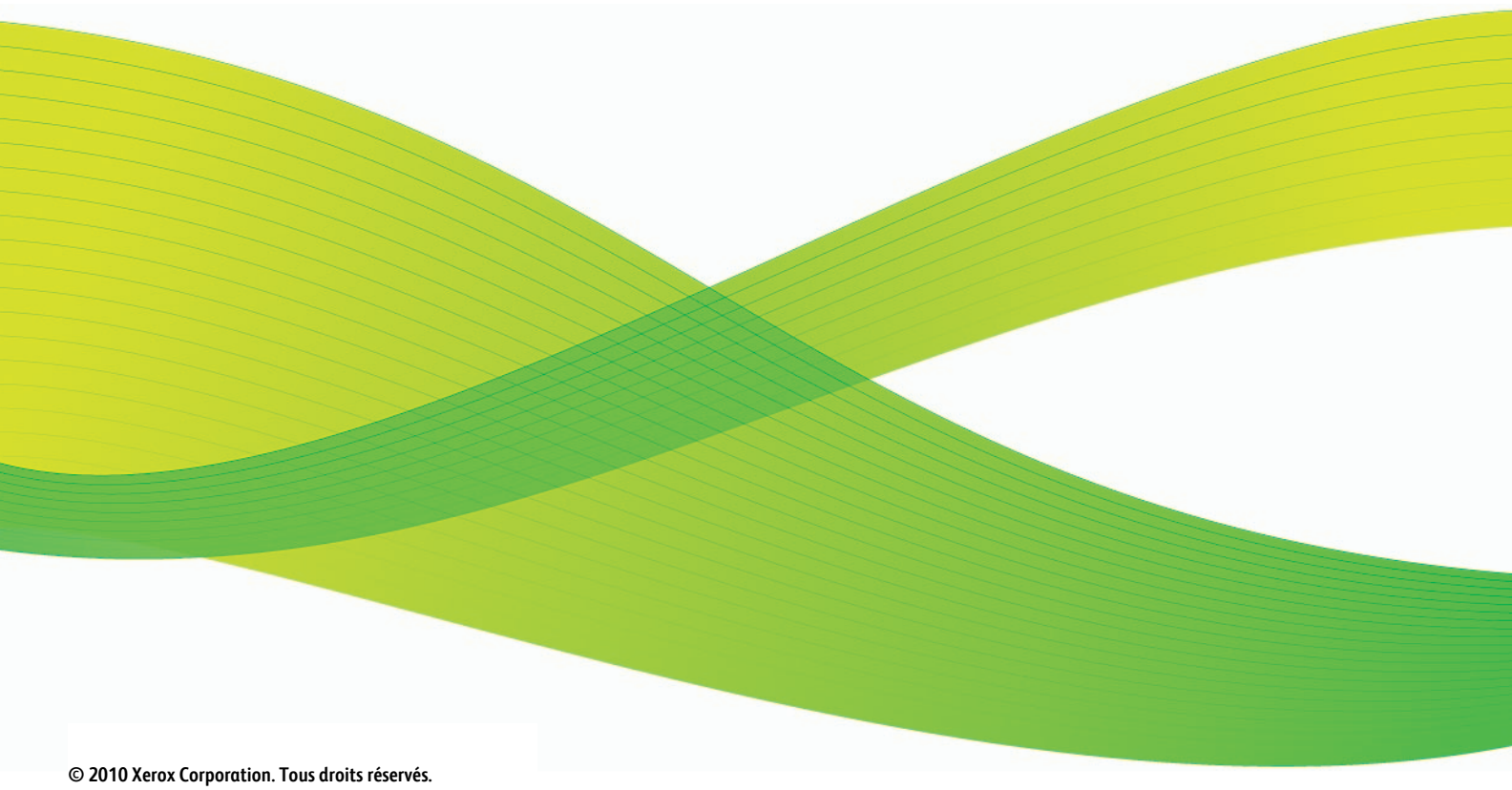
Version 1.6, Octobre 2010

Xerox Secure Access Unified ID System®

Guide d'installation



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

Table des matières

Consignes de sécurité 1

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

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

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

2 Liste de contrôle pour l'installation

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 : Préparation du réseau et de la base de données	*	*
3. Chapitre 4 Installation du serveur Secure Access : 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	*	*
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 l'installation

Ce chapitre contient les sections suivantes :

Le présent guide décrit l'installation du logiciel du serveur Xerox Secure Access Unified ID System™ ainsi que la configuration physique des périphériques d'authentification. Cette dernière opération nécessite l'installation préalable du serveur.

Une fois le logiciel du serveur Secure Access installé correctement, vous trouverez toutes les instructions nécessaires au déploiement physique de périphériques et à la configuration des logiciels dans le Guide d'administration Secure Access.

Ce chapitre traite les éléments suivants :

- Composants du serveur Secure Access
- Configurations système minimales

Composants de Secure Access

Xerox Secure Access Unified ID System (appelé ici Secure Access) est une solution matérielle et logicielle. Elle se compose des éléments suivants :

- Le logiciel serveur Secure Access qui gère la base de données utilisateur ; il contient également des services qui communiquent avec les imprimantes multifonctions et les périphériques d'authentification Secure Access.
- Un périphérique d'authentification Secure Access composé d'un lecteur de carte et qui contrôle l'accès aux imprimantes multifonctions Xerox.

