilisateur. Entrez le nom complet de manière à identifier facilement l'utilisateur dans le gestionnaire des comptes ou des départements. Ce nom apparaît également dans les relevés et rapports de compte.
Email address (Adresse de messagerie)	L'adresse de messagerie est fournie à l'imprimante multifonctions, pour des tâches telles que la numérisation dans un courrier électronique.
Primary PIN (Code confidentiel principal)	Le code confidentiel principal correspond généralement au numéro de carte.
Secondary PIN (Code confidentiel secondaire)	Le code confidentiel secondaire est utilisé comme mot de passe et l'utilisateur doit entrer ce code confidentiel sur le panneau avant de l'imprimante multifonctions après avoir glissé sa carte pour s'authentifier.
Confirm Secondary PIN (Confirmer le code confidentiel secondaire)	Tapez de nouveau le code confidentiel secondaire pour confirmer le mot de passe.

Contrôle des événements liés à l'authentification

Secure Access enregistre chaque événement lié à l'authentification dans la base de données . Vous pouvez générer un journal d'authentification pour n'importe quelle date et afficher l'historique d'événements, tels que les suivants :

- Echec de l'authentification
- Début de session (authentification réussie)

Chaque événement journalisé contient les informations suivantes :

- Source IP Address (Adresse IP source)
- Primary PIN (Code confidentiel principal)
- Validation Result (Résultat de la validation)
- Server type (Type de serveur)
- Username (Nom utilisateur)
- Email Address (Adresse électronique)
- Server Name (Nom du serveur)

Dans le gestionnaire Secure Access, cliquez sur **Authentication log** (Journal d'authentification), puis cliquez avec le bouton droit de la souris sur **View log by date** (Afficher le journal par date). Sélectionnez la date puis cliquez sur **OK**.

Configuration du service personnalisé Release My Documents (Libérer mes documents)

Le service personnalisé Release My Documents (Libérer mes documents) met à jour l'imprimante multifonctions afin d'ajouter l'option Release My Documents à l'écran des services personnalisés, sur le panneau avant de l'imprimante. Cet écran (illustré ci-dessous) affiche les travaux d'impression en attente appartenant à l'utilisateur actuel. L'utilisateur peut sélectionner un ou plusieurs travaux d'impression avant de les libérer ou de les supprimer directement à partir du panneau avant de l'imprimante multifonctions.

> Remarque : L'impression Follow-You doit également être configurée pour activer cette fonctionnalité. La section Configuration de l'impression Follow-You à la page 32 indique la procédure à suivre.

Lorsque le service personnalisé Release My Documents (Libérer mes documents) n'est pas installé, l'écran Release My Documents (Libérer mes documents) du panneau de l'imprimante multifonctions n'est pas disponible. L'utilisateur ne peut donc pas sélectionner des travaux d'impression individuels pour les libérer. Au lieu de cela, le système invite l'utilisateur à libérer tous les travaux d'impression en attente sur le serveur d'impression immédiatement après son authentification.

Lorsqu'un utilisateur s'authentifie, le serveur DCE est notifié de l'utilisateur actuel. Celui-ci contacte le(s) serveur(s) d'impression DRE pour obtenir la liste de tous les documents en attente destinés à cet utilisateur. L'écran Release My Documents (Libérer mes documents) du panneau avant affiche alors les travaux d'impression.

