RSA Authentication Agent 7.4
pour Microsoft Windows
Guide d’installation et d’administration

Informations de contact

RSA Link à l'adresse **https://community.rsa.com** contient une base de connaissances qui répond aux questions courantes et fournit des solutions aux problèmes connus, de la documentation produit, des discussions communautaires et la gestion de dossiers.

Marques commerciales

Dell, RSA, le logo RSA, EMC et les autres marques commerciales citées sont des marques commerciales de Dell Inc. ou de ses filiales. D'autres marques éventuellement citées sont la propriété de leurs détenteurs respectifs. Pour obtenir la liste des marques commerciales de RSA, rendez-vous à l'adresse suivante : **www.emc.com/legal/emc-corporation-trademarks.htm#rsa**.

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété de Dell Inc. ou de ses filiales, et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales.

Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part de Dell Inc.

Licences tierces

Ce produit peut inclure des logiciels développés par d'autres entreprises que RSA. Le texte des contrats de licence applicables aux logiciels tiers présents dans ce produit peut être consulté sur la page de la documentation produit du site RSA Link. En faisant usage de ce produit, l'utilisateur convient qu'il est pleinement lié par les conditions des contrats de licence.

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

L'utilisation, la copie et la diffusion de tout logiciel Dell décrit dans cette publication nécessitent une licence logicielle en cours de validité.

Dell Inc. estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

LES INFORMATIONS CONTENUES DANS CETTE PUBLICATION SONT FOURNIES « EN L'ÉTAT ». DELL INC. NE FOURNIT AUCUNE DÉCLARATION OU GARANTIE D'AUCUNE SORTE CONCERNANT LES INFORMATIONS CONTENUES DANS CETTE PUBLICATION ET REJETTE PLUS SPÉCIALEMENT TOUTE GARANTIE IMPLICITE DE QUALITÉ COMMERCIALE OU D'ADÉQUATION À UNE UTILISATION PARTICULIÈRE.

Septembre 2019

Contenu

Préface

À propos de ce guide

Ce guide explique comment installer et configurer RSA® Authentication Agent 7.4 pour Microsoft® Windows®. Il s'adresse aux administrateurs et autres membres de confiance du personnel. Il ne doit pas être mis à la disposition des utilisateurs généraux.

Documentation de RSA Authentication Agent pour Microsoft Windows

Pour plus d'informations sur RSA Authentication Agent 7.4, consultez la documentation suivante et l'aide :

***Notes de mise à jour* :** Fournit des informations sur les nouveautés et les modifications de cette version, ainsi que les solutions aux problèmes connus. La dernière version des *notes de mise à jour* est disponible sur RSA Link à l'adresse **https://community.rsa.com/community/products/securid/authentication-agent-windows**.

Guide de modèle d'objet de stratégie de groupe. Décrit comment utiliser des modèles d'objet de stratégie de groupe pour configurer RSA Authentication Agent 7.4 for Microsoft Windows. Par exemple, vous pouvez utiliser un modèle de stratégie pour définir la façon dont les utilisateurs s'authentifient, définir des groupes d'authentification et définir le libellé de champ de connexion.

Aide Agents d'authentification RSA Décrit les tâches d'utilisateur et d'administration effectuées dans RSA Control Center. (Le Control Center est l'interface utilisateur de l'agent d'authentification). Par exemple, il contient les procédures permettant aux utilisateurs d'actualiser les jours en mode hors ligne ou de vérifier leurs options de connexion. Pour les administrateurs, cela comprend les procédures de test de l'authentification, d'activation d'un mot de passe de réserve, de remplacement d'une adresse IP, d'activation du suivi, d'authentification des utilisateurs, d'effacement d'un secret de nœud ou de données hors ligne et d'examen des informations relatives au serveur.

Documentation connexe

Pour plus d'informations sur les produits associés à RSA Authentication Agent 7.4, reportez-vous aux éléments suivants :

Ensemble de documentation de RSA Authentication Manager. Consultez l'intégralité de la documentation de RSA Authentication Manager 8.2 SP1 ou version supérieure. Pour accéder à un ensemble de documentation, accédez à **https://community.rsa.com**.

Programme de partenariat RSA Ready RSA travaille avec un certain nombre de fabricants pour qualifier des logiciels fonctionnant avec les produits RSA. Les produits tiers qualifiés comprennent les réseaux privés virtuels (VPN) et les serveurs d'accès à distance (RAS), les routeurs, les serveurs Web et bien plus encore. Pour accéder au répertoire, y compris aux guides d'implémentation et à d'autres informations, accédez à **http://www.rsaready.com**.

Support et service

Vous pouvez accéder à la communauté et aux informations de support sur RSA Link à l'adresse **https://community.rsa.com**. RSA Link contient une base de connaissances qui répond aux questions courantes et fournit des solutions aux problèmes connus, de la documentation produit, des discussions communautaires et la gestion de dossiers.

Le site Web du programme Partenaires RSA Ready, accessible à l'adresse **www.rsaready.com**, fournit des informations concernant des produits matériels et logiciels tiers certifiés pour fonctionner avec les produits RSA. Ce site Web met à disposition des guides d'implémentation contenant des instructions détaillées et d'autres informations sur l'interopérabilité des produits RSA avec ces produits tiers.

Avant d'appeler le Support technique

Assurez-vous de disposer d'un accès direct à l'ordinateur qui exécute le logiciel RSA Authentication Agent 7.4 for Microsoft Windows.

Munissez-vous des informations indiquées ci-après.

- ❑ Votre ID de licence/client RSA. RSA Authentication Agent 7.4 est gratuit pour les clients. Utilisez le numéro de version du logiciel RSA Authentication Manager en tant qu'ID de client/de licence. Pour trouver ce numéro, procédez comme suit :

  Dans la console RSA Security, cliquez sur **Aide > À propos de la console RSA Security > Afficher des informations sur la version du logiciel**.
- ❑ La marque et le modèle de l'appareil sur lequel le problème se produit.
- ❑ Le nom et la version du système d'exploitation sous lequel le problème se produit.

1 Présentation du produit

RSA Authentication Agent pour Microsoft Windows

RSA Authentication Agent pour Microsoft Windows fonctionne avec RSA Authentication Manager pour permettre aux utilisateurs d'effectuer une authentification à deux facteurs afin d'accéder aux ordinateurs Windows. L'authentification à deux facteurs requiert la saisie d'un élément dont vous avez connaissance (par exemple, un code PIN RSA SecurID®) et d'un élément dont vous disposez (par exemple, un code de token généré par un authentificateur RSA SecurID).

Si vous souhaitez qu'un utilisateur se connecte via l'agent d'authentification, il peut être nécessaire de saisir un code d'accès pour accéder à l'ordinateur. Un code d'accès se compose d'un code PIN SecurID, suivi d'un code de token.

La première fois que les utilisateurs s'authentifient à l'aide d'un code d'accès RSASecurID, ils sont invités à générer, automatiquement ou manuellement, leurs codes PIN RSA SecurID. Pour saisir la partie de code de token du code d'accès,ils peuvent rechercher les numéros situés à l'avant de leurs authentificateurs RSA SecurID et les saisir manuellement en regard de leur code PIN (s'ils utilisent un authentificateur portatif). Ou bien, s'ils utilisent des authentificateurs RSA SecurID USB et qu'ils les insèrent dans leurs ports USB, l'agent d'authentification accède automatiquement aux codes de token à partir des authentificateurs après qu'ils aient saisi leur code PIN.

Afin de s'assurer qu'un code d'accès à usage unique (OTP) est utilisé pour chaque authentification, le code de token est remplacé par un ensemble unique de nombres, environ chaque minute. Cela permet d'empêcher un utilisateur non autorisé de deviner un code d'accès, même si cette personne connaît le code PIN.

Remarque : (En fonction des paramètres définis dans Authentication Manager, les utilisateurs RSA SecurID peuvent également se connecter en entrant uniquement leurs codes de token.)

Lorsqu'un utilisateur saisit un code d'accès, RSA Authentication Agent envoie le code d'accès à RSA Authentication Manager pour validation. Si le code d'accès et le mot de passe sont corrects, l'utilisateur accède à l'ordinateur de bureau. Pour plus d'informations sur les exigences, consultez la section Chapter 2, « Préparation de l'installation. ». Pour obtenir des informations sur l'installation, voir Chapter 3, « Installation de l'agent d'authentification RSA. »

Caractéristiques principales

Les sections suivantes résument les principales fonctions de RSA Authentication Agent 7.4 for Microsoft Windows. Celles-ci comprennent des informations sur les éléments suivants :

- Authentification des utilisateurs avec un code d'accès
- Authentification hors ligne
- Intégration des mots de passe Windows
- Compte administrateur exempté
- Gestion centralisée des stratégies d'agent d'authentification à l'aide des modèles d'objet de stratégie de groupe (GPO)
- Mise à jour automatique des adresses IP
- Accès aux ordinateurs protégés à l'aide d'un code PIN ou d'un mot de passe
- Prise en charge des groupes multidomaines

Authentification des utilisateurs avec des codes d'accès RSA SecurID

Vous pouvez configurer RSA Authentication Agent 7.4 for Microsoft Windows pour que tous les utilisateurs ou seulement quelques groupes spécifiques soient invités à s'authentifier avec un code d'accès RSA SecurID (code PIN ou code de token). Vous sélectionnerez les groupes d'utilisateurs à authentifier dans une liste que vous aurez déjà définie via l'interface de gestion de l'ordinateur Microsoft ou dans Active Directory. Si nécessaire, créez de nouveaux groupes avant d'utiliser l'agent d'authentification. Pour en savoir plus sur la création des groupes d'authentification, consultez « Créer des groupes d'utilisateurs qui devront s'authentifier avec RSA SecurID » à la page 25.

Vous pouvez également configurer les paramètres d'authentification d'un ordinateur individuel à partir de l'interface utilisateur de RSA Control Center. Pour plus d'informations, reportez-vous à la rubrique d'aide de RSA Control Center sur l'authentification des utilisateurs. Notez que si l'ordinateur est joint à un domaine, les paramètres configurés par la stratégie de groupe remplacent les paramètres de RSA Control Center.

Authentification RSA SecurID sans connexion à Authentication Manager

Vous pouvez configurer l'agent d'authentification RSA pour Microsoft Windows afin d'étendre l'authentification RSA SecurID aux utilisateurs lorsque la connexion à RSA Authentication Manager n'est pas disponible (par exemple, lorsque les utilisateurs ne sont pas au bureau ou si l'état du réseau entraîne une indisponibilité temporaire de la connexion). Pour plus d'informations, consultez Chapter 4, « Gérer les agents d'authentification. »

Intégration des mots de passe Windows au processus de connexion RSA SecurID

Vous pouvez configurer RSA Authentication Agent pour Microsoft Windows de sorte que le mot de passe Windows soit intégré dans le processus d'ouverture de session RSA SecurID. Lorsque vous configurez l'agent d'authentification de cette manière, les utilisateurs ne fournissent leur mot de passe Windows que lors de l'authentification initiale en ligne. Les mots de passe sont actuellement enregistrés avec les données d'authentification des utilisateurs dans la base de données RSA Authentication Manager et, pour l'authentification hors ligne, dans les données hors ligne. Lors des authentifications ultérieures, les utilisateurs n'indiquent que leurs noms d'utilisateur et les codes d'accès RSA SecurID, jusqu'à ce que le mot de passe soit modifié dans Active Directory. L'agent d'authentification récupère le mot de passe Windows auprès d'Authentication Manager et le transmet au fournisseur d'informations d'identification de l'agent d'authentification RSA. L'agent d'authentification RSA fonctionne en tant qu'interface de connexion pour les utilisateurs finaux.

Lorsque les mots de passe Microsoft Windows sont modifiés par les utilisateurs disposant d'un agent d'authentification installé sur leurs ordinateurs, ils sont automatiquement synchronisés dans les comptes correspondants de la base de données de RSA Authentication Manager. Pour plus d'informations, consultez « Synchronisation automatique du mot de passe », à la page 69.

Important : Si les utilisateurs disposent de plusieurs domaines et d'un nom d'utilisateur, votre administrateur Authentication Manager doit ajouter les différents comptes dans Authentication Manager. Si les comptes supplémentaires n'existent pas dans Authentication Manager, les utilisateurs ne peuvent pas se connecter à l'aide de l'authentification RSA SecurID. Pour plus d'informations, reportez-vous à la *Group Policy Object Template Guide*.

Vous pouvez activer l'intégration des mots de passe Windows à l'échelle du système, au niveau de chaque agent ou par groupe. Par exemple, pour activer l'agent d'authentification, vous créez un enregistrement d'agent dans la base de données RSA Authentication Manager. Vous pouvez activer la fonction d'intégration de mot de passe Windows pour tous les ordinateurs de l'agent d'authentification dans la base de données, ou sélectionner certains ordinateurs. Pour plus d'informations sur RSA Authentication Manager, consultez le *guide d'administration de RSA Authentication Manager*.

Remarque : La fonction d'intégration des mots de passe Windows nécessite également que la fonction d'authentification hors ligne soit activée sur l'agent et le serveur. Si vous utilisez l'intégration des mots de passe Windows, ne désactivez pas l'authentification hors ligne.

Accès aux ordinateurs de bureau protégés dans les situations d'urgence

Le compte administrateur exempté est une méthode d'accès d'urgence qui vous permet de vous authentifier auprès d'un ordinateur de bureau protégé à l'aide de votre compte administrateur avec uniquement un mot de passe Windows au lieu d'un code d'accès RSA SecurID.

Lorsque vous installez RSA Authentication Agent 7.4 for Microsoft Windows, l'assistant d'installation vous invite à sélectionner une option d'authentification. Si vous sélectionnez **Authentifier tous les utilisateurs à l'exception des administrateurs**, l'agent d'authentification invite tous les utilisateurs qui se connectent à l'ordinateur à s'authentifier en saisissant les informations d'identification RSA SecurID (code PIN et code de token), mais il n'exige pas d'authentification pour les utilisateurs appartenant au groupe d'administrateurs.

Si vous décidez de ne pas exempter les utilisateurs du groupe d'administrateurs lors de l'installation ou lorsque vous utilisez pour la première fois l'assistant de configuration pour créer un module d'installation, vous pouvez définir cette option ultérieurement. Par exemple, vous pouvez reconfigurer vos paramètres à l'aide de l'assistant de configuration de l'agent d'authentification pour créer un autre module d'installation et le déployer. Ou bien, vous pouvez apporter des modifications à la stratégie dans le modèle d'objet de stratégie de groupe. Pour plus d'informations, reportez-vous à la *Group Policy Object Template Guide*. Pour obtenir la liste des autres méthodes d'accès d'urgence, consultez « Choisir les méthodes d'accès d'urgence » à la page 26.

Gestion centralisée des paramètres d'authentification

Pour gérer RSA Authentication Agent 7.4 for Microsoft Windows, vous pouvez utiliser des modèles d'objet de stratégie de groupe pour modifier les stratégies d'agent d'authentification et appliquer ces stratégies aux ordinateurs appropriés. Vous pouvez charger les modèles dans l'outil Microsoft Group Policy Management Console (GPMC) de votre contrôleur de domaine et spécifier les stratégies dans les modèles. Les stratégies sont automatiquement téléchargées par les ordinateurs clients au sein du domaine.

Remarque : Vous devez installer ces modèles sur les ordinateurs que vous souhaitez protéger avec un agent d'authentification et qui ne font pas partie de votre domaine ou qui ne sont pas soumis à une stratégie de groupe, et spécifier les paramètres du modèle à l'aide de l'éditeur d'objet de stratégie de groupe local. Pour plus d'informations, consultez le *guide de modèle d'objet de stratégie de groupe.*

Avant que les utilisateurs ne commencent à utiliser l'agent d'authentification, vous pouvez définir des paramètres spécifiques afin d'adapter le produit à vos besoins. RSA Authentication Agent est fourni avec les modèles d'objet de stratégie de groupe (GPO) suivants :

- **RSA_Authentication_Agent** (installé par défaut)
- **RSA_Authentication_Agent_Password_Synchronization**
- **RSA_SecurID_Expiration_Warning** (installé par défaut)
- **RSACredProviderFilter_Microsoft** (installé par défaut)
- **RSACredProviderFilter_SecurID** (installé par défaut)
- **RSACredProviderFilter_SmartCard** (installé par défaut)
- **RSACredProviderFilter_ThirdParty** (installé par défaut)
- **RSADesktop_VerifyRSAComponents**
- **RSADesktop_PreserveFailedAuthHistory**

Chaque modèle est fourni aux formats **.adm** et **.admx/.adml**. Le format **.admx/.adml** est requis lors de l'importation de fichiers dans le magasin central de la stratégie globale.

Si vous souhaitez limiter les options d'ouverture de session pour les utilisateurs de l'agent d'authentification, vous devez installer et configurer un ou plusieurs modèles de stratégie de filtrage de fournisseur d'informations d'identification. Un filtre de fournisseur d'informations d'identification vous permet de masquer la mosaïque de connexion présentée par un fournisseur d'informations d'identification.

Vous pouvez utiliser les filtres suivants :

Fichier de modèle GPO	Description
RSACredProviderFilter_Microsoft	Filtre le fournisseur d'informations d'identification Microsoft.
RSACredProviderFilter_SmartCard	Filtre le fournisseur d'informations d'identification RSA Smart Card.
RSACredProviderFilter_ThirdParty	Filtre tous les fournisseurs d'informations d'identification tiers.
RSACredProviderFilter_SecurID	Filtre le fournisseur d'informations d'identification RSA SecurID.

Pour plus d'informations sur les options tierces, consultez « Fournisseurs d'informations d'identification tiers pris en charge » à la page 22. Pour plus d'informations sur l'utilisation des modèles, consultez le *guide de modèle d'objet de stratégie de groupe*.

Mise à jour automatique des adresses IP

L'adresse IP d'un ordinateur client d'agent d'authentification permet à Authentication Manager d'identifier l'ordinateur lors de l'authentification. Si vous installez l'utilitaire d'inscription automatique lors de l'installation de l'agent d'authentification, l'utilitaire ajoute automatiquement l'agent à la base de données Authentication Manager lors de la première connexion à l'ordinateur via l'authentification RSA SecurID.

L'agent d'authentification lance également l'utilitaire d'inscription automatique :

- Si l'adresse IP de l'ordinateur client de l'agent d'authentification est modifiée
- Lorsque vous utilisez RSA Control Center, pour effacer le secret de nœud sur l'ordinateur client de l'agent d'authentification

Pour plus d'informations, consultez Chapter 4, « Gérer les agents d'authentification. »

Accès aux ordinateurs protégés à l'aide d'un code PIN ou d'un mot de passe

Vous pouvez configurer RSA Authentication Agent 7.4 pour permettre aux utilisateurs de déverrouiller leurs ordinateurs protégés à l'aide de leur code PIN RSA SecurID ou de leurs mots de passe Windows. Les utilisateurs ne peuvent utiliser que leur code PIN ou leur mot de passe après s'être authentifiés avec succès à l'aide d'un code d'accès dans les délais configurés pour cette fonction.

En tant qu'administrateur, vous pouvez sélectionner l'option que vous souhaitez utiliser (code PIN ou mot de passe), activer et désactiver cette fonction, spécifier l'événement qui démarre la période de déverrouillage, définir un délai d'expiration de la fonction et définir le nombre de saisies incorrectes des codes PIN ou des mots de passe par les utilisateurs avant que ces derniers soient contraints de fournir un code d'accès. Vous configurez cette option à l'aide des modèles d'objet de stratégie de groupe après l'installation. Pour plus d'informations, reportez-vous à la *Group Policy Object Template Guide*.

Remarque : Pour que les utilisateurs puissent déverrouiller l'ordinateur à l'aide d'un code PIN RSA SecurID, l'administrateur Authentication Manager doit avoir activé la fonction d'authentification hors ligne pour ces éléments et l'authentification hors ligne doit être exécutée en tant que service sur l'agent. Si vous désactivez le service d'authentification hors ligne via le modèle de paramètres d'authentification local, les utilisateurs ne peuvent pas utiliser l'authentification hors ligne ou déverrouiller leurs ordinateurs avec un code PIN RSA SecurID. Pour plus d'informations sur les paramètres, reportez-vous au *guide de modèle d'objet de stratégie de groupe.*

Prise en charge des groupes multidomaines

Lorsque vous sélectionnez un groupe Windows en tant que groupe d'authentification RSA Authentication Agent à l'aide des modèles d'objet de stratégie de groupe, tous les utilisateurs du groupe doivent s'authentifier via RSA SecurID. L'agent d'authentification prend en charge la configuration des groupes disponibles dans Microsoft Active Directory. Toutefois, l'agent d'authentification ne peut pas déterminer l'appartenance à un groupe si un utilisateur se trouve dans une forêt différente de celle que vous avez sélectionnée. Pour plus d'informations sur la configuration des groupes d'authentification, consultez *Group Policy Object Template Guide*.

Il existe de nombreuses combinaisons de groupes Windows : universel, global et Domain local. Windows permet également d'imbriquer des groupes au sein d'autres groupes. Il est important de comprendre les différentes combinaisons de groupes, de sorte à obtenir les résultats escomptés en imposant ou en excluant l'authentification pour un groupe auprès de RSA SecurID.

Pour plus d'informations, consultez l'exemple « Prise en charge des groupes multidomaines » dans à la page 67.

Options de personnalisation de RSA Authentication Agent

Après l'installation de l'agent d'authentification, les utilisateurs peuvent afficher le fournisseur d'informations d'identification RSA Authentication Agent. Vous pouvez personnaliser RSA Authentication Agent de plusieurs manières. Voici quelques exemples :

- **Spécifier si les demandes d'ouverture de session exigent des mots de passe, des codes d'accès ou des codes PIN.**
- **Configurer l'option Déverrouiller pour autoriser l'accès à l'aide d'un code PIN RSA SecurID ou d'un mot de passe Windows.**
- **Avertir les utilisateurs du nombre de jours restants avant l'expiration d'un authentificateur RSA.**
- **Masquer ou afficher différents fournisseurs d'informations d'identification RSA.**
- **Installer le pack de langue pour afficher le produit dans une langue autre que l'anglais.** Lorsque vous installez l'application de l'agent d'authentification standard, les composants suivants s'affichent automatiquement en anglais :
  - Invites d'ouverture de session de l'agent d'authentification
  - Interface utilisateur (RSA Control Center)
  - Aide
  - Documentation

  Par exemple, si vous utilisez un système d'exploitation japonais et que vous installez le pack de langue japonais pour l'agent d'authentification, vous verrez ces composants en japonais. (Si vous installez le pack de langue japonais sur un ordinateur qui utilise un système d'exploitation en anglais, le produit restera affiché en anglais.) Pour plus d'informations, consultez « Installer un pack de langue », à la page 44.

Pour connaître les options de personnalisation, reportez-vous au *guide des modèles d'objet de stratégie de groupe*.

Authentificateurs pris en charge

RSA Authentication Agent 7.4 for Microsoft Windows prend en charge les types d'authentificateurs suivants :

- Key Fobs RSA SecurID
- Cartes standard RSA SecurID
- PINPads RSA SecurID
- Tokens logiciels RSA SecurID
- Authentificateur RSA SecurID 800
- code de token RSA à la demande

Remarque : Vous ne pouvez pas utiliser d'authentificateurs logiciels résidant sur l'ordinateur pour vous connecter à des ordinateurs de bureau Windows protégés. Toutefois, une fois que vous êtes connecté(e) à l'ordinateur de bureau en utilisant un autre type d'authentificateur, vous pouvez utiliser des authentificateurs logiciels pour vous connecter au réseau. Vous pouvez utiliser RSA Authentication Agent avec un authentificateur logiciel installé sur un appareil portable, par exemple, un BlackBerry. Pour plus d'informations sur les authentificateurs logiciels, consultez la documentation RSA fournie avec votre authentificateur logiciel.

L'authentificateur RSA SecurID 800 Authenticator (RSA SecurID 800) peut fonctionner comme un authentificateur RSA SecurID et une carte à puce. Pour l'utiliser en tant que token RSA SecurID, vous pouvez lire le code de token à l'avant et le saisir manuellement lorsque vous y êtes invité. Ou bien, si vous avez installé la fonction d'authentification connectée avec l'agent d'authentification, vous pouvez le connecter au port USB de l'agent pour qu'il accède automatiquement au code de token.

Le RSA SecurID 800 ressemble à ce qui suit :

Pour une utilisation de la carte à puce, RSA SecurID 800 dispose d'une carte à puce associée à un lecteur intégré. (La puce intelligente est un microprocesseur qui peut stocker et traiter les données.) Pour utiliser RSA SecurID 800 sous la forme d'une carte à puce, vous devez installer RSA Authentication Client et connecter l'authentificateur au port USB. Pour plus d'informations sur RSA Authentication Client, consultez la documentation fournie avec le produit RSA Authentication Client.

Remarque : Si RSA Authentication Agent est installé et que vous installez RSA Authentication Client, l'interface utilisateur (également appelée RSA Control Center) chargée de gérer la partie RSA SecurID ou carte à puce de votre authentificateur change. Vous disposez de plus ou moins d'options, en fonction de ce que vous avez installé. Pour plus d'informations, consultez « RSA Control Center », à la page 17.

