Release Notes
RSA Authentication Agent 8.0.2 for Web for IIS 7.5, 8.0, 8.5, and 10

March 2018

Introduction

This document lists what's new and changed in RSA Authentication Agent 8.0.2 for Web for IIS 7.5, 8.0, 8.5, and 10. It includes upgrade instructions, as well as 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 of these *Release Notes*, and the earlier *Web Agent 8.0.1 for IIS Release Notes*, can be found on RSA Link at **https://community.rsa.com/community/products/securid/authentication-agent-web-iis**.

What's New in This Release

RSA Authentication Agent 8.0.2 for Web for IIS 7.5, 8.0, 8.5, and 10 includes security fixes and other software updates. For more information, see Fixed Issues.

Windows Server 2016 Support. RSA Authentication Agent 8.0 for Web for IIS 7.5, 8.0, 8.5, and 10 supports Windows Server 2016 (64-bit).

Support for Internet Information Services 10. RSA Authentication Agent 8.0 for Web for IIS 7.5, 8.0, 8.5, and 10 adds support for IIS 10 on Windows Server 2016. (64-bit).

The Web Agent continues to support IIS 7.5 on Windows Server 2008 R2 SP1 (64-bit), IIS 8.0 on Windows Server 2012 (64-bit), and for IIS 8.5 on Windows 2012 R2 (64-bit).

Support for Outlook Web App on Windows Server 2016 (64-bit only). RSA Authentication Agent 8.0 for Web for IIS 7.5, 8.0, 8.5, and 10 supports Microsoft Exchange Server 2016 CU3 and later on Windows Server 2016 (64 bit).

The Web Agent continues to support the following

- Outlook Web App on Exchange Server 2016 on Windows Sever 2012 (64-bit) with IIS 8.0 and Windows Server 2012 R2 (64-bit) with IIS 8.5.
- Outlook Web App on Microsoft Exchange Server 2013 SP1 on Windows Server 2008 R2 SP1, Windows Server 2012, and Windows Server 2012 R2.
- Outlook Web App on Microsoft Exchange Server 2010 SP3 (64-bit only).

Note: After every RSA Authentication Agent 8.0 for Web for IIS installation or upgrade, RSA recommends restarting the machine on which the Web Agent is installed. Restarting clears the cache and ensures that any configuration changes take effect.

Product Documentation

The following documentation for RSA Authentication Agent 8.0.2 for Web for IIS 7.5, 8.0, and 8.5 is in the ***doc*** directory.

Title	Filename
RSA Authentication Agent 8.0 for Web for Internet Information Server Installation and Configuration Guide	**WebAgent_IIS.pdf**
RSA Authentication Agent 8.0 for Web for Internet Information Server Developer's Guide	**WebAgentDev_IIS.pdf**

Upgrading to Web Agent 8.0.2

You can upgrade to Web Agent 8.0.2 without uninstalling Web Agent 8.0 or Web Agent 8.0.1.

Before You Begin

If the Web Agent is configured for single sign-on (SSO) to Outlook Web App (OWA), you must disable this feature until the upgrade is complete. For instructions, see "Reconfigure Microsoft Exchange Server" in Chapter 6 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide.*

To upgrade from Web Agent 8.0 or 8.0.1:

1. Extract the files from the Web Agent kit.
2. Click **Setup.exe** and follow the prompts.
3. Restart the machine on which the Web Agent is installed.

Next Steps

- Re-enable SSO on OWA. For instructions, see "Enable Single Sign-On in Microsoft Exchange Server 2013 or 2016" or "Enable Single Sign-On in Microsoft Exchange Server 2010" in Chapter 6 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide.*
- By default, the Web Agent 8.0.2 supports UDP networking. After upgrading to Web Agent 8.0.2, you can enable TCP/IP networking support, instead, if it is required by your deployment. Even if TCP/IP networking support was configured for Web Agent 8.0 or 8.0.1, you must re-enable TCP/IP networking support after upgrading to Web Agent 8.0.1.

  For instructions, see "Change to TCP/IP Networking Support" in Chapter 3 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.
- By default, Web Agent 8.0 or higher enables the **Prevent Caching of Protected Pages on Clients** option on the RSA SecurID web access authentication properties sheet. This option prevents users from accessing protected pages without using RSA SecurID authentication.

  If you are upgrading and this option was not selected before, you should do the following:

  – Select this option. For instructions, see Chapter 4 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

  – Ask your users to clear their cached pages and data from their web browsers. For instructions, see your web browser documentation.
- Web Agent 8.0.2 includes a security change that restricts access to configuration data in the RSA Config Service.

  If any of your existing applications are prevented from running after the upgrade to Web Agent 8.0.2, then the application might not have the correct privileges. For the solution, contact RSA Customer Support.

Fixed Issues

The following issues are fixed in this release.

AAIIS-1409. Corrected an IIS caching issue in which a new user appeared to have the same sessionID as another user on another system.

AAIIS-1452. Updated the Web Agent to provide a workaround for an IIS issue related to using a custom app.