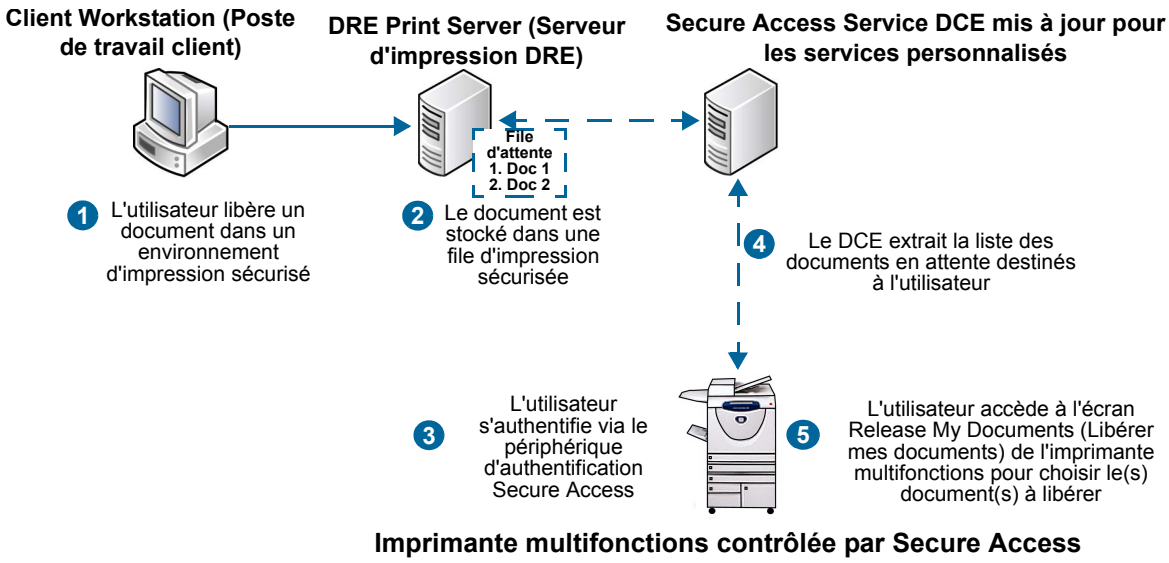


Figure 4-2: Architecture de Release My Documents (Libérer mes documents)

Ajouter le service personnalisé Release My Documents (Libérer mes documents) à l'imprimante multifonctions

Si vous ajoutez de nouveaux périphériques au gestionnaire Secure Access, vous êtes invité à installer le service personnalisé Release My Documents lorsque vous cliquez sur OK, après avoir effectué des modifications dans la fenêtre Device (Périphérique). Pour plus d'informations, voir Entrer les paramètres de périphérique à la page 25.

> Remarque : L'ajout du service personnalisé est facultatif. S'il n'est pas ajouté, l'utilisateur sera invité à libérer tous les documents pendant le processus d'authentification.

Pour ajouter le service personnalisé à un périphérique déjà configuré dans le gestionnaire Secure Access, exécutez les étapes suivantes :

1. Dans le gestionnaire Secure Access, cliquez sur **Devices** (Périphériques).
2. Dans la liste des périphériques, cliquez sur le périphérique que vous voulez mettre à jour.
3. Dans la boîte de dialogue Physical Device Summary (Récapitulatif des périphériques matériels) qui s'affiche, cliquez sur le bouton **Initialize Secure Access device** (Initialiser le périphérique Secure Access).
4. A l'invite "Do you want to enable Follow-You printing?" (Souhaitez-vous activer l'impression Follow-You ?), cliquez sur **Oui**.

   En s'exécutant en arrière plan, le programme met à jour le service DCE pour inclure l'écran Release My Documents (Libérer mes documents) dans les services personnalisés, sur le panneau avant de l'imprimante multifonctions.

Pour savoir si l'installation a réussi, authentifiez-vous sur l'imprimante multifonctions puis appuyez sur **All Services** (Tous les services). Le bouton portant la mention **Release my documents** (Libérer mes documents) doit apparaître. En fonction du modèle d'imprimante multifonctions, vous devrez peut-être appuyer sur le bouton **Custom Services** (Services personnalisés) pour voir cette fonction et y accéder.

Si l'installation a échoué, le bouton porte la mention **Servicex**, « x » étant un chiffre (par exemple, Service4 ou Service5). Voir Dépannage de l'installation du service personnalisé Release My Documents (Libérer mes documents) à la page 52 pour résoudre le problème.

Procédure de travail de l'utilisateur final Release My Documents (Libérer mes documents)

Le schéma ci-dessous illustre la procédure de travail de l'utilisateur final. Après avoir envoyé le travail d'impression, l'utilisateur se rend vers une imprimante multifonctions contrôlée. Il s'authentifie via un périphérique d'authentification Secure Access, puis sélectionne **Custom Services** > **Release My Documents** (Services personnalisés, Libérer mes documents) sur le panneau avant pour accéder aux fonctions de libération de documents sécurisées.

