Release Notes
RSA Authentication Agent 7.4.2 for Microsoft Windows

December 2018

Introduction

This document lists what's new in RSA® Authentication Agent 7.4.2 for Microsoft Windows. It also includes workarounds for known issues. Read this document before installing the software. This document contains the following sections:

These *Release Notes* may be updated. The most current version can be found on RSA Link at **https://community.rsa.com/**.

What's New in This Release

This section lists the new features and enhancements that are introduced in RSA Authentication Agent for Microsoft Windows.

Version 7.4.2, December 2018

The following updates were introduced in RSA Authentication Agent 7.4.2, released in December 2018:

Functionality. This release supports specifying selected subnets to include in auto registration.

Bug Fixes. For more information, see RSA Authentication Agent 7.4.2 December 2018 on page 8.

Version 7.4, September 2018

The following updates were introduced in RSA Authentication Agent 7.4, released in September 2018:

Support. This release is qualified with Windows Server 2016, Data Center edition (Server Core).

Functionality:

- This release supports the Windows V2 Credential Provider. This conforms to the logon UI experience introduced in Windows 8 and also automatically respects the Windows definitions for custom images.
- Ability to specify custom text when collecting RSA SecurID Credentials or the Windows password.
- Ability to not display a separate message when the Windows password is not available.
- Support for custom images for the RSA credential tiles for a handheld or connected authenticator
- Ability to not use a connected authenticator in Remote Desktop sessions

- Ability to encrypt Active Directory LDAP requests

Bug Fixes. For more information, see RSA Authentication Agent 7.4 September 2018 on page 9.

Version 7.3.3, June 2017

The following updates were introduced in RSA Authentication Agent 7.3.3, released in June 2017:

Functionality:

- The agent now can support multiple Remote Desktop applications, in addition to Microsoft's "Remote Desktop Connection". For more information, see RSA Authentication Agent 7.3.3 June 2017 on page 7.
- Added the option to configure the RSA Credential Provider credential tile to use the standard Windows image for Windows 7 and Server 2008.

Bug Fixes. For more information, see RSA Authentication Agent 7.3.3 June 2017 on page 9.

Version 7.3.2, February 2017

The following updates were introduced in RSA Authentication Agent 7.3.2, released in February 2017:

Support. This release officially supports Windows Server 2016.

Functionality. The agent now accepts credentials from remote applications such as Citrix® XenApp® and Microsoft Remote Desktop Connection, so that users who are not required to authenticate with RSA SecurID do not need to enter credentials twice when using those applications.

Bug fixes. For more information, see RSA Authentication Agent 7.3.2 February 2017 on page 10.

Version 7.3.1, June 2016

The following updates were introduced in RSA Authentication Agent 7.3.1, released in June 2016:

Functionality. The agent now includes GPO template files in **.admx/.adml** format, which is required when importing files to the group policy Central Store.

Bug fixes. For more information, see RSA Authentication Agent 7.3.1 June 2016 on page 10.

Version 7.3, May 2016

The following updates were introduced in RSA Authentication Agent 7.3, released in May 2016:

Support. This release officially supports Windows 10. RSA Authentication Agent 7.3 and later versions are not compatible with RSA Authentication Client 3.6 on Windows 10.

Note: Compatibility issues exist between RSA Authentication Client 3.6 and RSA Authentication Agent 7.2.1 or later. For details, see Known Issues.

Functionality. The agent now communicates using TLS 1.2 protocols if supported by the RSA Authentication Manager server.

Bug fixes. For more information, see RSA Authentication Agent 7.3 May 2016 on page 10.

Important: Fully read the next section, Installing This Product before performing the installation.

Version 7.2.1, May 2015

The following updates were introduced in RSA Authentication Agent 7.2.1, released in May 2015:

Functionality. A Preserve History mode is added to show the last successful authentication when a user logs on.

Bug fixes. For more information, see RSA Authentication Agent 7.2.1 May 2015 on page 11.

Version 7.2.1, June 2013

The following updates were introduced in RSA Authentication Agent 7.2.1, released in June 2013:

Performance. The digital signature verification process performance has been enhanced.

Bug fixes. For more information, see RSA Authentication Agent 7.2.1 June 2013 on page 11.

Version 7.2

The following updates were introduced in RSA Authentication Agent 7.2:

Support for Windows 8 and Windows Server 2012. Authentication Agent supports Windows 8 and Windows Server 2012 (in Server Core or Server with GUI mode). If you use Windows Server in Server Core mode, you do not use a user interface. You must install the application from the command line. You can switch between "Server Core" and "Server with GUI" mode after installing Authentication Agent and use it the same way. For more information, see the *Installation and Administration Guide*.

Support for new Microsoft Credential Providers. The **RSACredProviderFilter_Microsoft** Group Policy Object (GPO) template now supports the Picture Password, PIN (for Microsoft Live ID), and Microsoft Live ID Credential Providers in addition to the Password and Smart Card Credential Providers. For more information, see the *Group Policy Object Template Guide*.

Requires Microsoft .NET Framework 4 Client Profile or .NET Framework 4.5. RSA Authentication Agent 7.2 (and later versions) for Microsoft Windows requires Microsoft .NET Framework 4 Client Profile or .NET Framework 4.5. Windows 8 and Windows Server 2012 come with .NET Framework 4.5 already installed. If you plan to use Windows 7 or Windows Server 2008, you must install Microsoft .NET Framework 4 Client Profile before you install RSA Authentication Agent. To download the .NET Framework 4 Client Profile, see this Microsoft web site: **www.microsoft.com/en-us/download/details.aspx?id=24872**.