  OU
- Un lecteur de carte USB Secure Access

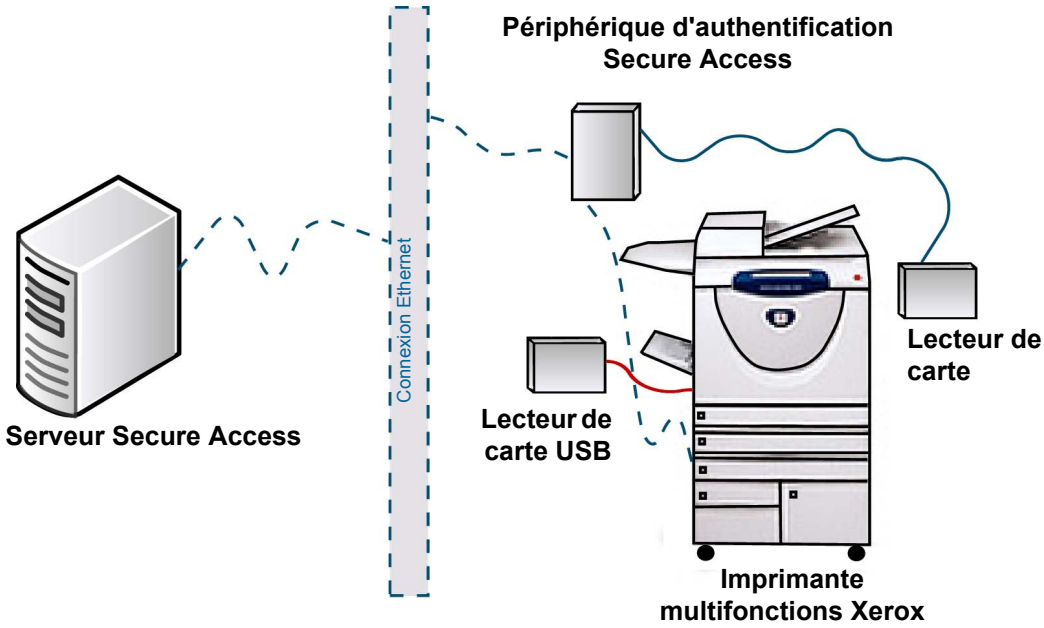


Figure 3-1: Composants de Secure Access

Chaque installation du logiciel serveur Secure Access requiert au moins trois services :

- Serveur d'authentification central (CAS)
- Moteur de contrôle de périphérique (DCE)
- Moteur d'acheminement de document (DRE)

En outre, vous devez également installer le gestionnaire Secure Access, l'outil d'administration utilisé pour établir la communication entre plusieurs composants Secure Access.

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 comptes regroupant toutes les informations relatives à l'utilisateur et au périphérique. Pour plus d'informations sur les bases prises en charge, voir Configuration du système de serveur Secure Access à la page 18.

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 copie, 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.

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.

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

Pour que les travaux d'impression soient conservés dans une file 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.

En outre, vous pouvez ajouter le service personnalisé Release My Documents (Libérer mes documents) à l'imprimante multifonctions. Ce service permet aux utilisateurs d'accéder à la file d'attente d'impression sécurisée directement à partir du panneau avant de l'imprimante multifonctions. Pour configurer ce service, voir le Guide d'administration Xerox Secure Access.

Déploiement multiserveurs

On qualifie de locale une installation où tous les services sont regroupés sur le même serveur. Cependant, certaines installations peuvent nécessiter plusieurs serveurs pour répartir la charge de gestion. Lorsque les services sont répartis sur deux serveurs ou plus, l'installation est dite distante .

Que l'installation consiste à déployer un seul serveur ou plusieurs, les services DRE et DCE doivent toujours se trouver sur le même serveur.

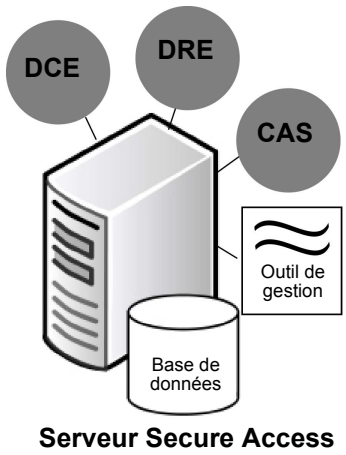


Figure 3-2: Scénario d'une installation locale

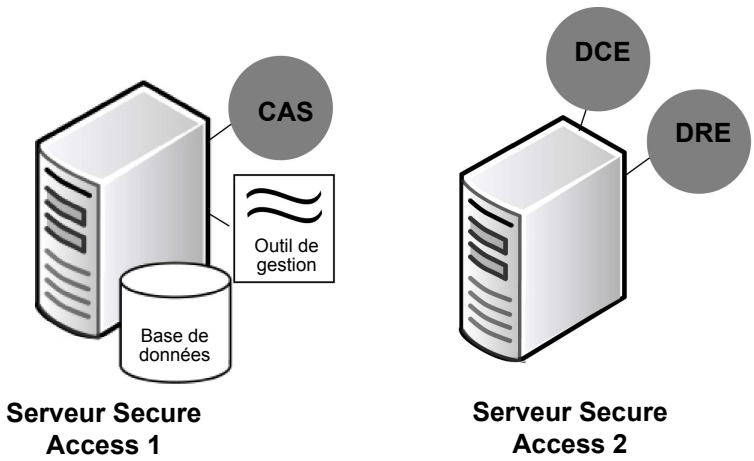


Figure 3-3: Scénario d'une installation distante

En outre, si Secure Access doit gérer un grand nombre d'imprimantes multifonctions, vous pouvez déployer plusieurs serveurs d'impression DRE pour mieux équilibrer la charge de communication.