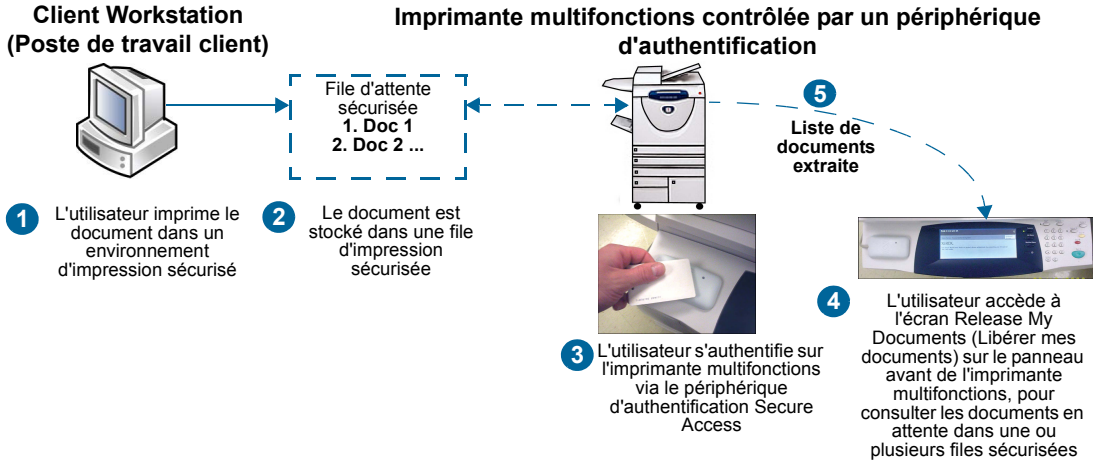


Figure 4-3: Procédure de travail de l'utilisateur final après l'installation de l'extension Release My Documents (Libérer mes documents)

Annexes

A

Ce chapitre contient les sections suivantes :

Autorisations d'accès à la synchronisation de l'annuaire

SAModifyDeletedContainerSecurity.exe modifie les autorisations d'accès administratif sur le conteneur des objets supprimés dans un annuaire Windows Active Directory, de manière à ce que Secure Access puisse accéder aux objets pendant les synchronisations de l'annuaire.

Par défaut, seuls les administrateurs Active Directory bénéficient de l'autorisation d'accès. Le compte Windows qui exécute les services Secure Access aura besoin de cet accès si vous souhaitez synchroniser les comptes supprimés entre Active Directory et Secure Access.

Le compte qui exécute cette commande doit être un administrateur dans le domaine Active Directory.

Pour plus d'informations sur la configuration des options de la synchronisation d'Active Directory, reportez-vous à Utiliser le serveur ADS pour importer des utilisateurs existants à la page 35.

Secure Access installe cet utilitaire par défaut sur le serveur d'authentification dans le répertoire : **Program Files > Xerox > Secure Access > Tools**.

L'utilitaire de ligne de commande accepte les commandes dans le format suivant :

```
SAModifyDeletedContainerSecurity.exe (-s serveur) [-p | {-r} -a nom_compte]
```

Les paramètres entre parenthèses ( ) sont obligatoires, tandis que ceux entre crochets [ ] sont facultatifs.

Paramètre	Description
-s serveur	Nom de serveur du contrôleur de domaine Active Directory.
-p	Afficher les autorisations actuelles sur le conteneur.
-r	Supprimer les autorisations d'accès pour le nom de compte spécifié.
- a nom_compte	Compte auquel accorder l'accès au conteneur. L'autorisation d'accès sera supprimée si l'option -r est utilisée par ailleurs.

Réinitialisation d'un périphérique d'authentification

Utilisez la clé de secours pour réinitialiser le périphérique d'authentification en fonction des paramètres par défaut. Cette clé a été fournie avec le périphérique et doit être conservée en lieu sûr.

1. Vérifiez que le périphérique d'authentification est sous tension.
2. Insérez la clé de secours dans son logement.
3. Tournez la clé d'un quart de tour VERS vous.
4. Tournez la clé vers sa position initiale.
5. Retirez la clé.

   Remarque : Le périphérique émettra un signal sonore toutes les 10 secondes si vous n'avez pas tourné la clé vers sa position initiale avant de la retirer.