Installing This Product

Important: If you intend to upgrade from a previous version of RSA Authentication Agent for Microsoft Windows to version 7.4, you must check your current pre-installation challenge settings. If the selected challenge group has a sAMAccountName value different than its Common Name, the challenge settings after installation may be incorrect. To correct these setting post-installation, use the RSA Control Center to reconfigure the challenge settings.

This package provides installers and Group Policy Object templates in the following zip files:

- **RSA_Authentication_Agent_7.4.zip** (which contains the installers and other supporting files for 32-bit and 64-bit platforms)
- **RSA_GPO_AuthAgent_74.zip** (which contains the Group Policy Object templates)

Procedure:

1. Log on to the computer as an Administrator.
2. Extract the **RSA_Authentication_Agent_7.4.zip** file to a local folder.
3. Locate the .msi file appropriate for the machine architecture. The .msi files are in the following locations:
   - For 32-bit platforms, **x32\RSA Authentication Agent.msi**.
   - For 64-bit platforms, **x64\RSA Authentication Agent x64.msi**.
4. If you are updating any version prior to RSA Authentication Agent for Windows 7.2, or if you are performing a new installation of RSA Authentication Agent for Windows 7.4, click the appropriate .msi file.
5. If you are updating an installation of RSA Authentication Agent for Windows 7.2 or later to RSA Authentication Agent for Windows 7.4:
   a. Open a command line window.
   b. Navigate to the folder that contains the .msi file that you want to install.
   c. At the command prompt, type
   msiexec /i “<yourarchitecture.msi>” REINSTALL=ALL REINSTALLMODE=vomus
6. When the installation completes, reboot the computer.

Product Usage Recommendations

This section contains recommendations intended to ensure proper operation of the Authentication Agent.

- The "Server" and "Workstation" Windows services should be running at all times. If an interruption affects the services, instruct users to restart their computers to restart the processes.
- Users who are in New PIN or Next Tokencode mode should complete the dialogs promptly. If the New PIN or Next Tokencode dialog times out, instruct users to press CTRL+ALT+DEL to start over.
- Perform push installations as instructed in the *Installation and Administration Guide*. For example, use Microsoft Systems Management Server (SMS) to push the MSI silently to users' computers. Performing a push operation through a Remote Desktop session is not recommended.
- Do not add alternate IP addresses to the Agent host record in the Authentication Manager server if you are using Auto-Registration.

Interoperability with RSA Authentication Agent for Web for IIS

RSA Authentication Agent 7.4 for Microsoft Windows and RSA Authentication Agent for Web for IIS both make use of the RSA Authentication API. In order to communicate with RSA Authentication Manager, the RSA Authentication API requires configuration files and a node secret. The Authentication Agent for Windows and the Authentication Agent for Web store these files in different locations. For both Agents to communicate with Authentication Manager, these files must always be the same in both locations.

The configuration files and node secret are stored in the following locations:

- Authentication Agent for Windows installations: **<<Program Files>>\Common Files\RSA Shared\Auth Data**
- Authentication Agent for Web installations: **<<Windows>>\System 32**

If you use the Node Secret Load utility, you can load the node secret into both locations. If the node secret is auto-generated during the test authentication with either the Authentication Agent for Windows or Authentication Agent for Web, you must copy the node secret to the other Agent's location.

The Authentication Agent for Windows and the Authentication Agent for Web share registry keys located under the following Windows registry settings:
HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT. The settings located here are used to control trace logging and IP address override. Both Agents use the same registry location, and the default registry settings are installed by whichever product is installed first. Because the settings are shared, a setting modified with one product is automatically reflected in the other product. For example, if you change the IP address override using the RSA Control Center of the Authentication Agent for Windows, it is not necessary to make the change using the Authentication Agent for Web Control Panel application. Additionally, the shared settings are not removed when you remove either product. If you remove both products, you should manually delete the registry settings.

RSA recommends that you use the following procedure to install and use both Windows and Web Agents on a single computer.

Before You Begin

The format of the node secret has recently been changed. The Authentication Agent for Windows expects the node secret to be in the new format. For interoperability, the version of the Authentication Agent for Web that you install must also use the new format. RSA Authentication Agent for Web 7.4 uses the new node secret format. If you are installing an earlier version of the Authentication Agent for Web, contact RSA Customer Support (**www.emc.com/support/rsa/index.htm**) to obtain the appropriate patch to support the new node secret format.

To install Authentication Agent for Windows and Authentication Agent for Web for interoperability:

1. Install the Authentication Agent for Web and perform a test authentication as described in the *RSA Authentication Agent for Web for IIS Installation and Configuration Guide*.
2. Install the Authentication Agent for Windows as described in the *RSA Authentication Agent for Microsoft Windows Installation and Administration Guide*.

Important: Do not attempt a test authentication using the Authentication Agent for Windows until you complete the following step.

3. Open a command prompt and then use the **XCOPY** command with the /O option to copy the node secret from **<<Windows>>\System32** to **<<Program Files>>\Common Files\RSA Shared\Auth Data**. The /O option specifies that ownership and Access Control List (ACL) information should also be copied, as shown in the following example:

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

   Important: Do not use the **COPY** command or Windows Explorer to copy the node secret file. Due to the sensitivity of the node secret, you must also copy ownership and ACL information.

4. Perform a test authentication of the Authentication Agent for Windows as described in the *RSA Authentication Agent for Microsoft Windows Installation and Administration Guide.*

Interoperability with Systems Secured by RSA Ready Partner Solutions

If you are using RSA Authentication Agent 7.4 for Microsoft Windows on a system that is part of the RSA Ready partner solution program, visit the RSA Ready site at **www.rsaready.com**. The site includes implementation guides and information on usability and compatibility.