RSA Control Center

Lors de l'installation de RSA Authentication Agent, vous installez également une interface utilisateur dénommée RSA Control Center. RSA Control Center permet aux utilisateurs et aux administrateurs d'utiliser des options de gestion de certains aspects de leurs paramètres RSA SecurID. Le Control Center contient des options qui permettent aux utilisateurs de vérifier l'offre de jours en mode hors ligne et de les actualiser si nécessaire.

Certains paramètres de configuration disponibles dans les interfaces utilisateur de RSA Authentication Agent 6.1, 6.4 et 7.0 sont désormais disponibles exclusivement dans les modèles d'objet de stratégie de groupe. Les paramètres indiquent si les ordinateurs doivent être déverrouillés à l'aide d'un code PIN RSA SecurID ou d'un mot de passe Windows au lieu d'un code d'accès, si les fournisseurs d'informations d'identification doivent être filtrés et si l'invite d'ouverture de session locale doit inviter à saisir un code d'accès ou un mot de passe. Pour plus d'informations, reportez-vous au *guide des modèles d'objet de stratégie de groupe.*

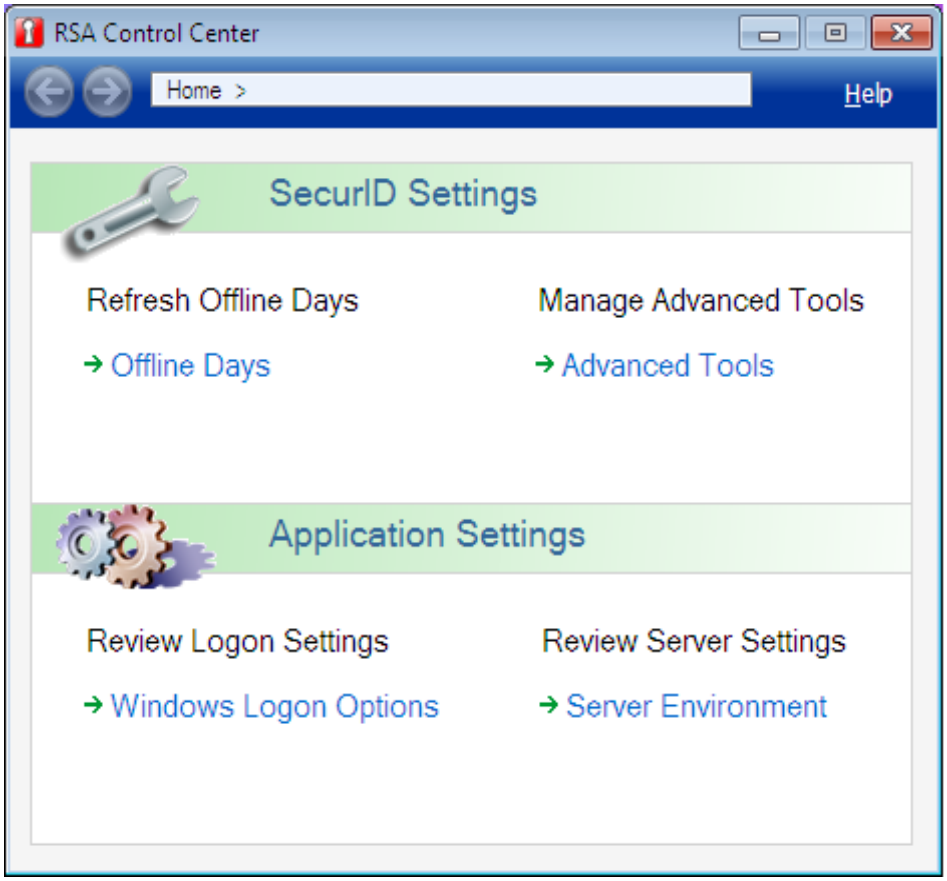
En tant qu'administrateur, vous pouvez effectuer les tâches suivantes à partir de RSA Control Center :

- Tester l'authentification.
- Afficher des informations sur l'environnement du serveur RSA Authentication.
- Activer, tester ou effacer le mot de passe de réserve. Un mot de passe de réserve permet aux utilisateurs de se connecter à un ordinateur si l'authentification hors ligne n'est pas en cours d'exécution ou si l'ordinateur ne parvient pas à se connecter à RSA Authentication Manager. Vous pouvez également définir le mot de passe de réserve à l'aide des modèles d'objet de stratégie de groupe. Pour plus d'informations, reportez-vous au *guide des modèles d'objet de stratégie de groupe.*
- Activer le remplacement d'une adresse IP pour empêcher tout échec de communication si RSA Authentication Agent s'exécute sur un hôte disposant de plusieurs cartes d'interface réseau et par conséquent de plusieurs adresses IP.
- Effacer le secret de nœud s'il est corrompu ou s'il ne correspond pas au secret de nœud dans la base de données Authentication Manager.
- Activez le traçage pour générer des fichiers log en vue de la résolution des problèmes.
- Spécifier les utilisateurs à authentifier et définir la manière dont les utilisateurs sont authentifiés lorsque leur appartenance à un groupe ne peut pas être déterminée sur cet ordinateur. Vous pouvez également spécifier les paramètres d'authentification avec une stratégie de groupe. Notez que les paramètres de stratégie de groupe remplacent ceux configurés dans RSA Control Center. Pour plus d'informations, reportez-vous au *guide des modèles d'objets de stratégie de groupe*.
- Effacer les données hors ligne en cas de désactivation de l'authentification hors ligne, de modification du nombre de jours hors ligne que RSA Authentication Manager génère et télécharge, ou en cas de réaffectation de l'ordinateur protégé à un autre utilisateur.

Utilisez RSA Control Center pour effectuer l'une des opérations suivantes :

- Cliquez sur **Démarrer** > **RSA** > **RSA Control Center**.
- Double-cliquez sur l'icône de RSA Control Center dans la zone de notification.

La figure ci-dessous présente la page d'accueil de RSA Control Center.



Remarque : Si vous installez RSA Authentication Client pour utiliser l'authentificateur RSA SecurID 800 en tant que carte à puce, le RSA Control Center qui est installé avec l'agent d'authentification se développe pour afficher davantage d'options de gestion du code PIN de votre carte à puce. Les options RSA SecurID de l'agent d'authentification restent visibles. Si vous supprimez RSA Authentication Client (ou l'agent d'authentification), les options liées à ce produit sont supprimées du Control Center. Pour plus d'informations, reportez-vous à l'aide de RSA Authentication Client (carte à puce) ou à l'aide de RSA Authentication Agent (RSA SecurID) installée avec le Control Center.

Pour obtenir une description de la zone de notification et des icônes de RSA Control Center, reportez-vous à « Icônes RSA Control Center. »

Icônes RSA Control Center

Lorsque vous installez RSA Authentication Agent, l'icône RSA Control Center s'affiche dans la zone de notification de la barre des tâches Windows. Vous pouvez utiliser cette icône pour ouvrir RSA Control Center et afficher cette icône pour plus d'informations sur RSA Authentication Agent.

Le tableau ci-dessous décrit l'icône RSA Control Center.

Icônes	Description
	Ouvre RSA Control Center Vous pouvez double-cliquer sur l'icône ou cliquer dessus avec le bouton droit et sélectionner une option pour ouvrir le Control Center. Pour supprimer l'icône de la barre des tâches, cliquez avec le bouton droit sur l'icône et sélectionnez l'option pour la fermer. Sans l'icône, vous devez utiliser le groupe de programmes (par exemple, Démarrer > Tous les programmes > RSA > RSA Control Center) pour ouvrir le Control Center.
	Signale que le nombre de jours en mode hors ligne est inférieur à un nombre donné, en affichant un point d'exclamation jaune dans le coin inférieur droit. Affiche également le nombre de jours restants avant l'expiration de l'authentificateur du port USB. Utilisez l'option Jours en mode hors ligne de la page d'accueil de Control Center pour vérifier ou actualiser vos jours. Pour plus d'informations sur les jours en mode hors ligne, reportez-vous àChapter 4, « Gérer les agents d'authentification » ou à l'aide de RSA Authentication Agent (RSA SecurID). Pour plus d'informations sur la définition de l'expiration d'un authentificateur, reportez-vous au guide de l'objet de stratégie de groupe.
	Indique que l'application reconnaît un authentificateur connecté au port USB en affichant une croix bleue dans le coin supérieur droit de l'icône. **Remarque :** Les utilisateurs peuvent insérer plusieurs authentificateurs dans différents ports USB et sélectionner celui qu'ils souhaitent utiliser. Pour plus d'informations, reportez-vous à l'aide de RSA Control Center (RSA SecurID).
	Indique les données auxquelles l'agent d'authentification est en train d'accéder sur l'authentificateur. **Remarque :** Un utilisateur ne doit pas supprimer un authentificateur tant que l'agent d'authentification n'a pas terminé le traitement des données.

2 Préparation de l'installation

Configuration système

RSA Authentication Agent 7.4 for Microsoft Windows possède la configuration suivante :

- Processeur 1 GHz (x86)
- 1 Go de RAM
- 35 Mo d'espace libre
- Gestion réseau TCP/IP
- Microsoft .NET Framework 4 Client Profile ou version ultérieure

Ports requis

Le tableau suivant répertorie les ports qui doivent être disponibles en vue d'une utilisation par l'agent d'authentification.

Port	Description
5500/udp	RSA Authentication Manager utilise ce port pour l'écoute. L'agent d'authentification se connecte à ce port lors de l'authentification.
5580/tcp	L'agent d'authentification utilise ce port pour prendre en charge l'authentification hors ligne, l'intégration des mots de passe et le déverrouillage avec les fonctions de code PIN RSA SecurID. Si vous n'utilisez pas ces fonctions et que vous souhaitez fermer ce port, vous devez également désactiver la stratégie de groupe RSA **Service d'authentification hors ligne**. Pour plus d'informations, reportez-vous au *guide de modèle d'objet de stratégie de groupe*.
5550/tcp	Utilisé par l'utilitaire d'inscription automatique de l'agent d'authentification. Vous pouvez installer l'utilitaire d'inscription automatique lors de l'installation de l'agent d'authentification ou de la création d'un package MSI. Cet utilitaire inscrit automatiquement l'adresse IP de l'hôte de l'agent dans la base de données Authentication Manager lors du premier démarrage par les utilisateurs de l'agent installé sur leur ordinateur.
389/tcp	Utilisé par l'agent d'authentification pour vérifier si l'utilisateur est membre d'un groupe d'authentification dans Microsoft Active Directory.

Systèmes d'exploitation pris en charge

RSA Authentication Agent 7.4 for Microsoft Windows est pris en charge sur les systèmes d'exploitation suivants :

- Windows 7 SP1, 32 bits et 64 bits, éditions Entreprise et Professionnel
- Windows 8.1, 32 bits et 64 bits, éditions Entreprise et Professionnel
- Windows Server 2008 SP2, 32 et 64 bits, éditions Standard, Entreprise, Datacenter et Web Server
- Windows Server 2008 R2 SP1, 64 bits, éditions Standard, Entreprise, Datacenter et Web Server
- Windows Server 2012 R2, éditions Standard ou Datacenter (Server Core ou Server avec interface utilisateur graphique [GUI])
- Windows 10, 32 bits et 64 bits, éditions Entreprise et Professionnel
- Windows Server 2016, éditions Standard ou Datacenter (Server Core ou Server avec interface utilisateur graphique [GUI])
- Windows Server 2019 édition Standard (Server Core ou Expérience utilisateur)

Pour obtenir des instructions sur la mise à niveau vers RSA Authentication Agent 7.4 for Microsoft Windows après la mise à niveau des ordinateurs clients vers un autre système d'exploitation, consultez « Mise à niveau vers RSA Authentication Manager 7.4 » à la page 50.

Produits d'accès à distance tiers pris en charge

RSA Authentication Agent protège les ouvertures de session sur un ordinateur distant via des applications qui prennent en charge le protocole RDP (Remote Desktop Protocol), à l'instar de Microsoft Remote Desktop Connection et de Citrix Virtual Delivery Agent.

Produits RSA Authentication Manager pris en charge

RSA Authentication Agent 7.4 fonctionne comme un produit client compatible avec RSA Authentication Manager 8.2 SP1 ou une version supérieure. Pour obtenir des instructions sur l'installation, rendez-vous sur RSA Link à l'adresse **https://community.rsa.com**.

Avant d'activer l'authentification RSA SecurID, vous devez comprendre RSA Authentication Manager le système et ses fonctionnalités. Pour plus d'informations, reportez-vous au *RSA Authentication Managerguide de l'administrateur* correspondant à votre version, ou contactez votre administrateur Authentication Manager.

Fournisseurs d'informations d'identification tiers pris en charge

Si vous laissez le paramètre par défaut sur le modèle d'objet de stratégie de groupe **RSACredProviderFilter_ThirdParty**, les utilisateurs ne peuvent pas accéder à la mosaïque de connexion pour le fournisseur d'informations d'identification tiers. Vous devez activer le paramètre de stratégie tierce pour permettre aux utilisateurs d'accéder au fournisseur d'informations d'identification tiers. Pour plus d'informations sur les modèles, consultez le *guide de modèle d'objet de stratégie de groupe*.

Prise en charge de l'accès à distance

RSA Authentication Agent protège les ouvertures de session sur un ordinateur distant via des applications qui prennent en charge le protocole RDP (Remote Desktop Protocol), à l'instar de Microsoft Remote Desktop Connection. Vous pouvez ouvrir l'une de ces applications sur votre ordinateur local pour vous connecter aux ordinateurs distants.

Lorsque Authentication Agent est installé sur votre ordinateur local, le processus par lequel une application RDP se connecte à un ordinateur distant ne change pas. Dans la plupart des cas, lorsque vous tentez de vous connecter à un ordinateur distant, vous êtes invité(e) à vous authentifier avec les informations d'identification Windows. Ces informations d'identification sont utilisées par l'application RDP pour permettre l'authentification Windows NLA (Network Level Authentication) avant d'établir une connexion avec l'ordinateur distant.

Lorsque l'agent d'authentification est installé sur l'ordinateur distant, une invite s'affiche pour vous demander de vous authentifier avec les informations d'identification RSA SecurID avant de pouvoir accéder au bureau à distance.

Vous êtes invité(e) à fournir des informations d'identification RSA SecurID en fonction de la configuration de l'agent d'authentification.

Pour plus d'informations sur l'authentification au niveau du réseau, consultez le site **web site.Web de Microsoft**.

Préparation de l'installation de l'agent d'authentification

Cette section décrit les tâches que vous devez effectuer avant d'installer et de configurer RSA Authentication Agent 7.4.

Tâche	Référence
Configuration de RSA Authentication Manager	« Configuration de RSA Authentication Manager », à la page 24
Créer des groupes d'utilisateurs qui devront s'authentifier avec RSA SecurID	« Créer des groupes d'utilisateurs qui devront s'authentifier avec RSA SecurID », à la page 25
Choisir les méthodes d'accès d'urgence	« Choisir les méthodes d'accès d'urgence », à la page 26
Préparer les utilisateurs à l'authentification RSA SecurID	« Préparer les utilisateurs à l'authentification RSA SecurID », à la page 28

Configuration de RSA Authentication Manager

Avant d'installer et de configurer l'agent d'authentification, vous ou votre administrateur RSA Authentication Manager devez effectuer les tâches suivantes :

- Si vous ne l'avez pas encore fait, installez RSA Authentication Manager 8.2 SP1 ou une version supérieure. Pour savoir comment procéder, consultez le *RSA Authentication Manager Guide d'installation et de configuration*.
- Créez une copie du fichier de configuration du système (**sdconf.rec**) à partir de RSA Authentication Manager et fournissez une copie à l'administrateur installant RSA Authentication Agent 7.4 (ou demandez à l'administrateur comment le trouver sur le réseau). L'administrateur d'agent d'authentification doit importer ce fichier lors de l'utilisation de l'assistant de configuration pour créer le module d'installation ou lors de l'exécution d'une installation locale.

  Les utilisateurs peuvent rencontrer des problèmes de connexion avec un code d'accès RSA SecurID après le redémarrage de l'ordinateur (ou après la sortie du mode veille ou hibernation) si vous installez l'utilitaire d'inscription automatique avec l'agent et que celui-ci tente de contacter un serveur de réplica RSA Authentication Manager au lieu d'un serveur primaire Authentication Manager.

  Dans cet environnement, l'agent tente d'utiliser l'authentification hors ligne. Si l'utilisateur est à court de jours en mode hors ligne, le processus d'authentification de RSA SecurID échoue. Pour vous assurer que l'authentification RSA SecurID n'échoue pas après un redémarrage, vous devez utiliser une copie du fichier **sdconf.rec** à partir d'un serveur Authentication Manager qui permet l'inscription automatique et effectue l'authentification. (Le service d'authentification doit être en cours d'exécution sur ce serveur.)

  Si l'administrateur d'agent d'authentification envisage d'installer l'utilitaire d'inscription automatique pour inscrire automatiquement les ordinateurs des utilisateurs dans la base de données Authentication Manager lors du premier démarrage de leurs ordinateurs avec l'agent d'authentification, créez une copie du fichier **server.cer** à partir de RSA Authentication Manager en plus du fichier **sdconf.rec**. Envoyez-le à l'administrateur installant RSA Authentication Agent 7.4. L'administrateur peut l'importer lors de la création d'un module d'installation ou lors d'une installation locale.

  Pour plus d'informations sur les fichiers que vous devez importer, consultez Chapter 3, « Installation de l'agent d'authentification RSA. ». Pour plus d'informations sur l'utilitaire d'inscription automatique, consultez Chapter 4, « Gérer les agents d'authentification. ».
- Vérifiez que RSA Authentication Manager est installé et est en cours d'exécution sur un serveur.
- Enregistrez l'hôte RSA Authentication Agent 7.4 en tant qu'agent de RSA Authentication Manager. Pour plus d'informations, consultez le *RSA Authentication ManagerGuide d'administration* correspondant à votre version de. Vous n'avez pas besoin d'inscrire manuellement les ordinateurs des utilisateurs si vous installez l'utilitaire d'inscription automatique lors de l'installation de l'agent d'authentification. Pour plus d'informations, reportez-vous aux sections Chapter 3, « Installation de l'agent d'authentification RSA » et Chapter 4, « Gérer les agents d'authentification. »

Remarque : Si vous installez l'agent d'authentification sur un serveur multirésident et non un agent avec l'utilitaire d'inscription automatique, fournissez une adresse IP de remplacement pour l'agent d'authentification. (Un serveur multirésident est un ordinateur possédant plusieurs adresses IP pour les réseaux connectés. Cela permet à une session de survivre en cas de panne du réseau.) Pour plus d'informations sur la définition d'une adresse IP de remplacement, reportez-vous à l'aide de RSA Authentication Agent (RSA SecurID).

Inscrivez les utilisateurs de RSA SecurID dans la base de données RSA Authentication Manager et distribuez les authentificateurs RSA SecurID à ces utilisateurs. Pour plus d'informations sur l'inscription manuelle des utilisateurs, reportez-vous au *RSA Authentication ManagerGuide d'administration* de votre version.

Créer des groupes d'utilisateurs qui devront s'authentifier avec RSA SecurID

Vous contrôlez l'accès aux ressources protégées par RSA Authentication Agent 7.4 en spécifiant les utilisateurs qui doivent s'authentifier avec des codes d'accès RSA SecurID. Vous pouvez configurer un agent d'authentification afin d'instaurer une authentification pour :

- Aucun utilisateur
- Tous les utilisateurs
- Un groupe d'utilisateurs
- Tous les utilisateurs, à l'exception d'un certain groupe d'utilisateurs

L'agent d'authentification utilise des groupes Windows pour contrôler l'accès aux ressources. Ces groupes peuvent être des groupes Windows par défaut ou des groupes que vous créez à l'aide de l'interface de gestion de l'ordinateur Windows ou d'Active Directory. Si vous souhaitez utiliser des groupes autres que les groupes par défaut Windows, vous devez les créer avant de configurer l'agent d'authentification. Vérifiez que les groupes que vous créez sont reconnus par Active Directory en tant que tels et qu'ils peuvent être interrogés. Pour obtenir des instructions détaillées sur la création de groupes, reportez-vous à la documentation Microsoft Windows.

Vous pouvez appliquer des paramètres d'authentification à des ordinateurs individuels à l'aide de RSA Control Center. Pour obtenir des instructions et des informations supplémentaires, reportez-vous à l'aide de RSA Control Center, sous la rubrique Authentification des utilisateurs. Si vous utilisez l'assistant de configuration pour configurer un module d'installation, comme décrit dans la section Chapter 3, « Installation de l'agent d'authentification RSA, », vous pouvez uniquement sélectionner une option pour authentifier tous les utilisateurs, à l'exception de ceux appartenant au groupe d'administrateurs local. Si vous utilisez les modèles d'objet de stratégie de groupe, vous pouvez utiliser les options répertoriées dans cette section. Pour plus d'informations, reportez-vous à la *Group Policy Object Template Guide*.

Choisir les méthodes d'accès d'urgence

RSA Authentication Agent 7.4 inclut des options qui permettent aux utilisateurs et aux administrateurs d'accéder aux ordinateurs de bureau protégés s'ils perdent leur authentificateurs, s'ils oublient leur code PIN ou s'ils sont à cours de jours en mode hors ligne. Avant d'installer et de configurer l'agent d'authentification, vous devez choisir les méthodes d'accès d'urgence que vous souhaitez utiliser. Les tableaux suivants décrivent les méthodes d'accès d'urgence et indiquent où trouver plus d'informations.

Pour les utilisateurs hors ligne.

Méthode d'accès d'urgence	Description	Caractéristiques	Référence
Code de token d'accès d'urgence hors ligne	Les utilisateurs peuvent accéder à leurs ordinateurs protégés sans code de token (par exemple, s'ils ont perdu leurs authentificateurs)	• Doit être combiné au code PIN RSA SecurID de l'utilisateur • Est modifié lors de la prochaine authentification de l'utilisateur en ligne • Expire après un laps de temps spécifié	Consultez « Accès d'urgence », à la page 58.
Code d'accès d'urgence hors ligne	Les utilisateurs peuvent accéder à leurs ordinateurs protégés sans code PIN RSA SecurID ou code de token (par exemple, s'ils ont oublié leur code PIN ou si ce dernier a été compromis)	• Aucun code PIN RSA SecurID requis • Est modifié lors de la prochaine authentification de l'utilisateur en ligne • Expire après un laps de temps spécifié	Consultez « Accès d'urgence », à la page 58.

Pour les utilisateurs en ligne

Méthode d'accès d'urgence	Description	Caractéristiques	Référence
Mots de passe à usage unique	Les utilisateurs peuvent accéder à leurs ordinateurs protégés sans code de token (par exemple, s'ils ont perdu leurs authentificateurs)	• Doit être combiné au code PIN RSA SecurID de l'utilisateur • Généré par le RSA Authentication Manager • Valide pour une authentification unique	Consultez le *RSA Authentication Manager Guide de l'administrateur* correspondant à votre version.

Pour les utilisateurs en ligne

Méthode d'accès d'urgence	Description	Caractéristiques	Référence
Mots de passe permanents	Les utilisateurs peuvent accéder à leurs ordinateurs protégés sans code de token (par exemple, s'ils ont perdu leurs authentificateurs)	• Doit être combiné au code PIN RSA SecurID de l'utilisateur • Créé par un administrateur RSA Authentication Manager • Valide jusqu'à ce que l'état de l'authentificateur perdu soit modifié.	Consultez le *RSA Authentication Manager Guide de l'administrateur* correspondant à votre version.
Code de token à la demande	Les utilisateurs ayant des appareils mobiles numériques et des comptes de messagerie personnelle peuvent recevoir des codes de token à usage ponctuel sous la forme de messages SMS.	• Doit être combiné avec le code PIN de l'authentificateur de l'utilisateur. • Les appareils mobiles et les comptes de messagerie des utilisateurs doivent être autorisés à recevoir des codes de token à la demande.	Consultez le *RSA Authentication Manager guide de l'administrateur* correspondant à votre version.

Pour les administrateurs

Méthode d'accès d'urgence	Description	Caractéristiques	Référence
Reserve mot de passe	Le mot de passe de réserve permet à l'administrateur ou à l'utilisateur de contourner les exigences de code d'accès. Les administrateurs (ou un utilisateur qui a obtenu le mot de passe de réserve d'un administrateur) peuvent se connecter à l'ordinateur de l'utilisateur avec le compte de l'utilisateur (ou n'importe quel nom d'utilisateur valide pour l'ordinateur) et le mot de passe de réserve.	• Défini par un administrateur sur chaque agent après l'installation via RSA Control Center ou du modèle de stratégie de groupe des paramètres d'authentification locaux • N'expire jamais	Reportez-vous à l'aide de RSA Authentication Agent (RSA SecurID) (dans RSA Control Center) ou dans *Group Policy Object Template Guide.*

Pour les administrateurs			
Méthode d'accès d'urgence	**Description**	**Caractéristiques**	**Référence**
Compte administrateur exempté	Les administrateurs peuvent s'authentifier auprès des ordinateurs protégés avec un mot de passe uniquement	• Défini lors de l'installation de l'agent via le fichier MSI, l'assistant de configuration ou le modèle de stratégie de groupe des paramètres d'authentification locaux • Membre du groupe d'administrateurs sur chaque agent • Protection par mot de passe simple Windows	Voir « Accès aux ordinateurs de bureau protégés dans les situations d'urgence » à la page 11 ou *Group Policy Object Template Guide.*

Préparer les utilisateurs à l'authentification RSA SecurID

Avant de déployer RSA Authentication Agent 7.4, préparez vos utilisateurs RSA SecurID comme suit :

- Inscrivez les utilisateurs qui seront invités à fournir des codes d'accès en tant qu'utilisateurs RSA SecurID dans la base de données RSA Authentication Manager et activez leurs authentificateurs. Pour plus d'informations sur l'inscription des utilisateurs, consultez le *RSA Authentication Managerguide de l'administrateur* correspondant à votre version.

