Release Notes
RSA® Authentication Agent 7.1.2 for Web for IIS 7.0, 7.5, and 8.0 Web Server

October, 2013

Introduction

This document lists what is new and what has changed in RSA® Authentication Agent 7.1.2 for Web for IIS 7.0, 7.5 and 8.0 Web Server. It includes descriptions of fixed issues, as well as workarounds for known issues. RSA recommends that you read this document before installing RSA Authentication Agent 7.1.2 for Web for IIS 7.0, 7.5 and 8.0 Web Server. 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 section describes the changes introduced in this release. To install this release, follow the instructions for a full product installation as described in the *RSA Authentication Agent for Web for IIS Installation and Configuration Guide.*

Support for Additional Platforms. This release adds support for:

- Microsoft Internet Information Services (IIS) 8 Server on Windows Server 2012 [x64]
- Microsoft Exchange Server 2013 for Outlook Web Access (OWA) on Windows Server 2008 R2
- Microsoft Exchange Server 2013 for Outlook Web Access (OWA) on Windows Server 2012[x64]
- Microsoft Active Directory Federation Services for Office 365 on Windows Server 2008
- Microsoft Active Directory Federation Services for Office 365 on Windows Server 2008 R2
- Microsoft Active Directory Federation Services for Office 365 on Windows Server 2012
- Single Sign-On with Microsoft OWA on Exchange Server 2013

Silent Installation. As of the 7.1.2 release, RSA Authentication Agent for Web for IIS no longer supports silent installation.

Update to Address a Security Issue. This release fixes a security issue that under some circumstances left protected websites unprotected after a crash by RSA® Authentication Agent for Web for IIS.

Additional Bug Fixes. This release includes bug fixes that increase application stability and code quality.

Prerequisites for Installing RSA Web Agent 7.1.2 on Windows Server 2012

To install RSA Web Agent 7.1.2 for Windows Server 2012, you must have .NET framework 3.5 pre-installed on the Windows Server 2012 machine. Note that Windows Server 2012 come prepackaged with .NET 4.5. However, .NET 3.5 is required.

Product Documentation

The following documentation for RSA Authentication Agent 7.1.2 for Web for IIS 7.0, 7.5 and 8.0 Web Server is in the ***doc*** directory.

Title	Filename
RSA Authentication Agent for Web for IIS Installation and Configuration Guide	WebAgent_IIS.pdf
RSA Authentication Agent for Web for IIS Developer's Guide	WebAgentDev_Win.pdf
Integrating RSA Authentication Agent for Web with RSA Authentication Manager Express Risk-Based Authentication	RSAWebAgent_AMX.pdf

Fixed Issues

This section describes the issues fixed in this release.

The RSA Authentication Agent Applet is not working properly for an admin user other than the built-in administrator.

Tracking Number: AAIIS-477

For the RSA Authentication Agent applet to work properly, the administrator permissions from the following directories must be inherited by their child directories/keys:

HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT
HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\RSAWebAgent
HKEY_LOCAL_MACHINE\SOFTWARE\RSAACEAgents

Unable to protect a single page when the folder is defined as an application.

Tracking Number: AAIIS-774

On Windows 2012 with Exchange Server 2013, this issue no longer exists.

Protected websites may be left unprotected after agent crash.

Tracking Number: AAIIS-1038

In some cases, when the RSA® Authentication Agent for Web for IIS crashes, websites protected by this agent could be left unprotected. This is due to the fail open flaw in the agent code.

RSA ACE Agent for Web IIS 7.1 - Web application pool should run as a non-system account.

Tracking Number: AAIIS-1048

See "Running the Web Application Pool as a Non-System User."

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround or fix is available, it has been noted or referenced in detail. Many of the workarounds in this section require administrative privileges. If you do not have the required privileges, contact your administrator.

RSA Authentication Agent 7.1.2 does not support 32 -bit applications on 64-bit operating systems.

Tracking Number: AAIIS-572

Problem: RSA Authentication Agent 7.1.2 does not support 32-bit applications on 64-bit operating systems.

Workaround: None

WebAgent does not protect individual files having non-English characters.

Tracking Number: AAIIS-701

Problem: WebAgent does not protect individual files that have local language characters in the file name.

Workaround: None

“Disable IIS Server if agent fails to load” checkbox cannot be unchecked.

Tracking Number: AAIIS-786

Problem: The “Disable IIS Server if agent fails to load” checkbox cannot be unchecked.

