Release Notes
RSA Authentication Agent 7.1 for Microsoft Windows

February, 2012

Introduction

This document lists what's new in RSA® Authentication Agent 7.1 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 SecurCare® Online at **https://knowledge.rsasecurity.com**.

What's New in This Release

This release provides the following new features and enhancements:

Support for multi-domain (universal) user groups. Authentication Agent supports all Windows groups, including multi-domain groups. Users and groups must be in the same forest.

Support for logon with User Principal Names (UPNs). Users can now log on with UPNs. UPN format is used to specify an Internet-style name, such as UserName@Example.RSA.com.

Simpler Agent distribution. Previous releases required different versions of the Authentication Agent for 32-bit and 64-bit operating systems. This release provides a single Agent that can be deployed to both 32-bit and 64-bit versions of all supported operating systems.

Single version supports all product features.

- This version offers uniform control and management for all currently shipping versions of Microsoft Windows. Previous versions required separate controls and management for pre-Vista systems and post-Vista systems.
- This release supports connected RSA SecurID 800 Authenticators on all currently shipping versions of Microsoft Windows.

Support for fast user switching. The Authentication Agent supports fast user switching on the Windows operating systems that support this feature. With fast user switching, multiple user accounts can log on to a computer simultaneously.

Support for Remote Desktop Protocol (RDP) sessions. Users can log on with SecurID to an RDP session.

Changes to Configuration Settings. Some configuration settings that were available in the RSA Authentication Agent 6.1, 6.4, 7.0 user interfaces are now available exclusively in the Group Policy Object templates. For information about the changes, see:

- Chapter 1, "Overview," in the *RSA Authentication Manager 7.1 for Microsoft Windows Installation and Administration Guide.*
- Chapter 2, "Preference Settings and Agent Support," *in the RSA Authentication Agent 7.1 for Microsoft Windows Group Policy Object Template Guide.*

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 Manger server if you are using Auto-Registration.

Interoperability with RSA Authentication Agent for Web for IIS

RSA Authentication Agent 7.1 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 uninstall either product. If you uninstall 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. Version 7.1 of the Authentication Agent for Web uses the new node secret format. If you are installing an earlier version of the Authentication Agent for Web, contact **RSA Customer Support** 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 Certified Partner Solutions

If you are using RSA Authentication Agent 7.1 for Microsoft Windows on a system that is also a Secured By RSA Certified Partner Solution system, visit the site **Secured by RSA Certified Partner Solutions**. The site includes implementation guides and information on usability and compatibility.

Package Contents

RSA Authentication Agent is available from **RSA Authentication Agents for Microsoft Windows**.

The RSA Authentication Agent 7.1 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 7.1 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.
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	This folder contains product documentation. For details, see the following section, "Documentation and Application Help."

Documentation and Application Help

The product documentation is available from the following web locations:

- **RSA Authentication Agents for Microsoft Windows**
- **RSA SecurCare Online**. The RSA Authentication Agent 7.1 for Microsoft Windows Product Documentation page contains links to documentation files.

The following documentation is in the RSA Authentication Agent 7.1 package, in the **\documentation** directory.

Documentation

Title	Filename
RSA Authentication Agent 7.1 for Microsoft Windows Installation and Administration Guide	**auth_agent71_install_admin_guide.pdf**
RSA Authentication Agent 7.1 for Microsoft Windows Group Policy Object Template Guide	**auth_agent71_gpo_template_guide.pdf**

The following Help installs with RSA Authentication Agent 7.1 for Microsoft Windows.

Application Help

Title	Filename
RSA Authentication Agent (SecurID) Help	The Help is accessed from the RSA Control Center.
(Japanese) RSA Authentication Agent (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.

Known Issues

This section describes known issues and workarounds in RSA Authentication Agent 7.1 for Microsoft Windows.

RSA SecurID 800 tokens may have intermittent USB connectivity issues

Tracking Numbers: AAWIN-1954, AAWIN-1859
Problem: 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, or when a Windows Vista computer returns from sleep mode.
Workaround: Remove the SecurID 800 token and reinsert it. Be sure to connect the 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 SecurID 800 to a USB port.

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 both RSA Authentication Client and RSA Local Authentication Client are installed and you uninstall RSA Authentication Client on a 64-bit computer, the blue cross may not appear when the user connects an authenticator.
Workaround: If you uninstall and re-install RSA Authentication Client on a 64-bit computer, you should repair the RSA Authentication Agent installation.

64-bit Vista users may need to log on with the Other Credentials tile if they enter an incorrect PIN to unlock their system

Tracking Number: AAWIN-1948
Problem: If a user is logged on to a 64-bit Vista computer with the Unlock with SecurID PIN feature enabled, and the user enters an incorrect PIN to unlock the computer, the user may not be able to log on with the credential tile they typically use.
Workaround: Log on with the Other Credentials tile.

