Notes de mise à jour RSA Authentication Agent 7.4.3 pour Microsoft Windows

Août 2019

Introduction

Ce document présente les nouveautés de RSA® Authentication Agent 7.4.3 pour Microsoft Windows. Il inclut également des solutions de contournement pour les problèmes connus. Lisez ce document avant d'installer le logiciel. Ce document contient les sections suivantes :

Ces *Notes de mise à jour* peuvent faire l'objet d'une actualisation. La version la plus récente est disponible sur RSA link à l'adresse **https://community.rsa.com/**.

Nouveautés de cette version

Cette section répertorie les nouvelles fonctionnalités et améliorations introduites dans RSA Authentication Agent pour Microsoft Windows.

Version 7.4.3, août 2019

Les mises à jour suivantes ont été introduites dans RSA Authentication Agent 7.4.3, disponible en août 2019 :

Prise en charge. Cette version qualifie Windows Server 2019.

Fonctionnalité :

- Le paramètre « Libellé de l'invite d'authentification locale » inclut désormais une option de code PIN. Vous pouvez sélectionner l'option de code PIN, par exemple si vous avez connecté RSA Authentication Manager au service d'authentification Cloud et que vous utilisez la méthode d'authentification Approuver avec un code PIN.
- Les packs de langue sont désormais disponibles sur RSA Link et non dans le dossier du produit.

Corrections de bugs. Pour plus d'informations, reportez-vous à RSA Authentication Agent 7.4.3 août 2019 à la page 10.

Version 7.4.2, décembre 2018

Les mises à jour suivantes ont été introduites dans RSA Authentication Agent 7.4.2, lancée en décembre 2018 :

Fonctionnalité. Cette version prend en charge la spécification des sous-réseaux sélectionnés à inclure dans l'inscription automatique.

Corrections de bugs. Pour plus d'informations, reportez-vous à RSA Authentication Agent 7.4.2 décembre 2018 à la page 10.

Version 7.4, septembre 2018

Les mises à jour suivantes ont été introduites dans RSA Authentication Agent 7.4, disponible en septembre 2018 :

Prise en charge. Cette version est qualifiée avec Windows Server 2016, édition Datacenter (Server Core).

Fonctionnalité :

- Cette version prend en charge le fournisseur d'informations d'identification Windows v2. Elle est conforme à l'expérience de l'interface utilisateur de connexion introduite sous Windows 8 et respecte également automatiquement les définitions Windows des images personnalisées.
- Possibilité de spécifier un texte personnalisé lors de la collecte des informations d'identification RSA SecurID ou du mot de passe Windows.
- Possibilité de ne pas afficher un message distinct lorsque le mot de passe Windows n'est pas disponible.
- Prise en charge des images personnalisées pour les mosaïques d'informations d'identification RSA pour un authentificateur portatif ou connecté
- Possibilité de ne pas utiliser d'authentificateur connecté dans des sessions de bureau à distance
- Possibilité de chiffrer les demandes LDAP Active Directory

Corrections de bugs. Pour plus d'informations, reportez-vous à RSA Authentication Agent 7.4 septembre 2018 à la page 10.

Version 7.3.3, juin 2017

Les mises à jour suivantes ont été introduites dans RSA Authentication Agent 7.3.3, disponible en juin 2017 :

Fonctionnalité :

- L'agent peut désormais prendre en charge plusieurs applications de bureau à distance, en plus de la « Connexion Bureau à distance » de Microsoft. Pour plus d'informations, reportez-vous à RSA Authentication Agent 7.3.3 juin 2017 à la page 8.
- Ajout de l'option permettant de configurer la mosaïque d'informations d'identification du fournisseur d'informations d'identification RSA pour utiliser l'image Windows standard pour Windows 7 et le serveur 2008.

Corrections de bugs. Pour plus d'informations, reportez-vous à RSA Authentication Agent 7.3.3 juin 2017 à la page 11.

Version 7.3.2, février 2017

Les mises à jour suivantes ont été introduites dans RSA Authentication Agent 7.3.2, disponible en février 2017 :

Prise en charge. Cette version prend officiellement en charge le serveur Windows 2016.

Fonctionnalité. L'agent accepte désormais les informations d'identification des applications à distance telles que Citrix® XenApp® et Microsoft Remote Desktop Connection. Ainsi, les utilisateurs qui ne sont pas obligés de s'authentifier via RSA SecurID n'ont pas besoin de saisir les informations d'identification à deux reprises lorsqu'ils utilisent ces applications.

Corrections de bugs. Pour plus d'informations, reportez-vous à RSA Authentication Agent 7.3.2 février 2017 à la page 12.

Version 7.3.1, juin 2016

Les mises à jour suivantes ont été introduites dans RSA Authentication Agent 7.3.1, disponible en juin 2016 :

Fonctionnalité. L'agent inclut désormais des fichiers de modèle d'objet de stratégie de groupe au format **.admx/.adml**, lesquels sont requis pour l'importation des fichiers vers la zone de stockage centrale de la stratégie de groupe.

Corrections de bugs. Pour plus d'informations, reportez-vous à RSA Authentication Agent 7.3.1 juin 2016 à la page 12.

Version 7.3, mai 2016

Les mises à jour suivantes ont été introduites dans RSA Authentication Agent 7.3, disponible en mai 2016 :

Prise en charge. Cette version prend officiellement en charge Windows 10. RSA Authentication Agent 7.3 et les versions ultérieures ne sont pas compatibles avec RSA Authentication Client 3.6 sous Windows 10.

Remarque : Il existe des problèmes de compatibilité entre RSA Authentication Client 3.6 et RSA Authentication Agent 7.2.1 ou version ultérieure. Pour plus d'informations, reportez-vous à Problèmes connus.

Fonctionnalité. L'agent communique désormais à l'aide des protocoles TLS 1.2 s'ils sont pris en charge par le serveur RSA Authentication Manager.

Corrections de bugs. Pour plus d'informations, reportez-vous à RSA Authentication Agent 7.3 mai 2016 à la page 13.

Important : Lisez attentivement la section suivante Installation du produit avant d'effectuer l'installation.

Version 7.2.1, mai 2015

Les mises à jour suivantes ont été introduites dans RSA Authentication Agent 7.2.1, disponible en mai 2015 :

Fonctionnalité. Un mode de conservation de l'historique a été ajouté pour afficher la dernière authentification réussie lorsqu'un utilisateur se connecte.

Corrections de bugs. Pour plus d'informations, reportez-vous à RSA Authentication Agent 7.2.1 mai 2015 à la page 13.

Version 7.2.1, juin 2013

Les mises à jour suivantes ont été introduites dans RSA Authentication Agent 7.2.1, disponible en juin 2013 :

Performances. Les performances du processus de vérification de la signature numérique ont été améliorées.

Corrections de bugs. Pour plus d'informations, reportez-vous à RSA Authentication Agent 7.2.1 juin 2013 à la page 14.

Version 7.2

Les mises à jour suivantes ont été introduites dans RSA Authentication Agent 7.2 :

Prise en charge de Windows 8 et Windows Server 2012. L'agent d'authentification prend en charge Windows 8 et Windows Server 2012 (dans Server Core ou Serveur avec le mode GUI). Si vous utilisez Windows Server en mode Server Core, vous n'utilisez pas d'interface utilisateur. Vous devez installer l'application à partir de la ligne de commande. Vous pouvez 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, consultez le *guide d'installation et d'administration*.

Prise en charge des nouveaux fournisseurs d'informations d'identification Microsoft. Le modèle d'objet de stratégie de groupe (GPO) **RSACredProviderFilter_Microsoft** prend désormais en charge les mots de passe image, les codes PIN (pour Microsoft Live ID) et les fournisseurs d'informations d'identification Microsoft Live ID, en plus des fournisseurs d'informations d'identification de mots de passe et de carte à puce. Pour plus d'informations, reportez-vous au *guide de modèle d'objet de stratégie de groupe.*

Nécessite Microsoft .NET Framework 4 Client Profile ou .NET Framework 4.5. RSA Authentication Agent 7.2 (et versions ultérieures) pour Microsoft Windows requiert Microsoft .NET Framework 4 Client Profile ou .NET Framework 4.5. .NET Framework 4.5 est préinstallé sur Windows 8 et Windows Server 2012. Si vous envisagez d'utiliser Windows 7 ou Windows Server 2008, vous devez installer Microsoft .NET Framework 4 Client Profile avant d'installer RSA Authentication Agent. Pour télécharger .NET Framework 4 Client Profile, consultez le site Web Microsoft suivant : **www.microsoft.com/en-us/download/details.aspx?id=24872**.