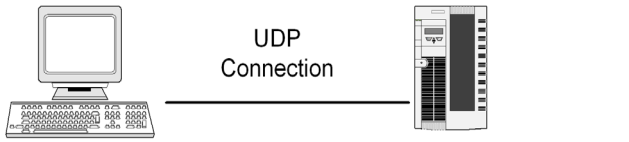
  Important : Les noms d'utilisateur Windows pour les utilisateurs RSA SecurID doivent être enregistrés dans la base de données RSA Authentication Manager. Ces noms d'utilisateur ne doivent pas contenir d'espaces ni dépasser 48 caractères.

- Fournissez des tokens affectés et activés aux utilisateurs qui devront fournir des codes d'accès.
- Fournissez les instructions d'authentification aux utilisateurs. Pour plus d'informations, reportez-vous à la documentation fournie avec votre authentificateur.

3 Installation de l'agent d'authentification RSA

Un agent d'authentification RSA doit communiquer avec RSA Authentication Manager pour procéder à l'authentification RSA SecurID. Avant d'installer RSA Authentication Agent 7.4 for Microsoft Windows, assurez-vous que l'une des versions prises en charge de RSA Authentication Manager est installée sur le serveur approprié.

Pour plus d'informations sur l'installation d'Authentication Manager, reportez-vous au *guide d'installation et de configuration de RSA Authentication Manager* correspondant à votre version. La figure suivante illustre la connexion UDP (User Datagram Protocol) entre l'ordinateur de l'utilisateur et le serveur Authentication Manager :



User's Computer with RSA Authentication Agent

RSA Authentication Manager

Pour effectuer une mise à niveau à partir d'une version antérieure de RSA Authentication Agent, reportez-vous à « Mise à niveau vers RSA Authentication Manager 7.4 » à la page 50.

Remarque : Après l'installation de l'agent d'authentification, vous pouvez configurer RSA Authentication Manager pour étendre le processus de connexion à RSA SecurID aux utilisateurs lorsque ceux-ci ne sont pas connectés à Authentication Manager via le réseau. Pour plus d'informations, consultez « Authentification hors ligne », à la page 53.

Méthodes d'installation

Utilisez l'une des méthodes suivantes pour installer l'agent d'authentification :

- Pour installer l'agent d'authentification sur un seul ordinateur, exécutez le fichier MSI (**RSA Authentication Agent.msi**) sur l'ordinateur local.
- Dans le cadre d'un déploiement à grande échelle, utilisez l'assistant de configuration (**ConfigWizard.exe**) pour créer un module d'installation MSI personnalisé et le déployer aux utilisateurs appropriés.

Important : Si vous avez installé Windows Server 2012 en mode Server Core (sans interface utilisateur ou interface GUI), vous devez installer l'agent d'authentification à partir de la ligne de commande. Par exemple, vous pouvez exécuter l'assistant de configuration (**ConfigWizard.exe**) pour créer un module d'installation de l'agent d'authentification et l'installer en saisissant : msiexec/qn/i « RSA Authentication Agent. msi » sur la ligne de commande. (Votre module d'installation peut utiliser un autre nom msi). Une fois que vous avez installé le produit, vous pouvez accéder à l'interface utilisateur de l'agent d'authentification (RSA Control Center) et utiliser les options si vous le souhaitez. Vous pouvez également basculer entre les modes Server Core et Serveur avec GUI après l'installation de l'agent d'authentification et les utiliser de la même manière. Pour plus d'informations sur la création d'un module d'installation personnalisé et sur l'utilisation de la ligne de commande, reportez-vous à « Installer le produit sur plusieurs ordinateurs », à la page 36.

Si vous installez l'agent d'authentification sur le serveur Windows sur lequel vous envisagez de gérer vos modèles d'objet de stratégie de groupe RSA, vous n'avez pas besoin d'installer manuellement les modèles. L'agent d'authentification les installe automatiquement dans la stratégie de sécurité locale. Pour plus d'informations, reportez-vous au *guide de modèle d'objet de stratégie de groupe.*

Installations silencieuses

Vous aurez peut-être besoin d'installer l'agent d'authentification sur un seul ordinateur pour exécuter un test d'authentification avant de déployer un module d'installation sur un groupe plus vaste. Vous devrez peut-être installer le produit sur un ou deux ordinateurs seulement.

Lors du processus d'installation, vous devrez faire votre choix entre une installation **Standard** ou **Personnalisée**. Si vous choisissez une installation **Standard**, vous importez le fichier de configuration système (**sdconf.rec**). Si vous choisissez une installation **personnalisée**, vous pouvez sélectionner une option pour installer l'utilitaire d'inscription automatique et la fonction d'authentificateur connecté RSA SecurID.

L'utilitaire d'inscription automatique inscrit automatiquement l'ordinateur des utilisateurs dans la base de données d'Authentication Manager lorsque les utilisateurs démarrent leur ordinateur pour la première fois après l'installation de l'agent d'authentification. Si vous sélectionnez l'utilitaire d'inscription automatique, vous devez importer le fichier de certificat de serveur (**server.cer**). Si vous souhaitez que les utilisateurs s'authentifient à l'aide d'un authentificateur RSA SecurID 800 connecté au port USB, vous devez également sélectionner la fonction d'authentificateur connecté RSA SecurID.

Déploiements à grande échelle

Pour personnaliser les paramètres de connexion de l'agent d'authentification et installer le produit sur de nombreux ordinateurs, utilisez le fichier **ConfigWizard.exe** situé dans le dossier de l'assistant de configuration qui est fourni dans le dossier du produit au format .zip. Au cours du processus, vous importez le fichier de configuration système (**sdconf.rec**) et, si nécessaire, le fichier de certificat de serveur (**server.cer**). Les fichiers **sdconf.rec** et **server.cer** sont disponibles auprès de votre administrateur RSA Authentication Manager.

Après avoir créé un module d'installation à l'aide de l'assistant de configuration, vous pouvez le déployer à l'aide de Microsoft Systems Management Server (SMS), de la ligne de commande ou d'un script de connexion.

Remarque : Vous pouvez exécuter l'assistant de configuration (**ConfigWizard.exe**) pour créer un module d'installation de l'agent d'authentification sur n'importe quel système d'exploitation Windows pris en charge.

Pour plus d'informations sur les fichiers d'Authentication Manager, consultez suivante. Pour plus d'informations sur l'installation de l'agent d'authentification sur un seul ordinateur, consultez « Installer le produit sur un seul ordinateur » à la page 34. Pour plus d'informations sur l'utilisation de l'assistant de configuration, consultez « Installer le produit sur plusieurs ordinateurs » à la page 36.

Important : Si vous souhaitez utiliser l'agent d'authentification dans une langue autre que l'anglais, installez le pack de langue après l'installation du produit. Pour plus d'informations sur l'installation d'une langue, consultez « Installer un pack de langue » à la page 44.

Importer les fichiers Authentication Manager

Lors du processus d'installation unique ou lorsque vous utilisez l'assistant de configuration pour personnaliser un module d'installation, vous devez importer le fichier de configuration système (**sdconf.rec**) pour que l'agent d'authentification communique avec Authentication Manager. Pour installer l'utilitaire d'inscription automatique, vous devez également importer le fichier de certificat de serveur (**server.cer**).

Dans RSA Authentication Manager 8.2 SP1 ou une version ultérieure, l'administrateur Authentication Manager peut générer un fichier **sdconf.rec** et télécharger un fichier **server.cer** vers l'agent à partir des options du menu **Accès** de la console de sécurité RSA (**Agents d'authentification** > **Générer un fichier de configuration** pour le fichier sdconf.rec et **Agents d'authentication** > **Télécharger le fichier de certificat du serveur** pour le fichier server. cer). Le fichier **sdconf.rec** crée un snapshot des informations de serveur disponibles lors de la génération du fichier.

Les fichiers **sdconf.rec** et **server.cer** se trouvent dans le répertoire **ACEDATA** de l'ordinateur hôte Authentification Manager. Vous devez demander l'un de ces fichiers à votre administrateur Authentication Manager avant de commencer l'installation de l'agent d'authentification.

Pour plus d'informations sur l'installation de ces fichiers, reportez-vous à « Installer le produit sur un seul ordinateur » à la page 34 ou à « Installer le produit sur plusieurs ordinateurs » à la page 36.

Points à prendre en compte pour l'installation

Avant d'installer RSA Authentication Agent 7.4, rassemblez les informations suivantes :

- Si vous effectuez une mise à niveau à partir de RSA Authentication Agent 6.x ou 7.0, vous devez mapper les anciens paramètres aux nouvelles stratégies dans les modèles d'objet de stratégie de groupe RSA Authentication Agent 7.4. Pour plus d'informations, reportez-vous au *guide de modèle d'objet de stratégie de groupe.*
- L'agent d'authentification est disponible sous la forme d'un fichier. zip que vous devez télécharger à l'adresse **https://community.rsa.com/community/products/securid/authentication-agent-windows**.
- L'installation de RSA Authentication Agent sur un ordinateur à l'aide du client RSA EAP 6.1.3 supprime le client RSA EAP 6.1.3 de l'ordinateur.
- Vous devez disposer d'un compte administrateur ou de privilèges d'administration pour installer ce logiciel. Si vous envisagez de déployer un module d'installation, vous devez également définir les tégies de contrôle des privilèges sur les ordinateurs de bureau des utilisateurs. Pour plus d'informations, consultez « Fournir des privilèges de contrôle de compte aux ordinateurs des utilisateurs », à la page 39.
- Si vous installez l'agent d'authentification sur des ordinateurs qui ne sont pas rattachés à un domaine, vous devez définir manuellement les paramètres de la stratégie de groupe sur chaque ordinateur. Pour plus d'informations, reportez-vous au *guide de modèle d'objet de stratégie de groupe.*
- Si vous prévoyez d'installer l'agent d'authentification sur un seul ordinateur, copiez le fichier de configuration système (**sdconf.rec**) et le fichier de certificat de serveur (**server.cer**) depuis RSA Authentication Manager vers l'ordinateur sur lequel vous prévoyez d'installer l'agent d'authentification. (Vous avez uniquement besoin du fichier **server.cer** si vous envisagez d'installer l'utilitaire d'inscription automatique.) Accédez à ces fichiers lorsque vous exécutez le fichier **RSA Authentication Agent.msi**. Pour plus d'informations, consultez « Importer les fichiers Authentication Manager », à la page 31.
- Pour utiliser l'assistant de configuration (**ConfigWizard.exe)**, récupérez le fichier de configuration système (**sdconf.rec**) et le fichier de certificat de serveur (**server.cer**) auprès de l'administrateur RSA Authentication Manager afin de les importer dans votre package de configuration. (Vous avez uniquement besoin du fichier **server.cer** si vous envisagez d'installer l'utilitaire d'inscription automatique.) Les utilisateurs n'ont pas besoin d'accéder à ces deux fichiers pour un déploiement du package d'installation, car celui-ci les contient. Pour plus d'informations, consultez « Importer les fichiers Authentication Manager », à la page 31.

  Remarque : Vous devez demander l'un de ces fichiers à votre administrateur Authentication Manager avant d'installer l'agent d'authentification.

- Les utilisateurs peuvent rencontrer des problèmes de connexion avec un code d'accès RSA SecurID après le redémarrage de l'ordinateur (ou après la sortie du mode veille ou hibernation) si vous installez l'utilitaire d'inscription automatique avec l'agent et que celui-ci tente de contacter un serveur de réplica RSA Authentication Manager au lieu d'un serveur primaire Authentication Manager. Dans cet environnement, l'agent tente d'utiliser l'authentification hors ligne.

  Important : Si l'utilisateur est à court de jours en mode hors ligne, le processus d'authentification de RSA SecurID échoue. Pour vous assurer que l'authentification RSA SecurID n'échoue pas lorsque l'utilisateur tente de se connecter alors qu'il est à court de jours en mode hors ligne, vous devez utiliser une copie du fichier **sdconf.rec** d'un serveur Authentication Manager qui autorise l'inscription automatique et effectue l'authentification. (Le service d'authentification doit être en cours d'exécution sur ce serveur.) Si vous n'utilisez qu'un serveur primaire pour la gestion des bases de données, n'utilisez pas le fichier **sdconf.rec** à partir de ce serveur primaire. À la place, utilisez un fichier **sdconf.rec** à partir d'un serveur de réplica. Pour plus d'informations sur l'utilitaire d'inscription automatique, reportez-vous à « Processus d'inscription automatique » à la page 63.

- Si vous souhaitez utiliser une méthode plus sécurisée pour établir un secret de nœud entre Authentication Manager et l'ordinateur agent, vous pouvez utiliser l'utilitaire de chargement du secret de nœud fourni avec l'agent d'authentification. Cet utilitaire vous permet de copier le secret de nœud à partir d'Authentication Manager et de le charger sur l'ordinateur d'agent d'authentification approprié avant que les utilisateurs ne commencent à utiliser l'authentification RSA SecurID. Ainsi, vous n'aurez pas besoin d'attendre la première authentification pour établir le secret de nœud. Pour plus d'informations, consultez « Utiliser l'utilitaire de chargement du secret de nœud », à la page 46.

Installer le produit sur un seul ordinateur

Pour installer RSA Authentication Agent sur un ou plusieurs ordinateurs, suivez les étapes décrites dans cette section. Pour installer l'agent d'authentification sur plusieurs ordinateurs, reportez-vous à « Installer le produit sur plusieurs ordinateurs » à la page 36.

Remarque : Si vous avez installé Windows Server 2012 en mode Server Core, vous n'utilisez pas d'interface utilisateur. Vous devez installer l'agent d'authentification à partir de la ligne de commande. Pour plus d'informations, consultez « Installer le produit sur plusieurs ordinateurs », à la page 36.

Avant de commencer

Passez en revue les éléments suivants avant d'installer le produit :

- L'agent d'authentification est disponible sous la forme d'un fichier. zip que vous devez télécharger à partir de RSA Link à l'adresse **https://community.rsa.com**.
- L'agent d'authentification requiert le certificat racine de confiance *VeriSign Universal Root Certification Authority*. Ce certificat est automatiquement provisionné sur les systèmes d'exploitation Windows, à condition que l'appareil dispose d'un accès Internet. Sur les appareils qui n'ont pas accès à Internet, vous devez utiliser le mécanisme de mise à jour racine Microsoft approprié afin d'installer le certificat dans le magasin d'autorités de certification racine de confiance du compte d'ordinateur. Pour savoir comment procéder, consultez **l'article 931125 de la base de connaissances Microsoft**.
- Avant de commencer l'installation de l'agent d'authentification, contactez votre administrateur Authentication Manager pour obtenir les fichiers **sdconf.rec** et **server.cer** (si vous prévoyez d'installer l'utilitaire d'inscription automatique). Copiez les deux fichiers sur l'ordinateur local ou contactez l'administrateur Authentication Manager pour connaître leur emplacement au sein du répertoire. Pour plus d'informations, consultez « Importer les fichiers Authentication Manager », à la page 31.

Pour installer l'agent d'authentification sur un ordinateur unique :

1. Connectez-vous à l'ordinateur en tant qu'administrateur (ou installez avec les privilèges d'administration).
2. Double-cliquez sur **RSA Authentication Agent.msi** pour lancer l'assistant d'installation.
3. Cliquez sur **Suivant** pour passer à l'étape suivante de la boîte de dialogue d'accueil.
4. Lisez le contrat de licence ou cliquez sur **Imprimer** pour l'imprimer. Sélectionnez **J'accepte les conditions du contrat de licence** et cliquez sur **Suivant**.
5. Exécutez l'une des opérations suivantes :
   - Pour installer uniquement RSA Authentication Agent sans l'utilitaire d'inscription automatique ou l'authentificateur RSA SecurID Connected, sélectionnez **Standard**, puis cliquez sur **Suivant**.

- Pour installer RSA Authentication Agent ainsi que des fonctions supplémentaires telles que l'utilitaire d'inscription automatique et les fonctions de RSA SecurID Connected Authenticator, sélectionnez **Personnalisé**. Cliquez sur **Suivant** pour ouvrir la boîte de dialogue Configuration personnalisée :
  - Sélectionnez la flèche déroulante située en regard d'**Utilitaire d'inscription automatique**. Sélectionnez l'option de votre choix dans la liste déroulante.
  - Sélectionnez la flèche déroulante située en regard d'**Authentificateur connecté**. Sélectionnez l'option de votre choix dans la liste déroulante.

6. Conservez le répertoire par défaut du dossier d'installation ou cliquez sur **Modifier** pour sélectionner un autre emplacement. Cliquez sur **Suivant**.
7. Cliquez sur **Parcourir** pour rechercher et ouvrir le fichier de configuration système (**sdconf.rec**). Cliquez sur **Suivant**. (Vous devez obtenir le fichier ou l'emplacement de ce fichier auprès de votre administrateur RSA Authentication Manager.)
8. Conservez l'emplacement par défaut du dossier de données hors ligne ou cliquez sur **Modifier** pour accéder à un autre emplacement. Cliquez sur **Suivant**.
9. Si vous avez sélectionné l'utilitaire d'inscription automatique, cliquez sur **Parcourir** pour rechercher et ouvrir le fichier de certificat de serveur (**server.cer**), puis cliquez sur **Suivant**. Vous devez obtenir le fichier ou l'emplacement de ce fichier auprès de votre administrateur RSA Authentication Manager.
10. Si vous souhaitez que tous les utilisateurs qui ne sont pas des administrateurs puissent se connecter à l'ordinateur de bureau avec l'authentification RSA SecurID, sélectionnez **Authentifier tous les utilisateurs à l'exception des administrateurs**. Les administrateurs locaux peuvent se connecter à l'aide de leur méthode Windows (mot de passe ou carte à puce). Cliquez sur **Suivant**.
11. Cliquez sur **Installer**. L'agent d'authentification est installé sur l'ordinateur local. Windows vous invite à autoriser les privilèges de contrôle de compte si vous les avez configurés. Cliquez sur **Autoriser**.
12. Cliquez sur **Terminer**.

Étapes suivantes

- Pour utiliser une méthode sécurisée d'établissement d'un secret de nœud entre l'ordinateur de l'agent d'authentification et le serveur Authentication Manager, utilisez l'utilitaire de chargement du secret de nœud fourni avec le kit RSA Authentication Agent 7.4 for Microsoft Windows. Utilisez cet utilitaire afin que les utilisateurs puissent s'authentifier à l'aide des codes d'accès RSA SecurID. Pour plus d'informations, consultez « Utiliser l'utilitaire de chargement du secret de nœud », à la page 46.
- Pour tester l'installation sur un ordinateur local, reportez-vous à « Tester l'installation » à la page 41.
- Pour afficher le produit dans une langue autre que l'anglais, vous pouvez installer un pack de langue après l'installation du produit standard. Pour plus d'informations, consultez « Installer un pack de langue », à la page 44.
- Pour les ordinateurs que vous souhaitez protéger avec un agent d'authentification et qui ne font pas partie de votre domaine ou qui ne sont pas soumis à une stratégie de groupe, vous devez configurer les paramètres de modèle à l'aide de l'éditeur d'objet de stratégie de groupe local. Pour plus d'informations, consultez le guide de modèle d'objet de stratégie de groupe.

Installer le produit sur plusieurs ordinateurs

Pour installer RSA Authentication Agent pour Microsoft Windows sur plusieurs ordinateurs en même temps, procédez comme suit :

1. Vérifiez ou personnalisez les options de l'agent d'authentification à l'aide de l'assistant de configuration de l'agent d'authentification pour créer un module d'installation (fichier MSI).
2. Fournissez les privilèges de contrôle de compte appropriés aux ordinateurs des utilisateurs pour permettre l'installation.
3. Déployez le module d'installation Par exemple, vous pouvez utiliser Microsoft Systems Management Server (SMS) ou un autre produit tiers, comme Tivoli. Ou bien, vous pouvez utiliser la ligne de commande.
4. Déployez le pack de langue si les utilisateurs ont besoin d'afficher le produit dans une langue autre que l'anglais et s'ils utilisent le système d'exploitation dans une autre langue.

Les sections suivantes expliquent comment effectuer ces tâches dans l'ordre indiqué.

Créer un module d'installation

L'assistant de configuration **ConfigWizard.exe**, vous permet de configurer rapidement les paramètres de l'agent d'authentification afin de déployer un module d'installation personnalisé sur plusieurs ordinateurs.

Avant de commencer

- Déterminez si vous avez besoin de créer plusieurs modules d'installation. Par exemple, vous pouvez configurer un module pour les utilisateurs de systèmes d'exploitation 32 ou 64 bits, et configurer un module pour les utilisateurs de systèmes d'exploitation 32 ou 64 bits afin d'utiliser des authentificateurs RSA SecurID 800.
- L'agent d'authentification est disponible sous la forme d'un fichier. zip que vous devez télécharger à partir de RSA Link à l'adresse **https://community.rsa.com**. Avant l'installation, vous devez télécharger le fichier.zip et extraire le fichier **RSA Authentication Agent.zip** ou **RSA Authentication Agent x64.zip** en fonction du module d'installation que vous avez créé (32 ou 64 bits).
- L'agent d'authentification requiert le certificat racine de confiance *VeriSign Universal Root Certification Authority*. Ce certificat est automatiquement provisionné, à condition que l'appareil dispose d'un accès à Internet. Sur les appareils qui n'ont pas accès à Internet, vous devez utiliser le mécanisme de mise à jour racine Microsoft approprié afin d'installer le certificat dans le magasin d'autorités de certification racine de confiance du compte d'ordinateur. Pour savoir comment procéder, consultez **l'article 931125 de la base de connaissances Microsoft**.

- Avant de commencer l'installation de l'agent d'authentification, contactez votre administrateur Authentification Manager pour obtenir les fichiers **sdconf.rec** et **server.cer** si vous prévoyez d'installer l'utilitaire d'inscription automatique. Copiez les deux fichiers sur l'ordinateur local ou contactez l'administrateur Authentication Manager pour connaître leur emplacement au sein du répertoire. Pour plus d'informations sur l'obtention de ces fichiers, reportez-vous à « Importer les fichiers Authentication Manager » à la page 31.

Pour créer un module d'installation RSA Authentication Agent personnalisé à l'aide de l'assistant de configuration, procédez comme suit :

1. Pour démarrer l'assistant de création de l'installation de RSA Authentication Agent, ouvrez le dossier de l'assistant de configuration, puis double-cliquez sur **ConfigWizard.exe**.
2. Cliquez sur **Parcourir** pour rechercher le fichier **RSA Authentication Agent.msi** ou **RSA Authentication Agent x64.msi**. Cliquez sur **Suivant**.
3. Cliquez sur **Parcourir** pour importer le fichier de configuration système (**sdconf.rec**) qui identifie le serveur Authentication Manager que vous souhaitez utiliser. Vous devez obtenir le fichier de configuration système auprès de votre administrateur Authentication Manager. Cliquez sur **Suivant**.
4. Sélectionnez **Activer l'utilitaire d'inscription automatique** pour inscrire automatiquement l'ordinateur des utilisateurs dans la base de données d'Authentication Manager lorsque les utilisateurs démarrent leur ordinateur pour la première fois après l'installation de l'agent d'authentification.
5. Si vous activez l'inscription automatique, conservez le fichier de certificat du serveur dans son emplacement par défaut (**server.cer**) ou cliquez sur **Parcourir** pour le rechercher, puis sur **Suivant**. Vous pouvez obtenir ce certificat de fichier auprès de l'administrateur d'Authentication Manager.
6. Si vous souhaitez autoriser les utilisateurs à se connecter à l'aide d'un authentificateur RSA SecurID 800 connecté au port USB pour que l'agent puisse accéder automatiquement au code de token, sélectionnez **Activer l'authentificateur connecté RSA SecurID**. Dans le cas contraire, ne sélectionnez pas la valeur par défaut. Cliquez sur **Suivant**.
7. Si vous souhaitez que tous les utilisateurs s'authentifient avec un code d'accès RSA SecurID afin de se connecter à l'ordinateur, à l'exception des utilisateurs appartenant au groupe d'administrateurs, sélectionnez **Activer l'authentification, sauf pour le groupe d'administrateurs**. Dans le cas contraire, ne sélectionnez pas la valeur par défaut. Cliquez sur **Suivant**.

   Important : Sélectionnez cette option uniquement si tous les utilisateurs appropriés disposent de leur authentificateurs RSA SecurID et savent comment se connecter à l'aide d'un code d'accès. Si tel n'est pas le cas, ils pourront toujours se connecter à leurs ordinateurs s'ils n'appartiennent pas à un groupe d'authentification ou s'ils peuvent accéder à l'option Fournisseur d'informations d'identification de mots de passe Microsoft. Pour plus d'informations sur la définition des options de connexion, reportez-vous au *guide de modèle d'objet de stratégie de groupe*.