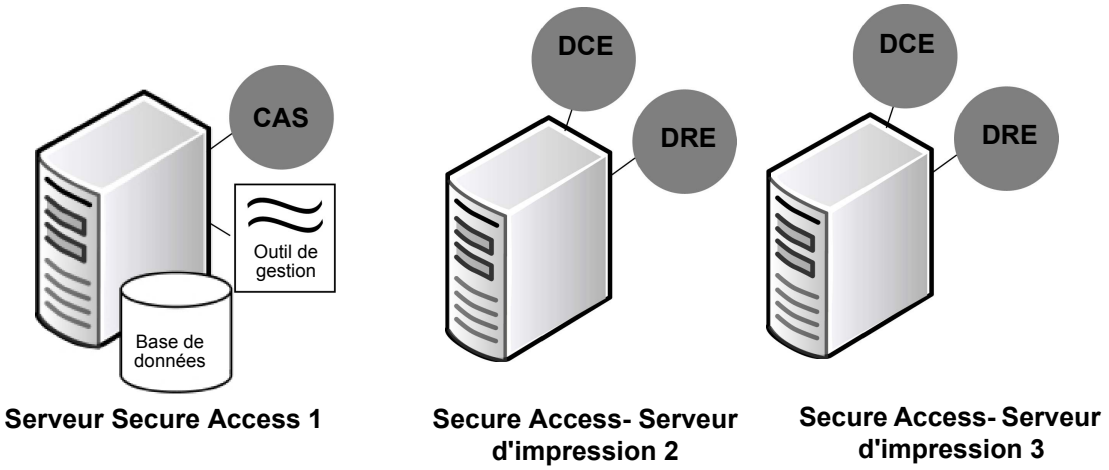


Figure 3-4: Déploiement de plusieurs serveurs d'impression

Reportez-vous à la section Exécution de l'Assistant d'installation à la page 23 pour plus d'informations sur l'installation et la configuration du déploiement multiserveurs. L'Assistant d'installation vous permet de sélectionner uniquement les composants à installer sur chaque serveur. Les services DRE et DCE peuvent être installés sur plusieurs serveurs et ils doivent toujours être installés sur le même serveur.

Configuration du système de serveur Secure Access

Avant de procéder à l'installation de Secure Access, assurez-vous que les serveurs que vous comptez utiliser sont conformes aux configurations d'exploitation minimales indiquées ci-après.

Le tableau ci-après répertorie uniquement les configurations d'exploitation minimales. Pour optimiser les performances dans des environnements d'impression haut-volume, prévoir de l'espace disque et de la mémoire supplémentaires, ainsi qu'un processeur plus rapide.

Composant	Configuration minimale requise
Matériel	• Processeur : Pentium III, Athlon ou supérieur • Mémoire système : 512 Mo au minimum • Espace disque pour l'application : 100 Mo • Espace disque pour la base de données : 20 Mo • Résolution d'affichage : 1024 x 768
Système d'exploitation pour CAS/DCE/DRE	Au choix : • Windows Server 2003 (32 bits uniquement) • Windows XP Professionnel (32 bits uniquement)[1] • Windows Server 2008 (32 et 64 bits), 2008 R2 (64 bits) Remarque : Toutes les mises à jour critiques de système d'exploitation doivent être installées avant l'installation du logiciel serveur Secure Access.
Bases de données	• Microsoft SQL Server 2005 Express[2] • Microsoft SQL Server 2008 Express (64 bits) Remarque : Secure Access ne peut pas être installé sur un serveur qui exécute une application MSDB, telle que FreeFlow™ SMARTsend™, qui entrerait en conflit avec la base SQL Server.

[1] Si vous avez l'intention d'installer le service CAS sur un serveur Windows XP Professionnel qui n'est pas associé à un domaine, suivez les instructions de la page 15 pour configurer les paramètres d'authentification de l'utilisateur.

[2] SQL Server 2005 Express requiert Windows Service Pack 2 (SP2) ou une version ultérieure afin d'être exécuté sur Windows Server 2008 ou 2008 R2

Configuration de l'authentification utilisateur sous Windows XP Pro

Si vous avez l'intention d'installer le service CAS Secure Access sur une plate-forme Microsoft Windows XP Professionnel et que l'ordinateur n'est pas associé à un domaine, vous devez modifier les paramètres de sécurité Windows XP afin que ce dernier accepte des connexions à des comptes utilisateurs nominatifs.

Par défaut, sous Windows XP Professionnel, les ouvertures de session réseau utilisant des comptes locaux sont automatiquement mappées au compte Invité. Si vous voulez que les utilisateurs s'authentifient sous leur propre nom, vous devez modifier ce paramètre.

Exécutez ces étapes avant de lancer l'Assistant d'installation Secure Access.

1. Ouvrez la boîte de dialogue Paramètres de sécurité locaux sur l'ordinateur où vous allez installer le service CAS.
2. Dans le volet de navigation gauche, double-cliquez sur **Stratégies locales**, puis double-cliquez sur **Options de sécurité**.
3. Dans le volet droit, déroulez la liste pour faire apparaître l'entrée **Accès réseau : modèle de partage et de sécurité pour les comptes locaux**.
4. Double-cliquez sur cette entrée, puis sélectionnez **Classique : les utilisateurs locaux s'authentifient eux-mêmes**.
5. Cliquez sur **Appliquer** puis sur **OK** pour fermer la boîte de dialogue.
6. Fermez les Paramètres de sécurité locaux.