Package Contents

RSA Authentication Agent is available at **https://community.rsa.com/community/products/securid/authentication-agent-windows**.

The RSA Authentication Agent 7.4 product folder contains:

File or Folders	Description
Configuration Wizard	This folder contains the **ConfigWizard.exe** file you can use to customize the installer and deploy it to multiple computers.
x86 and x64	These folders contain Windows Installer Packages for local installation of RSA Authentication Agent 7.4 on 32-bit and 64-bit computers.
Language Packs	This folder contains the Japanese language packs you install after installing the English version of the product. If you install the Japanese language pack (after installing the standard English version of the product) and you use a Japanese operating system, the user interface and Help are displayed in Japanese. For more information, see the *Installation and Administration Guide*.
Licenses	This folder contains the RSA License Agreement (RSA_License_Agreement.doc).
Policy Templates	This folder contains the Group Policy Object (GPO) administrative templates for managing authentication settings. This folder includes templates in both **.admx**/.**adml** format and the older **.adm** format. The new template files are located in the **Policy Templates\admx** folder.

File or Folders	Description
Node Secret Load Utility	This folder contains the Node Secret Load utility (**agent_nsload.exe**), which you can use to securely copy the node secret from an Authentication Manager server to an Authentication Agent computer before you use RSA SecurID authentication. **Note:** The Node Secret Load utility is not required for establishing a node secret. For more information, see the *Installation and Administration Guide*.

Documentation and Application Help

The product documentation is available from the following location:

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

Documentation

Title	Filename
RSA Authentication Agent 7.4 for Microsoft Windows Installation and Administration Guide	**auth_agent_install_admin_guide.pdf**
RSA Authentication Agent 7.4 for Microsoft Windows Group Policy Object Template Guide	**auth_agent_gpo_template_guide.pdf**

The following Help installs with RSA Authentication Agent 7.4 for Microsoft Windows.

Application Help

Title	Filename
RSA Authentication Agent (RSA SecurID) Help	The Help is accessed from the RSA Control Center.
(Japanese) RSA Authentication Agent (RSA SecurID) Help	The Help is accessed from the RSA Control Center. If you install the Japanese language pack (after installing the standard English version of the product) and you use a Japanese operating system, the user interface and Help are displayed in Japanese.

New Features and Enhancements

RSA Authentication Agent 7.4.2 December 2018

Specify Selected Subnets to Include in Auto Registration

This release allows you to specify selected subnets to include in auto registration using the IncludeNetworkMasks option.

RSA Authentication Agent 7.4 September 2018

Windows 2016 Data Center Edition (Server Core) Support

This release is qualified with Windows Server 2016, Data Center edition (Server Core).

Windows V2 Credential Provider Support

This release supports the Windows V2 Credential Provider. This conforms to the logon UI experience introduced in Windows 8 and also automatically respects the Windows definitions for custom images.

New Features to Control Text, Images, Remote Desktop connections, and Encryption

The Authentication Agent now supports the following:

- Ability to specify custom text when collecting RSA SecurID Credentials or the Windows password.
- Ability to not display a separate message when the Windows password is not available.
- Support for custom images for the RSA credential tiles for a handheld or connected authenticator
- Ability to not use a connected authenticator in Remote Desktop sessions
- Ability to encrypt Active Directory LDAP requests

You can enable these features with new Group Policy Object templates. For more information, see the *Group Policy Object Template Guide*.

RSA Authentication Agent 7.3.3 June 2017

Multi-app Support in RDC Application policy

The Local Authentication Settings - Remote Desktop Connection Application policy in the RSA Authentication Agent GPO now accepts a comma-delimited list of applications to exclude from RSA SecurID authentication. This can be used to prevent RSA SecurID authentication from being applied to Remote Desktop applications such as Microsoft's "Remote Desktop Connection Manager" when the agent is installed on a system that serves as a jump host. For more information, see the *Group Policy Object Template Guide*.

Credential Provider Image

Authentication prompts by the agent can now be configured to display the Windows credential image rather than the RSA SecurID image on Windows 7 and Server 2008 machines.

RSA Authentication Agent 7.3.2 February 2017

Windows Server 2016 Support

This release officially supports Windows Server 2016.

Streamlined Authentication for Citrix XenApp and Remote Applications

This feature allows the Agent to accept credentials from remote applications such as Citrix XenApp and Microsoft Remote Desktop Connection, so that users do not need to enter credentials twice when using those applications unless an RSA SecurID tokencode or passcode is required.

This feature is disabled by default. To enable the feature, you use a Group Policy Object. For instructions, see the *Group Policy Object Template Guide.*

RSA Authentication Agent 7.3.1 June 2016

GPO Templates in .admx/.adml Format

Authentication Agent 7.3.1 includes GPO templates in **.admx**/**.adml** format in addition to the older **.adm** format. The new template format is required when importing files to the group policy Central Store. The new template files are located in the **Policy Templates\admx** folder.

RSA Authentication Agent 7.3 May 2016

Windows 10 Support

This release officially supports Windows 10.

Note: Compatibility issues exist between RSA Authentication Client 3.6 and RSA Authentication Agent 7.2.1 or later. For details, see Known Issues.

Authentication Agent 7.3 Uses TLS 1.2 Mode When Supported by the Authentication Manager Server

Authentication Agent 7.3 is part of the TLS 1.2 Mode update for RSA Authentication Manager, which helps support security best practices and regulatory compliance by using the TLS 1.2 cryptographic protocol for secure network communications within your RSA Authentication Manager 8.1 SP1 environment.