AAIIS-1453. Fixed the option that allows the caching of protected pages. Caching was prevented, even when the administrator wanted to allow caching.

AAIIS-1467. Updated the Web Agent to prevent a buffer overflow issue that was found by a security scanner.

AAIIS-1468, AIIS-1469. Addressed potential security vulnerabilities caused by unexpected input. For more information, see the Security Advisory on RSA Link: **DSA-2018-040**.

AAIIS-1470. Restricted access to configuration data for non-privileged accounts. For more information, see the Security Advisory on RSA Link: **DSA-2018-040**.

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 require administrative privileges. If you do not have the required privileges, contact your administrator.

Web Agent does not protect individual files having non-English characters

Tracking Number: AAIIS-701

Problem: Web Agent 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

The “Use JavaScript pop-up window to authenticate in frames” feature 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 appears again.

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

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

Tracking Number: AAIIS-1014

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

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

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: Select one of the following workarounds:

- **Modify web.config.** Add the following entry in **C:\inetpub\wwwroot\web.config**:

```
<handlers>
      <remove name="ExtensionlessUrlHandler-ISAPI-4.0_64bit" />
      <remove name="ExtensionlessUrlHandler-ISAPI-4.0_32bit" />
</handlers>
```

- **Update the RSA SecurID Pool.** Modify your IIS application pool “RSA SecurID Pool” to point to .NET v2.0 and restart the IIS server.
  - If ASP.NET 4 is not required to run the web site, remap the site to use ASP.NET 2.0 instead.
  - If ASP.NET 4 is required to run the web site, move any child ASP.NET 2.0 virtual directories to a different web site that is mapped to ASP.NET 2.0.

  Note: Microsoft SharePoint Server 2013 SP1 on Windows Server 2012 or Windows Server 2012 R2 requires ,NET Framework 4.x for the “RSA SecurID Pool.” For more information, see the *RSA Authentication Agent 8.0 for Web for IIS 7.5, 8.0, and 8.5 Installation and Configuration Guide*.

- **Edit the Windows Registry.** Do the following:
  1. In the Windows registry, open the following node:

     HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ASP.NET\4.0.30319.0
  2. Create a new DWORD value named **EnableExtensionlessUrls**.
  3. Set **EnableExtensionlessUrls** to **0**. This disables extensionless URL behavior.
  4. Save the registry value and close the registry editor.
  5. Run **IISReset** from the command prompt, which causes IIS to read the new registry value.

     Note: Setting **EnableExtensionlessUrls** to **1** enables extensionless URL behavior. This is the default setting if no value is specified.

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

Cannot verify RSA Authentication Manager Server Status through the Control Panel Utility

Tracking Number: AAIIS-1217

Problem: The RSA ACE/Server Status test in the RSA Authentication Agent Control Panel always displays “Available for Authentications.” If the test fails, the utility does not display any details. In a TCP/IP networking environment, the **Server Release** field displays an ASCII value for the RSA Authentication Manager version.

Workaround: To verify authentication, click **Test Authentication with RSA Authentication Manager** and then click **RSA ACE/Server Test Directly**. Use another approach to verify the RSA Authentication Manager status.

Cannot delete a shared document from the menu bar in Microsoft SharePoint Server 2010 SP2

Tracking Number: AAIIS-1237

Problem: In Microsoft SharePoint Server 2010 SP2, an administrator cannot use the menu bar to delete a shared document.

Workaround: To delete a shared document, right-click the document, and select **Delete** from the drop-down menu.

Authenticating after the keep-alive timeout in Internet Explorer results in an HTTP 400 error

Tracking Number: AAIIS-1283

Problem: When an Internet Explorer user tries to authenticate after the RSA SecurID logon request is left idle for the KeepAliveTimeout number of seconds, an HTTP 400 error message displays. This known issue with Internet Explorer can also occur when the Web Agent is enabled. For more information, go to **https://support.microsoft.com/en-us/** and search for “KeepAliveTimeout.”

Workaround: None.

Users must authenticate a second time when opening Microsoft Office 2010 files with Mozilla Firefox

Tracking Number: AAIIS-1320

Problem: When a SharePoint site is configured to open documents in client applications, Mozilla FireFox users (with the plugin for Microsoft Office 2010) are prompted for RSA SecurID credentials. This issue occurs while opening documents even if persistent cookies are configured.

Workaround: Use a different supported browser. For all supported browsers, persistent cookies must be configured in order to open SharePoint documents in their native applications, such as Microsoft Word documents in Microsoft Office. Follow the configuration procedures in the *Installation and Configuration Guide* or the Web Agent Help.

User must use the Help button to open RSA Authentication Agent Control Panel Help

Tracking Number: AAIIS-1356

Problem: Pressing the F1 key or clicking the ? icon in the RSA Authentication Agent Control Panel does not open the Help.

Workaround: To open the Help, click the **Help** button.

Microsoft Exchange Server 2016 returns users to a different Outlook Web App page after an idle timeout

Tracking Number: AAIIS-1397

Problem: A Microsoft Exchange Server 2016 user who is logged off from the Outlook Web App by an idle timeout might be returned to a different web page after re-authenticating. For example, a user on the options page is returned to the mail page.