Configuration des composants matériels Secure Access

Assurez-vous d'avoir tous les matériels fournis :

Configuration 1

- Alimentation
- Câble d'alimentation
- Clé de contournement (clé métallique utilisée pour rétablir les valeurs par défaut du périphérique). Voir Réinitialisation d'un périphérique d'authentification dans les annexes du Guide d'administration.
- Câble réseau Ethernet 10/100 Base-T
- Lecteur de carte

OU

Configuration 2

- Lecteur de carte USB Secure Access

Lecteurs de carte pris en charge

Secure Access prend en charge les lecteurs de carte suivants :

- ABA Magstripe
- Mifare (y compris les lecteurs HID iCLASS)
- Legic
- HID 125 kHz
- Indala
- EM Marin
- Hitag

4 Installation du serveur Secure Access

Ce chapitre contient les sections suivantes :

Cette section décrit l'utilisation de l'Assistant d'installation du serveur Secure Access. Il convient de suivre les instructions fournies avec attention et de veiller à ce que les machines serveur soient conformes aux configurations minimales requises indiquées à la section Configuration du système de serveur Secure Access à la page 18.

Ce chapitre traite des éléments suivants :

- préparation du réseau et de la base de données avant l'installation ;
- sélection des composants à installer par serveur Secure Access à l'aide de l'Assistant d'installation.

Préparation du réseau et de la base de données

Même si le sous-programme d'installation de Secure Access est très simple, il convient d'effectuer les tâches suivantes préalablement à l'exécution de l'Assistant d'installation :

1. Planifier les rôles système.
2. Activer Xerox Secure Access sur l'imprimante multifonctions à l'aide du logiciel de services Internet CentreWare.

   Remarques :

   - À l'aide d'un navigateur Web, connectez-vous au logiciel de services Internet CentreWare sur l'imprimante multifonctions. Accédez à la page pour activer Xerox Secure Access. Cette installation nécessitera l'activation du protocole SSL ainsi que la création d'un certificat. Pour plus d'informations, consultez le CD d'administration du système de l'imprimante multifonctions.
   - En ce qui concerne les lecteurs de carte USB, il se peut que l'imprimante multifonctions ait besoin d'une mise à niveau logicielle. Veuillez contacter votre agent commercial Xerox ou consultez la page de support dédiée à votre imprimante multifonctions spécifique, à partir de la section Assistance et pilotes du site www.xerox.com.
3. Préciser la destination de chaque composant Secure Access à installer.

   Remarque : Avant de déployer Secure Access sur le réseau, assurez-vous de disposer des droits d'administrateur sur toutes les machines à installer et configurer.
4. Vérifier la configuration réseau ; elle doit être capable de gérer les communications entre les différents composants de Secure Access.
5. À l'aide du service de mises à jour de Windows, vérifier que toutes les mises à jour critiques de système d'exploitation sont installées.
6. Installer Microsoft .NET Framework 2.0.

   Remarque : Reportez-vous au site Web de Microsoft pour obtenir une liste exhaustive des conditions préalables à l'installation de SQL Server 2005 ou 2008 Express.
7. Installer et configurer la base de données.

   Remarque : Si vous utilisez SQL Server 2005 ou 2008 Express, vous devez configurer la base de données afin d'utiliser le mode d'authentification Windows. Secure Access ne prend pas en charge l'authentification en mode mixte.

Exécution de l'Assistant d'installation

Lors de l'installation de Secure Access, l'Assistant vous permet de sélectionner les fonctions à installer par machine serveur. Si vous répartissez les différents composants entre plusieurs machines serveur, vous devez exécuter l'Assistant sur chacune d'elle, en veillant à ne sélectionner que les composants voulus. En revanche, si vous procédez à l'installation sur une même machine serveur, une seule exécution de l'Assistant suffit.

Chaque déploiement requiert au moins un composant CAS, DCE, DRE et un Gestionnaire Secure Access.

1. Vérifiez que toutes les étapes de la section Préparation du réseau et de la base de données ont été effectuées avant de procéder à l'installation.
2. Fermez toute autre application sur la machine serveur avant de lancer l'installation de Secure Access.
3. Démarrez l'Assistant d'installation de Secure Access.
   - Si vous procédez à l'installation à partir du CD Secure Access, sélectionnez le fichier **32-bit Setup.exe** pour commencer l'installation sur une machine 32 bits ou le fichier **64-bit Setup.exe** pour une machine 64 bits.

   OU

   - Si vous procédez à l'installation à partir d'une distribution électronique, téléchargez le fichier ZIP et exécutez le fichier **Setup.exe** 32 ou 64 bits.

   Remarque : Si lors de la tentative d'exécution du fichier setup.exe, vous recevez un message d'erreur, il peut être nécessaire de mettre à jour votre version du programme d'installation de Microsoft. Pour ce faire, rendez-vous sur le site Web de Microsoft, puis téléchargez et installez la dernière version du programme Microsoft Installer correspondant à votre système d'exploitation.
4. Dans l'écran de bienvenue, cliquez sur **Suivant** (Next) pour commencer le processus d'installation.
5. Lisez le contrat de licence logiciel, cliquez sur **I accept** (J'accepte), puis sur **Next**.
6. Choisissez les options à installer sur cette machine, puis cliquez sur **Next**.