8. Passez en revue vos sélections Par exemple, vous pouvez utiliser la barre de défilement pour vérifier les éléments suivants :
   - Chemin d'accès du fichier de configuration système (**sdconf.rec**)
   - État de l'utilitaire d'inscription automatique (activé ou désactivé) et chemin d'accès du fichier de certificat de serveur (**server.cer**)
   - État de l'authentificateur connecté pour utiliser un authentificateur RSA SecurID 800 dans un port USB, afin que l'agent puisse accéder automatiquement au code de token (activé ou désactivé)
   - État de l'authentification (activé ou désactivé)
9. Pour modifier les paramètres, cliquez sur la flèche vers la gauche (<) et effectuez les modifications nécessaires. Cliquez sur **Terminer** lorsque vous avez terminé.
10. Saisissez un nom pour le fichier du module d'installation.

    Veillez à attribuer à ce fichier un nom unique pour le différencier des autres modules d'installation que vous pourriez créer.
11. Si nécessaire, accédez à l'emplacement où vous souhaitez enregistrer le fichier du module d'installation. Cliquez ensuite sur **Save**.
12. Cliquez sur **OK** pour enregistrer ces paramètres et fermer l'assistant.

Étapes suivantes

- Pour installer un pack de langue afin de convertir l'interface et la documentation de l'agent d'authentification dans une langue autre que l'anglais, reportez-vous à « Installer un pack de langue » à la page 44.
- Pour utiliser une méthode plus sécurisée d'établissement d'un secret de nœud entre l'ordinateur de l'agent d'authentification et le serveur Authentication Manager, utilisez l'utilitaire de chargement du secret de nœud fourni avec le kit RSA Authentication Agent 7.4 for Microsoft Windows. Utilisez cet utilitaire afin que les utilisateurs puissent s'authentifier à l'aide des codes d'accès RSA SecurID. Pour plus d'informations, consultez « Utiliser l'utilitaire de chargement du secret de nœud », à la page 46.
- Pour modifier les paramètres de l'installation après l'avoir déployée, vous pouvez répéter les étapes de cette section afin de créer un autre package et le déployer. Les nouveaux paramètres remplacent les paramètres précédents. Pour plus d'informations, consultez « Modifier une installation », à la page 47. Ou bien, vous pouvez définir les paramètres à l'aide des modèles d'objet de stratégie de groupe, en fonction du nombre d'ordinateurs nécessitant des modifications. Vous pouvez également définir certains paramètres sur un ordinateur local via Control Center. Pour plus d'informations, reportez-vous à l'aide de RSA Authentication Agent (RSA SecurID).

Les paramètres suivants qui figuraient dans les versions précédentes de l'assistant de configuration sont désormais des stratégies configurées par les modèles d'objet de stratégie de groupe. Pour en savoir plus sur ces paramètres, consultez *Group Policy Object Template Guide* :

- Définir l'invite de connexion pour utiliser un code d'accès ou un mot de passe
- Définir le code PIN RSA SecurID pour permettre aux utilisateurs de déverrouiller les ordinateurs à l'aide d'un code PIN au lieu d'un code d'accès complet
- Définir le fournisseur d'informations d'identification et le filtrage tiers

Fournir des privilèges de contrôle de compte aux ordinateurs des utilisateurs

Les administrateurs peuvent installer l'agent d'authentification sur tous les ordinateurs d'un domaine. Les utilisateurs qui sont membres du groupe administrateurs peuvent installer l'agent d'authentification sur leurs propres ordinateurs. Si vous souhaitez que l'agent d'authentification soit installé sur les ordinateurs des utilisateurs, vous devez définir les stratégies appropriées afin de vous assurer qu'il peut être installé sur tous les ordinateurs appropriés. Par exemple, l'agent d'authentification doit accéder aux clés de registre Windows. Les utilisateurs ne disposent pas des privilèges nécessaires pour afficher ou modifier le registre. Vous devez donc déployer le logiciel en tant qu'application gérée.

Une application gérée utilise des privilèges élevés pour installer l'application et apporter les modifications nécessaires aux clés de registre. Cela garantit que les utilisateurs peuvent installer le logiciel sur leur ordinateur.

Pour accorder des privilèges aux ordinateurs utilisateur, procédez comme suit :

Utilisez les outils suivants pour contrôler les privilèges :

- Microsoft Management Console (MMC) 3.0
- Utilisez la stratégie de groupe pour contrôler l'utilisation de la console MMC Pour en savoir plus sur la stratégie de groupe, consultez **Utiliser la stratégie de groupe pour contrôler l'utilisation de la console MMC 3.0** sur le site Web de Microsoft

Remarque : Avoir des privilèges élevés sur l'ordinateur permet d'installer RSA Authentication Agent pour Microsoft Windows, et permet à un utilisateur disposant de privilèges élevés de le supprimer. Les utilisateurs standard peuvent utiliser l'option **Réparer** pour réparer l'installation, si nécessaire.

Déployer le module d'installation sur plusieurs ordinateurs

Une fois que vous avez créé un module d'installation, comme décrit à la section « Créer un module d'installation » à la page 36, et que vous avez défini les privilèges du compte sur les groupes nécessaires, vous pouvez déployer l'agent d'authentification. Si vous souhaitez tester l'installation sur un ordinateur local après l'avoir déployée, reportez à « Tester l'installation » à la page 41.

Important : Si vous avez précédemment déployé RSA Authentication Agent 7.4 et que vous déployez ultérieurement un autre module d'installation RSA Authentication Agent 7.4, toutes les modifications que vous avez effectuées via l'assistant de configuration remplaceront les paramètres précédents. Avant de déployer un fichier MSI, assurez-vous que tous les paramètres incluent les options souhaitées.

Pour déployer le module d'installation sur plusieurs ordinateurs, procédez comme suit :

Choisissez l'une des méthodes suivantes :

- Microsoft Systems Management Server (SMS) ou un autre produit tiers, tel que Tivoli
- Installation à partir de la ligne de commande
- Installation silencieuse à partir de la ligne de commande msiexec

Remarque : Assurez-vous que RSA Authentication Manager est installé avant de déployer l'agent d'authentification. Pour plus d'informations sur l'installation d'Authentication Manager, reportez-vous au *guide d'installation et de configuration de RSA Authentication Manager* correspondant à votre version.

Choisissez le déploiement SMS uniquement si vous êtes familiarisé avec les opérations SMS, telles que l'ajout de points de distribution et de programmes et la création de publicités. Pour plus d'informations sur SMS, consultez le **site Web de Microsoft Systems Management Server**.

Installation silencieuse

Pour effectuer une installation silencieuse à partir de la ligne de commande msiexec, utilisez l'option /qn. Une fois l'installation terminée, le programme d'installation redémarre l'ordinateur chaque fois que nécessaire, sans afficher d'invite ni d'avertissement à l'utilisateur.

Remarque : Vous pouvez effectuer une installation silencieuse uniquement sur les fichiers MSI que vous avez créés à l'aide de l'assistant de configuration.

Pour installer à partir de la ligne de commande msiexec, procédez comme suit :

1. Cliquez sur l'invite de commande de l'icône avec le bouton droit de la souris à partir du menu **Démarrer**, puis cliquez sur **Exécuter en tant qu'administrateur** pour ouvrir l'invite de commande.
2. Accédez au répertoire qui contient le fichier de package **RSA Authentication Agent.msi** (ou un fichier MSI d'agent d'authentification renommé). Dans le cas contraire, vous devrez fournir le chemin d'accès complet au fichier du package sur la ligne de commande.
3. Saisissez une commande similaire à la suivante, en fonction du nom de votre package MSI :

   msiexec /qn /i "RSA Authentication Agent.msi"

Pour consigner les erreurs, ajoutez l'option **/lv** (log verbose) à la fin de la commande. Le produit réalise l'installation et le système redémarre automatiquement.

Tester l'installation

Avant de déployer le produit dans votre organisation, vous devez le tester sur un ordinateur local. Effectuez les tâches décrites dans le tableau suivant pour tester l'installation.

Tâche	Référence
Afficher l'état de l'environnement de serveur.	« Vérifier les paramètres du serveur », à la page 41
Tester l'authentification.	« Tester l'authentication », à la page 42

Si l'exécution réussit, vous pouvez déployer le produit sur plusieurs utilisateurs, comme décrit à la section « Déployer le module d'installation sur plusieurs ordinateurs » de la page 40.

Vérifier les paramètres du serveur

Vérifiez les paramètres du serveur en affichant des informations sur RSA Authentication Manager dans RSA Control Center pour vous assurer que l'environnement du serveur est configuré correctement. Pour plus d'informations sur les paramètres du serveur, reportez-vous à l'aide de RSA Authentication Agent (RSA SecurID).

Pour passer en revue les paramètres du serveur, procédez comme suit :

1. Connectez-vous à un ordinateur doté de l'agent d'authentification à l'aide d'un compte administrateur ou exécutez le système en tant qu'administrateur.
2. Cliquez **Démarrer** > **RSA** > **RSA Control Center** pour ouvrir RSA Control Center.
3. Sous **Paramètres d'application**, cliquez sur **Environnement du serveur**.
4. Passez en revue les limites de RSA Authentication Manager, et les informations statiques et dynamiques.
5. (Facultatif) Cliquez sur le menu déroulant **Nom du serveur** pour afficher des informations sur les autres serveurs.

Tester l'authentication

Il est important de tester l'authentification, car, en plus de vérifier l'environnement du serveur, celle-ci crée un secret de nœud pour l'agent d'authentification et le stocke dans la base de données RSA Authentication Manager.

Important : Si vous souhaitez utiliser une méthode plus sécurisée pour établir un secret de nœud entre l'ordinateur de l'agent d'authentification et le serveur Authentication Manager, utilisez l'utilitaire de chargement du secret de nœud fourni avec le kit RSA Authentication Agent 7.4 for Microsoft Windows. Si vous créez le secret de nœud avant l'authentification des utilisateurs, vous pouvez utiliser l'authentification chiffrée immédiatement au lieu d'attendre la première utilisation. Pour plus d'informations, consultez « Utiliser l'utilitaire de chargement du secret de nœud », à la page 46.

Secret de nœud

Le secret de nœud est une clé de chiffrement symétrique qui est utilisée par RSA Authentication Manager et RSA Authentication Agent pour chiffrer et déchiffrer les paquets de données circulant sur le réseau. La première fois qu'un utilisateur réussit à s'authentifier ou teste l'authentification d'un hôte d'agent, RSA Authentication Manager crée un secret de nœud pour cet hôte d'agent et le stocke dans la base de données RSA Authentication Manager. Une copie du secret de nœud est chiffrée et envoyée à l'agent d'authentification. Le secret de nœud n'est pas stocké sur l'agent.

Si le secret de nœud sur l'hôte de l'agent d'authentification est corrompu ou ne correspond pas au secret de nœud présent dans la base de données de RSA Authentication Manager, les communications chiffrées entre l'agent d'authentification et Authentication Manager ne pourront pas fonctionner. Si cela se produit, Authentication Manager consigne le message d'échec de la vérification du nœud dans le moniteur d'activité de RSA Authentication Manager. Pour plus d'informations sur le test de l'authentification ou sur la suppression du secret de nœud, reportez-vous à l'aide de RSA Authentication. Pour plus d'informations sur la façon dont Authentication Manager consigne les échecs de vérification de nœuds, consultez le *guide d'administration de RSA Authentication Manager*.

Pour tester l'authentification à l'aide d'un authentificateur RSA SecurID, procédez comme suit :

1. Connectez-vous à un ordinateur avec l'agent d'authentification à l'aide d'un compte d'administrateur (ou exécutez le système en tant qu'administrateur).
2. Cliquez sur **Démarrer** > **RSA** > **RSA Control Center** pour ouvrir RSA Control Center.
3. Sous **Gérer les outils avancés**, cliquez sur **Outils avancés**.
4. Cliquez sur **Tester l'authentication**.

5. Dans le champ **Choisir l'authentificateur**, procédez de l'une des façons suivantes :
   - Si vous disposez d'un authentificateur portatif (un authentificateur qui n'est pas inséré dans un port USB), conservez la valeur par défaut du champ **Token portatif**.
   - Si vous disposez d'un authentificateur RSA SecurID 800 inséré dans le port USB, conservez le numéro de série par défaut ou le nom de l'authentificateur dans le champ.
   - Si plusieurs authentificateurs RSA SecurID 800 sont insérés dans les ports USB, conservez le numéro de série ou le nom actuel de l'authentificateur dans le champ ou sélectionnez-en un autre dans la liste déroulante.
6. Dans le champ **Nom d'utilisateur**, conservez le nom d'utilisateur actuel ou remplacez-le.
7. Dans le champ **Code d'accès** ou **Code PIN SecurID**, effectuez l'une des opérations suivantes :
   - Si vous utilisez un authentificateur portatif sans code RSA PIN SecurID défini, saisissez le code de token indiqué sur la face avant de l'authentificateur. Cliquez sur **OK**. La boîte de dialogue Set New RSA SecurID PIN s'ouvre. Passez à l'étape 8.
   - Si vous utilisez un authentificateur RSA SecurID 800 sans code PIN RSA SecurID défini, laissez le champ vide. Cliquez sur **OK**. La boîte de dialogue Set New RSA SecurID PIN s'ouvre. Passez à l'étape 8.
   - Si vous utilisez un authentificateur portatif doté d'un code PIN RSA SecurID défini, entrez le code d'accès (code PIN suivi du code de token indiqué sur la face avant de l'authentificateur). Cliquez sur **OK**. Passez à l'étape 10 (si nécessaire).
   - Si vous utilisez un authentificateur RSA SecurID 800 doté d'un code PIN RSA SecurID défini, entrez le code PIN. Cliquez sur **OK**. (L'agent d'authentification accède automatiquement au code de token à partir de l'authentificateur.) Passez à l'étape 10 (si nécessaire).
8. Si vous devez générer ou créer un code PIN RSA SecurID, procédez de l'une des façons suivantes :
   - Pour générer votre code PIN, sélectionnez **Générer mon code PIN SecurID**. Cliquez sur **OK**. Le système vous invite à mémoriser votre code PIN. Cliquez sur **Oui** pour le mémoriser en moins de 10 secondes. Ne l'écrivez pas. Cliquez sur **OK**.
   - Pour créer votre code PIN, sélectionnez **Créer mon propre code PIN SecurID**. Dans le champ **Code PIN SecurID**, saisissez un code PIN. Saisissez-le à nouveau dans le champ **Confirmer le code PIN SecurID**. Cliquez sur **OK**.

   Remarque : Les options disponibles dépendent des paramètres de RSA Authentication Manager. Il est possible qu'une seule option soit disponible.

9. Si vous venez de recevoir un code PIN généré par le système ou si vous en avez créé un, procédez de l'une des façons suivantes :
   - Si vous utilisez un authentificateur portatif, attendez que votre token soit modifié, puis saisissez votre code PIN et votre code de token dans le champ **Code d'accès**. Cliquez sur **OK**.
   - Si vous utilisez un token USB, un message s'affiche pour attendre que RSA Authentication Agent accède au code de token suivant. Vous n'avez pas besoin de saisir de code PIN.
10. Si vous êtes invité(e) à saisir le code de token suivant afin de confirmer votre possession du token et de le synchroniser avec RSA Authentication Manager, procédez de l'une des façons suivantes :
    - Si vous utilisez un authentificateur de poche, attendez que votre token soit modifié. Saisissez le code de token dans le champ **Code de token suivant**, puis cliquez sur **OK**.
    - Si vous utilisez un authentificateur USB, un message s'affiche pour attendre que RSA Authentication Agent accède au code de token suivant. Vous n'avez pas besoin de saisir de code PIN.

Une fois l'authentification réussie, un message de réussite s'affiche. Si vous ne parvenez pas à vous authentifier, vous devrez peut-être vérifier les paramètres de RSA Authentication Manager. Consultez le *guide d'administration de RSA Authentication Manager*.

Installer un pack de langue

Si vous avez installé RSA Authentication Agent pour Microsoft Windows et que vous ne souhaitez pas l'afficher en anglais, vous pouvez installer un fichier de pack de langue pour l'afficher dans une autre langue. Les fichiers de pack de langue sont disponibles sur RSA Link.

L'ordinateur de bureau doit utiliser un système d'exploitation dans une langue autre que l'anglais, sans quoi le produit restera en anglais.

Avant de commencer

Vérifiez que les paramètres suivants sont appliqués sur l'ordinateur Windows ou Windows Server, si vous modifiez la langue par défaut du système. Les instructions peuvent varier selon la version du système d'exploitation. Les étapes suivantes s'appliquent à Windows 10.

- Désactivez la synchronisation de la langue si l'ordinateur est synchronisé avec d'autres ordinateurs dans une autre langue par défaut:
  - Dans Paramètres, cliquez sur **Comptes > Synchroniser vos paramètres**.
  - Désactivez les **Préférences de langue**.
- Lorsque vous installez le pack de langue du système d'exploitation, sélectionnez l'option **Définir comme langue d'affichage**.

- Vérifiez que les paramètres **Pays ou région** et **Format régional** appropriés sont appliqués. Copiez ensuite les paramètres de la langue d'administration sur l'ordinateur.
  - Dans Paramètres, cliquez sur **Heure & langue > Région**.
  - Dans Paramètres associés, cliquez sur **Paramètres de la langue d'administration**.
  - Sous l'onglet Administration, cliquez sur **Copier les paramètres**.
  - Dans Copier vos paramètres actuels dans, sélectionnez **Écran d'accueil et comptes système** et **Nouveaux comptes utilisateur**.

Pour installer un pack de langue sur un ordinateur unique, procédez comme suit :

1. Connectez-vous avec des privilèges élevés (un compte administrateur), puis double-cliquez sur le fichier MSI approprié.
2. Double-cliquez sur le fichier **RSA Authentication Agent <*language*> Language.msi**.
3. Redémarrez l'ordinateur lorsque vous y êtes invité pour effectuer l'installation.

Pour installer un pack de langue sur plusieurs ordinateurs, procédez comme suit :

Déployez le fichier **RSA Authentication Agent <*language*> Language.msi** à l'aide de la méthode de votre choix. Si vous utilisez la ligne de commande, saisissez le nom du fichier du pack de langue. Pour consigner toute erreur, utilisez l'option **/lv** (log verbose). Par exemple, saisissez la commande suivante pour procéder à une installation silencieuse du pack de langue :

msiexec /qn /i "RSA Authentication Agent <*language*> Language.msi"

Le système redémarre automatiquement les ordinateurs des utilisateurs pour effectuer l'installation.

Si vous souhaitez à nouveau afficher l'agent d'authentification en anglais, supprimez le pack de langue. Si vous supprimez l'agent d'authentification et que vous conservez la langue, les utilisateurs ne pourront plus accéder à leur ordinateur via l'agent d'authentification. Pour plus d'informations sur la suppression d'un pack de langue, reportez-vous à « Désinstaller le pack de langue » à la page 52.

Utiliser l'utilitaire de chargement du secret de nœud

Un secret de nœud unique est associé à chaque ordinateur d'agent d'authentification. Le secret de nœud permet à l'ordinateur de l'agent d'authentification RSA et au serveur RSA Authentification Manager d'utiliser des communications chiffrées au cours du processus d'authentification RSA SecurID. Pour assurer la sécurité de la transaction lors de la première tentative d'authentification d'un utilisateur à l'aide d'un code d'accès RSA SecurID, l'agent d'authentification et Authentication Manager communiquent automatiquement à l'aide d'une valeur de hachage du secret de nœud unique, qu'ils stockent sur l'ordinateur hébergeant l'agent. Toutes les opérations d'authentification ultérieures utilisent le secret de nœud pour chiffrer la communication entre les deux systèmes.

Si vous souhaitez utiliser une méthode plus sécurisée pour établir un secret de nœud entre l'ordinateur de l'agent d'authentification et le serveur Authentication Manager, utilisez l'utilitaire de chargement du secret de nœud (**agent_nsload.exe**) fourni avec le kit RSA Authentication Agent. Vous pouvez utiliser cet utilitaire pour copier le secret de nœud à partir d'Authentication Manager et le charger sur l'ordinateur de l'agent d'authentification avant que les utilisateurs ne commencent à s'authentifier à l'aide des codes d'accès RSA SecurID.

Utilisation de l'utilitaire de chargement du secret de nœud :

1. Recherchez le fichier de secret de nœud de l'hôte de l'agent sur le serveur RSA Authentication Manager approprié.

   Remarque : L'administrateur d'Authentication Manager crée un secret de nœud unique sur Authentication Manager. Pour plus d'informations, consultez la rubrique d'aide d'Authentification Manager/

2. Copiez le fichier de secret de nœud et l'utilitaire **agent_nsload.exe** dans le répertoire <<Program Files>>\RSA Shared\Auth API sur l'ordinateur de l'agent.
3. Ouvrez une invite de commande et accédez au répertoire <<Program Files>>\Common Files>>\RSA Shared\Auth API Saisissez :

   agent_nsload -f <*path*> -d "..\AuthData"

   <*path*> correspond à l'emplacement du répertoire et au nom du fichier de secret de nœud. Vous devrez saisir le mot de passe avec lequel le fichier de secret de nœud a été chiffré. L'utilitaire de chargement du secret de nœud charge le nouveau fichier de secret de nœud sur l'ordinateur de l'agent.
4. Répétez cette procédure pour chaque ordinateur nécessitant une protection supplémentaire par chiffrement lors de la première authentification RSA SecurID.

Modifier une installation

Si vous devez modifier les paramètres de RSA Authentication Agent pour Microsoft Windows, la méthode à employer dépendra du nombre d'ordinateurs nécessitant une modification. Pour un seul ordinateur, vous pouvez apporter des modifications à l'aide de la ligne de commande msiexec ou à partir du panneau de configuration. Pour plusieurs ordinateurs, vous devez utiliser la ligne de commande. Consultez les deux sections suivantes en fonction de vos besoins.

Remarque : Vous devez disposer des privilèges d'administration pour modifier le module d'installation et vous devez ouvrir l'invite de commande en tant qu'administrateur pour exécuter les commandes msiexec.

Modification de l'installation pour un seul ordinateur

Pour modifier l'installation d'un seul ordinateur, vous pouvez :

- Reconfigurer le package MSI
- Utiliser le panneau de configuration pour accéder à l'option **Modifier**.

Vous pouvez exécuter les commandes msiexec sur un ou plusieurs ordinateurs.

Pour modifier l'installation sur un seul ordinateur avec le package MSI :

1. Double-cliquez sur le fichier **ConfigWizard.exe** et accédez au package **RSA Authentication Agent.msi** que vous avez utilisé lors de l'installation initiale.
2. Apportez les modifications nécessaires, puis enregistrez le package avec le même nom que celui que vous avez utilisé à l'origine.
3. Ouvrez une invite de commande avec privilèges d'administration.
4. Utilisez une commande sensible à la casse similaire à l'exemple suivant pour réinstaller le programme.

   msiexec /qn /i "RSA Authentication Agent.msi" REINSTALL=ALL REINSTALLMODE=vomus

Remarque : Pour plus d'informations sur les modifications de l'installation à partir de la ligne de commande, y compris sur la suppression ou l'ajout d'une fonction, reportez-vous à « Modification de l'installation de plusieurs ordinateurs » à la page 48.

Pour modifier l'installation d'un seul ordinateur via le panneau de configuration, procédez comme suit :

1. Cliquez sur **Démarrer > Panneau de configuration**. Cliquez sur **Programmes**. Cliquez ensuite sur l'icône **Programmes et fonctionnalités**. Cliquez sur **RSA Authentication Agent**. Cliquez sur **Modifier** pour ouvrir l'assistant. Cliquez sur **Suivant** pour ouvrir la boîte de dialogue Maintenance du programme. Laissez l'option **Modifier** sélectionnée ou sélectionnez-la si nécessaire. Cliquez sur **Suivant**.
2. Cliquez sur la liste déroulante **Utilitaire d'inscription automatique de l'agent** Sélectionnez **Installer cette fonctionnalité sur le disque dur local**, **Installer cette fonctionnalité et toutes les sous-fonctions sur le disque dur local**, ou **Ne pas installer cette fonctionnalité**.
3. Cliquez sur la liste déroulante **Authentificateur connecté** et sélectionnez **Installer cette fonctionnalité sur le disque dur local**, **Installer cette fonctionnalité et toutes les sous-fonctions sur le disque dur local** ou **Ne pas installer cette fonctionnalité.**
4. Cliquez sur **Suivant**.
5. Désactivez ou sélectionnez l'option **Authentifier tous les utilisateurs à l'exception des administrateurs**. Si vous sélectionnez cette option, les utilisateurs devront se connecter à l'aide de l'authentification RSA SecurID. Les administrateurs locaux n'ont pas besoin de se connecter à l'aide de l'authentification RSA SecurID. Cliquez sur **Suivant**.
6. Cliquez sur **Installer**.
7. Lorsque vous êtes invité à redémarrer l'ordinateur, cliquez sur **Terminer**.

Modification de l'installation de plusieurs ordinateurs

Les procédures suivantes décrivent comment modifier les paramètres de configuration et les fonctionnalités des installations d'agent d'authentification à partir d'une invite de commande. Vous pouvez également utiliser ces procédures sur un seul ordinateur.

Modifier une installation existante

Modifiez les paramètres de configuration à l'aide de l'assistant de configuration, puis redéployez le package à l'aide de la commande suivante :

```
msiexec /qn /i « RSA Authentication Agent.msi » REINSTALLMODE=vomus
REINSTALL=ALL
```

Pour plus d'informations sur l'assistant de configuration, reportez-vous à « Créer un module d'installation » à la page 36.