You do not need to configure the agent to use TLS 1.2 Mode. If the Authentication Manager server supports TLS 1.2 communication, then the agent uses TLS 1.2 Mode by default. If TLS 1.2 Mode is not supported, the agent uses SSLv3 communication instead.

To support TLS 1.2 communication, you must install the TLS 1.2 Mode update (Authentication Manager 8.1 SP1 Patch 13) or a later update on the Authentication Manager server, and enable TLS 1.2 Mode using a configuration script. For instructions, see the *TLS 1.2 Mode Update and Configuration Guide for RSA Authentication Manager 8.1 SP1.*

RSA Authentication Agent 7.2.1 May 2015

Preserve History Mode Displays Last Successful Authentication

Defect AAWIN-2168 prevented display of information at logon about previous successful and failed log ons. This issue is addressed by providing two operating agent modes:

The **Do Not Preserve History** (default) mode enables display of descriptive authentication failure messages to users during log on but does not preserve failed authentication history for display at successful log on, when Windows is configured to show last interactive log on information.

The **Preserve History** mode returns a generic authentication failure message in response to a failed authentication attempt during log on but correctly shows the number of failed authentication attempts within Windows last interactive log on information.

The two modes of agent execution are configured by a new GPO template.

RSADesktop_PreserveFailedAuthHistory

This template is provided in the "Policy Templates" portion of the kit.

Use "gpedit.msc" to install the new gpo template. Invoke the GPO for configuring the Agent. The presentation of choices for Mode, are the following for response to:

Preserve Failed Auth History:

1. Do Not Preserve Auth History

2. Preserve History

To direct the agent to run in default mode:

Select "Do Not Preserve Auth History."

To correct the behavior described in the Jira defect AAWIN-2168:

Select "Preserve History" Be sure to "Apply" selections.

After applying the selection, "Preserve History", all subsequent, failed logon attempts will be recorded with Windows for correct display, at successful logon when Windows is configured according to:

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

Important: The server must be running at the Windows Server 2008 domain functional level or more recent level before configuring for last interactive logon. If the server is not configured to run at one of these levels, users, including the administrator, will be locked out from logging on to their desktops.

Fixed Issues

RSA Authentication Agent 7.4.2 December 2018

This release includes corrections for the following issues:

- **AAWIN-2482** - The Windows Agent times out more quickly when Active Directory is unreachable.
- **AAWIN-2504** - The installer no longer writes a registry value that prevented Cisco AnyConnect from “wrapping” the RSA Credential Provider.
- **AAWIN-2509** - If users connect to a Windows 10 Version 1709 machine in a Remote Desktop Connection session, disconnect the session, and then re-connect the session, they are now prompted for RSA SecurID passcode and a password, instead of only a password or an RSA SecurID PIN.
- **AAWIN-2510** - Improvements have been made to reduce the time needed to perform offline authentication in order to avoid blocking logon or unlock.

RSA Authentication Agent 7.4 September 2018

This release includes corrections for the following issues:

- **AAWIN-2313** - A Windows 10 user is now prompted for a PIN right after the user inserts the smart card.
- **AAWIN-2286** - On Windows 10, the order of displayed user tiles is now determined by Microsoft Windows.
- **AAWIN-2301** - Quick Unlock now displays a name for the logged-on user's deselected credential tile in Windows 10 console sessions.
- **AAWIN-2385**, **AAWIN-2209, AAWIN-2040, and AAWIN-2101** - You can now add a custom image to replace the RSA image when an RSA credential tile is displayed. You specify this custom image using a Group Policy Object template.
- **AAWIN-2315** - If a user logs into a Windows host protected by the agent and attempts to connect to another Windows system using Microsoft Remote Desktop Connection that is not protected by the agent, the user is now prompted for Windows username and password.
- **AAWIN-2457** - User in special challenge group is now challenged.
- **AAWIN-2426** - The interface ping can be disabled if offline authentication is slow.
- **AAWIN-2441** - Updated the time used to determine whether the proof of authentication is valid.
- **AAWIN-2436** - RSA Credential Provider marks the "Other User" credential tile as the default tile.
- **AAWIN-2429** - The 90-second delay for password unlock on disconnected systems has been fixed.
- **AAWIN-2421** - The Windows Agent now recognizes an additional error status from the server for invalid proof error.
- **AAWIN-2395** - Users can now unlock on Windows 10 when an Active Directory password must change.
- **AAWIN-2222** - Windows password integration works if the password contains special characters such as åäöÅÄÖ. The code now sends and receives the user's password as UTF-8 rather than the system default character set.
- **AAWIN-2392** - The auto-registration service now properly closes all handles used to register IP address changes with the server.
- **AAWIN-2384** - When the Offline Authentication Service queues users for offline data download, it now excludes users whose proof of authentication had expired.
- **AAWIN-2369** - Users can log onto desktops if their Windows passwords must be changed during logon on Windows 10 (Anniversay Update) or Windows Server 2016.
- **AAWIN-2339** - If a user is enabled for offline authentication and successfully authenticates through UAC, the authentication succeeds and the offline data is now downloaded.

RSA Authentication Agent 7.3.3 June 2017

This release includes corrections for the following issues:

- **AAWIN-2343** - The **sdconf.rec** file now correctly syncs with the primary and replica instances used by a server accepting only TLS 1.2 connections when the machines are physically moved and reconnected to the network.
- **AAWIN-2347** - RSA Quick Unlock authentication now performs correctly when a system locks because the Microsoft group policy “Interactive Logon: Machine Inactivity Limit” has been configured.