Workaround: None

In Outlook Web Access2010, refreshing the modal popup page does not redirect to the RSA SecurID logon page.

Tracking Number: AAIIS-808

Problem: In OWA 2010 after the idle cookie time expires, a modal popup is displayed. Refreshing this directs the user to the OWA page instead of to the RSA SecurID logon page, useridandpasscode.htm.

Workaround: None

The ‘Use JavaScript pop-up window to authenticate in frames’ features does not work properly.

Tracking Number: AAIIS-839

Problem: When the Javascript popup option is disabled, authentication with separate frames is successful but the authentication page is thrown again.

Workaround: To use the 'JavaScript popup' feature you must disable cross frame busting by setting the environment variable RSA_NO_FRAME_BUSTING=1 in the WebAgent machine.
In general, it is recommended to protect the main page, instead of protecting individual frames in the page.

On cookie expiry, all unsaved data in Active sync is lost.

Tracking Number: AAIIS-982

Problem: In Active sync, if the cookie expires while composing an e-mail message, the message is not saved in the Drafts folder.

Workaround: None

For an agent configured with AMX, all unsaved data in OWA 2010 will be lost on cookie expiry.

Tracking Number: AAIIS-984

Problem: If the agent is configured with AMX, all unsaved data in OWA 2010 will be lost after cookie expiry.

Workaround: Refresh the page.

Single sign-on does not work during an upgrade.

Tracking Number: AAIIS-1004

Problem: During an upgrade, if single sign-on (SSO) is enabled, the configuration UI settings are carried forward but a module required for SSO is not added in the modules section.As a result, SSO does not work.

Workaround: To enable SSO for Exchange, disable the ‘Target this resource for Single Sign-On’ checkbox and enable it again in the IIS Manager Configuration UI.

To enable SSO for Sharepoint, follow the steps in the section Prepare WebAgent for Single Sign-On to the Microsoft Office SharePoint Server in the *IIS Installation and Configuration Guide* and remove the *RSAsinglesignonExtension* in the handler mapping section.

After a successful (multiple domain) authentication, SharePoint 2007 site does not redirect to requested site.

Tracking Number: AAIIS-1006

Problem: SharePoint 2007 site with multiple domain authentication is not redirecting to the requested page after a successful authentication.

Workaround: None

After configuring SharePoint 2007 32-bit for SSO, all users get an Access Denied message.

Tracking Number: AAIIS-1009

Problem: After configuring SSO for SharePoint 2007 32-bit, all users trying to sign in get an 'Access Denied, Sign in as a different user' message.

Workaround: None

If a user tries to access multi-domain SSO with the password only feature enabled, access is denied to the user.

Tracking Number: AAIIS-1014

Problem: If a user tries to access multi-domain SSO with password only feature enabled, an 'Access Denied' message is displayed.

Workaround: After generating or importing the domain Secret, restart the RSA Pipe Service.

Windows Mobile 6.5 ActiveSync is not able to Sync with Exchange 2013 on Windows 2012 Server.

Tracking Number: AAIIS-1092

Problem: Windows Mobile 6.5 ActiveSync is not able to Sync with Exchange 2013 on Windows 2012 Server.

Workaround: None

Logging out of Exchange produces an error when used with single sign-on.

Tracking Number: AAIIS-1094

Problem: When a user clicks Sign Out, Microsoft Exchange returns a "404 File Note Found" error.

Workaround: Close the browser window to log out.

Help not working in the RSA Authentication Agent Control Panel applet.

Tracking Number: AAIIS-1101

Problem: Help does not work in the RSA Authentication Agent Control Panel applet.

Workaround: None. Microsoft has deprecated this feature. See **http://technet.microsoft.com/en-us/library/hh831568.aspx**.

Redirect HTTP connection to Secure Server option is not working in Windows Server 2012.

Tracking Number: AAIIS-1103

Problem: If you access a protected resource with HTTP when the "Require Secure Connection to Access Protected Page" and "Redirect HTTP Connections to Secure Server" options are enabled in RSA SecurID Features in IIS Manager, you are not automatically redirected to HTTPS.

Workaround: None

Authentication Successful pop-up window appears when authenticating with "Use Java Script Pop-Up Window to Authenticate" enabled.

Tracking Number: AAIIS-1108

Problem: After successful authentication when "Use Java Script Pop-Up Window to Authenticate in Frames" is enabled, an "Authentication Successful" window is displayed instead of displaying the protected resource.

Workaround: Click **OK** to display the protected resource.

A remote IIS Manager closes when you open the RSA SecurID feature.