   Par défaut, tous les composants sont sélectionnés. Vous devez néanmoins limiter votre sélection aux seuls services nécessaires, selon la machine serveur. Par exemple, si cette machine vous sert de serveur d'impression, seuls les composants DRE et DCE sont pertinents. Il convient ensuite de ré-exécuter le programme d'installation sur une autre machine serveur pour installer le reste des composants, selon les besoins.

   Remarque : Lisez la description des différents composants avant d'en installer un (voir Composants de Secure Access à la page 14). Ces informations vous aideront à optimiser le déploiement de ces services selon les besoins de votre entreprise.
7. Choisissez la langue d'interface dans l'écran **Select Language** (Sélectionner une langue). Il s'agit de la langue qui sera utilisée dans le gestionnaire Secure Access uniquement. La langue employée dans les invites de panneau avant des différents périphériques multifonctions est contrôlée par les paramètres de ces derniers.

8. Dans l'écran **Instance for SQL Express** (Instance de SQL Express), indiquez le nom d'instance que vous avez créé pour la base SQL Express. Cliquez sur **Next**.

   Remarque : Le nom d'instance que vous saisissez dans ce champ DOIT correspondre à celui que vous avez créé pour la base Secure Access à l'installation de SQL Express. En effet, vous ne pourrez pas procéder à l'installation si le nom d'instance est incorrect. Si vous avez exécuté une installation SQL Express standard en conservant les valeurs par défaut, maintenez le nom SQLEXPRESS, puis cliquez sur Next.

9. Dans l'écran **User Name for Services** (Nom d'utilisateur pour les services), précisez un **ID utilisateur** et un **mot de passe** associés aux services.

   Dans le cas du déploiement des composants sur plusieurs machines, vous DEVEZ entrer les mêmes données d'identification utilisateur pour chaque installation. En effet, ces données sont utilisées pour démarrer et exécuter tous les services. Par conséquent, si vous omettez d'indiquer les mêmes informations d'identification pour tous les composants, le Serveur d'authentification central ne répondra pas aux demandes émanant du moteur DCE ou DRE.

   Les comptes de domaine doivent utiliser le même nom de domaine (par exemple, domaine\nom_utilisateur).

   Bien que ce compte ne nécessite pas de droits d'administrateur sur le serveur Secure Access, il doit être doté de droits d'opérateur d'impression pour autoriser le moteur DRE à traiter les demandes d'impression.

10. Entrez le nom du serveur d'authentification Xerox Secure Access.

    Ce nom vous sera demandé au démarrage du gestionnaire Secure Access.

11. Cliquez sur **Install** (Installer) pour démarrer le processus d'installation. L'Assistant d'installation copie les fichiers, définit les services et crée des raccourcis vers le gestionnaire Secure Access.

12. À la fin du processus, cliquez sur **Finish** (Terminer) pour quitter l'Assistant d'installation.

13. L'installation du serveur Secure Access est maintenant terminée. Reportez-vous au chapitre 5 pour configurer le matériel Secure Access.

Mise à niveau de Secure Access

Si vous effectuez une mise à niveau par étape ou une mise à niveau de tous les composants pendant une période d'arrêt planifié, les instructions ci-après vous guideront au travers des étapes de l'Assistant d'installation pour la mise à niveau de Secure Access.

Remarque : Il est recommandé de sauvegarder votre base de données avant d'effectuer une mise à niveau.

Pendant la mise à niveau de Secure Access, l'Assistant d'installation détecte les composants Secure Access déjà installés sur la machine (par ex. : la base de données). Ces composants seront automatiquement sélectionnés dans l'Assistant d'installation. Vous pouvez maintenir les sélections par défaut ou sélectionner des composants supplémentaires à installer.

Pour mettre à niveau Secure Access, procédez comme suit :

1. Fermez toute autre application sur la machine serveur avant de lancer l'installation de Secure Access.
2. Démarrez l'Assistant d'installation de Secure Access.
   - Si vous procédez à l'installation à partir du CD Secure Access, sélectionnez le fichier **32-bit Setup.exe** pour commencer l'installation sur une machine 32 bits ou le fichier **64-bit Setup.exe** pour une machine 64 bits.

   OU

   - Si vous procédez à l'installation à partir d'une distribution électronique, téléchargez le fichier ZIP et exécutez le fichier **Setup.exe** 32 ou 64 bits.

   Remarque : Si lors de la tentative d'exécution du fichier setup.exe, vous recevez un message d'erreur, il peut être nécessaire de mettre à jour votre version du programme d'installation de Microsoft. Pour ce faire, rendez-vous sur le site Web de Microsoft, puis téléchargez et installez la dernière version du programme Microsoft Installer correspondant à votre système d'exploitation.
3. Dans l'écran de bienvenue, cliquez sur **Suivant** (Next) pour commencer le processus d'installation.
4. Lisez le contrat de licence logiciel, cliquez sur **I accept** (J'accepte), puis sur **Next**.
5. Choisissez les options à installer sur cette machine, puis cliquez sur **Next**.

   Par défaut, tous les composants sont sélectionnés. Vous devez néanmoins limiter votre sélection aux seuls services nécessaires, selon la machine serveur. Par exemple, si cette machine vous sert de serveur d'impression, seuls les composants DRE et DCE sont pertinents. Il convient ensuite de ré-exécuter le programme d'installation sur une autre machine serveur pour installer le reste des composants, selon les besoins.
6. Entrez le nom du serveur d'authentification Xerox Secure Access.
7. Cliquez sur **Finish** (Terminer) pour quitter l'Assistant.

