Release Notes
RSA® Authentication Agent 7.1.3 for Web for IIS 7.0, 7.5, and 8.0 Web Server

April, 2014

Introduction

This document describes what is new and what has changed in RSA® Authentication Agent 7.1.3 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 7.1.3 for Web for IIS 7.0, 7.5 and 8.0 Web Server. This document contains the following sections:

- What's New in This Release
- Prerequisites for Installing RSA Web Agent 7.1.3 on Windows Server 2012
- Product Documentation
- Fixed Issues
- Known Issues
- Documentation Addenda
- Support and Service

These *Release Notes* may be updated. The most current version can be found on RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

Note: This release incorporates all changes included in earlier releases of RSA Authentication Agent for Web for IIS 7.0, 7.5 and 8.0 Web Server.

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 7.1 for Web for IIS Installation and Configuration Guide.*

Support for Microsoft SharePoint 2013. This release qualifies RSA Authentication Agent for Web for IIS to work with SharePoint 2013. For instructions on how to configure the Web Agent to work with Microsoft Office SharePoint Server 2013, see Configuring SharePoint Server 2013 in Documentation Addenda, below.

Note: RSA recommends using short-term persistent cookies instead of long-term persistent cookies to access SharePoint content. Short-term persistent cookies are more secure and support a larger set of SharePoint document features.

Microsoft Office 2003. As of release 7.1.3, RSA Authentication Agent for Web for IIS no longer supports Microsoft Office 2003.

Support for Additional Platforms. As of release 7.1.2, RSA Authentication Agent for Web for IIS supports the following platforms:

- Microsoft Internet Information Services (IIS) 8 Server on Windows Server 2012 [x64 only]
- 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 only]
- 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 release 7.1.2, RSA Authentication Agent for Web for IIS no longer supports silent installation.

Prerequisites for Installing RSA Web Agent 7.1.3 on Windows Server 2012

To install RSA Web Agent 7.1.3 for Windows Server 2012, you must have .NET framework 3.5 pre-installed on the Windows Server 2012 machine. Note that Windows Server 2012 comes prepackaged with .NET 4.5. However, .NET 3.5 is required.

Product Documentation

The following documentation for RSA Authentication Agent 7.1.3 for Web for IIS 7.0, 7.5 and 8.0 Web Server is in the ***\doc*** directory.

Title	Filename
RSA Authentication Agent 7.1 for Web for Internet Information Services Installation and Configuration Guide	WebAgent_IIS.pdf
RSA Authentication Agent 7.1 for Web for Internet Information Services Developer's Guide	WebAgentDev_IIS.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.

Domain secret exported from Apache Linux cannot be imported into Windows.

Tracking Number: AAIIS-1034

To export domain secret from Apache Linux and import into Windows, follow the procedure described in Configuring Multiple Domain Authentication, under Documentation Addenda, below.

SSO not working with Sharepoint 2010.

Tracking Number: AAIIS-1111

SSO now works with Sharepoint 2010.

Additional changes have been made to defend against click-jacking.

Tracking Number: AAIIS-1128

Code changes have been made in RSA Web Agent 7.1.3 to further protect against forms of click-jacking. In addition, the web site should use Frame Options HTTP Header **X-Frame-Options**, as described in the following steps:

1. On RSA Web Agent protected IIS server, click **Start > Control Panel > RSA Web Agent**.
2. In the Connections pane of the IIS Manager, double-click *server_name*, and then click **Sites > Default Web Site**, where *server_name* is the name of the Microsoft IIS server protected by RSA Web Agent.
3. In the **Site Home** pane, double-click **HTTP Response Headers**.
4. In the **Action** pane, click **Add**.
5. In the **Add Custom HTTP Response Header** dialog box:

6. Under **Name**, enter **X-Frame-Options**.
7. Under **Value**, enter **SAMEORIGIN**.
8. Click **OK**.

Group security feature does not work with .aspx pages.

Tracking Number: AAIIS-1142

Group security feature now works properly with .aspx pages.

Selective SecurID authentication feature fails for domain created with non-default NETBIOS name.

Tracking Number: AAIIS-1148

Web Agent selective SecurID authentication now works correctly, if properly configured (see fix for AAIIS-1151, below), regardless of how the NETBIOS name is specified when creating a domain.

Selective SecurID authentication feature not working correctly.

Tracking Number: AAIIS-1151, AAIIS-1157

Steps on how to configure Selective SecurID Authentication so that it works correctly are provided under Documentation Addenda, below, in the procedure titled "Configuring Selective SecurID Authentication."

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

Tracking Number: AAIIS-1160

When using Outlook Web Access, the idle timeout pop-up no longer appears when there is ongoing activity.

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 and above does not support 32-bit applications on 64-bit operating systems.

Tracking Number: AAIIS-572

Problem: RSA Authentication Agent 7.1.2 and above 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 from 7.0 to 7.1.

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.

Tracking Number: AAIIS-1092

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

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 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 or above on Microsoft Windows 2008 SP2 Enterprise (64-bit only) is not supported.