Tracking Number: AAIIS-1118

Problem: After connecting to a remote IIS Manager, opening RSA SecurId Feature closes the IIS Manager.

Workaround: None

RSA SecurID is not populating in Features View of Virtual site when only Site is opened on remote IIS Manager.

Tracking Number: AAIIS-1119

Problem: After adding a virtual site through the IIS Manager, connect to the site by right clicking on IIS and connecting to another web server machine, The Features view of the newly added virtual site will not display RSA Securid Feature.

Workaround: None

Upgrading from RSA Authentication Agent for Web 7.1.1 to 7.1.2 on Microsoft Windows 2008 SP2 64-bit Enterprise is not supported.

Tracking Number: AAIIS-1122

Problem: Upgrading from RSA Authentication for Web 7.1.1 to 7.1.2 on 64-bit versions of Microsoftt Windows 2008 SP2 Enterprise produces the following error:

Error 2324: Could not open file. \Windows\System32\SdRepository\SDCONTRL.hlp GetLastError: 3.

Workaround: Perform the following procedure:

1. Back up the following files and delete the original version:
   - **\Windows\System32\SdRepository\SDCONTRL.hlp**
   - **\Windows\System32\SdRepository\sdcontrl.cnt**
   - **\Windows\System32\inetsrv\config\schema\securidsection_schema**
2. Start the upgrade process.

Web Agent timeout pop-up is not working correctly in OWA.

Tracking Number: AAIIS-1132

Problem: When using Outlook Web Access, the idle timeout popup appears after 15 minutes, even if there is ongoing activity.

Workaround: None

Documentation Addendum

Enabling Single Sign-On in Microsoft Exchange Server 2013

Perform the following steps to enable single sign-on in Microsoft Exchange 2013.

To enable single sign-on on Exchange Server 2013:

1. Open the Microsoft Exchange Administration Center (EAC).
2. On the left pane, click **Servers**.
3. Click **Virtual Directories**.
4. Click OWA and edit server properties.
5. Click **Authentication**.

6. Select **Use one or more standard authentication methods**.
7. Select **Integrated Windows authentication**.

   To enable integrated Windows authentication for SSO on IIS8 in Microsoft Exchange 2013, go to:

   http://blogs.msdn.com/b/mvpawardprogram/archive/2013/03/18/virtual-directories-exchange-2013.aspx"
8. Click **Save**.

Using the Web Agent with Active Directory Federation Services

Use the following resources to help you integrate the Web Agent 7.1.2 with ADFS.

Review the following topic from Microsoft:

http://technet.microsoft.com/en-us/library/hh344805%28WS.10%29.aspx

Review the RSA SecurID Implementation Guide for AD FS.

1. Click **https://gallery.emc.com/community/marketplace/rsa?view=overview.**
2. Search for ADFS.
3. From the search results, click Microsoft Active Directory Federation Service.
4. Click Collateral to access the *RSA SecurID Implementation Guide*.

Running the Web Application Pool as a Non-System User

To run the web application pool as a non-system user:

1. Grant permission to the following registry entries for the user:
   - HKLM\System\CurrentControlSet\Services\WinSock2\Parameters
   - HKLM\SOFTWARE\SDTI\RSAWebAgent
2. Grant the permissions Read and Execute, Execute, List folder contents, and Read to the directory \Program Files\RSA Security\RSAWebAgent
3. Grant the permissions Read and Execute, and Read to the file \Program Files\RSA Security\RSAWebAgent\securid
4. Grant the permissions Read and Execute, and Read to the file \Program Files\RSA Security\RSAWebAgent\sdstatus.12

Clearing the Node Secret

To clear the node secret:

1. Clear the node secret from RSA Authentication Manager. To do this, Open the Authentication Manager Security Console and click **Access > Authentication Agents > Manage Existing**.
2. Locate the affected agent host and click on the drop down menu.
3. Select **Manage Node Secret**.
4. Check **Clear the node secret**, and click **Save**.
5. Log on to the Agent Host machine and clear the node secret from the RSA Authentication Agent. To do this, rename or delete the node secret file. The file is located in \Program Files\RSA Security\RSAWebAgent"
6. Test authentication from RSA Web Agent 7.1.2.
7. Check your authentication logs and ensure a new node secret has been sent.
8. Restart your IIS server.

Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.emc.com/support/rsa/index.htm**
RSA Solution Directory	**https://gallery.emc.com/community/marketplace/rsa?view=overview**

Trademarks