La mise à niveau du serveur Secure Access est maintenant terminée. Reportez-vous au chapitre 5 pour configurer le matériel Secure Access.

5 Installation du matériel Secure Access

Ce chapitre contient les sections suivantes :

Ce chapitre décrit l'installation physique du matériel Secure Access. Cette procédure nécessite néanmoins l'installation préalable du logiciel du serveur Secure Access (voir les instructions du chapitre 4).

Si vous utilisez un lecteur de carte USB pour Secure Access, passez à la page 34.

1. définition de l'adresse IP pour chaque périphérique d'authentification ;
2. montage du matériel du périphérique d'authentification Secure Access sur ou à proximité du périphérique multifonctions ;
3. raccordement des différentes connexions (alimentation, série, extension, lecteur de carte).

Configuration de l'adresse IP du périphérique d'authentification

ATTENTION : Si vous n'utilisez pas un serveur DHCP pour attribuer des adresses IP, NE CONNECTEZ PAS LE PÉRIPHÉRIQUE D'AUTHENTIFICATION AU RÉSEAU tant que vous n'avez pas défini l'adresse IP manuellement. Reportez-vous à la section Attribution manuelle des adresses IP à la page 29.

Par défaut, les périphériques d'authentification Secure Access sont configurés en mode de communication DHCP. Vous devez attribuer à chacun d'eux une adresse IP, ainsi que définir l'adresse IP serveur du composant DCE. Pour affecter l'adresse IP, vous avez le choix entre deux méthodes :

- Vous pouvez affecter des adresses en utilisant un serveur DHCP. Suivez la procédure Configuration du serveur DHCP pour rechercher les périphériques d'authentification à la page 28.
- Si vous n'utilisez pas de serveur DHCP ou si vous préférez ne pas définir l'option 230 sur votre serveur DHCP, définissez les adresses manuellement à l'aide de l'application d'administration Web du périphérique d'authentification. Suivez la procédure Attribution manuelle des adresses IP à la page 29.

Configuration du serveur DHCP pour rechercher les périphériques d'authentification

Les instructions ci-après sont destinées à un serveur DHCP Windows. Si votre serveur DHCP fonctionne sur une autre plate-forme (par exemple, serveurs UNIX, Linux, OS X, OpenVMS, DHCP AS/400), configurez bien le serveur DHCP pour qu'il passe l'adresse de serveur DCE à la valeur 230.

Remarque : Pour obtenir des informations techniques supplémentaires sur l'affectation d'adresses IP aux périphériques d'authentification Secure Access à l'aide du serveur DHCP, consultez le Livre blanc sur la configuration de l'adresse IP des périphériques d'authentification Secure Access disponible sur le site www.xerox.com.

1. Dans les Outils d'administration Windows, ouvrez la console d'administration Windows DHCP.
2. Sélectionnez le nœud racine du serveur DHCP.
3. À partir du menu **Action**, sélectionnez **Définir les options prédéfinies**.
4. Dans la liste déroulante **Classe d'option**, sélectionnez **Options standard DHCP**.
5. Dans la section **Nom d'option**, cliquez sur **Ajouter**.
   a. Dans le champ **Nom**, tapez : Xerox Secure Access

   Remarque : Le champ **Nom** sert à des fins d'identification.

   b. Dans la liste déroulante **Type des données**, sélectionnez Chaîne.
   c. Dans le champ **Code**, tapez 230.
   d. Dans le champ **Description**, tapez : Secure Access.
6. Cliquez sur **OK**.

7. Dans le champ **Chaîne** de la section **Valeur de chaîne**, saisissez EQ;A;<adresse_IP_serveur_DCE>, où <adresse_IP_serveur_DCE> correspond à l'adresse IP de votre serveur DCE.
8. Développez le nœud **Étendue** et sélectionnez **Options d'étendue**.
9. À partir du menu **Action**, sélectionnez **Configurer les options**.
10. Sélectionnez **230**.
11. Cliquez sur **OK** pour enregistrer les modifications.

Attribution manuelle des adresses IP

Ces instructions s'appliquent uniquement si vous n'utilisez pas de serveur DHCP pour définir l'adresse IP du périphérique d'authentification OU si vous utilisez un serveur DHCP mais préférez opter pour des adresses IP statiques plutôt que pour l'option 230.

Lorsqu'il est mis sous tension pour la première fois, le périphérique d'authentification recherche un serveur DHCP afin de sécuriser une adresse IP. En l'absence de serveur DHCP, les périphériques passent en mode de communication statique et prennent l'adresse IP statique par défaut 192.168.2.1. Vous pouvez utiliser un câble Ethernet pour connecter un système (par exemple, un ordinateur portable) à chaque périphérique d'authentification, puis utiliser un outil d'administration Web pour modifier l'adresse IP et enfin saisir l'adresse IP du serveur DCE.

Imprimez la fiche de configuration détachable située à la page 35 avant de commencer. Cette fiche sert à consigner les adresses IP que vous attribuez à chaque périphérique d'authentification.

Configuration de l'ordinateur portable :

Le système qui exécute l'outil d'administration Web doit reconnaître l'adresse IP statique pour que vous puissiez accéder à ce dernier.