- **AAWIN-2368** - Remote authentication for the built-in domain account named “Administrator” now runs as expected.
- **AAWIN-2370** - Offline authentication data now successfully updates after an upgrade.
- **AAWIN-2371** - The authentication agent now properly maintains auto-registration after an upgrade.
- **AAWIN-2383** - The authentication agent no longer intermittently generates errors when administration credentials are entered for an application in Windows with UAC enabled.

RSA Authentication Agent 7.3.2 February 2017

This release includes corrections for the following issues:

- **AAWIN-2333** - After successfully logging onto the Agent host from a Windows computer using Remote Desktop Protocol, then subsequently locking the screen during the session, users were unable to unlock the Agent host again because the lock screen did not display any RSA SecurID Credential Provider logon options.
- **AAWIN-2328** - Login delays up to 30 seconds occurred on Windows 2012 R2 using Read-Only Domain Controllers.
- **AAWIN-2325** - All Authentication Agent hosts refreshed offline data simultaneously, which caused overwhelming server load in very large deployments.
- **AAWIN-2322** - The Authentication Agent used the local challenge cache to determine challenge status rather than challenging all users by default when the domain controller was not available.
- **AAWIN-2320** - The Authentication Agent was susceptible to vulnerabilities described in **CVE-2016-0923** and **CVE-2016-0924**.
- **AAWIN-2318** - In certain deployments, the **da_svc.exe** offline service crashed and caused slow authentication.
- **AAWIN-2309** - The auto-registration service did not retry registration if all servers were unreachable.
- **AAWIN-2299** - Quick Pin Unlock did not work when a user logged in using a Fully-Qualified Domain Name (FQDN).
- **AAWIN-2293** - Users belonging to challenge groups that included an FQDN received the error message “You are not authorized to access offline data/authentication” when attempting offline authentication, even when offline days existed on the user’s computer.

RSA Authentication Agent 7.3.1 June 2016

This release includes corrections for the following issues:

- **AAWIN-2295** - The Authentication Agent cannot determine the challenge group to which a user belongs if the user submits a fully qualified domain name (such as yourdomain.local/username) in the username field.
- **AAWIN-2287** - On Windows Server 2012 R2, when Challenge Mode policy is set to either a group of users, or all users except a certain group, logon takes longer than expected.
- **AAWIN-2284** - A windows 7 user can change an account password only for the domain under which the account is currently logged on.
- **AAWIN-2271** - Logon takes longer than expected for non-challenged users that belong to multiple groups in an identity source.
- **AAWIN-2254** - The Authentication Agent includes GPO template files in **.adm** format, but not **.admx/.adml** format, which is required when importing files to the group policy Central Store.
- **AAWIN-2246** - When Quick PIN Unlock is enabled on Windows 10 systems, challenged users are prompted for RSA SecurID Passcode on the unlock screen, rather than PIN. When logging on over a Remote Desktop Protocol connection, Quick PIN Unlock works normally.

RSA Authentication Agent 7.3 May 2016

This release includes corrections for the following issues:

- **AAWIN-2243** - After installing the agent on Windows 10, the user-specific tiles that are normally displayed on the logon screen for individual user accounts are replaced by a single, generic RSA SecurID logon tile.
- **AAWIN-2221** - If a challenged domain user's account is set to require password change after the user has already logged into Windows and re-locked the system, that user becomes unable to reset the password and login again.
- **AAWIN-2206** - sdconf.rec can become corrupted.
- **AAWIN-2194** - When users get locked out due to incorrect passcode entry when not connected to the network, they must enter the offline emergency token and passcode twice to log in.
- **AAWIN-2193** - Successful online authentication does not clear offline account lockout status.
- **AAWIN-2188** - Unlock functionality does not work if the Windows policy **Interactive Logon: Display user information when the session is locked** is set to anything other than **User display name, domain and user names**.
- **AAWIN-2185** - Users cannot download offline data to offsite Windows systems.
- **AAWIN-2183** - The **Refresh** button on the Refresh Offline Days page in RSA Control Center does not work.
- **AAWIN-2181** - The Offline Authentication Service crashes when the token count is greater than three.
- **AAWIN-2168** - The **Display information about previous logons** option in Windows does not work when RSA Authentication Agent for Windows is installed.
- **AAWIN-2147** - LogonUI.exe encounters a fault when calling DASvcAPIWrapper.DLL.
- **AAWIN-2135** - On Windows 8 systems, RSA Authentication Agent prompts for PIN after Quick PIN Unlock has timed out.
- **AAWIN-2123** - Automatic Password Synchronization does not work consistently.
- **AAWIN-2108** - Exempting a local group that contains a domain local security group does not work.
- **AAWIN-2107** - The Windows Security Log displays an audit failure message if a user does not have permission to log in locally, and logs on using Terminal Services.
- **AAWIN-2102** - Users experience lengthy authentication delays after providing login credentials using Remote Desktop Protocol.

RSA Authentication Agent 7.2.1 May 2015

This release includes corrections for the following issues:

- **AAWIN-2127** - Coding errors resulting in corrupted agent trace logs.
- **AAWIN-2161** - Disable Disconnected Authentication Status not communicated to the Authentication API correctly.
- **AAWIN-2195** - RSA Control Center will eventually crash.
- **AAWIN-2198** - Invalid proof messages appearing in server log.