Installation du produit

Important : Si vous avez l'intention de procéder à une mise à niveau à partir d'une version antérieure de RSA Authentication Agent pour Microsoft Windows vers la version 7.4, vous devez vérifier les paramètres d'authentification actuels de la préinstallation. Si le groupe d'authentification sélectionné a une valeur sAMAccountName différente de son nom commun, les paramètres d'authentification peuvent être incorrects après l'installation. Pour corriger ces paramètres après l'installation, utilisez RSA Control Center pour reconfigurer les paramètres d'authentification.

Ce package fournit des programmes d'installation et des modèles d'objet de stratégie de groupe dans les fichiers zip suivants :

- **RSA_Authentication_Agent_ 7.4.3.zip** (qui contient les programmes d'installation et d'autres fichiers de support pour les plate-formes 32 et 64 bits)
- **RSA_GPO_AuthAgent_743.zip** (qui contient les modèles d'objet de stratégie de groupe)

Procédure :

1. Connectez-vous à l'ordinateur en tant qu'administrateur.
2. Extrayez le fichier **RSA_Authentication_Agent_7.4.3.zip** vers un dossier local.
3. Recherchez le fichier .msi adapté à l'architecture de l'appareil. Les fichiers .msi résident aux emplacements suivants :
   - Pour les plate-formes 32 bits **x86\RSA Authentication Agent.msi**.
   - Pour les plate-formes 64 bits **x64\RSA Authentication Agent x64.msi**.
4. Si vous mettez à jour une version antérieure à RSA Authentication Agent pour Windows 7.2 ou si vous effectuez une nouvelle installation de RSA Authentication Agent pour Windows 7.4, cliquez sur le fichier .msi approprié.
5. Si vous mettez à jour une installation de RSA Authentication Agent pour Windows 7.2 ou version supérieure vers RSA Authentication Agent pour Windows 7.4 :
   a. Ouvrez une fenêtre de ligne de commande.
   b. Accédez au dossier contenant le fichier .msi que vous souhaitez installer.
   c. À partir de l'invite de commande, saisissez
   msiexec /i "<yourarchitecture.msi>" REINSTALL=ALL REINSTALLMODE=vomus
6. Une fois l'installation effectuée, redémarrez l'ordinateur.

Recommandations relatives à l'utilisation du produit

Cette section contient des recommandations destinées à garantir le bon fonctionnement de l'agent d'authentification.

- Les services Windows « Serveur » et « Station de travail » doivent être exécutés en tout temps. Si ces services sont interrompus, demandez aux utilisateurs de redémarrer leur ordinateur pour redémarrer les processus.
- Les utilisateurs en mode Nouveau code PIN ou Code de token suivant doivent suivre immédiatement les invites des boîtes de dialogue. Si la boîte de dialogue Nouveau code PIN ou Code de token suivant expire, demandez aux utilisateurs d'appuyer sur CTRL+ALT+SUPPR pour recommencer la procédure.
- Effectuez les installations Push comme indiqué dans le *guide d'installation et d'administration*. Par exemple, utilisez Microsoft Systems Management Server (SMS) pour transmettre le MSI en mode silencieux aux ordinateurs des utilisateurs. Il n'est pas recommandé d'effectuer une opération Push via une session de bureau à distance.
- N'ajoutez pas d'adresses IP de substitution à l'enregistrement de l'hôte de l'agent sur le serveur Authentication Manager si vous utilisez l'inscription automatique.

Interopérabilité avec RSA Authentication Agent pour Web pour IIS

RSA Authentication Agent 7.4 pour Microsoft Windows et RSA Authentication Agent pour Web pour IIS utilisent tous deux l'API d'authentification RSA. Pour pouvoir communiquer avec RSA Authentication Manager, l'API d'authentification RSA nécessite des fichiers de configuration et un secret de nœud. L'agent d'authentification pour Windows et l'agent d'authentification pour le Web stockent ces fichiers à des emplacements différents. Pour que les deux agents communiquent avec Authentication Manager, ces fichiers doivent toujours être identiques dans les deux emplacements.

Les fichiers de configuration et le secret de nœud sont stockés dans les emplacements suivants :

- Agent d'authentification pour les installations Windows : **<<Program Files>>\Common Files\RSA Shared\Auth Data**
- Agent d'authentification pour les installations Web : **<<Windows>>\System 32**

Si vous utilisez l'utilitaire de chargement du secret de nœud, vous pouvez charger le secret de nœud dans les deux emplacements. Si le secret de nœud est généré automatiquement au cours de l'authentification test avec l'agent d'authentification pour Windows ou l'agent d'authentification pour le Web, vous devez copier le secret de nœud vers l'autre emplacement de l'agent.

L'agent d'authentification pour Windows et l'agent d'authentification pour le Web partagent des clés de registre situées sous les paramètres de registre Windows suivants : **HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT**. Les paramètres qui se trouvent ici servent à contrôler la consignation du traçage et les remplacements d'adresses IP. Les deux agents utilisent le même emplacement du registre, et les paramètres de registre par défaut sont installés par le premier produit installé. Dans la mesure où les paramètres sont partagés, un paramètre modifié avec un seul produit est automatiquement reflété dans l'autre produit. Par exemple, si vous modifiez le remplacement de l'adresse IP à l'aide du RSA Control Center de l'agent d'authentification pour Windows, il n'est pas nécessaire d'effectuer la modification avec l'application Authentication Agent pour Panneau de configuration Web. En outre, les paramètres partagés ne sont pas supprimés lorsque vous supprimez l'un des deux produits. Si vous supprimez les deux produits, vous devez supprimer manuellement les paramètres du registre.

RSA recommande d'utiliser la procédure suivante pour installer et utiliser des agents Windows et Web sur un ordinateur unique.

Avant de commencer

Le format du secret de nœud a récemment été modifié. L'agent d'authentification pour Windows exige que le secret de nœud soit au nouveau format. En ce qui concerne l'interopérabilité, la version de l'agent d'authentification pour Web que vous installez doit également utiliser le nouveau format. RSA Authentication Agent pour Web 7.4 utilise le nouveau format de secret de nœud. Si vous installez une version antérieure de l'agent d'authentification pour le Web, contactez le support technique RSA (**www.emc.com/support/rsa/index.htm**) afin d'obtenir le correctif approprié et prendre en charge le nouveau format de secret de nœud.

Procédez comme suit pour installer l'agent d'authentification pour Windows et l'agent d'authentification pour Web en vue de l'interopérabilité :

1. Installez l'agent d'authentification pour Web et effectuez un test d'authentification comme décrit dans le *guide d'installation et de configuration de RSA Authentication Agent pour Web pour IIS*.
2. Installez l'agent d'authentification pour Windows, comme décrit dans le *guide d'installation et d'administration de RSA Authentication Agent pour Microsoft Windows*.

   Important: N'essayez pas de tester l'authentification à l'aide de l'agent d'authentification pour Windows tant que vous n'avez pas effectué l'étape suivante.

3. Ouvrez une invite de commande, puis utilisez la commande **XCOPY** avec l'option /O pour copier le secret de nœud depuis **<<Windows>>\System32** vers **<<Program Files>>\Common Files\RSA Shared\Auth Data**. L'option /O spécifie que les informations de propriété et de liste de contrôle d'accès (ACL) doivent également être copiées, comme indiqué dans l'exemple suivant :

   ```
   XCOPY C:\Windows\System32\securid "C:\Program Files\Common Files\RSA Shared\Auth Data\" /O
   ```

Important: N'utilisez pas la commande **COPY** ou l'Explorateur Windows pour copier le fichier de secret de nœud. En raison de la sensibilité du secret de nœud, vous devez également copier les informations de propriété et d'ACL.

4. Effectuez un test d'authentification de l'agent d'authentification pour Windows, comme décrit dans le *guide d'installation et d'administration de RSA Authentication Agent pour Microsoft Windows.*

Interopérabilité avec les systèmes sécurisés par RSA Ready Partner Solutions

Si vous utilisez RSA Authentication Agent 7.4 pour Microsoft Windows sur un système faisant partie du programme RSA Ready Partner Solutions, rendez-vous sur le site RSA Ready à l'adresse **www.rsaready.com**. Ce site comprend des guides d'implémentation et des informations sur la facilité d'utilisation et la compatibilité.

Contenu de l'emballage

RSA Authentication Agent est disponible à l'adresse **https://community.rsa.com/community/products/securid/authentication-agent-windows**.