Affectations des ports

Secure Access communique sur les ports suivants :

Composant	Port
CAS	TCP 2910
DRE	TCP 2938
DCE	TCP 1824, TCP 2939, UDP 2613
Périphérique d'authentification Secure Access	TCP 1234

Lorsque vous installez Secure Access, ces ports sont automatiquement ouverts. Toutefois, si vous devez contourner les paramètres de pare-feu Windows, vous pouvez ajouter les ports à la liste approuvée, sur chaque ordinateur où vous avez déployé un composant serveur Secure Access.

Dépannage

Avant de nous contacter pour obtenir de l'aide, veuillez consulter ci-après les symptômes et les instructions de dépannage indiquant comment résoudre le problème.

	Symptôme	Instruction
1	La lampe témoin du lecteur est-elle éteinte ?	**Périphérique d'authentification** : si la lampe témoin du lecteur de carte n'est pas allumée, cela signifie que le lecteur n'est pas sous tension. Périphérique d'authentification : vérifiez que le câble du lecteur est branché et que le connecteur est fermement fixé au connecteur mini-DIN sur l'unité de contrôle. Si le câble est correctement branché et que la lampe témoin demeure éteinte, passez à l'étape suivante. **Lecteur USB** : assurez-vous que l'imprimante multifonctions comporte la version logicielle adéquate. Vérifiez que le lecteur est correctement branché à l'imprimante multifonctions. Si la diode lumineuse reste éteinte après avoir vérifié le branchement et après avoir mis l'imprimante multifonctions hors tension puis à nouveau sous tension, essayez de remplacer le lecteur.
2	L'unité de contrôle est-elle sous tension ?	**Périphérique d'authentification** : vérifiez l'arrière (côté connecteur) de l'unité de contrôle. Le dispositif est sous tension si la lampe témoin jaune en regard de la prise femelle marquée « Ethernet » est allumée. Vérifiez que le câble d'alimentation électrique est fermement positionné et que le cordon d'alimentation est branché au bloc d'alimentation électrique et à la prise murale. Vérifiez que la prise murale est sous tension.
3	La lampe témoin du lecteur est-elle de couleur rouge et clignote-t-elle lentement ?	**Périphérique d'authentification** : si la lampe témoin du lecteur clignote lentement, cela signifie que le lecteur est correctement branché à l'unité de contrôle, mais que celle-ci n'a pas pu se connecter au serveur. Vérifiez que le câble Ethernet est branché à la prise femelle marquée « Ethernet » de l'unité de contrôle et à la prise Ethernet murale. **Lecteur USB :** le module de lecteur de l'imprimante multifonctions ne peut pas communiquer avec le serveur. Vérifiez que l'imprimante multifonctions dispose d'une connexion réseau et que l'appareil a été correctement initialisé dans le gestionnaire Secure Access.
4	La lampe témoin de la liaison Ethernet est-elle éteinte ?	**Périphérique d'authentification** : si la lampe témoin verte en regard de la prise femelle marquée « Ethernet » est éteinte, cela signifie qu'il n'y a pas de connexion Ethernet. Vérifiez que le cordon de raccordement Ethernet est correct en le testant à l'aide d'un autre câble, puis que la prise murale Ethernet est active.