Ajouter une fonction à une installation existante.

Pour ajouter une fonctionnalité à une installation existante, vous devez utiliser l'assistant de configuration pour créer un autre package MSI et exécuter une commande msiexec en tant qu'administrateur pour le déploiement du package. Par exemple, si vous n'avez pas activé l'utilitaire d'inscription automatique lors du premier déploiement de l'agent d'authentification, vous pouvez l'activer en créant un autre package MSI. Pour plus d'informations sur l'assistant de configuration, reportez-vous à « Créer un module d'installation » à la page 36. Après avoir créé le nouveau package MSI avec l'inscription automatique activée et avoir importé le fichier **server.cer**, déployez le package avec la commande suivante :

msiexec /qn /i « RSA Authentication Agent.msi » ADDLOCAL=ALL REINSTALLMODE=vomus REINSTALL=LAC

Supprimer une fonctionnalité d'une installation existante

Vous pouvez supprimer une fonctionnalité d'une installation sans créer d'autre package MSI. Toutefois, vous devez utiliser une commande msiexec différente pour supprimer la fonctionnalité. Utilisez les commandes ci-dessous pour supprimer l'inscription automatique, l'authentificateur connecté, ou les deux. Vous devez ouvrir une invite de commande en tant qu'administrateur pour exécuter ces commandes.

Pour supprimer l'inscription automatique :

msiexec /qn /i « RSA Authentication Agent.msi » REINSTALLMODE=vomus REMOVE=AutoReg_*x86 or 64*

Pour supprimer l'authentificateur connecté :

msiexec /qn /i « RSA Authentication Agent.msi » REINSTALLMODE=vomus REMOVE=SID_C_*x86 or 64*

Pour supprimer l'inscription automatique et l'authentificateur connecté :

msiexec /qn /i « RSA Authentication Agent.msi » REINSTALLMODE=vomus REMOVE=AutoReg_*x86 or 64*,SID_C_*x86 or 64*

Réparer une installation

La réparation d'une installation remplace les fichiers manquants dans une installation endommagée.

Remarque : Pour réparer une installation, vous devez vous connecter en tant qu'administrateur sur l'ordinateur où l'agent d'authentification est installé, mais vous n'avez pas besoin d'élever vos privilèges d'utilisateur Microsoft Windows.

Pour réparer une installation sur un ordinateur unique, procédez comme suit :

- Cliquez sur **Démarrer > Panneau de configuration**. Cliquez sur **Programmes**. Cliquez ensuite sur l'icône **Programmes et fonctionnalités**. Cliquez sur **RSA Authentication Agent**. A **Le** bouton Réparer s'affiche dans la barre de menus. Cliquez sur **Réparer**.

Remarque : Si vous double-cliquez sur le fichier MSI pour réparer l'installation, sélectionnez **Réparer** et cliquez sur **Suivant**. Cliquez ensuite sur **Installer** pour réparer l'installation. Cliquez sur **Terminer** lorsque vous avez terminé.

Mise à niveau vers RSA Authentication Manager 7.4

Pour effectuer une mise à niveau à partir d'une version précédente de RSA Authentication Agent vers RSA Authentication Agent 7.4, effectuez les tâches suivantes :

1. Si vous avez installé Authentication Agent 7.0 ou une version antérieure, prenez note des paramètres de votre version actuelle de l'agent d'authentification. L'agent d'authentification utilise désormais des modèles d'objet de stratégie de groupe (GPO) pour configurer ses paramètres de stratégie. Vous devrez mapper vos anciens paramètres aux nouveaux paramètres de stratégie GPO après l'installation de RSA Authentication Agent 7.4. (les versions Authentication Agent 7.1.x et 8.*x* conservent les paramètres de votre stratégie lors de la mise à jour vers une version ultérieure)
2. Si vous avez installé RSA Authentication Agent 5.x ou une version antérieure, supprimez-la, comme décrit dans la documentation qui l'accompagne.
3. Installez RSA Authentication Agent 7.4 en suivant la procédure décrite dans « Installer le produit sur un seul ordinateur » à la page 34 ou « Installer le produit sur plusieurs ordinateurs » à la page 36.
4. Mappez les paramètres de votre version précédente de RSA Authentication Agent que vous avez notés, aux nouveaux modèles d'objet de stratégie de groupe. Pour plus d'informations, reportez-vous au *guide de modèle d'objet de stratégie de groupe.*

Désinstallation du produit

Si vous avez besoin de supprimer RSA Authentication Agent 7.4, la méthode à employer dépendra du nombre d'ordinateurs sur lesquels vous devez supprimer ce programme. Si vous avez seulement besoin de supprimer l'agent d'authentification sur un ordinateur, vous pouvez utiliser la méthode pour un seul ordinateur. Si vous avez besoin de le supprimer sur plusieurs ordinateurs, vous pouvez utiliser la méthode décrite pour plusieurs ordinateurs.

Important : Vous devrez peut-être désactiver un paramètre de sécurité local pour supprimer correctement l'agent d'authentification de certains ordinateurs. Par exemple, vous pouvez installer l'agent d'authentification si la règle de sécurité locale possède le **Contrôle des comptes utilisateur (UAC)** : Le paramètre **Élever uniquement les fichiers exécutables qui sont signés et validés** est activé, mais Windows ne vous autorise pas à supprimer l'application.

Pour supprimer l'application si Windows ne vous permet pas de la supprimer :

1. Cliquez sur **Démarrer** > **Panneau de configuration** > **Outils d'administration** > **Stratégie de sécurité locale**.
2. Ouvrez le dossier **Stratégie de sécurité locale**.
3. Ouvrez ensuite le dossier **Options de sécurité**. Faites défiler l'écran vers le bas jusqu'au paramètre **Contrôle des comptes utilisateur (UAC) : Élever uniquement les fichiers exécutables qui sont signés et validés**.
4. Si ce paramètre est activé, cliquez avec le bouton droit de la souris et sélectionnez **Propriétés**.
5. Sous l'onglet **Paramètres de sécurité locaux**, sélectionnez **Désactivé**, puis cliquez sur **OK**. Vous pouvez maintenant supprimer l'application de l'ordinateur.

Désinstaller le produit à partir d'un seul ordinateur

Cette section explique comment désinstaller l'agent d'authentification d'un ordinateur. Si vous avez besoin de supprimer le produit sur plusieurs ordinateurs, consultez « Désinstaller le produit de plusieurs ordinateurs » à la page 52.

Pour désinstaller le produit d'un seul ordinateur, procédez comme suit :

1. Cliquez sur **Démarrer > Panneau de configuration > Programmes et fonctionnalités.**
2. Cliquez sur **RSA Authentication Agent pour Microsoft Windows**. Un bouton **Désinstaller** s'affiche dans la barre d'outils du menu.
3. Cliquez sur **Désinstaller**.
4. Procédez de l'une des manières suivantes (si vous y êtes invité) :
   - Si vous êtes connecté en tant qu'administrateur, cliquez sur **Autoriser** pour élever vos privilèges.
   - Si vous êtes connecté en tant qu'utilisateur, saisissez un nom d'utilisateur administrateur et un mot de passe pour élever vos privilèges et permettre au processus de désinstallation de se poursuivre.
5. Redémarrez l'ordinateur si vous y êtes invité. Si vous annulez le processus de désinstallation à un moment donné, l'application revient à son état précédent.

Remarque : Si vous avez installé un pack de langue et que vous souhaitez le supprimer, consultez « Désinstaller le pack de langue » à la page 52.

Désinstaller le produit de plusieurs ordinateurs

Pour supprimer un agent d'authentification sur plusieurs ordinateurs d'utilisateurs, utilisez une commande msiexec. Pour consigner les erreurs de suppression, utilisez l'option **/lv** (log verbose). Placez le fichier log, par exemple uninstall.log, dans un emplacement connu, comme %USERPROFILE%.

Vous pouvez saisir une commande similaire à la suivante avec l'option **/x** (REMOVE=ALL) (et l'option **/qn** pour le mode silencieux) et le chemin d'accès complet pour supprimer l'agent d'authentification. sur plusieurs ordinateurs sans intervention des utilisateurs :

```
msiexec /qn /x "RSA Authentication Agent.msi" /lv uninstall.log
```

Remarque : L'option **/lv** de la commande consigne toutes les erreurs. Exécutez la commande sur plusieurs ordinateurs à l'aide de Microsoft Systems Management Server (SMS) ou d'un autre produit tiers. Si vous avez installé un pack de langue et que vous souhaitez le supprimer, consultez « Désinstaller le pack de langue » à la page 52.

Désinstaller le pack de langue

Si vous avez installé un pack de langue pour afficher l'agent d'authentification dans une autre langue, vous pouvez le supprimer pour afficher le produit en anglais.

Remarque : Vous pouvez supprimer l'agent d'authentification ou le pack de langue dans n'importe quel ordre. Toutefois, si vous supprimez l'agent et laissez le pack de langue installé, les utilisateurs ne pourront plus se connecter via l'agent d'authentification. Si vous supprimez le pack de langue et laissez l'agent d'authentification, les utilisateurs verront l'agent d'authentification en anglais.

Pour supprimer le pack de langue d'un ordinateur unique :

1. Cliquez sur **Démarrer > Panneau de configuration > Programmes et fonctionnalités.**
2. Cliquez sur **RSA Authentication Agent pour Windows - <*name of language*> Langue**. Un bouton **Désinstaller** s'affiche dans la barre d'outils du menu.
3. Cliquez sur **Désinstaller**.
4. Procédez de l'une des manières suivantes (si vous y êtes invité) :
   - Si vous êtes connecté en tant qu'administrateur, cliquez sur **Autoriser** pour élever vos privilèges.
   - Si vous êtes connecté en tant qu'utilisateur, saisissez un nom d'utilisateur administrateur et un mot de passe pour élever vos privilèges et permettre au processus de désinstallation de se poursuivre.
5. Redémarrez l'ordinateur si vous y êtes invité.

Pour retirer le pack de langue de plusieurs ordinateurs en mode silencieux, saisissez la commande suivante :

```
msiexec /qn /x "RSA Authentication Agent <name of language> Language.msi"
```

Remarque : Déployez la commande sur plusieurs ordinateurs à l'aide de Microsoft Systems Management Server (SMS) ou d'un autre produit tiers.

4 Gérer les agents d'authentification

Authentification hors ligne

L'authentification hors ligne étend l'authentification RSA SecurID aux utilisateurs lorsque la connexion à RSA Authentication Manager n'est pas disponible (par exemple, lorsque les utilisateurs ne sont pas au bureau) Vous pouvez activer et désactiver l'authentification hors ligne et définir le nombre de jours en mode hors ligne que les utilisateurs reçoivent pour les agents d'authentification, les groupes d'utilisateurs ou à l'échelle du système via RSA Authentication Manager. Pour plus d'informations, consultez le *RSA Authentication Managerguide d'administration*.

Si l'authentification hors ligne est activée, Authentication Manager génère des données hors ligne (également appelées jours en mode hors ligne) et les télécharge sur l'hôte de l'agent d'authentification lorsque l'agent d'authentification se connecte à l'hôte. Les hôtes d'agent d'authentification commencent à recevoir les données hors ligne au cours de leur deuxième authentification connectée à Authentication Manager. Par exemple, si vous effectuez le test d'authentification comme décrit dans « Tester l'authentication » à la page 42, puis que vous vous authentifiez, Authentication Manager génère et télécharge les données hors ligne. L'utilisateur d'agent peut ainsi s'authentifier en mode hors ligne.

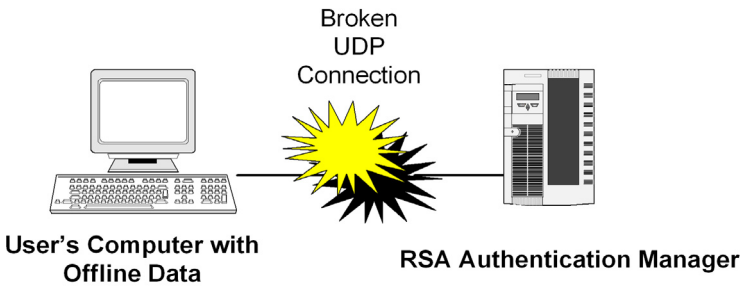
Par défaut, les données hors ligne se trouvent à l'emplacement suivant :

C:\ProgramData\RSA\RSA Authentication Agent\Local\dayfiles

Vous pouvez spécifier l'emplacement lors de l'installation. Si vous spécifiez un emplacement, les données hors ligne sont stockées dans ***specified_path*\RSA\RSA Authentication Agent\Local\dayfiles**.

Lorsqu'un utilisateur s'authentifie hors ligne, l'agent d'authentification vérifie les informations d'authentification de l'utilisateur par rapport aux données hors ligne stockées sur l'ordinateur de l'utilisateur. Si les informations d'authentification de l'utilisateur sont correctes, l'utilisateur peut accéder à l'ordinateur protégé.

Le schéma suivant illustre un scénario dans lequel l'ordinateur d'un utilisateur, qui n'est pas connecté à RSA Authentication Manager, peut utiliser les données hors ligne pour accéder à un ordinateur protégé.



Modifications du mot de passe et authentification hors ligne

Les utilisateurs qui modifient leur mot de passe en mode hors ligne peuvent toujours s'authentifier, même si le nouveau mot de passe ne correspond pas à celui de leur fichier de jours en mode hors ligne. Dans ce scénario, le système invite les utilisateurs à saisir leur nouveau mot de passe après avoir saisi leur code secret SecurID. Authentication Manager ne peut pas capturer ou stocker le nouveau mot de passe dans les fichiers des jours en mode hors ligne lorsque l'utilisateur travaille hors ligne. Authentication Manager peut synchroniser automatiquement les mots de passe et mettre à jour les fichiers de jours en mode hors ligne de l'utilisateur lorsque celui-ci travaille à nouveau en ligne.

Modifications de l'horloge et authentification hors ligne

L'authentification hors ligne surveille les modifications d'horloge et maintient un décalage d'horloge système entre l'horloge du PC et les données hors ligne. Les utilisateurs qui modifient leurs horloges PC lorsqu'ils sont hors ligne au lieu de modifier les fuseaux horaires ne peuvent pas s'authentifier. Par exemple, si vous travaillez généralement aux États-Unis et que vous effectuez un voyage au Japon, vous ne pouvez pas modifier votre horloge sur votre ordinateur à l'heure du Japon et vous authentifier hors ligne. Vos fichiers de jours en mode hors ligne continuent d'utiliser l'heure définie pour le fuseau horaire. Si cette heure ne correspondent pas au fuseau horaire approprié, vous ne pourrez pas vous authentifier. Modifiez le fuseau horaire de l'ordinateur au lieu de l'horloge. Vous pourrez ensuite utiliser vos fichiers de jours en mode hors ligne pour procéder à l'authentification hors ligne. Vous devez utiliser les privilèges d'administrateur pour modifier le fuseau horaire sur un ordinateur.

Gérer les jours en mode hors ligne

Cette section décrit la procédure d'actualisation des jours en mode hors ligne dans diverses circonstances et la vérification de l'offre de jours en mode hors ligne.

Pour qu'un utilisateur puisse utiliser des jours en mode hors ligne, l'administrateur RSA Authentication Manager définit les éléments suivants dans Authentication Manager :

- Agents d'authentification autorisés à utiliser l'authentification hors ligne
- Nombre de jours en mode hors ligne émis
- Nombre qui déclenche l'avertissement d'offre faible.

Pour plus d'informations sur les paramètres d'Authentification Manager, consultez le *RSA Authentication Managerguide de l'administrateur*.

Actualiser les jours en mode hors ligne

Les jours en mode hors ligne sont actualisés automatiquement lorsque l'utilisateur :

- S'authentifie directement sur le réseau.
- Établit une connexion en ligne après l'authentification hors ligne.

Même si l'utilisation des jours en mode hors ligne de l'utilisateur est saturée, les jours en mode hors ligne sont automatiquement mis à jour dans les cas suivants :

- L'utilisateur modifie le mot de passe Windows lors de l'authentification en ligne.
- Un administrateur publie une nouvelle stratégie sur l'agent d'authentification sur l'ordinateur de l'utilisateur, ce qui permet d'obtenir des codes d'accès d'urgence lorsque l'utilisateur est en ligne. Pour plus d'informations sur les codes d'urgence, consultez « Accès d'urgence » à la page 58.

Les jours en mode hors ligne ne sont pas actualisés automatiquement si la session d'authentification a expiré (l'utilisateur reste en ligne pendant 24 heures ou plus). Dans ce cas, l'utilisateur doit actualiser manuellement les jours en mode hors ligne. En outre, le fait de déverrouiller un ordinateur avec uniquement un code PIN RSA SecurID ne déclenche pas l'actualisation automatique.

Vous pouvez également configurer le nombre de jours de données hors ligne qu'un utilisateur est autorisé à télécharger. Il s'agit du nombre de jours équivalents aux codes de token téléchargés sur l'ordinateur de l'utilisateur. Cela est configuré dans la console de sécurité RSA sur le serveur RSA Authentication Manager, dans le cadre d'une stratégie d'authentification hors ligne.

Les sections suivantes décrivent les scénarios d'actualisation.

Actualisation lorsqu'une connexion réseau existe

L'agent d'authentification reconnaît qu'une connexion réseau existe et tente de télécharger des jours en mode hors ligne.

Actualisation en l'absence de connexion réseau

Lorsque l'utilisateur se connecte sans connexion au réseau, l'agent d'authentification tente de télécharger automatiquement les jours en mode hors ligne, mais il reconnaît qu'il n'existe aucune connexion réseau. Il affiche une alerte sur l'icône RSA Control Center pour avertir l'utilisateur que l'offre de jours en mode hors ligne est faible. L'utilisateur peut cliquer sur le message dans la zone de notification pour ouvrir RSA Control Center et actualiser les jours manuellement.

Remarque : Si l'icône RSA Control Center n'apparaît pas dans la zone de notification de la barre des tâches Windows, cliquez sur la flèche pour afficher les icônes masquées, cliquez sur Personnaliser, recherchez **l'icône de notification RSA Control Center** dans la boîte de dialogue Icônes de la zone de notification, puis Sélectionnez **Afficher les icônes et les notifications** dans la liste déroulante.

Pour actualiser les jours en mode hors ligne sans connexion réseau, l'utilisateur peut procéder comme suit :

1. Cliquer sur l'icône de RSA Control Center La boîte de dialogue Jours en mode hors ligne s'ouvre dans RSA Control Center.
2. Connectez-vous au réseau, puis cliquez sur **Actualiser** pour actualiser manuellement les jours en mode hors ligne.

   L'agent d'authentification procède de l'une des manières suivantes :

Description	Icône
Si la connexion au réseau réussit, le système télécharge automatiquement les jours en mode hors ligne et l'icône RSA Control Center revient à la normale.	
En cas d'échec de la connexion au réseau, le système informe l'utilisateur qu'un problème est survenu et invite l'utilisateur à réessayer ultérieurement. L'icône RSA Control Center reste dans l'état d'alerte et continue d'afficher le message de notification « Offre faible de jours en mode hors ligne » chaque fois que l'utilisateur se connecte.	

3. Cliquez sur **OK**.

Actualisation lorsque la session d'authentification a expiré

Si l'agent d'authentification tente de télécharger automatiquement des jours en mode hors ligne, mais reconnaît que la session d'authentification a expiré, l'agent d'authentification attribue à l'icône RSA Security Center l'état d'alerte pour indiquer que l'offre de jours en mode hors ligne est faible. (Par exemple, cela peut se produire lorsque l'utilisateur est connecté au réseau depuis plus de 24 heures.)

Pour actualiser les jours en mode hors ligne après l'expiration d'une session d'authentification, l'utilisateur peut :

1. Cliquer sur le message de notification à partir de l'icône RSA Control Center. La boîte de dialogue Jours en mode hors ligne s'ouvre dans RSA Control Center.
2. Cliquer sur **Actualiser**. L'agent d'authentification invite l'utilisateur à saisir un code d'accès.
3. Saisir ce code d'accès. L'agent d'authentification procède de l'une des manières suivantes :

Description	Notification Icône
Il télécharge les jours en mode hors ligne et définit l'icône RSA Control Center sur un état normal.	
Il informe l'utilisateur qu'un problème s'est produit et lui indique de réessayer plus tard. L'icône RSA Control Center reste dans l'état d'alerte.	

Vérifier l'offre de jours en mode hors ligne

Les utilisateurs peuvent vérifier leur offre de jours en mode hors ligne en examinant l'icône dans la zone de notification. L'état de l'icône indique l'état général de l'offre. Le tableau suivant décrit les icônes qui indiquent l'offre de jours en mode hors ligne.

Notification Icônes	Description
	Indique que l'offre de jours en mode hors ligne n'est pas inférieure à un nombre spécifié.
	Une icône d'avertissement s'affiche sur le trou de serrure pour vous avertir que le nombre de jours en mode hors ligne est inférieur à un nombre spécifique. Pour plus d'informations, consultez l'aide de RSA Authentication Agent (SecurID)

Effacer les données hors ligne

L'effacement des données hors ligne les supprime de l'agent. Sans données hors ligne, les utilisateurs ne peuvent pas accéder à la ressource protégée hors connexion réseau. Vous devez effacer les données hors ligne dans les circonstances suivantes :

- Vous avez modifié les paramètres hors ligne sur RSA Authentication Manager (par exemple, vous avez désactivé l'authentification hors ligne pour un agent ou vous avez modifié le nombre de jours en mode hors ligne que génère et télécharge Authentication Manager).
- Vous modifiez les propriétés de l'authentificateur d'un utilisateur (par exemple, vous effacez le code PIN de l'utilisateur ou synchronisez l'authentificateur de l'utilisateur).
- Vous souhaitez réattribuer un ordinateur protégé à un autre utilisateur.
- Vous désactivez l'authentificateur de l'utilisateur.
- Vous définissez l'état d'un token sur Perdu dans RSA Authentication Manager.

Une fois que vous avez supprimé les données hors ligne d'un agent, RSA Authentification Manager génère de nouvelles données en mode hors ligne et les télécharge sur l'agent à la prochaine authentification de l'ordinateur auprès de RSA Authentication Manager. Pour obtenir des instructions sur l'effacement des données hors ligne, reportez-vous à l'aide de RSA Authentication Agent (SecurID).

Accès d'urgence

Les utilisateurs hors ligne peuvent remplacer les codes d'accès d'urgence hors ligne par des codes d'accès en contactant l'administrateur du centre d'assistance SecurID Authentication Manager. L'administrateur du centre d'assistance fournit aux utilisateurs les codes d'accès d'urgence hors ligne dont ils ont besoin. Par exemple, si des utilisateurs hors ligne :

Oublient leur code PIN ou sont à cours de jours en mode hors ligne, ils peuvent s'authentifier à l'aide d'un code d'accès d'urgence hors ligne. Saisissent le code d'accès d'urgence hors ligne au lieu d'un code d'accès RSA SecurID.

Perdent leur token ou ne parviennent pas à se connecter ou à déverrouiller l'ordinateur en raison d'un nombre trop important de tentatives d'authentification infructueuses, ils peuvent s'authentifier avec un code de token d'accès d'urgence hors ligne. Les utilisateurs s'authentifient hors ligne au moyen du code de token d'accès d'urgence hors ligne et de leur code PIN RSA SecurID.

La première fois qu'un utilisateur tente de s'authentifier à l'aide d'un token après avoir effectué une authentification hors ligne à l'aide d'un code de token d'accès d'urgence hors ligne, Authentication Manager place l'authentificateur de l'utilisateur dans le mode « mot de passe temporaire de l'authentificateur perdu » (si possible)

Le mot de passe temporaire est le même que celui du code de token d'accès d'urgence hors ligne. Il peut avoir une date d'expiration définie par l'administrateur du centre d'assistance. Avant l'expiration du mot de passe, l'utilisateur doit contacter l'administrateur du centre d'assistance d'Authentication Manager pour remplacer l'authentificateur perdu par un nouveau ou rétablir l'authentificateur perdu à l'état « Non perdu ». Pour plus d'informations sur le mode de gestion des codes d'accès d'urgence par Authentication Manager, consultez le *guide d'administration de RSA Authentication Manager*.

Options d'accès d'urgence

Prévoyez la méthode d'authentification des utilisateurs lorsqu'ils perdent, égarent ou endommagent leurs tokens. Authentication Manager fournit les méthodes d'accès d'urgence SecurID suivantes pour les déploiements Windows.

Pour les utilisateurs en ligne :

- Code de token fixe temporaire. Pour les utilisateurs dont les ordinateurs sont en ligne sur le réseau. Ils peuvent accéder à leurs ordinateurs protégés sans code de token (par exemple, en cas de perte de leurs tokens).
- Code de token à usage unique Pour les utilisateurs dont les ordinateurs sont en ligne sur le réseau. Ils peuvent accéder à leurs ordinateurs protégés à l'aide d'un code de token, ne permettant qu'un seul accès.
- Code de token à la demande Pour les utilisateurs disposant d'appareils mobiles numériques et de comptes de messagerie personnels. Si cette option est activée, les utilisateurs peuvent recevoir des codes de token à usage ponctuel sous la forme de messages SMS.