Le dossier produit de RSA Authentication Agent 7.4 contient les éléments suivants :

Fichier ou dossiers	Description
Assistant de configuration	Ce dossier contient le fichier **ConfigWizard.exe** que vous pouvez utiliser pour personnaliser le programme d'installation et le déployer sur plusieurs ordinateurs.
x86 et x64	Ces dossiers contiennent des modules d'installation Windows pour l'installation locale de RSA Authentication Agent 7.4 sur les ordinateurs 32 bits et 64 bits.
Licences	Ce dossier contient le contrat de licence RSA (RSA_License_Agreement. doc).
Modèles de stratégie	Ce dossier contient les modèles d'administration de l'objet de stratégie de groupe (GPO) pour la gestion des paramètres d'authentification. Ce dossier inclut des modèles à la fois dans le format **.admx**/.**adml** et dans le format **.adm**, plus ancien. Les nouveaux fichiers de modèles se trouvent dans le dossier **Policy Templates\admx**.
Utilitaire de chargement du secret de nœud	Ce dossier contient l'utilitaire de chargement du secret de nœud (**agent_nsload.exe**), que vous pouvez utiliser pour copier en toute sécurité le secret de nœud à partir d'un serveur Authentication Manager sur un ordinateur d'agent d'authentification avant d'utiliser l'authentification RSA SecurID. **Remarque :** L'utilitaire de chargement du secret de nœud n'est pas nécessaire pour créer un secret de nœud. Pour plus d'informations, consultez le *Guide d'installation et d'administration*.

Documentation et aide sur les applications

La documentation suivante est mise à disposition à l'emplacement suivant :

https://community.rsa.com/community/products/securid/authentication-agent-windows

Documentation

Titre	Nom de fichier
Guide d'installation et d'administration de RSA Authentication Agent 7.4 pour Microsoft Windows	**auth_agent_install_admin_guide.pdf**
Guide de modèle d'objet de stratégie de groupe RSA Authentication Agent 7.4 pour Microsoft Windows	**auth_agent_gpo_template_guide.pdf**

L'aide suivante s'installe avec RSA Authentication Agent 7.4 pour Microsoft Windows.

Aide sur les applications

Titre	Nom de fichier
Aide de l'agent d'authentification RSA SecurID	L'aide est accessible à partir du RSA Control Center.

Nouvelles fonctions et améliorations

RSA Authentication Agent 7.4.3 août 2019

Prise en charge de Windows 2019 édition Standard

Cette version est qualifiée avec Windows Server 2019, édition Standard (Server Core ou Expérience utilisateur).

Le paramètre d'invite d'authentification locale inclut l'option de libellé de champ Code PIN

Le paramètre « Libellé de l'invite d'authentification locale » inclut désormais une option de code PIN. Par exemple, sélectionnez l'option Code PIN si vous avez connecté RSA Authentication Manager au service d'authentification Cloud et que vous utilisez la méthode d'authentification Approuver avec un code PIN. Pour plus d'informations, reportez-vous au *guide de modèle d'objet de stratégie de groupe* et à **Connecter RSA Authentication Manager au service d'authentification Cloud**.

Packs de langue disponibles sur RSA Link

Les packs de langue sont désormais disponibles sur RSA Link et non dans le dossier du produit.

RSA Authentication Agent 7.4.2 décembre 2018

Spécifiez les sous-réseaux sélectionnés à inclure dans l'inscription automatique

Cette version vous permet de spécifier les sous-réseaux sélectionnés à inclure dans l'inscription automatique à l'aide de l'option IncludeNetworkMasks.

RSA Authentication Agent 7.4 septembre 2018

Prise en charge de Windows 2016 édition Datacenter (Server Core)

Cette version est qualifiée avec Windows Server 2016, édition Datacenter (Server Core).

Prise en charge du fournisseur d'informations d'identification Windows v2

Cette version prend en charge le fournisseur d'informations d'identification Windows v2. Elle est conforme à l'expérience de l'interface utilisateur de connexion introduite sous Windows 8 et respecte également automatiquement les définitions Windows des images personnalisées.

Nouvelles fonctions Contrôle texte, Images, Connexions Bureau à distance et Chiffrement

L'agent d'authentification prend désormais en charge les éléments suivants :

- Possibilité de spécifier un texte personnalisé lors de la collecte des informations d'identification RSA SecurID ou du mot de passe Windows.
- Possibilité de ne pas afficher un message distinct lorsque le mot de passe Windows n'est pas disponible.
- Prise en charge des images personnalisées pour les mosaïques d'informations d'identification RSA pour un authentificateur portatif ou connecté
- Possibilité de ne pas utiliser d'authentificateur connecté dans des sessions de bureau à distance
- Possibilité de chiffrer les demandes LDAP Active Directory

Vous pouvez activer ces fonctions avec les nouveaux modèles d'objet de stratégie de groupe. Pour plus d'informations, reportez-vous au *guide de modèle d'objet de stratégie de groupe.*

RSA Authentication Agent 7.3.3 juin 2017

Prise en charge de plusieurs applications dans la stratégie d'application RDC

La stratégie Paramètres d'authentification locale - Application de connexion au bureau à distance dans l'objet de stratégie de groupe RSA Authentication Agent accepte désormais une liste délimitée par des virgules des applications à exclure de l'authentification RSA SecurID. Celle-ci peut être utilisée pour éviter d'appliquer l'authentification RSA SecurID à des applications de bureau à distance telles que « Remote Desktop Connection Manager » de Microsoft lorsque l'agent est installé sur un système qui sert d'hôte intermédiaire. Pour plus d'informations, reportez-vous au *guide de modèle d'objet de stratégie de groupe.*

Image du fournisseur d'informations d'identification

Les invites d'authentification de l'agent peuvent désormais être configurées pour afficher l'image d'informations d'identification Windows plutôt que l'image RSA SecurID sur les appareils Windows 7 et Server 2008.

RSA Authentication Agent 7.3.2 février 2017

Prise en charge de Windows Server 2016

Cette version prend officiellement en charge le serveur Windows 2016.

Authentification rationalisée pour les applications Citrix XenApp et les 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.*

RSA Authentication Agent 7.3.1 juin 2016

Modèles d'objet de stratégie de groupe au format .admx/.adml

L'agent d'authentification 7.3.1 inclut les modèles d'objet de stratégie de groupe au format **.admx**/**.adml**, en plus de l'ancien format **.adm**. Le nouveau format de modèle est requis lors de l'importation de fichiers dans la zone de stockage de la stratégie de groupe. Les nouveaux fichiers de modèles se trouvent dans le dossier **Policy Templates\admx**.

RSA Authentication Agent 7.3 mai 2016

Prise en charge Windows 10

Cette version prend officiellement en charge Windows 10.

Remarque : Il existe des problèmes de compatibilité entre RSA Authentication Client 3.6 et RSA Authentication Agent 7.2.1 ou version ultérieure. Pour plus d'informations, reportez-vous à Problèmes connus.

L'agent d'authentification 7.3 utilise le mode TLS 1.2 lorsqu'il est pris en charge par le serveur Authentication Manager.

L'agent d'authentification 7.3 fait partie de la mise à jour du mode TLS 1.2 pour RSA Authentication Manager, qui permet de prendre en charge les bonnes pratiques de sécurité et de conformité légale en utilisant le protocole de chiffrement TLS 1.2 pour les communications réseau sécurisées au sein de RSA Environnement Authentication Manager 8.1 SP1.

Vous n'avez pas besoin de configurer l'agent pour utiliser le mode TLS 1.2. Si le serveur Authentication Manager prend en charge la communication TLS 1.2, l'agent utilise par défaut le mode TLS 1.2. Si le mode TLS 1.2 n'est pas pris en charge, l'agent utilise la communication SSLv3 à la place.

Pour prendre en charge la communication TLS 1.2, vous devez installer la mise à jour du mode TLS 1.2 (Authentication Manager 8.1 SP1 correctif 13) ou une mise à jour ultérieure sur le serveur Authentication Manager et activer le mode TLS 1.2 à l'aide d'un script de configuration. Pour savoir comment procéder, consultez le *guide de mise à jour et de configuration du mode TLS 1.2 pour RSA Authentication Manager 8.1 SP1.*

RSA Authentication Agent 7.2.1 mai 2015

Le mode Conserver l'historique affiche la dernière authentification réussie

AAWIN-2168 par défaut empêchait l'affichage lors de la connexion des informations sur les précédentes connexions réussies et échouées. Ce problème est résolu en fournissant deux modes d'agent d'exploitation :

Le mode **Ne pas conserver l'historique** (par défaut) permet d'afficher des messages descriptifs d'échec d'authentification aux utilisateurs lors de la connexion mais ne conserve pas ni n'affiche l'historique des échecs d'authentification lors d'une tentative de connexion réussie lorsque Windows est configuré pour afficher la dernière connexion interactive à titre indicatif.