	Symptôme	Instruction
5	La lampe témoin de la liaison Ethernet est-elle de couleur verte continue ?	**Périphérique d'authentification** : si la lampe témoin verte en regard de la prise femelle marquée « Ethernet » est de couleur verte continue, cela signifie qu'il y a une connexion Ethernet, mais aucune activité. Vérifiez que la prise murale Ethernet est connectée au concentrateur ou commutateur adéquat.
6	Le périphérique est-il répertorié sur le serveur Secure Access ?	**Périphérique d'authentification** : dans la console Secure Access, vérifiez que la liste déroulante des périphériques d'authentification contient l'adresse MAC du périphérique problématique. Si l'adresse MAC du périphérique (telle que la mentionne l'étiquette du numéro de série sur l'unité de contrôle) n'est pas répertoriée, le périphérique n'a pas pu établir un contact avec le serveur. **Lecteur USB :** aucun périphérique d'authentification n'est identifié pour l'utilisation d'un lecteur USB.
7	Le périphérique a-t-il obtenu une adresse IP ?	**Périphérique d'authentification** : si vous avez utilisé DHCP pour configurer le périphérique, consultez le serveur DHCP afin de vérifier qu'une adresse IP lui a été affectée (utilisez l'adresse MAC pour procéder à la vérification). Si aucune adresse IP n'a été affectée, le périphérique n'est pas en mesure de communiquer avec le serveur DHCP ou il n'a pas été paramétré au moyen d'une configuration IP manuelle.
8	Le périphérique a-t-il obtenu une adresse serveur via DHCP ?	**Périphérique d'authentification** : si vous utilisez DHCP pour configurer les périphériques, vérifiez que le serveur DHCP attribue la valeur 230 à l'adresse IP du serveur. Vérifiez que la valeur est l'adresse IP adéquate pour le serveur. Notez que le serveur Secure Access lui-même ne doit pas être configuré avec DHCP. Si la valeur 230 n'a pas été définie ou l'a été incorrectement, le périphérique ne sera pas en mesure de contacter le serveur.
9	L'adresse IP a-t-elle été définie manuellement ?	**Périphérique d'authentification** : si l'adresse IP a été définie manuellement, vérifiez les enregistrements afin de déterminer l'adresse IP du périphérique et connectez-vous à celui-ci à l'aide d'un navigateur Web. Si vous ne parvenez pas à vous connecter à la page Web avec l'adresse IP du périphérique, cela signifie que celui-ci n'est pas connecté correctement, qu'il n'est pas en mesure de communiquer ou que l'adresse IP a été incorrectement enregistrée. Pour éliminer la première possibilité, connectez le périphérique directement au PC à l'aide d'un câble inverseur, puis renouvelez la tentative de connexion. Une fois la connexion établie, vérifiez que les paramètres de gestion de réseau et l'adresse IP serveur sont corrects.

	Symptôme	Instruction
10	Le périphérique est-il inaccessible à son adresse IP ?	**Périphérique d'authentification :** si vous ne pouvez pas vous connecter à l'adresse IP du périphérique avec un câble Ethernet standard raccordé au port de liaison, rétablissez le paramétrage usine du périphérique. Pour ce faire, vous pouvez mettre l'unité de contrôle hors tension, insérer la clé, tourner celle-ci jusqu'à la position « on » puis remettre l'unité sous tension. Au bout de 30 secondes, coupez l'alimentation, retirez la clé, puis remettez l'unité sous tension. Vous devez maintenant pouvoir vous connecter à l'adresse IP par défaut (192.168.2.1) du périphérique (vérifiez que le paramétrage réseau de votre PC lui permettra de lire cette adresse). Si vous pouvez maintenant atteindre la page Web du périphérique, vous pouvez configurer les informations de gestion de réseau manuellement ou essayer la configuration DHCP en renouvelant la connexion au réseau. Si la page Web n'est toujours pas accessible, il se peut que l'unité de contrôle soit défectueuse.
11	La lampe témoin du lecteur est-elle de couleur rouge et clignote-t-elle rapidement lors d'un glissement de carte ?	Si la lampe témoin du lecteur est de couleur rouge et clignote rapidement, cela indique un glissement de carte incorrect dans le lecteur ; le serveur Secure Access a déterminé que l'ID carte ne correspond pas à un utilisateur valide sur le réseau. Testez le lecteur avec une carte d'utilisateur opérationnelle sur les autres lecteurs. Si les cartes sont mal lues sur tous les lecteurs, la configuration du serveur est peut-être en cause ; contactez le support technique pour vérifier la configuration de votre serveur.
12	La lampe témoin du lecteur est-elle de couleur rouge continue lors d'un glissement de carte ?	Si la lampe témoin du lecteur ne change pas lors d'un glissement de carte, cela indique que le lecteur n'a pas détecté de carte. Il est possible que la carte magnétique ait été codée selon une norme différente ou glissée verticalement ou horizontalement à l'envers ou du mauvais côté ; il peut aussi arriver qu'une carte de proximité ou sans contact ne soit pas placée suffisamment proche du lecteur ou qu'elle soit d'un type incorrect. Vérifiez que le glissement de carte a été réalisé correctement. Si la même carte fonctionne sur d'autres lecteurs du même site, le module du lecteur est peut-être en cause. Si la carte ne fonctionne pas sur d'autres lecteurs, vérifiez sa technologie auprès de son fournisseur et déterminez si elle est mentionnée dans la liste de compatibilité des cartes de lecteur.
13	La lampe témoin du lecteur devient-elle verte lors d'un glissement de carte ?	Une lampe témoin de couleur rouge indique une session Secure Access active. Cela signifie que la carte a été correctement lue et qu'elle correspond à un utilisateur Secure Access valide. Si la lumière devient verte, mais que l'imprimante multifonctions demeure désactivée, il est possible que le périphérique Secure Access soit associé à un périphérique multifonctions incorrect. Examinez la configuration des périphériques dans la console Secure Access afin de vérifier que le périphérique Secure Access est associé à l'imprimante multifonctions adéquate.