Pour une utilisation hors ligne :

- Code de token d'accès d'urgence hors ligne. Pour les utilisateurs dont les ordinateurs ne sont pas connectés au réseau. Ils peuvent accéder à leurs ordinateurs protégés sans code de token (par exemple, en cas de perte de leurs tokens).
- Code d'accès d'urgence hors ligne Pour les utilisateurs dont les ordinateurs ne sont pas connectés au réseau. Ils peuvent accéder à leurs ordinateurs protégés sans code PIN (par exemple, en cas de perte de leur code PIN).

Mots de passe de réserve

La fonction de mot de passe de réserve est une méthode d'accès d'urgence qui permet à l'administrateur de s'authentifier auprès de l'ordinateur protégé par un utilisateur, sans avoir à saisir un code d'accès RSA SecurID, dans les circonstances suivantes :

- Le service d'authentification hors ligne n'est pas en cours d'exécution sur l'ordinateur local
- L'ordinateur ne peut pas se connecter à RSA Authentication Manager
- Aucun fichier de jours en mode hors ligne n'est disponible pour autoriser l'authentification hors ligne

Pour configurer un mot de passe de réserve, utilisez l'une des options d'agent d'authentification suivantes :

- Modèle d'objet de stratégie de groupe (GPO) des paramètres d'authentification locaux
- RSA Control Center

Si vous sélectionnez **Tous les utilisateurs** en tant qu'option d'authentification et que la connexion réseau échoue, personne, pas même un administrateur, ne peut accéder au bureau sur l'ordinateur protégé. C'est la raison pour laquelle RSA recommande vivement de définir un mot de passe de réserve ou d'utiliser une autre méthode d'accès d'urgence pour les administrateurs. (Pour plus d'informations sur les autres méthodes d'accès d'urgence, consultez « Choisir les méthodes d'accès d'urgence » à la page 26.)

Seul l'administrateur d'agent d'authentification connaît le mot de passe de réserve. Si un utilisateur a besoin de se connecter à l'ordinateur qui nécessite un mot de passe de réserve, l'utilisateur doit contacter l'administrateur approprié pour obtenir de l'aide.

Important : Le mot de passe de réserve est moins sûr que les autres méthodes d'accès d'urgence. Par exemple, il ne nécessite pas de code PIN SecurID et reste valide, sauf si un administrateur le modifie. Avec un mot de passe à usage unique, l'utilisateur doit inclure le code PIN SecurID et l'utilisateur ne peut l'utiliser qu'une seule fois.

Si la fonction de mot de passe de réserve est activée et que le système Windows ne parvient pas à communiquer avec RSA Authentication Manager lors de l'authentification, le système vous invite à saisir un mot de passe de réserve au lieu d'afficher un message indiquant qu'Authentication Manager est inaccessible. Les utilisateurs doivent également saisir un mot de passe Windows.

Pour plus d'informations sur la définition de l'option de mot de passe de réserve via le modèle d'objet de stratégie de groupe (GPO) des paramètres d'authentification locaux, consultez le *guide d'objet de stratégie de groupe.* Pour plus d'informations sur la définition du mot de passe de réserve via RSA Control Center, consultez l'aide de RSA Authentication Agent (SecurID).

Configuration de l'authentification hors ligne

Pour gérer les différents environnements de travail, vous pouvez définir différentes méthodes de déploiement de l'authentification hors ligne pour les utilisateurs qui travaillent à distance.

Utilisateurs travaillant en local et à distance

Si vous souhaitez configurer l'authentification hors ligne pour les utilisateurs qui travaillent à la fois au bureau et à distance, vous pouvez déployer l'authentification hors ligne pour ces utilisateurs en leur demandant d'effectuer une authentification initiale en ligne au bureau avant de mettre leurs ordinateurs hors ligne.

Pour configurer l'authentification hors ligne lorsque les utilisateurs distants sont au bureau :

1. Connectez l'ordinateur de l'utilisateur au réseau.
2. Ajoutez l'ordinateur de l'utilisateur au domaine (facultatif).
3. Demandez à l'utilisateur d'effectuer une authentification connectée à RSA Authentication Manager. (Si nécessaire, vous pouvez effectuer le test d'authentification décrit dans « Tester l'authentication » à la page 42.)
4. Si l'authentificateur de l'utilisateur est en mode Nouveau code PIN, demandez à l'utilisateur de s'authentifier une seconde fois, en utilisant le nouveau code PIN RSA SecurID. Si l'authentification réussit, le RSA Authentication Manager télécharge les données hors ligne vers l'ordinateur de l'utilisateur.
5. Vérifiez que les données hors ligne ont été téléchargées sur l'ordinateur de l'utilisateur. Pour cela, utilisez l'Explorateur Windows pour vérifier que les données hors ligne sont stockées sur l'ordinateur de l'utilisateur. Pour plus d'informations sur l'emplacement de stockage des données hors ligne, consultez « Authentification hors ligne » à la page 53. Les répertoires où sont stockées les données hors ligne sont masqués. Pour consulter les fichiers de données hors ligne, vous devez configurer l'Explorateur Windows de sorte qu'il affiche les fichiers masqués.

Utilisateurs distants partageant un même ordinateur

Si vous souhaitez configurer l'authentification hors ligne pour plusieurs utilisateurs partageant un même ordinateur afin qu'ils travaillent à distance, vous pouvez demander à ces utilisateurs de télécharger leurs données hors ligne à distance au lieu de demander à chaque utilisateur d'effectuer une authentification connectée et de télécharger les données d'authentification hors ligne au bureau.

Pour configurer un ordinateur partagé en vue de l'authentification hors ligne, procédez comme suit :

1. Créer un groupe d'authentification incluant les noms de tous les utilisateurs qui partagent l'ordinateur. Si vous avez besoin de créer de nouveaux groupes Windows, reportez-vous à la documentation Microsoft appropriée.
2. Définissez un mot de passe de réserve pour l'ordinateur.

   Pour plus d'informations, consultez l'aide de RSA Control Center (SecurID).
3. Spécifiez l'authentification pour le groupe que vous avez créé à l'aide du modèle d'objet de stratégie de groupe. Pour plus d'informations, reportez-vous à la *Group Policy Object Template Guide*.

4. Demandez à l'utilisateur distant de contacter l'administrateur afin d'obtenir le mot de passe de réserve, puis de se connecter à l'ordinateur. Lorsqu'un utilisateur tente d'accéder à l'ordinateur alors qu'il est hors ligne, ce dernier est d'abord invité à saisir le mot de passe de réserve, puis le mot de passe Windows.
5. Demandez à l'utilisateur de se connecter au réseau à distance.
6. Demandez à l'utilisateur de verrouiller l'ordinateur, puis de le déverrouiller en fournissant un code d'accès RSA SecurID lorsqu'il y est invité. Les données hors ligne seront alors téléchargées sur l'ordinateur de l'utilisateur. À ce stade, l'utilisateur doit fournir des codes d'accès RSA SecurID pour s'authentifier en local.
7. Répétez les étapes 5 et 6 pour chaque compte d'utilisateur partageant l'ordinateur.

Utilisateurs travaillant à distance uniquement

Vous pouvez déployer l'agent d'authentification et l'authentification hors ligne pour les utilisateurs distants qui ne peuvent pas se rendre à votre bureau, afin d'installer l'agent d'authentification et d'effectuer une authentification initiale en ligne. Étant donné que les utilisateurs sont ajoutés à la liste des authentifications hors ligne uniquement après le téléchargement de leur ensemble initial de jours en mode hors ligne, les utilisateurs distants peuvent accéder à leurs ordinateurs de bureau à l'aide de leurs mots de passe Windows, puis ouvrir une connexion à distance pour télécharger les jours en mode hors ligne. Une fois qu'un utilisateur télécharge un ensemble initial de jours en mode hors ligne, il est invité à spécifier des codes d'accès RSA SecurID sur toutes les authentifications ultérieures sur l'ordinateur de bureau.

Pour déployer l'authentification hors ligne pour les utilisateurs distants qui ne peuvent pas se rendre au bureau :

1. Demandez à l'utilisateur d'installer RSA Authentication Agent 7.4 à l'aide du fichier msi. Pour plus d'informations, consultez « Installer le produit sur un seul ordinateur », à la page 34.
2. Demandez à l'utilisateur de se connecter à l'ordinateur de bureau à l'aide d'un mot de passe Windows, puis de se connecter à distance au réseau.
3. Demandez à l'utilisateur de verrouiller l'ordinateur, puis de le déverrouiller en fournissant un code d'accès RSA SecurID lorsqu'il y est invité. Les données hors ligne seront alors téléchargées sur l'ordinateur de l'utilisateur.

Important : Les utilisateurs distants peuvent actualiser leurs données hors ligne à distance, mais ils doivent le faire avant l'expiration du dernier jour en mode hors ligne. Sinon, ils devront procéder à une authentification connectée pour télécharger davantage de jours en mode hors ligne. Les utilisateurs peuvent continuer d'actualiser leurs offres de jours en mode hors ligne jusqu'à ce que leurs authentificateurs RSA SecurID expirent.

Processus d'inscription automatique

Chaque ordinateur hébergeant RSA Authentication Agent doit disposer d'un enregistrement d'hôte d'agent correspondant dans la base de données de RSA Authentication Manager. Si l'utilitaire d'inscription automatique de l'hôte d'agent (**sdadmreg.exe**) est installé sur un nouvel ordinateur hôte de l'agent d'authentification, l'utilitaire inscrit l'ordinateur dans la base de données Authentication Manager, ce qui évite à l'administrateur de créer manuellement l'enregistrement d'hôte d'agent.

L'adresse IP d'un ordinateur client d'agent d'authentification permet à Authentication Manager d'identifier l'ordinateur lors de l'authentification. Si l'utilitaire d'inscription automatique est installé sur un ordinateur client de l'agent d'authentification, l'utilitaire inscrit automatiquement l'adresse IP de l'hôte d'agent dans la base de données Authentication Manager lors du premier démarrage de l'ordinateur.

En outre, l'agent d'authentification lance l'utilitaire dans les circonstances suivantes :

- En cas de modification de l'adresse IP de l'ordinateur client de l'agent d'authentification
- Lors de l'authentification RSA SecurID sur l'ordinateur de bureau local
- Lorsque vous utilisez RSA Control Center, pour effacer le secret de nœud sur l'ordinateur client de l'agent d'authentification

Lorsque l'utilitaire est démarré, il détermine si l'adresse IP de l'ordinateur client de l'agent d'authentification a été modifiée. Si l'adresse IP a changé, l'utilitaire la met à jour dans la base de données Authentication Manager. Si l'adresse IP n'a pas changé, l'utilitaire se ferme.

L'utilitaire d'inscription automatique permet aux systèmes d'utiliser le protocole DHCP (Dynamic Host Configuration Protocol) pour attribuer des adresses IP, et aux environnements utilisant des connexions VPN (Virtual Private Network) sans fil et virtuelles d'accéder au réseau d'entreprise. L'utilitaire permet également à un agent d'authentification inscrit de mettre à jour ses propres informations pour introduire les modifications issues du fichier de configuration **sdconf.rec** d'Authentification Manager.

L'utilitaire d'inscription automatique vous aide également à gérer le secret de nœud. Pour plus d'informations, consultez « Inscription automatique et secret de nœud », à la page 66.

Pour utiliser l'utilitaire, vous devez l'installer lors du processus d'installation, comme décrit dans la section Chapter 3, « Installation de l'agent d'authentification RSA. »

En outre, un administrateur RSA Authentication Manager doit configurer Authentication Manager pour autoriser l'inscription automatique. Pour plus d'informations, consultez la rubrique d'aide de RSA Authentification Manager.

Remarque : Lorsque vous utilisez l'utilitaire d'inscription automatique pour inscrire un nouvel agent d'authentification dans la base de données Authentication Manager, le nouvel agent d'authentification est inscrit avec les paramètres de l'authentification hors ligne et le mot de passe du système intégré, spécifié dans le base de données d'Authentication Manager.

Vous pouvez configurer l'utilitaire d'inscription automatique pour exempter les événements qui, par défaut, déclenchent l'exécution de l'utilitaire. Pour plus d'informations, consultez « Empêcher l'inscription automatique pendant les événements spécifiés », à la page 64.

Empêcher l'inscription automatique pendant les événements spécifiés

Pour réduire le trafic réseau et optimiser les performances, vous pouvez configurer l'utilitaire d'inscription automatique pour exempter les événements qui, par défaut, déclenchent l'exécution de l'utilitaire. Par exemple, vous pouvez spécifier que les modifications apportées aux adresses IP des appareils tels que les hôtes VMware ou les routeurs sans fil ne déclenchent pas l'exécution de l'utilitaire. Pour spécifier des exemptions, créez la chaîne ExcludeAdaptor dans le registre Windows. Les modifications apportées à l'adresse IP des appareils répertoriés dans la liste de valeurs de chaîne ExcludeAdaptor n'entraînent pas l'exécution de l'utilitaire d'inscription automatique.

Pour configurer l'utilitaire d'inscription automatique de sorte à exempter un événement :

1. Sur l'ordinateur client de l'agent d'authentification, connectez-vous à l'aide d'un compte administrateur.
2. Ouvrez l'Éditeur de registre. Par exemple, cliquez **sur** Démarrer. Ensuite, saisissez **regedit** dans l'invite **Lancer la recherche** et cliquez sur **regedit** dans la liste **Programmes**.
3. Dans l'éditeur de registre, cliquez sur **HKLM\ SOFTWARE\RSA\RSA Authentication Agent\AgentAutoRegistration**.
4. Dans le volet de droite de la fenêtre Éditeur de registre, cliquez avec le bouton droit, puis cliquez sur **Nouveau > Valeur de chaîne**.
5. Pour le nouveau nom de la valeur, saisissez **ExcludeAdapters**.
6. Dans le volet de droite de la fenêtre Registry Editor, cliquez avec le bouton droit sur **ExcludeAdapters**, puis sur **Modify**.
7. Pour le nom de la valeur, saisissez les informations permettant d'identifier chacun des appareils que l'utilitaire d'inscription automatique doit exclure de la surveillance. Utilisez des points-virgules pour séparer les identifiants de chaque appareil. Par exemple, si vous saisissez VPN;VMWARE, la valeur ExcludeAdapter exemptera tous les appareils dont le nom inclut VPN et tous les appareils dont le nom inclut VMWARE.

Important : La valeur ExcludeAdapter est sensible à la casse.

Empêcher l'inscription automatique pour des sous-réseaux sélectionnés

Dans certains environnements, les appareils clients utilisant l'inscription automatique peuvent être connectés à plusieurs réseaux actifs. L'activité réseau, par exemple les modifications d'adresse IP sur ces réseaux, déclenchera en temps normal l'inscription automatique.

Dans la plupart des cas, certains de ces sous-réseaux doivent être ignorés aux fins de l'inscription automatique. Ces sous-réseaux peuvent désormais être exclus de l'inscription automatique en définissant une valeur dans le registre.

Pour configurer l'utilitaire d'inscription automatique afin d'ignorer un sous-réseau, procédez comme suit :

1. Sur l'ordinateur client de l'agent d'authentification, connectez-vous à l'aide d'un compte administrateur.
2. Ouvrez l'Éditeur de registre. Par exemple, cliquez sur **Démarrer**. Ensuite, saisissez **regedit** dans l'invite **Lancer la recherche** et cliquez sur **regedit** dans la liste **Programmes**.
3. Dans l'éditeur de registre, cliquez sur **HKLM\ SOFTWARE\RSA\RSA Authentication Agent\AgentAutoRegistration**.
4. Dans le volet de droite de la fenêtre Éditeur de registre, cliquez avec le bouton droit, puis cliquez sur **Nouveau > Valeur de chaîne**.
5. Pour le nouveau nom de la valeur, saisissez **ExcludeNetworkMasks**.
6. Dans le volet de droite de la fenêtre Éditeur de registre, cliquez avec le bouton droit sur **ExcludeNetworkMasks**, puis sur **Modifier**.
7. Pour le nom de la valeur, saisissez une liste de sous-réseaux séparés par un point-virgule au format CIDR.

   Exemple : 172.16.0.0/12;192.168.0.0/16;169.254.0.0/16

Spécifier l'inscription automatique pour les sous-réseaux sélectionnés

Vous pouvez spécifier les sous-réseaux sélectionnés à inclure dans l'inscription automatique.

Pour configurer l'utilitaire d'inscription automatique de sorte qu'il utilise un sous-réseau, procédez comme suit :

1. Sur l'ordinateur client de l'agent d'authentification, connectez-vous à l'aide d'un compte administrateur.
2. Ouvrez l'Éditeur de registre. Par exemple, cliquez sur **Démarrer**. Ensuite, saisissez **regedit** dans l'invite **Lancer la recherche** et cliquez sur **regedit** dans la liste **Programmes**.
3. Dans l'Éditeur de registre, cliquez sur **HKLM\ SOFTWARE\RSA\RSA Authentication Agent\AgentAutoRegistration**.
4. Dans le volet de droite de la fenêtre Éditeur de registre, cliquez avec le bouton droit, puis cliquez sur **Nouveau > Valeur de chaîne**.
5. Pour le nom de la nouvelle valeur, saisissez **IncludeNetworkMasks**.
6. Dans le volet de droite de la fenêtre Éditeur de registre, cliquez avec le bouton droit sur **IncludeNetworkMasks**, puis sur **Modifier**.
7. Pour le nom de la valeur, saisissez une liste de sous-réseaux séparés par un point-virgule au format CIDR.

   Exemple : 10.0.0.0/8

Inscription automatique et secret de nœud

Le secret de nœud est requis pour la communication entre RSA Authentication Agent et RSA Authentication Manager. Pour une communication réussie, le secret de nœud généré par Authentication Manager doit être installé sur l'ordinateur client de l'agent d'authentification. Le secret de nœud est transféré d'Authentication Manager à l'agent d'authentification lors de l'authentification initiale. Des problèmes d'authentification peuvent se produire si le secret de nœud sur l'ordinateur client de l'agent d'authentification ne correspond pas à celui de la base de données Authentication Manager.

Lorsque l'utilitaire d'inscription automatique se connecte à Authentication Manager, Authentication Manager détecte si le secret de nœud sur le client de l'agent d'authentification ne correspond plus à celui qui est stocké dans l'enregistrement de l'hôte d'agent, dans la base de données d'Authentication Manager. Authentication Manager efface le secret de nœud dans l'enregistrement d'hôte d'agent et fait en sorte que l'agent d'authentification efface le secret de nœud sur l'ordinateur client de l'agent d'authentification. Authentication Manager génère un nouveau secret de nœud et le télécharge sur l'ordinateur client de l'agent d'authentification lors de l'authentification subséquente. Pour plus d'informations sur la résolution des problèmes liés au secret de nœud, consultez « Échec de la vérification du nœud » à la page 73. Pour plus d'informations sur l'utilitaire de secret de nœud, consultez « Utiliser l'utilitaire de chargement du secret de nœud » à la page 46.

Inscription automatique et authentification hors ligne

L'authentification hors ligne étend l'authentification RSA SecurID aux utilisateurs lorsque la connexion à RSA Authentication Manager n'est pas disponible (par exemple, lorsque les utilisateurs ne sont pas au bureau ou si l'état du réseau entraîne une indisponibilité temporaire de la connexion). Si l'authentification hors ligne est activée, Authentication Manager génère des données hors ligne (également appelées jours en mode hors ligne) et les télécharge sur l'ordinateur client de l'agent d'authentification lorsque l'agent d'authentification se connecte au serveur RSA Authentication Manager.

L'agent d'authentification lance l'utilitaire d'inscription automatique lors de l'authentification RSA SecurID sur l'ordinateur de bureau Windows local. Si l'utilitaire d'inscription automatique ne parvient pas à se connecter à Authentication Manager au cours du processus, l'agent d'authentification vérifie les données hors ligne. S'il existe des données hors ligne, l'agent d'authentification tente d'authentifier l'utilisateur hors ligne. Si aucune donnée hors ligne n'existe, l'agent d'authentification tente d'effectuer une authentification en ligne auprès d'Authentication Manager. En cas d'échec de l'authentification en ligne, l'agent d'authentification émet un message indiquant que l'authentification a échoué. Pour plus d'informations, consultez « Authentification hors ligne », à la page 53.

Conserver l'adresse IP principale de l'hôte de l'agent d'authentification

Chaque adresse IP de l'hôte d'agent doit être identifié dans son enregistrement d'hôte d'agent dans la base de données RSA Authentication Manager. Vous pouvez également répertorier d'autres adresses IP pour l'hôte en tant que « nœuds secondaires » pour le basculement.

Si votre système RSA Authentication Manager inscrit automatiquement les hôtes d'agent, l'adresse IP principale de chaque hôte d'agent est automatiquement saisie dans l'enregistrement de l'agent d'authentification sur RSA Authentication Manager. L'adresse est mise à jour dans l'enregistrement chaque fois qu'elle est modifiée. Pour plus d'informations, consultez « Processus d'inscription automatique », à la page 53.

Si votre système n'utilise pas l'inscription automatique, vous devez vous assurer que l'administrateur RSA Authentication Manager connaît l'adresse IP principale et secondaire de l'hôte de l'agent d'authentification dès que ce dernier est configuré initialement. Si l'adresse de l'hôte de l'agent change, informez-en immédiatement l'administrateur RSA Authentication Manager pour qu'il mette à jour l'enregistrement de l'hôte de l'agent d'authentification dans RSA Authentication Manager.

Si les hôtes d'agent sont inscrits manuellement, l'administrateur RSA Authentication Manager doit s'assurer que l'adresse IP principale dans l'enregistrement d'hôte de l'agent d'authentification dans la base de données RSA Authentication Manager correspond à celui spécifié dans le RSA Control Center, dans l'enregistrement d'hôte de l'agent d'authentification, ou dans le fichier d'options d'équilibrage de la charge (**sdopts.rec**). Si les adresses ne correspondent pas, la communication entre l'hôte de l'agent d'authentification et le serveur RSA Authentication Manager échoue. Si des adresses IP secondaires sont spécifiées pour l'hôte de l'agent d'authentification, elles doivent également être saisies dans l'enregistrement, et toutes les adresses doivent être mises à jour en cas de modifications.

Prise en charge des groupes multidomaines

Lorsque vous sélectionnez un groupe Windows en tant que groupe d'authentification RSA Authentication Agent à l'aide des modèles de stratégie GPO, tous les utilisateurs du groupe doivent être authentifiés auprès de RSA SecurID. L'agent d'authentification prend en charge tous les groupes Windows. Pour plus d'informations sur la configuration des groupes d'authentification, consultez *Group Policy Object Template Guide*.

Il existe de nombreuses combinaisons de groupes Windows différents : universel, global et domaine local. Windows permet également d'imbriquer des groupes au sein d'autres groupes. Il est important de comprendre les différentes combinaisons de groupes, de sorte à obtenir les résultats escomptés en imposant ou en excluant l'authentification pour un groupe auprès de RSA SecurID.

Les directives suivantes définissent quels utilisateurs doivent être authentifiés auprès de RSA SecurID :

- Les utilisateurs d'un groupe Windows doivent s'authentifier lorsque le groupe Windows se trouve dans un groupe d'authentification.
- Les utilisateurs d'un groupe Windows ne sont pas invités à s'authentifier lorsque ce dernier se trouve dans un groupe pour lequel l'authentification est exclue.

Le tableau suivant présente un exemple d'environnement multidomaine qui comporte deux domaines et différents types de groupes. Tous les utilisateurs et groupes se trouvent dans la même forêt. L'agent d'authentification ne peut pas déterminer l'appartenance d'un utilisateur si celui-ci se trouve dans une autre forêt.

Exemple de groupes et de membres dans un environnement multidomaine

Type de groupe	Description	Membre
Groupes universels		
U1D1	Groupe universel 1 dans le domaine 1	Utilisateur 1 (qui se trouve dans le domaine 1)
U2D2	Groupe universel 2 dans le domaine 2	Utilisateur 2 (qui se trouve dans le domaine 2)
U3D1	Groupe universel 3 dans le domaine 1	U1D1 U2D2 G1D1 G3D1
Groupes globaux		
G1D1	Groupe global 1 dans le domaine 1	Utilisateur 3 (qui se trouve dans le domaine 1)
G2D2	Groupe global 2 dans le domaine 2	Utilisateur 4 (qui se trouve dans le domaine 2)
G3D1	Groupe global 3 dans le domaine 1	G2D2

Exemple de groupes et de membres dans un environnement multidomaine

Type de groupe	Description	Membre
Groupes locaux de domaine		
L1D1	Groupe local de domaine 1 dans le domaine 1	Utilisateur 5 (qui se trouve dans le domaine 1) Utilisateur 6 (qui se trouve dans le domaine 2)
L2D1	Groupe local de domaine 2 dans le domaine 1	U3D1
L3D1	Groupe local de domaine 3 dans le domaine 1	G1D1 G3D1

Le tableau suivant présente les utilisateurs qui sont contraints de s'authentifier à l'aide de l'authentification RSA SecurID ou pour lesquels l'authentification est exclue,en fonction des groupes que vous avez sélectionnés dans le tableau précédent.