Le mode **Conserver l'historique** renvoie un message d'échec d'authentification générique en réponse à une tentative d'authentification échouée lors de la connexion, mais affiche correctement le nombre de tentatives d'authentification échouées au cours de la dernière connexion interactive Windows à titre indicatif.

Les deux modes d'exécution d'agent sont configurés par un nouveau modèle d'objet de stratégie de groupe.

RSADesktop_PreserveFailedAuthHistory

Ce modèle est fourni dans la section « Modèles de stratégie » du kit.

Utilisez « gpedit. msc » pour installer le nouveau modèle d'objet de stratégie de groupe. Appelez l'objet de stratégie de groupe pour configurer l'agent. Les choix de mode se présentent comme suit en réponse à :

Conserver l'historique des échecs d'authentification :

1. Ne pas conserver l'historique d'authentification

2. Conserver l'historique

Pour que l'agent s'exécute en mode par défaut :

Sélectionnez « Ne pas conserver l'historique d'authentification ».

Pour résoudre le problème décrit dans Jira AAWIN-2168 par défaut :

Sélectionnez « Conserver l'historique ». Veillez à « Appliquer » les sélections.

Après avoir appliqué la sélection « Conserver l'historique », toutes les tentatives de connexion échouées suivantes seront enregistrées et indiquées dans Windows lors d'une connexion réussie, lorsque Windows est configuré comme suit :

http://technet.microsoft.com/en-us/library/dd446680(v=ws.10).aspx

Important : Le serveur doit être en cours d'exécution au niveau fonctionnel du domaine Windows Server 2008 ou à un niveau plus récent avant de configurer la dernière connexion interactive. Si le serveur n'est pas configuré pour s'exécuter à l'un de ces niveaux, les utilisateurs, y compris l'administrateur, ne pourront pas se connecter à leur ordinateur de bureau.

Problèmes résolus

RSA Authentication Agent 7.4.3 août 2019

Cette version inclut des correctifs pour les problèmes suivants :

- **AAWIN-2444** - Correction d'un problème au niveau des paramètres d'authentification mis en cache, qui empêchait parfois l'authentification hors ligne.
- **AAWIN-2518** - Amélioration des performances de l'authentification hors ligne.
- **AAWIN-2536** - Les utilisateurs Windows 10 d'un domaine d'une forêt distante peuvent désormais utiliser l'authentification hors ligne.
- **AAWIN-2542** - Le verrouillage rapide du mot de passe invite les utilisateurs à saisir un mot de passe, au lieu de demander un code d'accès RSA SecurID sur certains systèmes Windows 10.
- **AAWIN-2550** - Un fournisseur d'informations d'identification Microsoft a été ajouté au filtre du fournisseur d'informations d'identification RSA. Cette mise à jour permet le chiffrement des e-mails lorsque le paramètre « Désactiver les fournisseurs d'informations d'identification tiers » est activé.
- **AAWIN-2911** - Par défaut, une nouvelle installation de l'agent Windows peut interroger Active Directory lorsque le service hors ligne est désactivé.

RSA Authentication Agent 7.4.2 décembre 2018

Cette version inclut des correctifs pour les problèmes suivants :

- **AAWIN-2482** - L'agent Windows se déconnecte plus rapidement lorsque Active Directory est inaccessible.
- **AAWIN-2504** - Le programme d'installation n'écrit plus de valeur de registre empêchant Cisco AnyConnect de « compléter » le fournisseur d'informations d'identification RSA.
- **AAWIN-2509** - Si les utilisateurs se connectent à un appareil Windows 10 version 1709 dans une session de connexion Bureau à distance, déconnectez, puis reconnectez la session. Les utilisateurs sont désormais invités à saisir un code d'accès RSA SecurID et un mot de passe, au lieu d'un mot de passe ou d'un code PIN RSA SecurID seulement.
- **AAWIN-2510** - Des améliorations ont été apportées afin de réduire le temps nécessaire pour effectuer l'authentification hors ligne, ce qui évite le blocage de la connexion ou du déverrouillage.

RSA Authentication Agent 7.4 septembre 2018

Cette version inclut des correctifs pour les problèmes suivants :

- **AAWIN-2313** - Un utilisateur Windows 10 est désormais invité à saisir un code PIN juste après que l'utilisateur a inséré la carte à puce.
- **AAWIN-2286** - Sous Windows 10, l'ordre des mosaïques utilisateur affichées est désormais déterminé par Microsoft Windows.

- **AAWIN-2301** - Le déverrouillage rapide affiche désormais le nom de la mosaïque des informations d'identification désélectionnée de l'utilisateur connecté dans les sessions de la console Windows 10.
- **AAWIN-2385**, **AAWIN-2209, AAWIN-2040 et AAWIN-2101** - Vous pouvez désormais ajouter une image personnalisée pour remplacer l'image RSA lorsqu'une mosaïque d'informations d'identification RSA s'affiche. Vous spécifiez cette image personnalisée à l'aide d'un modèle d'objet de stratégie de groupe.
- **AAWIN-2315** - Si un utilisateur se connecte à un hôte Windows protégé par l'agent et tente de se connecter à un autre système Windows à l'aide de la connexion Bureau à distance Microsoft qui n'est pas protégée par l'agent, l'utilisateur est invité à saisir le nom d'utilisateur et le mot de passe Windows.
- **AAWIN-2457** - Les utilisateurs appartenant à un groupe d'authentification spécifique doivent désormais s'authentifier.
- **AAWIN-2426** - L'interface ping peut être désactivée si l'authentification hors ligne est lente.
- **AAWIN-2441** - Mise à jour de l'heure utilisée pour déterminer si la preuve d'authentification est valide.
- **AAWIN-2436** - Le fournisseur d'informations d'identification RSA marque la mosaïque d'informations d'identification « Autre utilisateur » comme étant la mosaïque par défaut.
- **AAWIN-2429** - Le délai de 90-secondes du déverrouillage par mot de passe sur les systèmes déconnectés a été résolu.
- **AAWIN-2421** - L'agent Windows reconnaît désormais un état d'erreur supplémentaire du serveur pour une erreur de preuve non valide.
- **AAWIN-2395** - Les utilisateurs peuvent désormais déverrouiller le système sur Windows 10 lorsqu'un mot de passe Active Directory doit être modifié.
- **AAWIN-2222** - L'intégration des mots de passe Windows fonctionne si le mot de passe contient des caractères spéciaux, tels que åäöÅÄÖ. Le code envoie et reçoit désormais le mot de passe de l'utilisateur au format UTF-8 plutôt que dans le jeu de caractères par défaut du système.
- **AAWIN-2392** - Le service d'inscription automatique ferme désormais correctement tous les descripteurs utilisés pour enregistrer les modifications d'adresse IP avec le serveur.
- **AAWIN-2384** - Lorsque le service d'authentification hors ligne met en file d'attente des utilisateurs pour le téléchargement des données hors ligne, il exclut désormais les utilisateurs dont l'attestation d'authentification a expiré.
- **AAWIN-2369** - Les utilisateurs peuvent se connecter aux ordinateurs de bureau si leur mot de passe Windows doit être modifié lors de la connexion à Windows 10 (mise à jour anniversaire) ou à Windows Server 2016.
- **AAWIN-2339** - Si l'authentification hors ligne est activée pour un utilisateur et que celui-ci s'authentifie avec succès via UAC, l'authentification réussit et les données hors ligne sont désormais téléchargées.

RSA Authentication Agent 7.3.3 juin 2017

Cette version inclut des correctifs pour les problèmes suivants :

- **AAWIN-2343** - Le fichier **sdconf.rec** se synchronise désormais correctement avec les instances principale et de réplica utilisées par un serveur qui accepte uniquement les connexions TLS 1.2 lorsque les appareils sont déplacés physiquement, puis reconnectés au réseau.
- **AAWIN-2347** - L'authentification du déverrouillage rapide RSA s'effectue désormais correctement lorsqu'un système est verrouillé, car la stratégie de groupe Microsoft « Ouverture de session interactive : Limite d'inactivité de l'ordinateur » a été configurée.
- **AAWIN-2368** - L'authentification à distance pour le compte de domaine intégré dénommé « Administrateur » s'exécute désormais comme prévu.
- **AAWIN-2370** - Les données d'authentification hors ligne sont désormais correctement mises à jour après une mise à niveau.
- **AAWIN-2371** - L'agent d'authentification maintient désormais correctement l'inscription automatique après une mise à niveau.
- **AAWIN-2383** - L'agent d'authentification ne génère plus de messages d'erreur par intermittence lorsque les informations d'identification d'administration sont saisies pour une application sous Windows avec UAC activé.