	Symptôme	Instruction
14	Le panneau avant de l'imprimante multifonctions est-il toujours déverrouillé ?	Le panneau avant de l'imprimante multifonctions ne peut être verrouillé que sur les périphériques qui prennent en charge Xerox Secure Access. Vérifiez que le modèle que vous essayez d'utiliser est pris en charge et qu'il est doté de la bonne version du micrologiciel.
15	Que signifient les messages d'erreur « L'impression Follow-You n'a pas pu être activée » et « L'impression Follow-You n'a pas pu être activée : aucun site spécifié » ?	Ces messages peuvent apparaître si le service personnalisé Release My Documents (Libérer mes documents) n'est pas correctement installé. Reportez-vous à la section Dépannage de l'installation du service personnalisé Release My Documents (Libérer mes documents) à la page 52.
16	Les invites du périphérique (titre/ invite de connexion) ne s'affichent pas sur le panneau avant de l'imprimante multifonctions.	Dans le gestionnaire Secure Access, ouvrez le périphérique spécifique. Cliquez sur le bouton **Initialize Secure Access device** (Initialiser le périphérique Secure Access). Le panneau avant de l'imprimante multifonctions devrait maintenant afficher les invites appropriées.
17	La lampe témoin du lecteur est-elle de couleur verte continue après le réamorçage de l'imprimante multifonctions ?	**Lecteur USB** : assurez-vous que l'imprimante multifonctions comporte la version logicielle adéquate.

Dépannage de l'installation du service personnalisé Release My Documents (Libérer mes documents)

Si le bouton ‘Release my documents’ (Libérer mes documents) ne s'affiche pas sur l'écran des services personnalisés de l'imprimante multifonctions, il vous faudra peut-être exécuter le logiciel d'installation avec un paramétrage spécifique. Si votre DNS ne permet pas à l'imprimante multifonctions de gérer le nom d'hôte du serveur sur lequel s'exécute le moteur DCE, l'outil ne peut pas enregistrer correctement les périphériques. Consultez le tableau ci-dessous pour connaître les paramètres spécifiques à utiliser.

L'exécutable de l'extension Release My Documents (Libérer mes documents) se trouve dans le dossier Tools (Outils) de la machine hébergeant le serveur d'authentification central. Pour installer les fichiers nécessaires, assurez-vous d'avoir les autorisations Administrateur sur le serveur qui héberge les services CAS et DCE.

1. Ouvrez l'invite de commandes, puis entrez le chemin du dossier Tools. Par exemple :
   c:\Program Files\Xerox\SecureAccess\Tools\
2. Lancez l'exécutable avec les paramètres précisés dans le tableau ci-dessous :
   saxeroxeipregistration.exe

   Remarque : Pour supprimer l'installation qui a échoué, vous pouvez exécuter la commande avec ces paramètres. Il n'est pas nécessaire d'annuler l'enregistrement de l'extension.

Paramètre	Résultat
-i	Identifie l'adresse IP de l'imprimante multifonctions qui recevra l'extension Release My Documents (Libérer mes documents)
-r	Enregistre le serveur DCE spécifié sur l'imprimante multifonctions sélectionnée
-d	Annule l'enregistrement de l'extension Release My Documents (Libérer mes documents) sur l'imprimante multifonctions spécifiée
-v	Affiche les informations enregistrées. Exécutez cette commande pour confirmer l'installation de l'extension.
-u	Nom de l'utilisateur qui sera autorisé à mettre à jour le périphérique
-p	Mot de passe obligatoire pour autoriser la mise à jour du périphérique
-c	Enumère les périphériques du serveur CAS spécifié et enregistre l'extension sur toutes les imprimantes multifonctions Xerox répertoriées dans la liste des périphériques
/?	Affiche la liste des paramètres dédiés à cette extension

Exemple :

```
saxeroxeipregistration.exe -i 192.168.97.180 -r 192.168.97.137
```

Adresse IP de l'imprimante multifonctions **Adresse IP du serveur DCE**

Résultat : enregistre la mise à jour avec le serveur DCE spécifié, puis installe l'extension Release My Documents (Libérer mes documents) sur une seule imprimante multifonctions.