Tracking Number: AAIIS-1122

Problem: Upgrading from RSA Authentication for Web 7.1.1 to 7.1.2 or above 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.

Documentation Addenda

The following information will be added to the product documentation in a later release.

Configuring Multiple Domain Authentication

When configuring multiple domain support, observe the following guidelines:

- Add only one server per domain in the Manage Domain Configuration dialog box.
- A Web Agent for IIS in one domain can share multiple domain support with a Web Agent for Apache in another domain. However, the type of web server added must be the same as the configuring server. That is, if the configuring server is Web Agent for IIS, then only an IIS web server protected by Web Agent for IIS in the another domain should be added. If the other domain has only, say, Web Agent for Apache, then a Web Agent for IIS should be setup in that domain and be added to the configuring server for the multiple domain support to work.
- Do not mix secure and non-secure web servers. Multiple domain support will not work if in one domain, the server is accessed through non-secure HTTP and through secure HTTP in the the other domain. For example, if on one Apache server "Require secure connection to access protected pages" is enabled, authenticating to this server first does not allow access to other servers without another authentication. By disabling this setting, the problem is resolved.

Note: The browser should consider all Web Agent-protected domains in the local intranet. For example, a problem accessing ***.net** after first authenticating at ***.com:88** can be resolved by adding ***.net** as a local intranet. To do this in Internet Explorer, perform the following steps:

1. Select **Tools > Internet options > Security > Local intranet > Sites > Advanced**.
2. Add the ***.net** domain to the web sites.

Configuring Selective SecurID Authentication

To ensure that Web Agent selective authentication operates successfully, configure it exactly as follows:

Group specification

Valid groups (in combination with any other setting) are:

1. Local groups

   To specify a local group, the syntax is ***groupName***. No prefix, such as ".\", is acceptable.

2. Domain groups, defined as domain local

   To specify a domain group, the syntax is ***domainName**groupName*** where *domainName* must be the “flat” domain name, as specified by the NETBIOS name.

For either a Local or Domain group, the members must be domain users. No other type of group content is acceptable.

User specification

A username can represent a local user or a domain user.

To specify a user name, the syntax is ***username***. No prefix specifying a domain is acceptable.

Multiple group and/or user specification

When specifying multiple groups and/or users in a selective auth configuration, the groups and/or users must be separated by a semi-colon (;), with no spaces before or after each semi-colon.

Configuring SharePoint Server 2013

This section describes how to configure the Web Agent to work with SharePoint Server 2013. You must perform these procedures before following the instructions provided in chapter 7, “Configuring the Web Agent to Microsoft Office SharePoint Server,”of the *RSA Authentication Agent 7.1 for Web for IIS 7.0 and 7.5 Installation and Configuration Guide*.

Configuring Persistent Cookies with SharePoint Server 2013

SharePoint Server 2013 uses short-term persistent cookies to process Microsoft Word documents. The cookies are created when a URL is accessed, and they exist until they either time out, or are deleted when the next URL is accessed. In order to properly open, edit, and close Word documents, the web server hosting the web agent, and the browser machines accessing the web agent machine must be closely synced to GMT time. However, such close syncing is difficult to achieve for applications that do not use time synchronization services. In this case, the default setting of 30 seconds for Short Term Persistent Cookies might be too short for successful transfer between machines. To increase the likelihood of successful transfer, you can increase the lifetime of Short Term Persistent Cookies.

Note: For SharePoint 2013, the **core.js** file that must be modified to configure persistent cookies is in the following directory: **C:\Program Files\Common Files\microsoft shared\Web Server Extensions\15\TEMPLATE\LAYOUTS**. If you use a non-default layout template, this path may be different.

To run the web Application Pool as a Network Service:

1. Grant permission to the following registry entries for the Network Service:
   - HKLM\System\CurrentControlSet\Services\WinSock2\Parameters
   - HKLM\SOFTWARE\SDTI\RSAWebAgent
2. Grant Read and Execute, List folder contents, and Read permissions to the directory:

   \Program Files\RSA Security\RSAWebAgent
3. Grant Read and Execute, and Read permissions to the file:

   \Program Files\RSA Security\RSAWebAgent\securid

4. Grant Read and Execute, and Read permissions to the file:

   \Program Files\RSA Security\RSAWebAgent\sdstatus.12

To verify Application Pool settings for the site:

1. In the Connection pane of the IIS Manager, click ***<server_name>*** **> Application Pools**.
2. Click the application pool for the SharePoint website.
3. In the Actions pane, click **Advanced Settings**.
4. Under Process Model, click the **Identity** field and change the identity to **NetworkService**.

Note: If using a SharePoint farm configuration, see the following Microsoft topic about using a domain administrator for the application pool identity: http://technet.microsoft.com/en-us/library/ff805066%28v=office.14%29.aspx

To change the RSA SecurID Pool Application Pool setting (for Windows 2008 R2):

1. Go to Application Pools in IIS Manager.
2. Change the .Net Framework Version setting for RSA SecurID Pool to **.NET Framework v4.x**.