RSA Authentication Agent 7.3.2 février 2017

Cette version inclut des correctifs pour les problèmes suivants :

- **AAWIN-2333** - Après avoir réussi à vous connecter à l'hôte de l'agent à partir d'un ordinateur Windows à l'aide du protocole Remote Desktop Protocol, puis à verrouiller ensuite l'écran lors de la session, les utilisateurs ne pouvaient pas déverrouiller l'hôte de l'agent à nouveau car l'écran de verrouillage ne présentait pas d'options de connexion au fournisseur d'information d'identification RSA SecurID.
- **AAWIN-2328** - Les retards de connexion jusqu'à 30 secondes se produisaient sous Windows 2012 R2 avec des contrôleurs de domaine en lecture seule.
- **AAWIN-2325** - Tous les hôtes d'agent d'authentification hébergeaient simultanément les données hors ligne, ce qui entraînait une charge trop importantes pour les serveurs lors des déploiements très volumineux.
- **AAWIN-2322** - L'agent d'authentification utilisait le cache d'authentification local pour déterminer l'état de l'authentification, au lieu d'authentifier les utilisateurs par défaut lorsque le contrôleur de domaine n'était pas disponible.
- **AAWIN-2320** - L'agent d'authentification était exposé aux vulnérabilités décrites dans **CVE-2016-0923** et **CVE-2016-0924**.
- **AAWIN-2318** - Dans certains déploiements, le service hors ligne **da_svc.exe** se bloquait et entraînait un ralentissement de l'authentification.
- **AAWIN-2309** - Le service d'inscription automatique ne retentait pas l'inscription si tous les serveurs étaient inaccessibles.
- **AAWIN-2299** - Le déverrouillage rapide par code PIN ne fonctionnait pas lorsque l'utilisateur s'était connecté à l'aide d'un nom de domaine complet (FQDN).
- **AAWIN-2293** - Les utilisateurs appartenant à des groupes d'authentification incluant un FQDN recevait le message d'erreur « Vous n'êtes pas autorisé à accéder aux données/à l'authentification hors ligne » lors d'une tentative d'authentification hors ligne, même lorsque l'ordinateur de l'utilisateur disposait de jours en mode hors ligne.

RSA Authentication Agent 7.3.1 juin 2016

Cette version inclut des correctifs pour les problèmes suivants :

- **AAWIN-2295** - L'agent d'authentification ne parvient pas à déterminer le groupe d'authentification auquel un utilisateur appartient si celui-ci envoie un nom de domaine complet (par exemple, yourdomain.local/username) dans le champ du nom d'utilisateur.
- **AAWIN-2287** - Sous Windows Server 2012 R2, lorsque la stratégie de mode d'authentification est définie sur un groupe d'utilisateurs, ou sur tous les utilisateurs à l'exception d'un groupe spécifique, l'ouverture de session prend plus de temps que prévu.
- **AAWIN-2284** - Un utilisateur Windows 7 ne peut modifier le mot de passe d'un compte que pour le domaine sur lequel le compte est actuellement connecté.
- **AAWIN-2271** - L'ouverture de session prend plus de temps que prévu pour les utilisateurs sans authentification qui n'appartiennent pas à plusieurs groupes d'un référentiel d'identité.
- **AAWIN-2254** - L'agent d'authentification inclut des fichiers de modèle GPO au format **.adm** mais pas au format **.admx/.adml**, qui est requis lors de l'importation de fichiers vers la zone de stockage centrale de la stratégie de groupe.
- **AAWIN-2246** - Lorsque le déverrouillage rapide par code PIN est activé sur les systèmes Windows 10, les utilisateurs authentifiés sont invités à saisir un code d'accès RSA SecurID sur l'écran de déverrouillage au lieu d'un code PIN. Lorsque vous vous connectez via une connexion Remote Desktop Protocol, le déverrouillage rapide par code PIN fonctionne correctement.

RSA Authentication Agent 7.3 mai 2016

Cette version inclut des correctifs pour les problèmes suivants :

- **AAWIN-2243** - Après l'installation de l'agent sous Windows 10, les mosaïques propres à l'utilisateur, qui s'affichent normalement sur l'écran de connexion de chaque compte utilisateur, sont remplacées par une mosaïque de connexion RSA SecurID unique et générique.
- **AAWIN-2221** - Si un compte d'utilisateur de domaine authentifié est configuré de telle sorte que le mot de passe doit être modifié après qu'un utilisateur s'est connecté à Windows, puis a réverrouillé le système, cet utilisateur ne peut plus réinitialiser le mot de passe et se reconnecter.
- **AAWIN-2206** - sdconf.rec peut être corrompu.
- **AAWIN-2194** - Lorsque les utilisateurs sont verrouillés en raison d'une saisie incorrecte du code d'accès lorsqu'ils ne sont pas connectés au réseau, ils doivent saisir le token d'accès d'urgence hors ligne et le code d'accès à deux reprises pour se connecter.
- **AAWIN-2193** - Une authentification en ligne réussie ne supprime pas l'état de verrouillage du compte hors ligne.
- **AAWIN-2188** - La fonctionnalité de déverrouillage ne fonctionne pas si la stratégie Window **Connexion interactive : Afficher les informations d'utilisateur lorsque la session est verrouillée** n'est pas définie sur **Nom d'affichage de l'utilisateur, noms de domaine et d'utilisateur**.
- **AAWIN-2185** - Les utilisateurs ne peuvent pas télécharger les données hors ligne vers les systèmes Windows hors site.
- **AAWIN-2183** - Le bouton **Actualiser** de la page Actualiser les jours en mode hors ligne dans RSA Control Center ne fonctionne pas.
- **AAWIN-2181** - Le service d'authentification hors ligne se bloque lorsque le nombre de tokens est supérieur à trois.
- **AAWIN-2168** - L'option **Afficher les informations sur les ouvertures de session précédentes** dans Windows ne fonctionne pas lorsque RSA Authentication Agent pour Windows est installé.
- **AAWIN-2147** - LogonUI.exe est en échec lors de l'appel de DASvcAPIWrapper.DLL.
- **AAWIN-2135** - Sous les systèmes Windows 8, les invites de saisie de code PIN de RSA Authentication Agent s'affichent après que le verrouillage rapide par code PIN a expiré.
- **AAWIN-2123** - La synchronisation automatique du mot de passe ne fonctionne pas de manière cohérente.
- **AAWIN-2108** - L'exemption d'un groupe local contenant un groupe de sécurité local de domaine ne fonctionne pas.
- **AAWIN-2107** -Le journal de sécurité Windows affiche un message d'échec d'audit si un utilisateur n'est pas autorisé à se connecter en local et se connecte à l'aide des services de terminal.
- **AAWIN-2102** - Les utilisateurs connaissent des délais d'authentification trop longs après avoir fourni les informations d'identification de connexion à l'aide du protocole Remote Desktop. Protocol

RSA Authentication Agent 7.2.1 mai 2015

Cette version inclut des correctifs pour les problèmes suivants :

- **AAWIN-2127** - Erreurs de codage entraînant des fichiers logs de traçage d'agent corrompus.
- **AAWIN-2161** - L'état Désactiver l'authentification déconnectée n'est pas communiqué correctement à l'API d'authentification.
- **AAWIN-2195** - RSA Control Center finit par se bloquer.
- **AAWIN-2198** - Des messages de preuve non valides s'affichent dans le fichier log du serveur.

RSA Authentication Agent 7.2.1 juin 2013

Cette version inclut des correctifs pour les problèmes suivants :

- **AAWIN-1977**. Les utilisateurs du groupe Administrateurs de domaine ne sont pas correctement authentifiés dans les conditions suivantes :
  - Le contrôleur de domaine exécute Windows 2003.
  - La version 7.1 ou 7.2 de RSA Authentication Agent pour Microsoft Windows est configurée pour authentifier tous les utilisateurs, à l'exception des administrateurs
  - Les administrateurs de domaine sont membres du groupe Administrateurs local.
- **AAWIN-2051**. Si l'agent est configuré pour authentifier un groupe de domaine volumineux, la connexion Windows pour les utilisateurs non authentifiés est très lente.
- **AAWIN-2060**. Si l'agent est configuré pour authentifier un groupe Active Directory dont la valeur sAMAccountName est différente de celle de son nom commun (cn), tous les utilisateurs doivent s'authentifier.
- **AAWIN-2067**. Si un domaine de connexion par défaut est spécifié via les stratégies de l'ordinateur local ou le registre système, l'agent ne parvient pas à récupérer le domaine correctement lors de la connexion de l'utilisateur.
- **AAWIN-2090**. Si l'agent est configuré pour utiliser l'intégration des mots de passe avec l'interface Web Citrix 5.4, la fonction d'intégration des mots de passe échoue, sauf si l'utilisateur effectue sa première authentification via une connexion Bureau à distance.