A local Windows XP administrator may not be able to force a logoff of a remote user

Tracking Number: AAWIN-1947
Problem: If a Windows XP computer has multiple remote users and the Unlock with an RSA SecurID PIN feature enabled, and a remote user locks the system with a connected RSA SecurID 800, the local administrator may not be able to force a logoff of a remote user.
Workaround: Do not enable the Unlock with SecurID PIN feature for a Windows XP computer that will have multiple remote users.

You must reboot the computer if you change the level of tracing or the location the trace files are written to

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 *RSA Authentication Agent 7.1 for Microsoft Windows Installation and Administration Guide.*

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 *RSA Authentication Agent 7.1 for Microsoft Windows Installation and Administration Guide.*

RSA Control Center incorrectly displays the number of available offline days after a user authenticates for the first time from a machine 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.

Invalid error message in the RSA Authentication Manager 7.1 log after changing an Agent's IP address and authenticating

Tracking Number: AAWIN-1839
Problem: After an Agent machine with Auto Registration has its IP address changed, if a user performs a test authentication from that Agent, RSA Authentication Manager 7.1 incorrectly logs an error message. The error message states Offline Authentication Data Download Failed.
Workaround: Ignore the message.

You may need to manually install the trusted root certificate *thawte Primary Root CA* before installing Authentication Agent on computers without Internet access

Tracking Number: AAWIN-1801
Problem: Authentication Agent requires the trusted root certificate *thawte Primary Root CA*. This certificate is automatically provisioned, provided the computer has Internet access.
Workaround: Before installing Authentication Agent on computers without Internet access, you may need to install the trusted root certificate *thawte Primary Root CA* on the Computer account. For information or instructions, see the **Microsoft Knowledge Base Article 931125**.

To unlock with an RSA SecurID PIN, authenticated users may need to log off their computer and re-authenticate if they changed their Windows password

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.

Cisco GINA chaining breaks if you install RSA Authentication Agent and RSA Authentication Client and then remove the Authentication Client

Tracking Number: AAWIN-1770
Problem: If you install the Cisco VPN Client, RSA Authentication Agent, and RSA Authentication Client, the Cisco VPN connection and the RSA GINA are properly displayed after you restart the system. If you subsequently remove RSA Authentication Client and restart the system, only the Microsoft GINA is displayed. Removing RSA Authentication Client breaks Cisco GINA chaining and incorrectly resets the Cisco GINA registry settings. This occurs because the removal of the Authentication Client removes support for third-party GINA chaining. The problem occurs only on Windows XP Pro SP3 and Windows Server 2003.
Workaround: To restore Cisco GINA chaining, you must manually edit the Windows registry settings and then restart the system so that the changes take effect. Edit the registry settings as follows:

- Under **HKEY_LOCAL_MACHINE\Cisco Systems\VPN Client**, set **PreviousGinaPath** to **MSGina.dll**.
- Under **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon**, set **GinaDLL** to **CSGina.dll**.

RSA SecurID tiles are not displayed 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.

Users logging through Remote Desktop Connection with connected SecurID 800 are prompted twice for PIN

Tracking Number: AAWIN-1625
Problem: Users who log on through Remote Desktop Connection with a connected SecurID 800 are prompted twice for their PINs. This occurs on Windows XP and Windows Server 2003.
Workaround: Users must enter the PIN when prompted for the first time. When prompted again, the user must wait for the tokencode to change on the device before entering the PIN.

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 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.

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.

Unidentified Program message appears in the User Account Control (UAC) dialog box while repairing or removing RSA Authentication Agent 7.1 for Microsoft Windows

Tracking Number: AAWIN-398
Problem: If you enabled User Account Control (UAC) on a Windows Vista computer and you need to repair or remove RSA Authentication Agent, a message is displayed that an unidentified program wants to access your computer. This occurs when the installation program uses a Microsoft Windows Installer package that was digitally signed.
Workaround: Click **Allow** in the UAC dialog box to safely continue the repair or removal process.

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 Vista or later operating systems. You can manually enable it on Windows XP SP3 operating systems. For more information on using Network Level Authentication, see the Microsoft web site.

If a user has three tokens and logs off after authenticating with the first token, when the user logs on with another token, authentication is successful, but offline data does not download and the RSA Authentication Agent Offline Local service stops
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 successfully with the first token, and offline data is downloaded. When the user logs off and attempts to authenticate with the other tokens, the user successfully authenticates, but offline data is not downloaded, and the RSA Authentication Agent Offline Local service stops. This issue only occurs with RSA Authentication Manager 7.1 SP4.
Workaround: Do not assign a third token to a user who must authenticate offline.

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 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.

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsa.com/support**
RSA Secured Partner Solutions Directory	**www.rsasecured.com**

Trademarks