RSA Authentication Agent 7.2.1 June 2013

This release includes corrections for the following issues:

- **AAWIN-1977**. Users in the group Domain Admins are incorrectly challenged to authenticate under the following conditions:
  - The domain controller is running Windows 2003.
  - Version 7.1 or 7.2 of RSA Authentication Agent for Microsoft Windows is configured to challenge all users except administrators
  - Domain Admins is a member of the local Administrators group
- **AAWIN-2051**. If the agent is configured to challenge a large domain group, Windows login for non-challenged users is very slow.

- **AAWIN-2060**. If the agent is configured to challenge an Active Directory group that has a sAMAccountName value that is different than its common name (cn), all users are challenged.
- **AAWIN-2067**. If a default logon domain is specified through the Local Computer Policies or the System Registry, the agent is not able to retrieve the domain correctly during user logon.
- **AAWIN-2090**. If the agent is configured to use password integration with Citrix Web Interface 5.4, the password integration feature fails unless the user performs his or her first authentication through a Remote Desktop connection.

Known Issues

This section describes known installation, authentication, authenticator (token), and log file issues in RSA Authentication Agent 7.4 for Microsoft Windows. It also includes workarounds, if available.

Installation

This section lists known installation issues and workarounds.

Using update.exe on the command line to install an update and then uninstalling from the command line is unsuccessful
Tracking Number: AAWIN-2488
Problem: If you update to the most recent version of the agent using **Update*.exe** on the command line and then uninstall the update using the **.msi** on the command line, the uninstall is unsuccessful.
Workaround: Uninstall using the Windows Add/Remove functionality. Or to uninstall from the command line, use the product ID instead of the **.msi**. For example, msiexec /qn /x "{1CBBF615-E223-45A3-BE98-4B67EC6846DA}"

Repairing agent using Programs and Features > Repair reverts the agent to the previous version
Tracking Number: AAWIN-2493
Problem: If you try to repair the agent using the Windows Programs and Features Repair option, the repair reverts the agent to the previous version.
Workaround: Repair the agent using the **.msi** normally or on the command line.

Windows crashes when RSA Authentication Client 3.6 and RSA Authentication Agent (version 7.2.1 or later) are installed on the same host

Tracking Number: ACLT-862
Problem: If RSA Authentication Client 3.6 and RSA Authentication Agent (version 7.2.1 or later) are installed on the same host, Windows crashes when you log off or restart the host.
Workaround: Disable code signature verification using the RSADesktop_VerifyRSAComponents.adm Group Policy Object (GPO) template included with RSA Authentication Agent. For instructions, see the *Group Policy Object Template Guide* for your agent version.

Local administrators may encounter a fatal error when modifying an Authentication Agent installation through the Windows Control Panel

Tracking Number: AAWIN-1909
Problem: If Authentication Agent was installed in silent mode, local administrators may encounter a fatal error if they attempt to modify the installation through the Control Panel.
Workaround: Create a new MSI package with the following command:
msiexec /qn /i "RSA Authentication Agent.msi" ADDLOCAL=ALL REINSTALLMODE=vomus REINSTALL=LAC. For instructions on creating and deploying an MSI package, see Chapter 3, “Installing RSA Authentication Agent,” in the *Installation and Administration Guide*.

Cannot access RSA SecurID logon tiles if you install the Authentication Agent through a Remote Desktop Connection
Tracking Number: AAWIN-1688
Problem: If you install the Authentication Agent through a Remote Desktop Connection, a user logging on sees Microsoft password tiles instead of RSA SecurID tiles.
Workaround: The user must restart the machine to display the RSA SecurID tiles.

Cannot reinstall Authentication Agent in a directory different from the original installation directory

Tracking Number: AAWIN-408
Problem: You can use the configuration wizard (**ConfigWizard.exe**) to create a unique MSI package and deploy it for multiple installations. If you later want to reinstall the product, and you create another installation package and install it to a different directory, the installation fails.
Workaround: If you need to reinstall Authentication Agent, install it to the same directory you originally used. You can use the default name for the installation package or give it another name. If you give the installation package another name, for example, to modify the application, run the package from the same path as the original installation.

Error message appears during the installation process after logging on to the computer for the first time

Tracking Number: AAWIN-359
Problem: If you attempt to install RSA Authentication Agent on a computer you never logged on to before (as an elevated administrator user or a standard user), an application error message is displayed with a prompt to click **OK** to terminate. You cannot continue the installation.
Workaround: Click **OK** to close the error message. Restart the computer, and log on again. You can then install RSA Authentication Agent.

Authentication

This section lists known authentication issues and workarounds, including offline authentication.

Routine network activity launches the Auto-Registration utility on computers connected to multiple, active networks

Tracking Number: AAWIN-2330
Problem: Routine network activity, such as IP address changes on subnets, launches the Auto-Registration utility on computers connected to multiple, active networks. In most cases, some of these subnets should be ignored for the purpose of auto-registration.
Workaround: Set a registry value to ignore selected subnets. For instructions, see “Prevent Automated Registration for Selected Subnets” in the *Installation and Administration Guide.*

Users cannot always use the Quick Unlock feature to unlock with an RSA SecurID PIN or Windows Password within an RDP session

Tracking Number: AAWIN-2359, 2390
Problem: If the Quick Unlock feature is enabled, users who lock an RDP session are sometimes prompted to unlock with a SecurID passcode rather than a SecurID PIN or Windows password. This happens when the Windows events managing the timer for RDP unlocks do not successfully publish to the Agent.
Workaround: Unlock the session with the SecurID passcode. Or configure the **Unlock Computer with RSA SecurID PIN or Windows Password** policy to specify **RSA SecurID passcode authentication** as the event that starts the period during which users will be able unlock with an RSA SecurID PIN or a Windows password.