Problèmes connus

Cette section décrit les problèmes connus d'installation, d'authentification, d'authentificateur (token) et de fichier log de RSA Authentication Agent 7.4 pour Microsoft Windows. Il inclut également des solutions de contournement, le cas échéant.

Installation

Cette section répertorie les problèmes d'installation connus et leurs solutions de contournement.

L'utilisation du fichier update. exe sur la ligne de commande pour installer une mise à jour, puis sa désinstallation à partir de la ligne de commande, a échoué.
Numéro de suivi : AAWIN-2488
Problème : Si vous procédez à la mise à jour vers la version la plus récente de l'agent à l'aide de **Update*.exe** sur la ligne de commande, puis que vous désinstallez la mise à jour à l'aide du fichier **.msi** sur la ligne de commande, la désinstallation échoue.
Contournement : Procédez à la désinstallation à l'aide de la fonctionnalité d'ajout/de suppression de Windows. Ou bien, pour procéder à la désinstallation à partir de la ligne de commande, utilisez l'ID du produit au lieu du fichier **.msi**. Par exemple, msiexec /qn /x « {1CBBF615-E223-45A3-BE98-4B67EC6846DA} »

La réparation de l'agent à l'aide de l'option Programmes et fonctionnalités > Réparation rétablit l'agent vers la version précédente
Numéro de suivi : AAWIN-2493
Problème : Si vous tentez de réparer l'agent à l'aide de l'option de réparation de Programmes et fonctionnalités de Windows, la réparation rétablit l'agent vers la version précédente.
Contournement : Réparez l'agent à l'aide de la commande **.msi** normalement ou sur la ligne de commande.

Windows se bloque lorsque RSA Authentication Client 3.6 et RSA Authentication Agent (version 7.2.1 ou supérieure) sont installés sur le même hôte

Numéro de suivi : ACLT-862
Problème : Si RSA Authentication Client 3.6 et RSA Authentication Agent (version 7.2.1 ou supérieure) sont installés sur le même hôte, Windows se bloque lorsque vous vous déconnectez ou redémarrez l'hôte.
Contournement : Désactivez la vérification de la signature de code à l'aide du modèle d'objet de stratégie de groupe (GPO) RSADesktop_VerifyRSAComponents.adm inclus avec l'agent d'authentification RSA. Pour savoir comment procéder, reportez-vous au *guide de modèle d'objet de stratégie de groupe* pour la version de votre agent.

Les administrateurs locaux peuvent rencontrer une erreur irrécupérable lors de la modification de l'installation d'un agent d'authentification via le panneau de configuration Windows

Numéro de suivi : AAWIN-1909
Problème : Si l'agent d'authentification a été installé en mode silencieux, il se peut que les administrateurs locaux rencontrent une erreur irrécupérable s'ils tentent de modifier l'installation via le panneau de configuration.
Contournement : Créez un nouveau package MSI à l'aide de la commande suivante :
msiexec /qn /i « RSA Authentication Agent.msi » ADDLOCAL=ALL REINSTALLMODE=vomus REINSTALL=LAC.
Pour obtenir des instructions sur la création et le déploiement d'un package MSI, reportez-vous au chapitre 3, « Installation de RSA Authentication Agent », dans le *guide d'installation et d'administration.*

Impossible d'accéder aux mosaïques de connexion RSA SecurID si vous installez l'agent d'authentification via une connexion Bureau à distance
Numéro de suivi : AAWIN-1688
Problème : Si vous installez l'agent d'authentification à l'aide d'une connexion Bureau à distance, un utilisateur qui se connecte verra les mosaïques de mot de passe Microsoft au lieu des mosaïques RSA SecurID.
Contournement : L'utilisateur doit redémarrer l'appareil pour afficher les mosaïques RSA SecurID.

Impossible de réinstaller l'agent d'authentification dans un répertoire différent du répertoire d'installation d'origine
Numéro de suivi : AAWIN-408
Problème : Vous pouvez utiliser l'assistant de configuration (**ConfigWizard.exe**) pour créer un package MSI unique et le déployer pour plusieurs installations. Si vous souhaitez réinstaller ultérieurement le produit et que vous créez un autre module d'installation, puis l'installez dans un autre répertoire, l'installation échoue.
Contournement : Si vous avez besoin de réinstaller l'agent d'authentification, installez-le dans le même répertoire que celui que vous avez utilisé à l'origine. Vous pouvez utiliser le nom par défaut du module d'installation ou lui attribuer un autre nom. Si vous attribuez un autre nom au module d'installation, par exemple pour modifier l'application, exécutez le module à partir du même chemin d'accès que l'installation d'origine.

Un message d'erreur s'affiche au cours du processus d'installation après la première connexion à l'ordinateur
Numéro de suivi : AAWIN-359
Problème : Si vous tentez d'installer RSA Authentication Agent sur un ordinateur sur lequel vous ne vous êtes jamais connecté auparavant (en tant qu'utilisateur administrateur élevé ou utilisateur standard), un message d'erreur s'affiche et vous invite à cliquer sur **OK** pour terminer. Vous ne pouvez pas poursuivre l'installation.
Contournement : Cliquez sur **OK** pour fermer le message d'erreur. Redémarrez l'ordinateur et reconnectez-vous. Vous pouvez maintenant installer
RSA Authentication Agent.

Authentification

Cette section répertorie les problèmes d'authentification connus et les solutions de contournement, y compris l'authentification hors ligne.

L'activité réseau habituelle lance l'utilitaire d'inscription automatique sur les ordinateurs connectés à plusieurs réseaux actifs

Numéro de suivi : AAWIN-2330
Problème : L'activité réseau habituelle, par exemple les modifications d'adresse IP sur les sous-réseaux, lance l'utilitaire d'inscription automatique sur les ordinateurs connectés à plusieurs réseaux actifs. Dans la plupart des cas, certains de ces sous-réseaux doivent être ignorés aux fins de l'inscription automatique.
Contournement : Définissez une valeur de registre pour ignorer les sous-réseaux sélectionnés. Pour savoir comment procéder, consultez la section « Empêcher l'inscription automatique pour les sous-réseaux sélectionnés » dans le *guide d'installation et d'administration.*

Les utilisateurs ne peuvent pas toujours utiliser la fonction de déverrouillage rapide pour déverrouiller le système avec un code PIN RSA SecurID ou un mot de passe Windows dans une session RDP.

Numéro de suivi : AAWIN-2359, 2390
Problème : Si la fonction de déverrouillage rapide est activée, les utilisateurs qui verrouillent une session RDP sont parfois invités à déverrouiller avec un code d'accès SecurID plutôt qu'avec un code PIN SecurID ou un mot de passe Windows. Cela se produit lorsque les événements Windows qui gèrent le minuteur des déverrouillages RDP ne sont pas correctement publiés sur l'agent.
Contournement : Déverrouillez la session avec le code d'accès SecurID. Vous pouvez également configurer la stratégie **Déverrouiller l'ordinateur avec un code PIN RSA SecurID ou un mot de passe Windows** pour spécifier **l'authentification par code d'accès RSA SecurID** en tant qu'événement de démarrage de la période durant laquelle les utilisateurs pourront déverrouiller le système avec un code PIN RSA SecurID ou un mot de passe Windows.

Impossible de se connecter à Windows 8.1 après la mise à jour Windows à l'aide de l'option « Mettre à jour et redémarrer » tant que le système n'est pas redémarré une seconde fois.

Numéro de suivi : AAWIN-2355
Problème : Lorsque des mises à jour sont appliquées à certains systèmes Windows 8.1 et que le système est automatiquement redémarré, Windows verrouille le système avant que l'utilisateur n'accède au bureau après la première connexion. Lorsque cela se produit, les utilisateurs ne peuvent pas s'authentifier pour déverrouiller l'ordinateur de bureau tant que le système n'a pas été redémarré une deuxième fois.
Contournement : Appliquer une stratégie d'objet de stratégie de groupe Microsoft :

1. Ouvrez l'éditeur de stratégie de groupe approprié (gpedit.msc pour les stratégies locales ; l'outil de gestion des stratégies de groupe pour les stratégies de domaine)
2. Accédez à Configuration de l'ordinateur > Modèles d'administration > Composants Windows > Options de connexion Windows
3. Ouvrez la stratégie « Connecter le dernier utilisateur interactif automatiquement après un redémarrage du système »
4. Définissez cette stratégie sur « Désactivé »
5. Si vous définissez une stratégie de domaine, forcez une actualisation de la stratégie (par exemple, en appelant « gupdate/force »)

Les actions impliquant le contrôle du compte utilisateur (UAC) n'aboutissent pas lorsque des informations d'identification d'administrateur valides ont été fournies pour authentifier un utilisateur.