Accès à l'écran Release My Documents (Libérer mes documents)

Si vous avez installé l'extension Release My Documents (Libérer mes documents) (voir les instructions dans le Guide d'installation), les utilisateurs peuvent accéder à l'écran (Libérer mes documents) pour consulter leurs travaux d'impression dans une ou plusieurs files d'attente sécurisées, afin de libérer ou supprimer leurs travaux, comme requis.

1. Après vous être authentifié, appuyez sur **All Services** (Tous les services).
2. Appuyez sur **Custom Services** (Services personnalisés).
3. Appuyez sur **Release My Documents** (Libérer mes documents).
4. L'écran affiche tous les documents stockés à l'intention de l'utilisateur sur le serveur d'impression local. Le tableau ci-dessous décrit les différents boutons.

Bouton	Fonction
Imprimer	Effleurez un ou plusieurs documents de la liste, puis appuyez sur **Imprimer** pour imprimer les documents et supprimer les travaux d'impression de la liste. Si vous sélectionnez plusieurs copies, cliquez sur **OK** pour confirmer votre demande.
Imprimer et sauvegarder	Effleurez un ou plusieurs documents de la liste, puis appuyez sur **Imprimer et sauvegarder** pour imprimer les documents en conservant toutefois les travaux dans la liste. Si vous sélectionnez plusieurs copies, appuyez sur **OK** pour confirmer votre demande.
Supprimer	Effleurez un ou plusieurs documents de la liste, puis appuyez sur **Supprimer** pour supprimer les travaux dans la file d'attente sans les imprimer.
Sélectionner tous	Sélectionne tous les travaux présents dans la liste.
Actualiser	Contacte le serveur DCE pour déterminer si des travaux en attente doivent être ajoutés à la liste à l'intention de l'utilisateur en cours. Si le système trouve des documents, il les ajoute en fin de liste.
Détails	Effleurez un document de la liste, puis appuyez sur **Détails** pour afficher des informations telles que l'intitulé du travail d'impression, la date et l'heure de soumission, le nom de l'imprimante vers laquelle le travail avait été envoyé en premier lieu et le poste de travail client d'où provient le travail.
Sortie	Retour à l'écran Custom Services (Services personnalisés)

Sélectionner le nombre de copies pour un travail d'impression

Après s'être authentifiés, les utilisateurs peuvent se servir du clavier numérique de l'imprimante multifonctions pour saisir le nombre de copies à imprimer. Si ce nombre est supérieur à un, une boîte de dialogue de confirmation apparaît lorsque vous appuyez sur les boutons **Imprimer** ou **Imprimer et sauvegarder**. Pour imprimer le nombre de copies affiché, appuyez sur **OK**. Pour modifier ce nombre, appuyez sur **Annuler**, puis saisissez le nombre de copies approprié à l'aide du clavier numérique visible sur le panneau avant de l'imprimante multifonctions. Appuyez soit sur **Imprimer** soit sur **Imprimer et sauvegarder** pour libérer à nouveau votre travail d'impression.

Si le travail d'impression original a été imprimé en deux exemplaires à l'aide de cette fonction et si vous sélectionnez 2, vous obtiendrez 4 copies du document original.

Mettre fin à une session utilisateur

Une fois positionné dans l'écran Release My Documents (Libérer mes documents), vous devez d'abord appuyer sur **Sortie** pour retourner dans l'écran Custom Services (Services personnalisés). Appuyez ensuite sur **Fermer** pour revenir à l'écran principal du panneau avant. Pour vous déconnecter complètement de votre session active, appuyez deux fois sur le bouton **Effacer tout** situé à côté du clavier du panneau, puis choisissez **Déconnecter** dans la boîte de dialogue qui s'affiche.