Paramètres d'authentification ou d'exclusion du groupe

Paramètres de groupe	Utilisateurs authentifiés ou exclus
U1D1	Utilisateur 1
U3D1	Utilisateur 1, utilisateur 2, utilisateur 3, utilisateur 4
G1D1	Utilisateur 3
G3D1	Utilisateur 4
L1D1	Utilisateur 5, utilisateur 6
L2D1	Utilisateur 1, utilisateur 2, utilisateur 3, utilisateur 4
L3D1	Utilisateur 3, utilisateur 4

Synchronisation automatique du mot de passe

En cas de modification des mots de passe sur les ordinateurs exécutant RSA Authentication Agent, ceux-ci sont synchronisés dans les comptes RSA Authentication Manager correspondants. Toutefois, si le mot de passe d'un utilisateur est modifié hors bande (à partir d'un ordinateur qui n'exécute pas l'agent d'authentification ou par un administrateur sur le contrôleur de domaine), il ne sera pas automatiquement synchronisé, sauf si vous effectuez les étapes suivantes :

1. Installer l'agent d'authentification sur tous les contrôleurs de domaine de votre environnement. Redémarrer les contrôleurs de domaine une fois l'installation terminée.

   L'installation de l'agent d'authentification installe le composant de synchronisation du mot de passe requis pour la synchronisation des mots de passe hors bande. Les contrôleurs de domaine doivent exécuter la fonction d'authentification hors ligne.

   Remarque: Il n'est pas nécessaire d'activer l'authentification RSA SecurID sur les contrôleurs de domaine, car l'authentification et la synchronisation du mot de passe sont deux processus indépendants l'un de l'autre.

2. Effectuez un test d'authentification sur les contrôleurs de domaine.

   Le test d'authentification établit des secrets de nœud entre les contrôleurs de domaine et RSA Authentication Manager. Les secrets de nœud permettent la communication entre les contrôleurs de domaine et Authentication Manager.

3. Configurez le composant de synchronisation du mot de passe en spécifiant des paramètres dans les modèles d'objet de stratégie de groupe RSA. Si vous utilisez à la fois les modèles Synchroniser les mots de passe des utilisateurs et Authentifier les utilisateurs sur le contrôleur de domaine, les mots de passe seront synchronisés pour les utilisateurs de l'un ou l'autre des groupes. Pour plus d'informations, reportez-vous à la *Group Policy Object Template Guide*.

Si vous installez l'agent d'authentification sur les contrôleurs de domaine, mais que vous n'utilisez pas le paramètre de synchronisation du mot de passe pour spécifier les utilisateurs dont les mots de passe doivent être synchronisés, les paramètres d'authentification du contrôleur de domaine déterminent les utilisateurs dont les mots de passe sont synchronisés. Par exemple, si vous définissez l'authentification pour tous les utilisateurs, mais que vous ne configurez pas la synchronisation des mots de passe, ceux-ci sont synchronisés pour tous les utilisateurs.

Authentification rationalisée pour applications Citrix® XenApp® et applications à distance

Cette fonction permet à l'agent d'accepter les informations d'identification des applications à distance telles que Citrix XenApp et Microsoft Remote Desktop Connection, de sorte que les utilisateurs n'ont pas besoin de saisir les informations d'identification deux fois s'ils utilisent ces applications, sauf si un code de token RSA SecurID ou un code d'accès est obligatoire.

Par défaut, cette fonctionnalité est désactivée. Pour activer cette fonction, utilisez un objet de stratégie de groupe. Pour savoir comment procéder, reportez-vous au *guide de modèle d'objet de stratégie de groupe*.

5 Résolution des problèmes

Les sections suivantes contiennent des informations détaillées sur les problèmes de connexion et d'authentification que vous pouvez rencontrer lors de l'utilisation de l'agent d'authentification. Ce chapitre fournit également des informations de dépannage et une description détaillée des messages d'erreur. Pour obtenir des informations de dépannage supplémentaires, connectez-vous à RSA Link à l'adresse **https://community.rsa.com/**.

Remarque : RSA Link est uniquement disponible pour les clients disposant d'un contrat de service logiciel valide.

Authentification hors ligne et utilitaire d'inscription automatique

Si vous effectuez une installation personnalisée de RSA Authentication Agent pour Microsoft Windows et que vous choisissez d'installer l'utilitaire d'inscription automatique, l'agent d'authentification le lance lorsque les utilisateurs s'authentifient à l'aide de leur code d'accès RSA SecurID pour accéder au bureau local. L'inscription automatique détermine si l'adresse IP de l'ordinateur a été modifiée. Si l'adresse IP a changé, le service la met à jour dans la base de données Authentication Manager.

Si l'utilitaire d'inscription automatique ne parvient pas à se connecter à Authentication Manager, l'agent d'authentification vérifie les données hors ligne. S'il existe des données hors ligne, l'agent d'authentification tente d'authentifier l'utilisateur hors ligne. Si aucune donnée hors ligne n'existe, l'agent d'authentification tente d'effectuer une authentification en ligne auprès d'Authentication Manager. En cas d'échec de l'authentification en ligne, l'agent d'authentification envoie un message pour indiquer que le processus d'authentification a échoué.

Le délai entre une tentative d'authentification et la notification d'état d'authentification dépend de votre configuration. Par exemple, si vous disposez d'une configuration d'instance principale de RSA Authentication Manager et de cinq instances de réplica, chacune dotée d'un alias en plus de l'adresse IP principale, l'inscription automatique tente pendant deux secondes de se connecter au serveur Authentification Manager sur chaque adresse IP attribuée à chaque serveur Authentication Manager. Chaque serveur Authentication Manager peut avoir une adresse IP principale et trois adresses IP d'alias.

Pour cette configuration, si aucune instance Authentication Manager n'est disponible, l'utilitaire d'inscription automatique met 24 secondes avant de déterminer que le serveur Authentication Manager n'est pas disponible. L'utilitaire invite ensuite l'agent d'authentification à tenter l'authentification hors ligne. Si l'utilisateur n'est pas configuré pour l'authentification hors ligne, l'hôte de l'agent d'authentification tente de s'authentifier en ligne.

Par défaut, l'agent d'authentification tente de s'authentifier auprès d'Authentication Manager cinq fois et chaque tentative dure par défaut cinq secondes. Cela équivaut à une durée totale de 25 secondes. Les 24 secondes requises par l'utilitaire d'inscription automatique, en plus des 25 secondes consacrées aux tentatives d'authentification équivalent à un temps d'attente total de 49 secondes entre la tentative d'authentification et la notification d'état d'authentification.

Problèmes d'authentification

Les sections suivantes décrivent les problèmes que vous pouvez rencontrer lors de l'exécution de l'agent d'authentification.

Le pilote RSA SecurID 800 peut ne pas s'installer automatiquement

L'authentificateur RSA SecurID 800 (RSA SecurID 800) dispose d'un lecteur de carte à puce intégré. Sur la plupart des systèmes, la première fois que vous insérez le RSA SecurID 800 dans un port USB, l'assistant Nouveau matériel détecté par Microsoft reconnaît automatiquement l'appareil et installe le pilote USB Microsoft CCID requis. Si un système ne peut pas installer le pilote automatiquement, vous pouvez l'installer manuellement sur le site Web de Microsoft (**http://catalog.update.microsoft.com/v7/site/Home.aspx**).

Pour plus d'informations sur l'installation manuelle du pilote, reportez-vous au fichier d'informations d'expédition de l'authentificateur RSA SecurID 800, livré avec la commande RSA SecurID 800.

L'authentification échoue après la modification de l'option « Envoyer le domaine et le nom d'utilisateur »

Chaque fois que vous appliquez un nouveau modèle d'objet de stratégie de groupe à des utilisateurs, vous devrez peut-être redémarrer l'ordinateur pour que la règle soit prise en compte.

Le test d'authentification réussit, mais l'authentification réelle échoue

Si le test d'authentification réussit mais que l'authentification réelle échoue, redémarrez l'ordinateur de l'agent d'authentification. Authentication Manager crée et envoie automatiquement le secret de nœud à l'agent en réponse à la première authentification réussie sur l'agent. Par conséquent, si vous redémarrez l'ordinateur de l'agent d'authentification avant l'existence d'un secret de nœud, l'agent d'authentification n'a pas connaissance du secret de nœud, même si Authentication Manager le transmet à l'ordinateur hôte de l'agent d'authentification.

Important : Ce scénario ne se produit que si vous n'avez pas activé l'inscription automatique sur RSA Authentication Manager. Si vous l'activez (et si vous installez l'utilitaire d'inscription automatique lors de l'installation de l'agent d'authentification), vous ne devriez pas rencontrer ce problème.

Échec de la vérification du nœud

Si le secret de nœud sur l'hôte de l'agent d'authentification est corrompu ou ne correspond pas au secret de nœud dans la base de données Authentication Manager, les communications chiffrées entre l'agent d'authentification et Authentication Manager ne peuvent pas fonctionner. Si cela se produit, le message **Accès refusé, échec de la vérification du nœud** est consigné dans le moniteur d'activité Authentication Manager.

Important : Si Authentication Manager autorise l'inscription automatique et si vous avez installé l'utilitaire d'inscription automatique lors de l'installation de l'agent d'authentification, essayez de résoudre les problèmes de secret de nœud répertoriés dans cette section sans intervention de l'utilisateur.

Les événements suivants peuvent provoquer l'échec de la vérification du nœud :

- Le Authentication Manager authentifie un utilisateur avec succès et envoie le secret de nœud à RSA Authentication Agent 7.4, avec un message indiquant que l'authentification a réussi. L'agent d'authentification échoue ou son délai expire (par exemple, en raison d'une coupure d'alimentation) avant de stocker le secret de nœud.
- Un administrateur désinstalle l'agent d'authentification, puis l'installe à nouveau. Lors de la désinstallation de l'agent d'authentification, le secret de nœud est supprimé.
- L'agent d'authentification n'est pas identifié dans la base de données Authentication Manager. Cet événement peut générer un message d'erreur « Échec de la vérification du nœud » ou un message d'erreur « Hôte d'agent inconnu ».
- Vous utilisez des instances de réplica Authentication Manager et l'instance de réplica ayant envoyé le secret de nœud à l'agent d'authentification n'a pas encore notifié les autres instances de réplica. Dans ce cas, certains utilisateurs pourront s'authentifier avec succès et d'autres, non.
- Vous utilisez des instances de réplica, et une ou plusieurs instances de réplica ne sont pas en cours d'exécution. Dans ce cas, certains utilisateurs pourront s'authentifier avec succès et d'autres, non.
- Vous effacez le secret de nœud sur l'agent d'authentification ou Authentication Manager, mais pas sur les deux.
- Vous effacez le secret de nœud sur l'agent d'authentification et Authentication Manager, mais ne redémarrez pas l'agent d'authentification si l'utilitaire d'inscription automatique n'est pas installé.
- Vous saisissez un nom d'utilisateur non valide lors de la première authentification après avoir effacé le secret de nœud.

Corriger un échec de vérification du nœud

Après avoir passé en revue les événements susceptibles de provoquer l'échec de la vérification du nœud dans la section précédente, vous pouvez corriger l'échec de la vérification du nœud si l'utilitaire d'inscription automatique n'est pas installé et activé sur Authentication Manager.

Pour corriger l'échec de la vérification du nœud :

1. Effacez le secret de nœud de l'hôte de l'agent d'authentification.
2. Parallèlement à cela, votre administrateur Authentication Manager doit effacer le secret de nœud spécifié pour l'hôte de l'agent d'authentification dans la base de données Authentication Manager.
3. Effectuez un test d'authentification sur l'hôte de l'agent d'authentification.

Important : Vous devez effacer le secret de nœud sur l'hôte de l'agent d'authentification et sur le serveur Authentication Manager.

Pour obtenir des instructions sur la façon d'effacer le secret de nœud sur l'agent d'authentification, consultez Aide avec RSA Authentication Agent (RSA SecurID) Pour obtenir des instructions sur la façon d'effacer le secret de nœud sur Authentication Manager, consultez Aide de la console de sécurité RSA.

Activer le suivi

Vous pouvez activer le suivi à partir de RSA Control Center pour diagnostiquer une série de problèmes d'authentification. En règle générale, vous n'activez pas le suivi à moins d'y être invité(e) par le Support client RSA. Le support technique vous indiquera également les composants dont le suivi doit être effectué et les niveaux à définir pour le suivi.

Remarque : Par défaut, le suivi est désactivé. Lorsque le suivi est activé, les fichiers de sortie de suivi sont écrits dans **C:\ProgramData\RSA\Logfiles**.

Activer le suivi :

1. À partir de l'ordinateur sur lequel l'agent d'authentification est installé, ouvrez RSA Control Center.
2. Cliquez sur **Advanced Tools**.
3. Cliquez sur **Tracing**.
4. Configurez les paramètres de suivi comme indiqué par le support technique.
5. Cliquez sur **OK**.

Diagnostiquer les problèmes d'authentification

Les sections suivantes décrivent les tâches que vous pouvez effectuer pour diagnostiquer les problèmes d'authentification.

Vérifier l'exactitude de l'horloge de l'ordinateur

Si un utilisateur ne parvient pas s'authentifier, assurez-vous que l'horloge de l'ordinateur de l'utilisateur affiche l'heure exacte. Si vous constatez un écart entre l'horloge de l'ordinateur et son paramètre précédent, il se peut que l'utilisateur ne soit pas en mesure de s'authentifier.

Vérifier le fichier de configuration système (sdconf.rec)

Si les ordinateurs RSA Authentication Agent 7.4 et Authentication Manager n'ont pas de copie compatible du fichier de configuration système (**sdconf.rec**), les ordinateurs ne pourront pas communiquer les uns avec les autres.

Pour vous assurer que vous disposez du fichier **sdconf.rec** correct, vérifiez les paramètres du fichier en ouvrant la boîte de dialogue Environnement de serveur.

Pour afficher la boîte de dialogue Environnement de serveur et vérifier le fichier Sdconf. Rec :

1. Ouvrez RSA Control Center.
2. Cliquez sur **Environnement de serveur**. La partie gauche de la boîte de dialogue affiche des informations sur l'état du serveur RSA Authentication Manager et sur la façon dont il communique avec l'agent.
3. Si vous recevez un message d'erreur « Impossible de récupérer l'environnement de serveur », le fichier de configuration système (**sdconf.rec**) est corrompu. Vous devez remplacer le fichier **sdconf.rec**.

   Pour plus d'informations sur le remplacement du fichier, consultez « Remplacer le fichier de configuration du système (sdconf.rec). »

Remplacer le fichier de configuration du système (sdconf.rec)

Si vous recevez le message d'erreur « Impossible de récupérer l'environnement de serveur » lorsque vous affichez le fichier de configuration système dans la section précédente, cela signifie que le fichier de configuration système (**sdconf.rec**) est corrompu et que vous devez le remplacer.

Pour remplacer le fichier sdconf.rec :

1. Recherchez le fichier de configuration système (**sdconf.rec**) sur l'ordinateur.
2. Procurez-vous un nouveau fichier **sdconf.rec** auprès de votre administrateur RSA Authentication Manager.
3. Ouvrez le dossier contenant le fichier **sdconf.rec** corrompu et remplacez-le par le nouveau fichier.

Important : Veillez à ce que votre logiciel anti-spyware ou anti-virus ne supprime pas automatiquement le fichier de secret de nœud ou le fichier **sdconf.rec**.

Messages de log des erreurs et de l'observateur d'événements

Cette section répertorie RSA Authentication Agent 7.4 les messages d'erreur et d'événement et décrit les circonstances qui génèrent l'erreur. Les messages sont répertoriés par ordre alphabétique.

La commande AVOID (éviter) possède une adresse IP non valide dans le fichier SDOPTS.REC.

L'adresse IP associée au paramètre AVOID dans le fichier **sdopts.rec** n'est pas valide. Pour plus d'informations sur la création d'un fichier **sdopts.rec** correctement formaté, reportez-vous à « Gérer un fichier sdopts.rec » à la page 82.

Cannot AVOID default IP Address in SDOPTS.REC file address.

Le paramètre AVOID ne fonctionne pas avec l'adresse IP par défaut spécifiée dans le fichier **sdopts.rec**. Pour plus d'informations sur la création d'un fichier **sdopts.rec** correctement formaté, reportez-vous à « Gérer un fichier sdopts.rec » à la page 82.

Impossible de créer un socket lors de l'initialisation dans l'authentification RSA SecurID. Le code d'erreur WINSOCK figure dans les données.

Les services de sockets peuvent ne pas avoir démarré. Consultez le journal des événements pour savoir s'il existe un problème avec la carte réseau ou les services TCP/IP.

En outre, assurez-vous que les services sont en cours d'exécution sur votre Authentication Manager en effectuant l'une des opérations suivantes :

- Si Authentication Manager s'exécute sur un ordinateur Windows, ouvrez le panneau de configuration réseau et vérifiez que des **services TCP/IP simples** sont installés. Si ce n'est pas le cas, ajoutez les **servicesTCP/IP simples**.
- Si Authentication Manager s'exécute sur un ordinateur UNIX, assurez-vous que le service d'**écho** est en cours d'exécution sur l'ordinateur Authentication Manager. Pour plus d'informations sur le démarrage du service d'**écho**, consultez la documentation de votre système d'exploitation UNIX.

Erreur de téléchargement de données rencontrée pour l'utilisateur : <*user name*>.

Une erreur s'est produite lors du téléchargement des données hors ligne pour l'utilisateur spécifié.

Duplicate AVOID statements in SDOPTS.REC file.

Le fichier **sdopts.rec** contient deux instructions AVOID identiques. Pour plus d'informations sur la création d'un fichier **sdopts.rec** correctement formaté, reportez-vous à « Gérer un fichier sdopts.rec » à la page 82.

Échec de la création du thread de service, abandon.

Trop de processus annexes étaient en cours d'exécution, par conséquent le service n'a pas démarré.

Incorrect size for file: sdconf.rec.

Le fichier **sdconf.rec** n'a probablement pas été copié en mode binaire. Demandez à l'administrateur Authentication Manager une nouvelle copie du fichier **sdconf.rec**.

File not found: aceclnt.dll.

Le logiciel a peut-être été installé incorrectement ou **aceclnt.dll** a été supprimé. Réinstallez le logiciel RSA Authentication Agent 7.4 à partir du fichier MSI (**RSA Authentication Agent.msi**) pour résoudre le problème.

File not found: sdconf.rec.

Le fichier **sdconf.rec** est absent du répertoire **HKLM\Software\RSA\RSA Authentication Agent\AuthDataDir**. Il a été supprimé ou n'a jamais été copié à partir de Authentication Manager. Demandez à votre administrateur Authentication Manager une nouvelle copie du fichier **sdconf.rec**.

L'initialisation du service d'authentification hors ligne a échoué.

Le service d'authentification hors ligne a échoué le démarrage. Si cette erreur se reproduit, redémarrez l'ordinateur.

Expiration du délai du réseau : Authentification Manager répondait mais s'est interrompu.

Assurez-vous que le processus Authentication Manager est en cours d'exécution sur le serveur. Recherchez un problème réseau, tel qu'un dysfonctionnement du routeur ou un câble réseau débranché.

Authentification hors ligne : Accès refusé.

La tentative d'authentification de l'utilisateur hors ligne a échoué.

Authentification hors ligne : Accès refusé - Attaque par réutilisation du code d'accès détectée.

Une personne a tenté de réutiliser un code d'accès que l'utilisateur a saisi pour s'authentifier hors ligne.

Authentification hors ligne : Accès refusé - code de token précédent.

La tentative d'authentification hors ligne par l'utilisateur a échoué, car l'utilisateur a saisi le code de token précédemment émis au lieu du code en cours de validité.

Authentification hors ligne : Limite d'échec d'authentification atteinte Seule l'authentification d'accès d'urgence est autorisée.

La tentative d'authentification hors ligne par l'utilisateur a échoué et l'utilisateur a été verrouillé sur le système. L'utilisateur doit contacter le service d'assistance technique pour obtenir un code d'accès d'urgence.

Authentification hors ligne : Code d'accès d'urgence accepté.

L'utilisateur s'est authentifié avec succès à l'aide d'un code d'accès d'urgence.

Authentification hors ligne : Code de token d'accès d'urgence accepté.

L'utilisateur s'est authentifié avec succès à l'aide d'un code de token d'accès d'urgence.

Authentification hors ligne : Code d'accès accepté.

L'utilisateur s'est authentifié avec succès hors ligne.

Le service d'authentification hors ligne s'est arrêté de manière anormale.

Le service d'authentification hors ligne s'est arrêté en raison d'une condition inhabituelle.

Le service d'authentification hors ligne a démarré. Port : *port*.

Le service d'authentification hors ligne a été démarré et écoute sur le port local spécifié.

Le service d'authentification hors ligne a été interrompu.

Le service d'authentification hors ligne a été interrompu.

Le décalage de temps d'authentification hors ligne a été ajusté à <*time*>.

Le paramètre d'horloge sur RSA Authentication Agent 7.4 ou Authentication Manager a été modifié.

L'utilisateur <*user name*> annulé suite à la routine Nouveau code PIN.

L'utilisateur a annulé la tentative d'authentification en mode Nouveau code PIN.

L'utilisateur <*user name*> a annulé la routine Authentification.

L'utilisateur a annulé sans saisir de nom d'utilisateur.

User <*user name*>: ACCESS DENIED.

L'accès est refusé à l'utilisateur. Recherchez le motif spécifique dans le log d'activité Authentication Manager.

User <*user name*>: ACCESS DENIED. Échec du code de token suivant.

L'utilisateur n'est pas parvenu à s'authentifier en mode Code de Token suivant et doit tenter de s'authentifier à nouveau.

User <*user name*>: ACCESS DENIED. Server signature invalid.

Ce message indique que l'identité du Authentication Manager n'a pas pu être vérifiée par l'agent d'authentification. Si vous voyez ce message, contactez le support technique RSA.

Utilisateur <*user name*> : annulé suite à la routine Prochain code de token.

L'utilisateur a annulé le processus Code de token suivant.

User <*user name*>: Nouveau code PIN accepté.

Le nouveau code PIN RSA SecurID de l'utilisateur a été vérifié.

User <*user name*>: Nouveau code PIN rejeté.

Le code PIN RSA SecurID a été rejeté par Authentication Manager. L'utilisateur doit s'authentifier à nouveau pour définir le code PIN RSA SecurID. Consultez le log d'activité Authentication Manager.

User <*user name*>: CODE D'ACCÈS accepté.

Le code d'accès de l'utilisateur a été accepté.

User <*user name*>: Mot de passe de réserve accepté.

L'utilisateur est invité à saisir le mot de passe de réserve et doit l'avoir saisi correctement.

User <*user name*>: Connexion réussie avec Prochain code de token.

Authentication Manager a accepté le code de token suivant et a accordé l'accès à l'utilisateur.

USESERVER et AVOID ne peuvent pas être tous deux utilisés dans le fichier sdopts.

Le fichier **sdopts.rec** tente d'utiliser simultanément USESERVER et AVOID. Pour plus d'informations sur la création d'un fichier **sdopts.rec** correctement formaté, reportez-vous à « Gérer un fichier sdopts.rec » sur à la page 82.

A Configuration de l'équilibrage de charge automatique

Équilibrage de charge automatique

Vous configurez RSA Authentication Agent de telle façon qu'il équilibre automatiquement les charges de demandes d'authentification en créant un fichier d'options d'équilibrage de charge (**sdopts.rec**). Le fichier **sdopts.rec** est un fichier texte stocké sur l'hôte de l'agent d'authentification (la machine sur laquelle un agent est installé). Vous pouvez y spécifier un équilibrage de charge dynamique ou manuel.

Important : Si vous envisagez de modifier ce fichier **sdopts.rec**, vous devez vous connecter avec un compte administrateur.

Équilibrage de charge dynamique

Avec l'équilibrage de charge dynamique, l'agent d'authentification envoie une demande de temps à chaque serveur RSA Authentication Manager du realm et détermine une liste de priorités en fonction du temps de réponse de chaque serveur d'agent d'authentification. Le serveur Authentication Manager ayant le temps de réponse le plus rapide obtient la priorité la plus élevée et reçoit le plus grand nombre de demandes d'authentification. Les autres serveurs Authentication Manager obtiennent des priorités plus faibles et moins de demandes. Cette disposition dure jusqu'à ce qu'Authentication Manager envoie une nouvelle demande de temps ou dépasse le délai imparti.

Pour effectuer l'équilibrage de charge dynamique, l'agent d'authentification se connecte au serveur Authentication Manager via des pare-feux en utilisant des adresses IP de substitution (alias) pour les serveurs Authentication Manager. Les serveurs Authentication Manager fournissent les alias à l'agent d'authentification sur demande. Les adresses sont stockées dans le fichier d'enregistrement de configuration (**sdconf.rec**) sur l'hôte Authentication Manager.

Vous spécifiez l'équilibrage de charge dynamique en excluant l'instruction **USESERVER** du fichier **sdopts.rec**. Pour plus d'informations, consultez « Gérer un fichier sdopts.rec », à la page 82.

Équilibrage de charge manuel

Avec l'équilibrage de charge manuel, vous spécifiez le serveur RSA Authentication Manager utilisé par chaque hôte d'agent. Vous attribuez également une priorité à chaque serveur Authentication Manager, pour permettre à l'agent d'authentification de diriger les demandes d'authentification à certains serveurs Authentication Manager plus fréquemment qu'à d'autres. Vous spécifiez un équilibrage de charge manuel en incluant l'instruction **USESERVER** dans le fichier **sdopts.rec** et en associant les paramètres de priorité à chaque serveur Authentication Manager dont vous spécifiez l'utilisation. Pour plus d'informations, consultez « Gérer un fichier sdopts.rec », à la page 82.