Numéro de suivi : AAWIN-2244, AAWIN-2278
Problème : Lorsque vous tentez d'effectuer des actions qui nécessitent une vérification du contrôle des comptes utilisateur, par exemple le lancement de RSA Control Center ou de Windows Command Processor avec des privilèges d'administrateur, et si la fonction d'intégration des mots de passe Windows n'est pas activée, un utilisateur doit s'authentifier en saisissant le mot de passe Windows après l'authentification réussie de RSA SecurID. Si l'utilisateur appuie sur la touche ENTRÉE après avoir fourni un mot de passe Windows valide, la tentative d'authentification UAC s'interrompt et l'action ou l'opération tentée n'aboutit pas. Les actions et les opérations réussissent lorsque des informations d'identification des administrateurs non authentifiés sont fournies.
Contournement : Activez l'intégration des mots de passe Windows pour éviter ce problème. Pour contourner ce problème, vous pouvez demander aux utilisateurs de cliquer manuellement sur **OK** après avoir fourni les informations d'identification à l'invite UAC, plutôt que d'appuyer sur la touche ENTRÉE de leur clavier.

RSA Control Center répertorie les noms NetBios (versions antérieures à Windows 2000) dans les menus déroulants des groupes Windows.

Numéro de suivi : AAWIN-2248
Problème : Lors de la configuration des groupes d'authentification dans RSA Control Center, les menus déroulants fournissent l'attribut **Nom du groupe (version antérieure à Windows 2000)** pour le groupe (SamAccountName), plutôt que l'attribut **Nom de groupe** Windows moderne (cn). Si les deux valeurs d'attribut ne sont pas identiques pour un groupe spécifique, cela entraîne des erreurs lors de la vérification des groupes d'authentification par l'agent.
Contournement : Configurez manuellement la valeur **Nom de groupe** (cn) pour le groupe d'authentification au lieu d'utiliser la valeur dans le menu déroulant.

L'agent ne détecte pas correctement l'appartenance à un groupe pour certains utilisateurs.

Numéro de suivi : AAWIN-2231, AAWIN-2223
Problème : Dans certains cas, l'agent ne reconnaît pas que les utilisateurs appartiennent à des groupes Active Directory spécifiques, même lorsque l'appartenance à un groupe peut être confirmée par le serveur d'annuaire par d'autres moyens.
Contournement : Il n'existe actuellement aucune solution de contournement pour ce problème.

Une remontée des privilèges réussie est possible avec l'authentification à deux facteurs avec un mot de passe Windows ayant expiré.
Numéro de suivi : AAWIN-2227
Problème : Si un utilisateur utilisant l'authentification à deux facteurs est verrouillé sur Windows en raison d'un mot de passe expiré, un autre utilisateur sans authentification à deux facteurs peut se connecter au système et effectuer une remontée des privilèges réussie à l'aide des informations d'identification à deux facteurs du premier utilisateur.
Contournement : Il n'existe actuellement aucune solution de contournement pour ce problème.

Lorsqu'un groupe Active Directory contient des utilisateurs provenant de plusieurs domaines, les paramètres d'authentification du groupe ne s'appliquent pas aux utilisateurs appartenant à un domaine différent du système qui exécute l'agent d'authentification.
Numéro de suivi : AAWIN-2220
Problème : Si l'agent est configuré pour authentifier tous les utilisateurs, à l'exception de ceux d'un groupe Active Directory spécifique contenant des membres de plusieurs domaines, l'agent n'authentifie pas les membres du groupe du même domaine que le système sur lequel il est installé (comme prévu), mais authentifie de manière incorrecte les membres du groupe appartenant à d'autres domaines.
Contournement : Si possible, configurez des groupes distincts contenant des membres d'un seul domaine, puis attribuez les paramètres d'authentification appropriés à chaque groupe.

Dans certains cas, l'agent n'authentifie pas les utilisateurs appartenant à des groupes d'authentification désignés.
Numéro de suivi : AAWIN-2197
Problème : Les utilisateurs appartenant à des groupes d'authentification désignés ne sont pas authentifiés par l'agent dans certains cas, lorsque le jeu de caractères utilisé par le serveur de répertoire diffère de celui utilisé par l'agent.
Contournement : Assurez-vous que l'agent et le serveur de répertoire utilisent le même jeu de caractères.

Ne peut pas s'authentifier via la mosaïque Déverrouiller avec un code d'accès pour déverrouiller l'ordinateur après l'expiration du délai de déverrouillage rapide par code PIN ou mot de passe sur l'ordinateur.
Numéro de suivi : AAWIN-2041
Problème : Si vous autorisez les utilisateurs à déverrouiller leur ordinateur en définissant le paramètre **Déverrouiller avec le code PIN RSA SecurID ou le mot de passe Windows** dans le modèle de paramètres d'authentification local, les utilisateurs peuvent déverrouiller leurs ordinateurs en saisissant leur code PIN SecurID ou leurs mots de passe Windows plutôt que des codes d'accès complets (codes PIN et codes de token), à condition qu'ils déverrouillent leurs ordinateurs avant la fin de la période d'expiration (par exemple, dans les 15 minutes). Au terme de cette période, les utilisateurs doivent saisir des codes d'accès pour déverrouiller leurs ordinateurs. Toutefois, après l'expiration du délai de déverrouillage rapide par code PIN ou mot de passe, la mosaïque Déverrouiller n'invite pas l'utilisateur à saisir un code d'accès. Cela empêche l'utilisateur de déverrouiller l'ordinateur avec la mosaïque de déverrouillage rapide par code PIN ou mot de passe.
Contournement : Activez l'écran **Ctrl+Alt+Suppr** via les paramètres Stratégie de groupe pour éviter que ce problème ne survienne. Les utilisateurs peuvent également cliquer sur **Annuler** et sélectionner à nouveau la mosaïque Déverrouiller pour afficher l'invite de code d'accès.

RSA Control Center affiche de manière incorrecte le nombre de jours disponibles en mode hors ligne après la première authentification d'un utilisateur à partir d'un ordinateur sans la fonction d'inscription automatique.
Numéro de suivi : AAWIN-1894
Problème : Le champ Jours en mode hors ligne affiche les jours disponibles en mode hors ligne sous la forme d'un nombre et d'un graphique à barres. Après l'authentification d'un utilisateur pour la première fois sur un appareil où la fonction d'inscription automatique n'est pas installée, le graphique à barres indique qu'aucun jour en mode hors ligne n'est disponible, ce qui est incorrect. La valeur numérique s'affiche correctement. Cela n'affecte pas l'authentification.
Contournement : Pour que le graphique à barres affiche correctement les jours disponibles en mode hors ligne, demandez aux utilisateurs de s'authentifier à nouveau. RSA Control Center affiche correctement les jours disponibles en mode hors ligne après la ré-authentification.

Les utilisateurs avec des codes d'accès fixes ne peuvent pas actualiser les jours en mode hors ligne à partir de RSA Control Center
Numéro de suivi : AAWIN-1855
Problème : Les utilisateurs ayant des codes d'accès fixes ne peuvent pas actualiser les jours en mode hors ligne à partir de RSA Control Center.
Solution : N'émettez pas de code d'accès fixe pour les utilisateurs qui nécessitent une authentification hors ligne.

Les utilisateurs authentifiés devront peut-être se déconnecter et s'authentifier à nouveau s'ils ont modifié leur mot de passe Windows et souhaitent déverrouiller le système avec un code PIN RSA SecurID
Numéro de suivi : AAWIN-1791
Problème : Les administrateurs peuvent autoriser les utilisateurs authentifiés à déverrouiller leur ordinateur à l'aide de leur code PIN au lieu de leur code d'accès. Les administrateurs peuvent définir cette option dans la stratégie de groupe. Si les utilisateurs modifient leur mot de passe Windows après s'être connectés, puis verrouillent leur ordinateur, ils ne peuvent pas déverrouiller leur ordinateur avec leur code PIN.
Contournement : Les utilisateurs doivent se déconnecter de leur ordinateur et s'authentifier à l'aide de leur code d'accès afin de pouvoir à nouveau déverrouiller leurs ordinateurs à l'aide de leur code PIN.