Cannot log on to Windows 8.1 after Windows update is applied using “Update and Restart” until the system is rebooted a second time

Tracking Number: AAWIN-2355
Problem: When updates are applied to some Windows 8.1 systems and the system is automatically restarted, Windows locks the system before the user reaches the desktop after the first logon. When this happens, users are unable to authenticate to unlock the desktop until the system is rebooted a second time.
Workaround: Apply a Microsoft GPO policy:

1. Open the relevant Group Policy Editor (gpedit.msc for local policies; the Group Policy Management tool for domain policies)
2. Open Computer Configuration > Administrative Templates > Windows Components > Windows Logon Options
3. Open the policy “Sign-in last interactive user automatically after a system restart”
4. Set the policy to “Disabled”
5. If setting a domain policy, force a policy refresh (for example, by invoking “gupdate /force”)

Actions involving User Account Control (UAC) do not succeed when valid administrator credentials for a challenged user are provided

Tracking Number: AAWIN-2244, AAWIN-2278
Problem: When attempting to perform actions that require User Account Control verification, such as launching RSA Control Center or Windows Command Processor with administrator privileges, and the Windows Password Integration feature is not enabled, a challenged user is prompted for the Windows password after successful RSA SecurID authentication. If the user hits the ENTER key after providing a valid Windows password, the UAC authentication attempt stops and the attempted action or operation does not succeed. The actions and operations succeed when credentials for non-challenged administrators are provided.
Workaround: Enable Windows Password Integration to prevent this issue. As an alternative workaround, you can instruct users to manually click **OK** after providing credentials at the UAC prompt, rather than pressing ENTER on their keyboards.

The RSA Control Center lists NetBios (pre-Windows 2000) names in drop-down menus for Windows groups.

Tracking Number: AAWIN-2248
Problem: When configuring challenge groups in RSA Control center, the drop-down menus provide the **Group name (pre-Windows 2000)** attribute for the group (sAMAccountName), rather than the modern Windows **Group Name** attribute (cn). If the two attribute values are not the same for a specific group, this causes errors when the agent checks challenge groups during authentication.
Workaround: Manually configure the **Group Name** (cn) value for the challenge group instead of using the value from the drop-down menu.

The agent does not correctly detect group membership for some users.

Tracking Number: AAWIN-2231, AAWIN-2223
Problem: In some cases, the agent does not recognize that users belong to specific active directory groups, even when group membership can be confirmed by the directory server through other means.
Workaround: No workaround currently exists for this issue.

Successful privilege escalation is possible using two-factor authentication with an expired Windows password.

Tracking Number: AAWIN-2227
Problem: If a user with two-factor authentication is locked out of Windows due to an expired password, a different user without two-factor authentication can log into the system and perform successful privilege escalation using the first user's two-factor credentials.
Workaround: No workaround currently exists for this issue.

When an active directory group contains users from multiple domains, group challenge settings do not apply to users in a different domain from the system running the authentication agent.

Tracking Number: AAWIN-2220
Problem: If the agent is configured to challenge all users except those in a specific active directory group containing members from multiple domains, the agent does not challenge group members from the same domain as the system where it is installed (as expected), but incorrectly challenges group members that belong to other domains.
Workaround: If possible, configure separate groups that contain members from only one domain, and assign appropriate challenge settings to each group.

In some cases, the agent does not challenge users that belong to designated challenge groups

Tracking Number: AAWIN-2197
Problem: Users in designated challenge groups are not challenged by the agent in some cases where the character set used by the directory server is different from the character set used by the agent.
Workaround: Ensure that the agent and the directory server use the same character set.

Cannot authenticate through the Unlock tile with a passcode to unlock the computer after "Quick PIN or Password" unlock time elapses

Tracking Number: AAWIN-2041
Problem: If you allow users to unlock their computers by setting the **Unlock with RSA SecurID PIN or Windows Password** setting from the Local Authentication Settings template, users can unlock their computers by entering their SecurID PINs or Windows passwords instead of full passcodes (PINs and tokencodes) as long as they unlock their computers before the time-out period expires (for example, within 15 minutes). After that time, users need to enter passcodes to unlock their computers. However, after the Quick PIN or Password time expires, the unlock tile does not prompt the user for a passcode. This prevents the user from unlocking the computer with the Quick PIN or Quick Password tile.
Workaround: Enable the **Ctrl+Alt+Delete** screen through the Group Policy settings to prevent this issue from happening. Users can also click **Cancel** and select the Unlock tile again to see the passcode prompt.

RSA Control Center incorrectly displays the number of available offline days after a user authenticates for the first time from a computer without the Auto-Registration feature

Tracking Number: AAWIN-1894
Problem: The Offline days left field displays the available offline days as a number and as a bar graph. After a user authenticates for the first time on a machine without the Auto-Registration feature installed, the bar graph incorrectly displays zero available offline days. The numeric value displays correctly. This does not affect authentication.
Workaround: For the bar graph to correctly display available offline days, instruct users to re-authenticate. The RSA Control Center correctly displays the available offline days after re-authentication.

Users with Fixed Passcodes Cannot Refresh Offline Days from the RSA Control Center

Tracking Number: AAWIN-1855
Problem: Users assigned fixed passcodes cannot refresh offline days from the RSA Control Center.
Solution: Do not issue fixed passcodes to users that require offline authentication.