Configuring a New SharePoint Server 2010 Site to Use Claims-Based Authentication

In order for SharePoint Server 2010 to work with the single sign-on feature of RSA Authentication Agent for Web, SharePoint must be configured to use claims-based authentication. SharePoint Server 2013 uses claims-based authentication by default, but SharePoint Server 2010 does not. Changing an existing SharePoint site to use claims-based authentication, however, is irreversable. Therefore, RSA recommends creating a new, alternate SharePoint site configured to use claims-based authentication, while preserving the original site and configuration as a fallback.

The following procedures provide an example of how to configure a new Sharepoint 2010 site to use claims-based authentication.

Before You Begin

Access the SharePoint Central Administration home page as follows:

1. Click **Start > Internet Information Services (IIS) Manager > Sites**.
2. Right-click **SharePoint Central Administration** and then select **Manage Web Site > Browse**.

Create Backup

Create a backup of your existing SharePoint site.

1. On the Central Administration home page, click **Backup and Restore**.
2. Under “Granular Backup,” click **Perform a site collection backup**.
3. On the right hand side, make sure the **Site collection** is for the application that currently has your data.
4. Populate the file name, for example:

   c:\temp\sharepoint80.bak

5. Click **Start Backup**.

   The following output appears:

   ```
   Current Job
   Status No operation in progress.
   Previous Job
   Status Succeeded
   Completed 3/14/2014 9:12 AM
   Duration (hh:mm:ss) 0:00:02
   Recovery Step To recover the data, use the PowerShell restore command Restore-SPSite.  For more details, type
   Restore-SPSite -? at the PowerShell command prompt.
   ```

Create Alternate Site

Create a new SharePoint site that uses claims-based authentication.

1. On the Central Administration home page, below "Application Management," click **Manage web applications**.
2. In the uppper left toolbar click **New**.
3. Change the default Authentication from **Classic Mode Authentication** to **Claims Based Authentication**.
4. Select **Create a new IIS web site**. Complete settings as follows:
   - **Name**: For examplle, use **Sharepoint - New**.
   - **Port**: Specify an unused port such as **8080** (this will be changed later to 80/443 after site is tested).
   - **Host Header**: Leave this blank.
   - **Path**: Specify a location that has space similar to the original you are replicating.
   - Make sure the "Application Pool" section has the user you want for running the pool—either **Network Service**, or a domain user that is used on the original SharePoint site.
   - Leave the defaults for all other settings.
5. Scroll to the bottom and click **OK**.

Populate Alternate Site

Now that you have a new site, create a empty collection that you will overwrite with your backup.

1. On the Central Administration home page, click **Application Management**.
2. Under the “Site Collections,” click **Create site collections**.

   Important: Make sure the "Web application" on the right is the **site:8080**.

3. Specify any **Title**.
4. Select a primary and secondary collection administrator.
5. Click **OK.**
6. Test the site to make sure you can log in with the primary or secondary collection administrator, prior to restoring the backup.

Restore SharePoint Data to Alternate Site

Now restore the backup to this newly created IIS / SharePoint instance.

1. Click **Start > All Programs > Microsoft SharePoint 2010 Products > SharePoint 2010 Management Shell**.
2. Run the command **Restore-SPSite -Identity http://<*spssite*> -Path <*path to the .bak file*> -Force**.

   For example:

   ```
   Restore-SPSite -Identity http://sharepoint.rsa.com:8080 -Path c:\temp\sharepoint80.bak -Force
   ```

   If you do not know your SPSite, you can query it by running the following command:

   ```
   Get-SPSite
   ```

Bind Original SharePoint URL to New Site

Once you are confident that the site is working on port 8080, change the alternate access mapping for your original site.

1. On the Central Administration home page, under "System Settings," click **Configure alternate access mappings**.
2. Change the Default URLs to an invalid entry. For example, change **http://sharepoint.rsa.com** to **http://sharepoint.rsa.com.disable**.
3. Change the Alternate Site that was created to **http://sharepoint.rsa.com**.
4. Change the port bindings in IIS Manager as follows:
    a. Highlight the default site (typically **Sharepoint - 80**).
    b. Click **Bindings** in the far right pane.
    c. Change the ports **80** and **443** to invalid ports such as **1080** and **1443**.
    d. Highlight the **Sharepoint - New** instance on the left.
    e. Click **Bindings** in the far right pane.
    f. Change the port from **8080** to **80**.
    g. If using SSL, also add **443** and select the appropriate certificate.

If you encounter issues after performing this procedure, you can revert just the bindings and alternate access mappings to revert to using the original site.

Enabling Single Sign-On on IIS8 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**.
8. Click **Save**.

Using the Web Agent with Active Directory Federation Services

Use the following resources to help you integrate the Web Agent 7.1.3 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*.

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 select **Manage Node Secret** from the drop-down menu.
3. Select the **Clear the node secret** checkbox, and then click **Save**.
4. 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**.
5. Test authentication from RSA Web Agent.
6. Check your authentication logs and ensure a new node secret has been sent.
7. 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