Lorsque vous cliquez sur Effacer pour effacer les données hors ligne, le bouton Effacer ne se modifie pas comme prévu.
Numéro de suivi : AAWIN-664
Problème : Lorsque vous cliquez sur Effacer dans la section Données hors ligne du RSA Control Center, le bouton **Effacer** ne change pas d'apparence pour indiquer que les données hors ligne ont été effacées. Toutefois, les données hors ligne sont effacées.
Contournement : Aucun.

L'agent Windows ne gère pas correctement la stratégie d'authentification hors ligne qui oblige un utilisateur à saisir un code d'accès d'urgence après avoir atteint le nombre limite d'échecs hors ligne spécifié dans la stratégie.
Numéro de suivi : AAWIN-635
Problème : Lorsque vous configurez la stratégie d'authentification hors ligne pour obliger l'utilisateur à saisir un code d'accès d'urgence après un certain nombre d'échecs hors ligne, l'utilisateur est invité à saisir un code d'accès d'urgence lorsqu'il atteint la moitié du nombre d'échecs spécifié dans la stratégie.
Contournement : Doublez le nombre d'échecs hors ligne autorisés avant que les utilisateurs ne soient invités à saisir un code d'accès d'urgence dans la stratégie d'authentification hors ligne.

Plusieurs invites d'authentification s'affichent lors de l'accès à un ordinateur distant utilisant l'authentification au niveau du réseau
Numéro de suivi : AAWIN-564
Problème : Remote Desktop Connection 6.1 inclut l'authentification Windows NLA (Network Level Authentication). Si cette fonction est activée lorsque vous tentez de vous connecter à un ordinateur distant, vous êtes invité à vous authentifier pour pouvoir établir une connexion à distance. Si vous utilisez NLA avec un fournisseur d'informations d'identification RSA SecurID configuré sur l'ordinateur distant, deux messages d'invite s'affichent pour que vous puissiez accéder au bureau à distance. Une invite s'ouvre à partir de l'ordinateur local et l'autre s'ouvre à partir de l'ordinateur distant. Il s'agit d'une limitation de la mise en œuvre de l'authentification par Microsoft au niveau du réseau lorsque vous utilisez un fournisseur d'informations d'identification tiers. Après avoir saisi les informations de votre compte et réussi à vous authentifier via chaque invite, vous pouvez accéder à l'ordinateur distant.

Remarque : L'authentification au niveau du réseau est activée par défaut pour les systèmes d'exploitation Windows 7 ou version supérieure. Pour plus d'informations sur l'authentification au niveau du réseau, consultez le site Web de Microsoft.

Contournement : Vous pouvez l'adresser partiellement en configurant le modèle GPO **Connexion avec des informations d'identification des applications distantes**. Cette stratégie empêche l'affichage de l'invite d'authentification des utilisateurs authentifiés en passant par les noms d'utilisateur. Elle empêche également l'affichage de la seconde invite d'authentification pour les utilisateurs non authentifiés.

La boîte de dialogue Définir un nouveau code PIN RSA SecurID s'ouvre après la boîte de dialogue UAC (User Account Control)
Numéro de suivi : AAWIN-307
Problème : Vous vous connectez à un ordinateur avec des informations d'identification locales, mais vous avez besoin d'accéder à une application qui nécessite des privilèges élevés. Si vous devez utiliser un compte administrateur qui nécessite un code d'accès RSA SecurID et que vous n'avez pas créé votre code PIN RSA SecurID, l'agent d'authentification vous invite à en créer un. Toutefois, vous ne pourrez pas accéder aux champs de la boîte de dialogue Définir un nouveau code PIN RSA SecurID, car celui-ci s'ouvre après la boîte de dialogue de connexion UAC Windows.
Contournement : Déplacez la boîte de dialogue Définir un nouveau code PIN RSA SecurID derrière la boîte de dialogue de connexion UAC Windows. Vous pourrez alors accéder aux sélections et aux champs et définir votre code PIN.

Authentificateur (token)

Cette section répertorie les problèmes connus de l'authentificateur (token RSA SecurID 800) et les solutions de contournement.

L'icône RSA Control Center peut ne pas afficher correctement l'état d'un RSA SecurID 800 connecté
Numéro de suivi : AAWIN-1953
Problème : L'icône RSA Control Center indique que l'application reconnaît un authentificateur connecté au port USB en affichant une croix bleue dans le coin supérieur droit de l'icône. Si RSA Authentication Client et RSA Local Authentication Client sont installés et que vous supprimez RSA Authentication Client sur un ordinateur 64 bits, la croix bleue peut ne pas s'afficher lorsque l'utilisateur se connecte à un authentificateur.
Contournement : Supprimez et réinstallez RSA Authentication Client sur un ordinateur 64 bits pour réparer l'agent d'authentification RSA.

Les tokens RSA SecurID 800 peuvent rencontrer des problèmes de connectivité USB intermittents
Numéros de suivi : AAWIN-1859
Problème : Les tokens RSA SecurID 800 disposent d'un code de fabrication situés à l'arrière, sous le numéro de série. Les codes de fabrication commencent par A, C ou D et les lettres sont généralement suivies d'un chiffre. Des problèmes de connectivité USB intermittents peuvent se produire avec des tokens codés A, A2, A8 et A9.
Contournement : Supprimez le token RSA SecurID 800 et réinstallez-le. Connectez le RSA SecurID 800 directement à un port USB sur l'ordinateur plutôt qu'à un adaptateur ou à un câble d'extension. Les utilisateurs peuvent également s'authentifier en saisissant leur code PIN et code de token sans connecter leur RSA SecurID 800 à un port USB.

Les données hors ligne ne sont pas téléchargées et le service de l'agent d'authentification RSA hors ligne local s'interrompt si vous vous connectez avec plusieurs tokens, l'un après l'autre.
Numéro de suivi : AAWIN-650
Problème : Si vous attribuez trois tokens à un utilisateur et que vous activez l'authentification hors ligne avec RSA Authentication Manager 7.1 SP4, l'utilisateur peut s'authentifier avec le premier token et les données seront téléchargées hors ligne. Lorsque l'utilisateur se déconnecte et tente de s'authentifier avec les autres tokens, il s'authentifie correctement, mais les données hors ligne ne peuvent pas être téléchargées et le service d'authentification local hors ligne de l'agent d'authentification RSA s'interrompt. Ce problème se produit uniquement sur RSA Authentication Manager 7.1 SP4.
Contournement : N'attribuez pas plus d'un token à un utilisateur qui doit s'authentifier hors ligne.

Fichiers log

Cette section répertorie les problèmes relatifs aux fichiers logs connus et leurs solutions de contournement.

Redémarrez l'ordinateur si vous modifiez le niveau de traçage ou l'emplacement d'écriture des fichiers de traçage créés par Control Center.
Numéro de suivi : AAWIN-1933
Problème : RSA Control Center peut créer des fichiers logs de traçage pour résoudre ces problèmes. En règle générale, vous n'activez pas le suivi à moins d'y être invité(e) par le Support client RSA. Si vous modifiez le niveau de traçage, par exemple, de Verbose à Erreur, vous devrez redémarrer l'ordinateur pour que la modification soit prise en compte. En outre, vous devez redémarrer l'ordinateur si vous modifiez l'emplacement où les fichiers de traçage sont créés.
Contournement : Redémarrez votre ordinateur si vous modifiez le niveau de traçage ou l'emplacement où les fichiers de traçage sont créés. Pour plus d'informations, consultez « Activer le traçage » dans le *guide d'installation et d'administration*.

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.

Marques commerciales

RSA, le logo RSA, SecurID et EMC sont des marques déposées ou commerciales de Dell Inc. dans le monde entier. Toutes les autres marques citées dans le présent document 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**.

Clause de propriété intellectuelle

Ce logiciel contient la propriété intellectuelle de Dell Inc. ou est concédé sous licence à Dell Inc. par des tiers. L'utilisation de ce logiciel et la propriété intellectuelle incluse sont expressément limitées aux conditions générales du contrat de licence aux termes duquel le logiciel a été fourni par ou au nom de Dell Inc.

Licence Open Source

Ce produit peut être distribué avec un code Open Source qui vous est octroyé sous licence conformément à la licence Open Source applicable. Si vous souhaitez obtenir une copie du code source, adressez-vous à EMC qui vous la fournira, selon les termes de la licence Open Source applicable. EMC peut prélever les frais de gestion et d'expédition jugés raisonnables pour cette distribution. Envoyez une demande écrite au département juridique d'EMC Computer Systems France, River Ouest, 80 Quai Voltaire, CS21002, 95876 Bezons CEDEX, à l'attention du Service juridique.