Gérer un fichier sdopts.rec

Cette section décrit les composants que vous pouvez utiliser pour créer un fichier **sdopts.rec**. Il donne également des exemples sur la façon d'utiliser les composants pour configurer l'équilibrage de charge.

Créer un fichier sdopts.rec

Vous pouvez utiliser un éditeur de texte pour créer et modifier un fichier **sdopts.rec**. Après avoir créé le fichier, enregistrez-le dans le répertoire spécifié par le paramètre de registre suivant : Valeur **AuthDataDir** dans la clé **HKLM\Software\RSA\RSA Authentication Agent**. Pour protéger ce fichier contre les modifications non autorisées, modifiez les paramètres d'autorisation de telle sorte que seuls les administrateurs puissent le modifier.

Important : Chaque fois que vous modifiez le fichier **sdopts.rec**, redémarrez l'agent d'authentification pour enregistrer les modifications.

Ce fichier peut inclure les éléments suivants :

- Des lignes de commentaires, chacune étant précédée d'un point-virgule.
- Des paires mot-clé-valeur, selon les exemples suivants :
  - **CLIENT_IP=*ip_address***. Spécifie une adresse IP de substitution pour l'hôte de l'agent d'authentification. Le mot-clé **CLIENT_IP** ne peut figurer qu'une seule fois dans le fichier. Pour plus d'informations, consultez « Spécifier une adresse IP de substitution », à la page 88. (L'agent d'authentification ne tient pas compte de ce paramètre si le remplacement de l'adresse IP est déjà défini via l'option **Outils avancés** dans RSA Control Center. Pour plus d'informations, consultez la rubrique d'aide de RSA Authentication Agent (RSA SecurID)
  - **USESERVER=*ip_address*, *priority***. Spécifie quel serveur RSA Authentication Manager doit recevoir des demandes d'authentification de l'hôte d'agent d'authentification selon une valeur de priorité spécifiée. Utilisez un paramètre pour chaque serveur RSA Authentication Manager utilisé par l'hôte d'agent d'authentification. Vous pouvez spécifier jusqu'à 11 serveurs Authentication Manager au total dans les fichiers **sdopts.rec** et **sdconf.rec**.

    Remarque : L'ajout de cette valeur au fichier **sdopts.rec** active l'équilibrage de charge manuel.

Chaque valeur de mot-clé **USESERVER** doit se composer de l'adresse IP RSA Authentication Manager effective, séparée par une virgule de la priorité attribuée. La priorité indique la fréquence à laquelle un serveur RSA Authentication Manager reçoit les demandes d'authentification. Le tableau suivant répertorie les valeurs de priorité que vous pouvez indiquer.

Priorité	Signification
2–10	Envoie les demandes d'authentification à ce serveur RSA Authentication Manager selon une sélection aléatoire et la priorité attribuée au serveur Authentication Manager. La valeur de la priorité est comprise entre 2 et 10. Plus la valeur est élevée, plus le nombre de demandes reçues par le serveur Authentication Manager est élevé. Un serveur Authentication Manager ayant la priorité 10 reçoit environ 24 fois plus de demandes qu'un serveur Authentication Manager ayant la priorité 2.
1	N'utilisez cela RSA Authentication Manager que si aucun serveur Authentication Manager ayant une priorité supérieure n'est disponible.
0	Ignorez ce serveur RSA Authentication Manager. Un serveur Authentication Manager de priorité 0 peut uniquement être utilisé dans des circonstances particulières : • Il doit s'agir de l'un des quatre serveurs Authentication Manager répertoriés dans le fichier **sdconf.rec**. • Le serveur Authentication Manager de priorité 0 peut uniquement être utilisé pour l'authentification initiale de l'agent d'authentification, sauf si tous les serveurs Authentication Manager présentant des priorités comprises entre 1 et 10 répertoriés dans le fichier **sdopts.rec** sont considérés comme inutilisables par l'agent d'authentification. En règle générale, la valeur de priorité 0 vous permet de placer une entrée dans le fichier pour un serveur Authentication Manager sans l'utiliser. Vous pouvez modifier la valeur de priorité si vous décidez d'utiliser le serveur Authentication Manager. **Remarque :** Vous devez saisir les mots-clés en majuscules. Si aucun des serveurs avec des instructions **USESERVER** ne répond, le serveur maître sera soit le serveur par défaut (s'il en existe un), soit le serveur Authentication Manager utilisé pour créer le fichier **sdconf.rec**.

Vous devez attribuer une priorité à chaque RSA Authentication Manager que vous ajoutez au fichier **sdopts.rec**. Sinon, l'entrée n'est pas valide. Les adresses IP figurant dans le fichier sont vérifiées par rapport à la liste des serveurs RSA Authentication Manager valides que l'agent d'authentification reçoit dans le cadre de son authentification initiale.

– **ALIAS=*ip_address*, *alias_ip_address_1*, *alias_ip_address_2*, alias_ip_address_3**. Spécifie une ou plusieurs adresses IP de substitution (alias) pour un serveur Authentication Manager en plus des alias répertoriés pour ce serveur dans le fichier **sdconf.rec**. Vous pouvez spécifier jusqu'à trois alias dans le fichier **sdopts.rec**.

  La valeur de mot clé **ALIAS** doit contenir l'adresse IP effective du serveur RSA Authentication Manager, suivie d'un nombre maximal de trois alias pour ce serveur Authentication Manager. L'agent d'authentification envoie des demandes assorties d'un certain délai à l'adresse IP effective et aux alias.

  Seule l'adresse IP effective spécifiée par le mot-clé **ALIAS** doit être connue par le serveur RSA Authentication Manager spécifié. En outre, l'adresse IP effective réelle doit être incluse dans toute liste de serveurs Authentication Manager reçue par l'agent d'authentification. La liste des serveurs Authentication Manager fournit des informations sur les adresses IP réelles et sur les alias de tous les serveurs Authentication Manager connus du Realm. L'agent d'authentification reçoit la liste du serveur Authentication Manager une fois qu'Authentication Manager a validé une demande d'authentification.

– **ALIASES_ONLY=*ip_address***. Lorsque vous fournissez l'adresse IP effective d'un serveur RSA Authentication Manager comme valeur, ce mot clé indique à l'agent d'authentification de n'utiliser que les adresses IP d'alias pour contacter Authentication Manager.

  Lorsque vous ne fournissez aucune valeur, ce mot clé indique à l'agent d'authentification de n'envoyer des demandes qu'aux serveurs RSA Authentication Manager auxquels ont été attribuées des adresses IP d'alias. Vous pouvez créer des exceptions en spécifiant une limite maximale de 10 mots clés **IGNORE_ALIASES** dans le fichier **sdopts.rec**, pour indiquer les serveurs Authentication Manager devant être contactés via leurs adresses IP effectives. Pour obtenir un exemple illustrant ces exceptions, consultez « Spécifier les adresses IP d'alias à utiliser ou à exclure » à la page 86. (Si vous utilisez ce mot clé, vérifiez qu'au moins un RSA Authentication Manager possède une adresse IP d'alias spécifiée pour celui-ci dans le fichier **sdconf.rec** ou **sdopts.rec**.)

– **IGNORE_ALIASES=*ip_address***. Lorsque vous n'indiquez aucune valeur, ce mot clé indique que toutes les adresses IP d'alias figurant dans les fichiers **sdopts.rec** et **sdconf.rec** ou dans la liste RSA Authentication Manager sont ignorées. Vous pouvez créer des exceptions en spécifiant une limite maximale de 10 mots clés **ALIASES_ONLY** dans le fichier **sdopts.rec**, pour indiquer les serveurs Authentication Manager devant être contactés via leurs adresses IP d'alias. Pour obtenir un exemple illustrant ces exceptions, consultez « Spécifier les adresses IP d'alias à utiliser ou à exclure » à la page 86.

Lorsque vous fournissez une adresse IP réelle en tant que valeur, ce mot clé indique à l'agent d'authentification d'utiliser uniquement l'adresse IP réelle pour contacter Authentication Manager.

– **AVOID=*ip_address***. Lorsque vous fournissez une adresse IP réelle d'un serveur RSA Authentication Manager en tant que valeur, ce mot clé indique à l'agent d'authentification de ne pas utiliser le serveur Authentication Manager lors de l'équilibrage dynamique de la charge.

Important : N'utilisez le mot-clé **AVOID** que pour l'équilibrage de charge dynamique. Ne l'utilisez pas avec le mot-clé **USESERVER** pour l'équilibrage de charge manuel.

Exclure un serveur Authentication Manager pendant l'équilibrage de charge dynamique

Dans l'équilibrage de charge dynamique, vous pouvez empêcher l'utilisation d'un serveur RSA Authentication Manager pour l'authentification en incluant le mot clé **AVOID** dans le fichier **sdopts.rec** Lorsque vous fournissez une adresse IP réelle d'un serveur RSA Authentication Manager en tant que valeur, ce mot clé indique à l'agent d'authentification de ne pas utiliser le serveur Authentication Manager lors de l'équilibrage dynamique de la charge.

Important : N'utilisez le mot-clé **AVOID** que pour l'équilibrage de charge dynamique. Ne l'utilisez pas avec le mot-clé **USESERVER** pour l'équilibrage de charge manuel. Si le mot-clé **AVOID** figure dans un fichier **sdopts.rec** qui comporte une instruction **USESERVER**, l'instruction **AVOID** est considérée comme une erreur.

Si vous utilisez l'instruction **AVOID** avec l'adresse IP du serveur RSA Authentication Manager par défaut, l'instruction est ignorée, sauf si un autre serveur Authentication Manager est disponible. Le serveur Authentication Manager par défaut est celui sur lequel le fichier **sdconf.rec** a été créé. Cependant, si un serveur Authentication Manager est désigné comme serveur maître, il devient le serveur Authentication Manager par défaut, quel que soit l'emplacement où le fichier **sdconf.rec** a été créé.

L'exemple suivant montre comment utiliser les mots-clés **AVOID** dans le fichier **sdopts.rec** :

```
AVOID=192.100.123.5
```

Dans cet exemple, le serveur RSA Authentication Manager avec l'adresse IP 192.100.123.5 ne sera pas utilisé pour l'authentification.

Configurer l'équilibrage de charge manuel

Vous configurez l'équilibrage manuel de la charge en incluant le mot clé **USESERVER** dans le fichier **sdopts.rec** pour spécifier les adresses IP des serveurs RSA Authentication Manager que vous souhaitez que chaque hôte de l'agent utilise.

Vous pouvez répertorier les adresses IP dans le fichier **sdopts.rec** dans n'importe quel ordre, mais vous devez les répertorier chacune séparément, une par ligne. L'exemple suivant montre comment utiliser les mots-clés **USESERVER** pour spécifier les adresses IP.

```
; Toute ligne de texte précédée d'un point-virgule est ignorée
; (est considérée comme un commentaire).
; N'insérez pas d'espace entre un mot clé et son
; signe égal (=) Les espaces vides sont autorisés après
; le signe égal, après l'adresse IP et après
; la virgule qui sépare une adresse IP d'une valeur
; de priorité.
USESERVER=192.168.10.23, 10
USESERVER=192.168.10.22, 2
USESERVER=192.168.10.20, 1
USESERVER=192.168.10.21, 0
```

Dans cet exemple, le serveur Authentication Manager identifié par l'adresse IP 192.168.10.23 reçoit plus de demandes d'authentification que le serveur Authentication Manager 192.168.10.22. Le serveur Authentication Manager 192.168.10.20 n'est utilisé que si les serveurs Authentication Manager de priorité supérieure ne sont pas disponibles. Le serveur Authentication Manager 192.168.10.21 est ignoré sauf dans de rares cas « Gérer un fichier sdopts.rec » (comme décrit à la section de la page 82).

Remarque : vous pouvez utiliser les mots-clés **USESERVER** et **ALIAS** simultanément dans le fichier **sdopts.rec**. Cependant, les mots clés **USESERVER** n'affectent pas les adresses d'alias utilisées pour se connecter aux serveurs Authentication Manager et les mots clés **ALIAS** ne déterminent pas quels serveurs Authentication Manager sont destinés à être utilisés.

Spécifier les adresses IP d'alias à utiliser ou à exclure

Vous pouvez utiliser le fichier **sdopts.rec** pour spécifier des adresses IP d'alias à utiliser ou à exclure.

Important : L'agent d'authentification ne tient pas compte de ce paramètre si le remplacement de l'adresse IP est déjà défini via l'option **Paramètres avancés** de RSA Control Center. Pour plus d'informations sur la définition de l'adresse IP via Control Center, consultez Aide avec RSA Authentication Agent (RSA SecurID)

Vous pouvez répertorier les paramètres dans le fichier **sdopts.rec** dans n'importe quel ordre, mais vous devez répertorier chaque paramètre séparément, un paramètre par ligne. L'exemple suivant montre comment utiliser les mots-clés **ALIAS** dans le fichier **sdopts.rec**.

```
; Toute ligne de texte précédée d'un point-virgule est ignorée
; (est considérée comme un commentaire).
; N'insérez pas d'espace entre un mot clé et son
; signe égal (=) Les espaces vides sont autorisés après
; le signe égal, après l'adresse IP et après
; la virgule qui sépare une adresse IP d'une valeur
; de priorité.
USESERVER=192.168.10.23, 10
USESERVER=192.168.10.22, 2
USESERVER=192.168.10.20, 1
USESERVER=192.168.10.21, 0
ALIAS=192.168.10.23, 192.168.4.1, 192.168.4.2, 192.168.4.3
ALIAS=192.168.10.22, 192.168.5.2, 192.168.5.3
ALIAS=192.168.10.20, 192.168.5.1
ALIAS=192.168.10.21, 0, 192.168.1.1
ALIAS_ONLY=192.168.10.23
IGNORE_ALIASES=192.168.10.22
```

Dans cet exemple, la valeur par défaut consiste à utiliser les adresses IP effectives ou d'alias, à quelques exceptions près. Le serveur RSA Authentication Manager possédant l'adresse IP effective 192.168.10.23 dispose de trois adresses d'alias spécifiées pour lui, tandis que les serveurs Authentication Manager 192.168.10.20 et 192.168.10.21 n'ont chacun qu'un seul alias. Le serveur RSA Authentication Manager 192.168.10.22 possède deux adresses d'alias. Les alias spécifiés par les mots-clés **ALIAS** sont des ajouts aux alias spécifiés dans le fichier **sdconf.rec** et dans le serveur RSA Authentication Manager.

Cet exemple montre comment utiliser les mots clés **USESERVER** et **ALIAS** simultanément dans le fichier **sdopts.rec**. Cependant, les mots clés **USESERVER** n'affectent pas les adresses d'alias utilisées pour se connecter aux serveurs Authentication Manager et les mots clés **ALIAS** ne déterminent pas quels serveurs Authentication Manager sont destinés à être utilisés.

Dans l'exemple suivant, la valeur par défaut consiste à utiliser les alias, à deux exceptions près. Le serveur RSA Authentication Manager 192.168.10.23, comme spécifié par le mot clé **ALIASES_ONLY**, sera contacté uniquement via ses adresses IP d'alias. Le serveur RSA Authentication Manager 192.168.10.22, spécifié par le mot clé **IGNORE_ALIASES**, sera contacté uniquement à l'aide de son adresse IP effective.

Dans l'exemple suivant, la valeur par défaut consiste à ignorer les alias, à deux exceptions près :

```
IGNORE_ALIASES
ALIASES_ONLY=192.168.10.23
ALIASES_ONLY=192.168.10.22
```

Les exceptions **ALIASES_ONLY** indiquent que l'agent d'authentification ne doit envoyer les demandes au serveur RSA Authentication Manager 192.168.10.23 et 192.168.10.22 que via les adresses IP d'alias.

Dans l'exemple suivant, la valeur par défaut consiste à utiliser les alias, à deux exceptions près :

```
ALIASES_ONLY
IGNORE_ALIASES=192.168.10.23
IGNORE_ALIASES=192.168.10.22
```

Les exceptions **IGNORE_ALIASES** indiquent que l'agent d'authentification ne doit envoyer les demandes au serveur RSA Authentication Manager 192.168.10.23 et 192.168.10.22 que via les adresses IP effectives.

Spécifier une adresse IP de substitution

Lorsque l'agent d'authentification s'exécute sur un hôte qui dispose de plusieurs cartes d'interface réseau et donc de plusieurs adresses IP, vous devez spécifier une adresse IP d'hôte d'agent principale à utiliser pour les communications chiffrées entre l'agent d'authentification et RSA Authentication Manager. En général, les hôtes d'agent tentent de découvrir leurs propres adresses IP. Un hôte d'agent avec plusieurs adresses peut en sélectionner une qui n'est pas connue de RSA Authentication Manager, ce qui rend la communication impossible entre l'agent d'authentification et Authentification Manager. Vous pouvez spécifier une adresse IP principale de substitution en incluant le mot clé **CLIENT_IP** dans un fichier **sdopts.rec** sur l'hôte de l'agent d'authentification.

Remarque : Le protocole DHCP (Dynamic Host Configuration Protocol) alloue les adresses IP aux hôtes d'agent de manière dynamique. Pour éviter les conflits d'adressage, installez l'utilitaire d'inscription automatique lorsque vous installez l'agent d'authentification. Pour plus d'informations, reportez-vous aux sections Chapter 3, « Installation de l'agent d'authentification RSA » et Chapter 5, « Résolution des problèmes. »

Pour spécifier une adresse IP de substitution dans le fichier **sdopts.rec**, procédez comme suit :

CLIENT_IP=192.168.10.19

Cette instruction garantit que l'hôte de l'agent d'authentification utilise toujours l'adresse IP spécifiée pour communiquer avec Authentification Manager.

Important : L'agent d'authentification ignore ce paramètre si l'option de remplacement de l'adresse IP de l'ordinateur est définie dans RSA Control Center. Toutefois, si vous avez installé l'utilitaire d'inscription automatique (pendant ou après le processus d'installation de l'agent d'authentification), l'adresse que l'utilitaire inscrit remplace le paramètre IP dans Control Center. (Le champ du **paramètre Adresse IP de substitution** devient également inactif après avoir installé l'utilitaire d'inscription automatique.) Pour plus d'informations sur la définition de l'adresse IP via Control Center., reportez-vous à l'aide de RSA Authentication Agent (RSA SecurID).

Glossaire

Terme	Définition
accès d'urgence	Procédures alternatives que les utilisateurs peuvent suivre en cas d'urgence pour accéder à leurs appareils ou à d'autres ressources protégées lorsqu'ils n'ont pas accès à leurs informations d'identification standard.
accès d'urgence hors ligne	Il s'agit d'un autre moyen pour les utilisateurs d'accéder aux ressources protégées en mode hors ligne sans utiliser leurs informations d'identification normales.
actualiser les jours en mode hors ligne	Permet aux utilisateurs d'obtenir plus de jours en mode hors ligne.
administrateur de serveur	Individu disposant d'un accès à certaines fonctions d'administration sur un produit logiciel RSA Authentication Manager via l'interface utilisateur d'administration. Les privilèges d'administration peuvent aller de l'affichage des informations stockées sur le serveur à l'exécution d'opérations propres à l'utilisateur et à l'ensemble du système.
agent	Application logicielle installée sur un appareil (par exemple, un serveur de domaine, un serveur Web ou un ordinateur de bureau) et qui permet la communication avec Authentication Manager sur le serveur réseau à des fins d'authentification.
authentificateur connecté RSA SecurID	Le logiciel utilisé avec un authentificateur RSA SecurID 800 connecté. Le logiciel est installé sur l'ordinateur de bureau et est accessible via RSA Control Center.
authentificateur RSA SecurID 800	Il s'agit d'un authentificateur que les utilisateurs peuvent utiliser comme une carte à puce ou comme un token RSA SecurID. Les utilisateurs peuvent connecter RSA SecurID 800 à un port USB pour procéder à l'authentification RSA SecurID ou l'utiliser en tant qu'appareil portatif, en fonction de l'application RSA qu'ils utilisent.
authentificateur USB	Un authentificateur matériel doté d'un connecteur pour relier l'authentificateur à un port USB.
authentification à deux facteurs	Protocole d'authentification nécessitant deux différentes manières d'établir et de prouver l'identité, par exemple, un élément dont vous disposez (tel qu'un authentificateur) et quelque chose que vous connaissez (par exemple un code PIN).

Terme	Définition
authentification hors ligne	Option de RSA Authentication Agent qui oblige les utilisateurs à saisir des codes d'accès RSA SecurID pour s'authentifier sur leurs ordinateurs de bureau Windows, même lorsque leur ordinateur n'est pas connecté à RSA Authentication Manager via le réseau.
client d'authentification à distance	Il s'agit d'un ordinateur client d'authentification à distance qui héberge le composant client d'authentification à distance de RSA Authentication Agent.
client d'authentification local	Un composant RSA Authentication Agent qui oblige les utilisateurs à saisir des codes d'accès RSA SecurID valides pour accéder à leurs ordinateurs de bureau Microsoft Windows
code d'accès	Code utilisé dans l'authentification RSA SecurID pour accéder à une ressource protégée. Il se compose de deux facteurs : un code PIN (Personal Identification Number) et le code de token (nombre aléatoire) actuellement indiqué à l'avant d'un token RSA SecurID.
code d'accès d'urgence	Un code d'authentification complet qui, s'il est activé, peut être utilisé par un utilisateur pour s'authentifier hors ligne, sans authentificateur ou code PIN.
code de token	Le numéro aléatoire figurant à l'avant du token SecurID RSA d'un utilisateur. Les codes de token changent à intervalles réguliers, généralement toutes les 60 secondes.
code de token d'accès d'urgence	Code d'authentification partiel qui, s'il est activé, peut être utilisé par un utilisateur pour s'authentifier hors ligne sans authentificateur. L'utilisateur est tenu de fournir son code PIN.
code PIN RSA SecurID	Code PIN créé par l'utilisateur ou généré par le système (numéro d'identification personnel) qui est utilisé avec un code de token pour générer un code d'accès.
compte administrateur exempté	Un groupe d'agents qui n'est pas contraint à s'authentifier.
compte Windows	Le nom d'utilisateur, le mot de passe et le domaine qui identifient un utilisateur particulier sur le système d'exploitation Windows.
connecté	Fait référence à un authentificateur USB connecté à un port USB ou à un câble d'extension.
déconnecté	Fait référence à un authentificateur USB qui n'est pas connecté à un port USB ou à un câble d'extension.

Terme	Définition
domaine	Il s'agit d'un groupe de serveurs et d'appareils client qui existent dans la même structure de sécurité. Les domaines sont définis par l'administrateur et partagent une base de données commune.
données hors ligne	Données générées par RSA Authentication Manager et téléchargées sur l'agent pour activer l'authentification hors ligne. Ce terme est utilisé dans la documentation de l'administrateur. Voir aussi Jours en mode hors ligne.
fournisseur d'informations d'identification	Voir Ouverture de session Microsoft (fournisseur d'informations d'identification)
fournisseur d'informations d'identification RSA	Il s'agit d'un composant DLL remplaçable qui identifie l'utilisateur et les interactions d'authentification lors de la connexion.
groupe d'authentification	Un groupe d'utilisateurs qui sera invité par RSA SecurID Agent à s'authentifier
hôte d'agent	Machine sur laquelle un agent est installé.
icône d'état des jours en mode hors ligne	Icône dans la zone de notification Windows qui indique aux utilisateurs l'état général de leur offre de jours en mode hors ligne.
icônes Notifications	Icône dans la zone de notification qui peut contenir une icône contextuelle utilisée pour informer les utilisateurs des événements ou des actions à effectuer.
Intégration des mots de passe Windows	Une fonctionnalité qui intègre les mots de passe Microsoft Windows dans le processus de connexion via RSA SecurID.
jours en mode hors ligne	Données générées par RSA Authentication Manager et téléchargées sur l'agent pour activer l'authentification hors ligne. Ce terme est utilisé dans la documentation de l'utilisateur final. Voir aussi Données hors ligne.
mot de passe de réserve	Méthode d'accès d'urgence qui permet à l'administrateur de s'authentifier auprès de l'ordinateur protégé d'un utilisateur, sans avoir à saisir un code d'accès RSA SecurID dans les cas suivants : • Le service d'authentification hors ligne n'est pas en cours d'exécution sur l'ordinateur local. • L'ordinateur ne peut pas se connecter à RSA Authentication Manager

Terme	Définition
ouverture de session Microsoft (fournisseur d'informations d'identification)	Méthode de connexion qui utilise le fournisseur d'informations d'identification Microsoft et présente les boîtes de dialogue d'ouverture de session Windows standard.
secret de nœud	Clé symétrique de longue durée utilisée par l'agent pour chiffrer les données de la demande d'authentification. Authentication Manager génère la demande d'authentification lorsqu'un utilisateur effectue une tentative d'authentification réussie. Le secret de nœud est connu uniquement d'Authentication Manager et de l'agent.
utilitaire d'inscription automatique de l'agent	Il s'agit d'un utilitaire inclus dans le logiciel RSA Authentication Agent qui vous permet d'inscrire automatiquement les nouveaux agents d'authentification dans la base de données interne et qui met à jour les adresses IP des agents existants.
zone de notification	Zone de la barre des tâches d'un ordinateur utilisant Windows et qui affiche les notifications à l'utilisateur. La zone contient des icônes de petite taille pour chaque fonction de notification.

Index