1. Sur le système (ordinateur portable) qui exécutera l'outil d'administration Web, sélectionnez **Connexions réseau** > **Connexion au réseau local** > **Propriétés**.
2. Double-cliquez sur **Propriétés Internet** (TCP/IP), puis cliquez sur **Avancé**.
3. Dans la section Adresses IP, cliquez sur **Ajouter**.
4. Entrez les informations suivantes :
   Adresse IP : 192.168.2.x (où x est une adresse IP non attribuée)
   Masque de sous-réseau : 255.255.255.0
5. Cliquez sur **Ajouter** pour sauvegarder les modifications.

Définition des adresses IP à l'aide de l'outil d'administration Web :

Effectuez la procédure ci-après sur chaque périphérique d'authentification.

1. À l'aide d'un câble Ethernet ordinaire, raccordez un ordinateur portable au port de liaison descendante du périphérique d'authentification Secure Access.
2. Pour mettre sous tension le périphérique d'authentification, connectez une des extrémités du câble d'alimentation à ce dernier, puis branchez l'autre sur une prise secteur.

3. Démarrez un navigateur Web et tapez 192.168.2.1 dans le champ d'adresse.
   Il s'agit de l'adresse IP par défaut attribuée au périphérique d'authentification Secure Access.

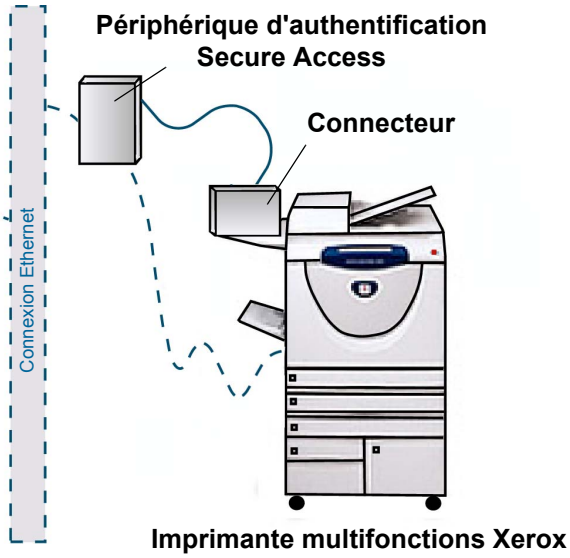
   Remarque : Pour obtenir la page en français, sélectionnez le lien fourni.
4. Cliquez sur le lien **Configure** (Configurer) en haut de la page.
5. Entrez les informations de connexion suivantes :
   Username (Nom de l'utilisateur) : deviceadmin
   Password (Mot de passe) : pc_passwd
6. Modifiez le mot de passe utilisé pour accéder à l'outil d'administration Web. Vous pouvez réinitialiser le mot de passe à tout moment. Veillez néanmoins à modifier le mot de passe par défaut avant que le système Secure Access ne soit opérationnel.
7. Dans la section **Configure Xerox Secure Access Authentication Device** (Configurer le périphérique d'authentification de Xerox Secure Access), choisissez Static IP (IP statique) dans le champ **Addressing mode** (Mode d'adressage).
8. Dans le champ **IP Address** (Adresse IP), saisissez une adresse IP statique à associer au périphérique d'authentification.
9. Dans le champ Server IP Address (Adresse IP du serveur) de la section **Configure Server** (Configurer le serveur), indiquez l'adresse IP du serveur DCE.
10. Cliquez sur le bouton **Update Configuration** (Actualiser la configuration) situé sous les champs de configuration du serveur.
11. Cliquez sur le lien **Restart** (Redémarrer) en haut de la page, puis sur "Click here to confirm restart" (Cliquer ici pour confirmer le redémarrage) afin de redémarrer le terminal.

Répétez ces instructions pour chaque périphérique d'authentification Secure Access à déployer.

Remarque : Lorsque vous avez défini toutes les adresses IP, veillez à reconfigurer les propriétés Internet de l'ordinateur portable.

Montage du périphérique d'authentification Secure Access

Imprimez la Fiche de configuration détachable à la page 35. Renseignez les différentes colonnes de cette fiche au fur et à mesure. Vous aurez besoin de ces informations lors de la configuration du mode de communication entre différents périphériques sur le serveur Secure Access.



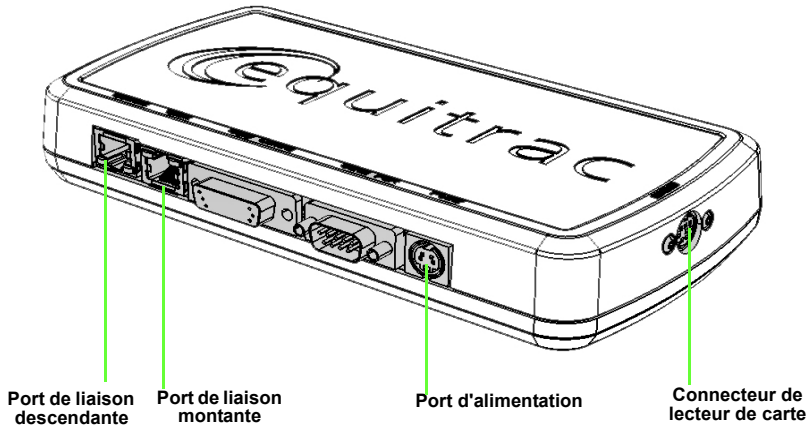
1. Placez le périphérique d'authentification sur le sol, derrière et vers le côté entrée du périphérique multifonctions. **Il doit se trouver dans un endroit discret ; assurez-vous néanmoins de disposer d'une longueur de câble suffisante (15 cm) pour assurer la connexion au lecteur de carte**.
2. À l'aide de la bande Velcro fournie, montez le lecteur de carte sur le plateau, à gauche du panneau avant du périphérique multifonctions. Si vous êtes équipé de l'agrafeuse externe en option, placez le lecteur de carte à droite de cette dernière. Le lecteur doit alors se trouver entre l'agrafeuse et le périphérique multifonctions. **Assurez-vous que le lecteur de carte ne gêne pas l'ouverture du chargeur de documents avant de fixer la bande Velcro**.
3. Consignez dans la fiche détachable l'adresse IP et MAC du périphérique d'authentification ainsi que l'adresse IP et le nom d'hôte de l'imprimante multifonctions qui sera contrôlée par ce périphérique d'authentification.