Authenticated users may need to log off and re-authenticate if they changed their Windows password and want to unlock with an RSA SecurID PIN

Tracking Number: AAWIN-1791
Problem: Administrators can allow authenticated users the option of unlocking their computer with their PIN instead of their passcode. Administrators can set this option in group policy. If users change their Windows password after logging in and then lock their computer, they cannot unlock their computer with their PIN.
Workaround: Users must log off their computers and reauthenticate with their passcode to reestablish the ability to unlock their computers with their PIN.

When you click Clear to clear offline data, the Clear button does not change appearance as expected

Tracking Number: AAWIN-664
Problem: When you click Clear in the Offline Data section of the RSA Control Center, the **Clear** button does not change appearance to indicate that the offline data has been cleared. However, the offline data is cleared.
Workaround: None required.

Windows Agent does not properly handle the offline authentication policy that requires a user to enter an emergency code after reaching the limit of offline failures specified in the policy

Tracking Number: AAWIN-635
Problem: When you configure the offline authentication policy to require a user to enter an emergency code after a certain number of offline failures, the user is prompted to enter an emergency code after half the number of failures specified in the policy.
Workaround: Double the number of offline failures allowed before users are requested to enter an emergency code in the offline authentication policy.

Multiple authentication prompts appear when accessing a remote computer that uses Network Level Authentication

Tracking Number: AAWIN-564
Problem: Remote Desktop Connection 6.1 includes Windows Network Level Authentication (NLA). If this feature is enabled when you attempt to connect to a remote computer, you are prompted to authenticate before you can establish a remote connection. If you use NLA with an RSA SecurID credential provider configured on the remote computer, two prompts to authenticate are displayed before you can access the remote desktop. One prompt opens from the local computer and the other opens from the remote computer. This is a limitation of how Microsoft implements Network Level Authentication when you use a third-party credential provider. After you enter your account information and successfully authenticate through each prompt, you can access the remote computer.

Note: Network Level Authentication is enabled by default for Windows 7 or later operating systems. For more information on using Network Level Authentication, see the Microsoft web site.

Workaround: You can partially address this by configuring the GPO template **Logon with credentials from remote applications**. This policy prevents the authentication prompt for challenged users by passing through the usernames. It also prevents the second authentication prompt for unchallenged users.

Set New RSA SecurID PIN dialog box opens behind the User Account Control (UAC) dialog box

Tracking Number: AAWIN-307
Problem: You log on to a computer with local credentials, but need to access an application that requires elevated privileges. If you need to use an administrator account that requires an RSA SecurID passcode and you have not created your RSA SecurID PIN, Authentication Agent prompts you to create one. However, you cannot access the fields in the Set New RSA SecurID PIN dialog box because it opens behind the Windows UAC logon dialog box.
Workaround: Move the Set New RSA SecurID PIN dialog box from behind the Windows UAC logon dialog box. You can then access the selections and fields and set your PIN.

Authenticator (Token)

This section lists known authenticator (RSA SecurID 800 token) issues and workarounds.

The RSA Control Center icon may not correctly display the status of a connected RSA SecurID 800

Tracking Number: AAWIN-1953
Problem: The RSA Control Center icon indicates that the application recognizes an authenticator connected to the USB port by displaying a blue cross in the upper-right corner of the icon. If RSA Authentication Client and RSA Local Authentication Client are installed and you remove RSA Authentication Client on a 64-bit computer, the blue cross may not appear when the user connects an authenticator.
Workaround: Remove and re-install RSA Authentication Client on a 64-bit computer to repair RSA Authentication Agent.

RSA SecurID 800 tokens may have intermittent USB connectivity issues

Tracking Numbers: AAWIN-1859
Problem: RSA SecurID 800 tokens have a manufacturing code on the back of the token below the serial number. Manufacturing codes begin with A, C, or D, and the letters are typically followed by a number. Intermittent USB connectivity issues can occur with tokens coded A, A2, A8, and A9.
Workaround: Remove the RSA SecurID 800 token and reinsert it. Be sure to connect the RSA SecurID 800 directly to a USB port on the computer rather than to an adapter or extender. Users can also authenticate by entering their PIN and tokencode without connecting their RSA SecurID 800 to a USB port.

Offline data does not download and the RSA Authentication Agent Offline Local service stops if logging on with multiple tokens—one after the other

Tracking Number: AAWIN-650
Problem: If you assign three tokens to a user and enable offline authentication with RSA Authentication Manager 7.1 SP4, the user can authenticate with the first token and offline data downloads successfully. When the user logs off and attempts to authenticate with the other tokens, the user successfully authenticates, but offline data cannot download and the RSA Authentication Agent Offline Local service stops. This issue only occurs with RSA Authentication Manager 7.1 SP4.
Workaround: Do not assign more than one token to a user who must authenticate offline.

Log Files

This section lists known log file issues and workarounds.

Restart the computer if you change the level of tracing or the location where the Control Center writes the trace files

Tracking Number: AAWIN-1933
Problem: For troubleshooting purposes, the RSA Control Center can write trace log files. Typically, you would not enable tracing unless instructed to do so by RSA Customer Support. If you change the level of tracing, for example, from verbose to error, you must reboot the computer for the change to take effect. Additionally, you must reboot the computer if you change the location the trace files are written to.
Workaround: Reboot your computer if you change the level of tracing or the location the trace files are written to. For more information, see “Enable Tracing” in the *Installation and Administration Guide.*

Support and Service

You can access community and support information on RSA Link at **https://community.rsa.com**. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

The RSA Ready Partner Program website at **www.rsaready.com** provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.

Trademarks

Intellectual Property Notice

Open Source License