   Remarque : Reportez-vous au CD d'administration système de l'imprimante multifonctions pour obtenir d'autres suggestions sur l'emplacement de montage.

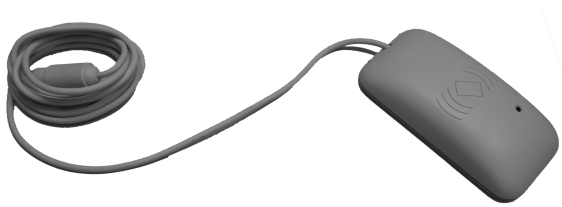
Connexion du matériel

Avant de procéder à la connexion du matériel du périphérique d'authentification Secure Access, vous devez avoir effectué les tâches de configuration décrites à la section Configuration de l'adresse IP du périphérique d'authentification à la page 28.

À l'aide de la figure ci-dessous, connectez les composants. Notez que le périphérique d'authentification comprend un port série et un port de contrôle de copie qui ne sont pas utilisés dans cette configuration.



1. Consignez l'adresse MAC du périphérique d'authentification dans la fiche détachable. Elle doit être inscrite sur la même ligne que le périphérique multifonctions contrôlé.
2. Raccordez le câble série du lecteur de carte au port approprié sur le périphérique d'authentification.



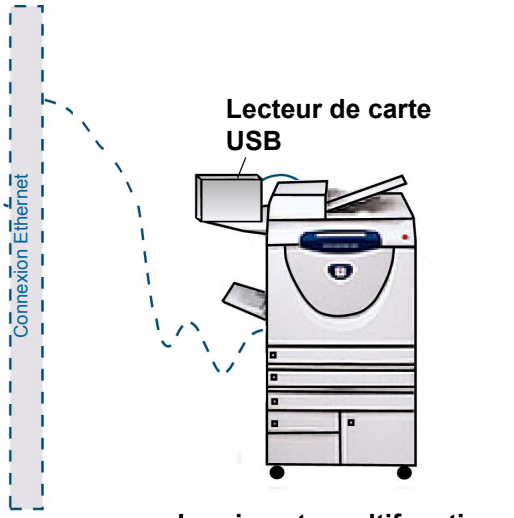
3. Connectez l'une des extrémités du câble Ethernet à un branchement réseau et l'autre extrémité au port de liaison montante sur le périphérique d'authentification Secure Access.
4. Connectez le câble Ethernet du périphérique multifonctions au port de liaison descendante sur le périphérique d'authentification.

   Remarque : Lorsque le périphérique d'authentification est hors tension, le port de liaison descendante n'assure plus aucune connectivité Ethernet. Vous pouvez dans ce cas brancher le câble Ethernet du périphérique multifonctions directement sur un autre port Ethernet. L'existence du port de liaison descendante permet simplement de remplacer un autre port Ethernet en cas d'indisponibilité de ce dernier.

5. Raccordez l'alimentation sur le périphérique d'authentification, puis branchez l'autre extrémité sur la prise secteur la plus proche.

L'installation du matériel est maintenant terminée. Pour configurer le serveur Secure Access et activer la communication entre les périphériques d'authentification et les périphériques multifonctions, reportez-vous aux instructions du Guide d'administration de Secure Access.

Montage/connexion du lecteur de carte USB Secure Access



1. À l'aide de la bande Velcro fournie, montez le lecteur de carte sur le plateau, à gauche du panneau avant du périphérique multifonctions. Si vous êtes équipé de l'agrafeuse externe en option, placez le lecteur de carte à droite de cette dernière. Le lecteur doit alors se trouver entre l'agrafeuse et le périphérique multifonctions. **Assurez-vous que le lecteur de carte ne gêne pas l'ouverture du chargeur de documents avant de fixer la bande Velcro**.
2. Branchez le câble du lecteur de carte USB Secure Access dans un port USB libre, sur la face arrière de l'imprimante multifonctions.

   Reportez-vous au CD d'administration système de l'imprimante multifonctions pour obtenir d'autres suggestions sur l'emplacement de montage.

Fiche de configuration détachable

Détachez cette fiche et utilisez-la lors de l'installation physique des périphériques d'authentification. Vous devez conserver les adresses IP et MAC de chaque périphérique d'authentification et du périphérique multifonctions qui lui est associé.

	Périphérique d'authentification		Périphérique multifonctions	
	Adresse MAC	Adresse IP	Adresse IP	Nom d'hôte
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				