Workaround: None.

Microsoft Exchange Server 2016 uses a Master Data Services (MDS) mode that separates URL arguments with hash tags, instead of the question marks used by other products. For example, Microsoft Exchange Server 2016 uses **/owa/#path=/options**, instead of **/owa/?path=/options**. The URL argument that follows the hash tag is not sent to the web server. After a successful authentication, the Web Agent can only return the first part of the URL to the user.

Inconsistent RSA SecurID authentication prompts when editing Microsoft SharePoint Server documents with their native applications

Tracking Number: AAIIS-1413

Problem: Microsoft SharePoint Server does not consistently prompt for RSA SecurID authentication when you edit SharePoint documents in their native applications, such as Microsoft Word documents in Microsoft Office. For example, you may be prompted to authenticate after eight minutes, even though you configured the Web Agent to require re-authentication after a 30-minute session.

This issue does not affect Office Online (Office Web Apps).

Workaround: None. Supporting this environment would require additional development work from Microsoft.

Blank documents and cookie timeout interference when editing Microsoft SharePoint Server 2010 and 2013 documents with their native applications

Tracking Number: AAIIS-1417

Problem: Users might experience issues while editing Microsoft SharePoint Server 2010 or 2013 documents in their native applications, such as Microsoft Word documents in Microsoft Office. A blank page might be displayed when a user opens a document, or when a cookie times out and the user cannot authenticate again, unless the document is closed.

This issue does not affect Office Online (Office Web Apps) because Office Online does not use persistent cookies.

Workaround: Do the following:

1. Configure the Web Agent for Single Sign-On (SSO). For instructions, see Chapter 7, “Configuring the Web Agent to Microsoft Office SharePoint Server” in the *IIS Installation and Configuration Guide*.
2. If you have configured long-term persistent cookies for Microsoft Office, use the asterisk character ***** to protect the ***/Shared/*** documents URL. For instructions, see “Configure Long-Term Persistent Cookies for Microsoft Office” in the *IIS Installation and Configuration Guide*.
3. Configure the system registry:
   a. In the Windows registry, access **HKLM\SOFTWARE\SDTI\RSAWebAgent**.
   b. Create a new REG_DWORD Value named **SharePointFarmSupport**.
   c. Set the Value to **1**.
   d. Create a new REG_SZ Value named **SharePointID**.
   e. Set the value to the SharePoint website ID. Enclose the value in parentheses.
      To determine the website ID, in the IIS Configuration Manager, select **Manage Web Site > Advanced Settings > ID**.
      For example, **SharePointID = (1)**.
   f. Restart IIS. On the IIS server, click **Start > Run**, type **IISReset**, and click **OK**.

When a cookie times out, close the document, authenticate with SecurID, and reopen the document. You can resume editing. No changes are lost.

Chrome returns a “Bad Request” error message when a user re-authenticates to Outlook Web App with more than one tab open

Tracking Number: AAIIS-1433

Problem: A Microsoft Exchange Server 2016 user who is logged off from the Outlook Web App by an idle timeout must re-authenticate. If there are two or more tabs open in the Google Chrome browser, after a successful re-authentication, the wrong URL is returned. This results in a “Bad Request” error message.

Workaround: None. Microsoft Exchange Server 2016 uses a Master Data Services (MDS) mode that separates URL arguments with hash tags, instead of the question marks used by other products. Chrome converts the hash tags into **%23**. For example, Microsoft Exchange Server 2016 uses **https://OWA-Machine-IP/owa/#path=/mail**, but Chrome returns **https://OWA-Machine-IP/owa/%23path=/mail**.

Only Chrome is affected. Other browsers, such as Mozilla Firefox and Internet Explorer, do not experience this issue.

Upgrade to Web Agent 8.0.2 requires disabling SSO to Outlook Web App

Tracking Number: AAIIS-1434

Problem: The upgrade from Web Agent 8.0.0 or Web Agent 8.0.1 to Web Agent 8.0.2 is not successful when the Web Agent is configured for SSO to Outlook Web App (OWA).

Workaround: You must disable SSO to OWA, upgrade to Web Agent 8.0.2, and then re-enable SSO. For instructions, see Upgrading to Web Agent 8.0.2.

When editing Microsoft SharePoint Server documents with their native applications a blank page displays after re-authenticating

Tracking Number: AAIIS-1436

Problem: When editing Microsoft SharePoint Server documents in their native applications, such as Microsoft Word documents in Microsoft Office, a user is prompted to re-authenticate because of an idle timeout. After a successful authentication, a blank page is displayed, instead of the SharePoint site.

Workaround: In some cases, the URLs that are generated when you edit SharePoint Server documents in their native applications do not support persistent cookies. Do the following:

1. Create a Windows registry entry that causes persistent cookies to expire only when the cookie lifetime expires. This prevents persistent cookies from expiring due to an idle timeout. For instructions, see “Remove the Idle Timeout Value for Persistent Cookies” in Chapter 4 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.
2. Enable long-term persistent cookies for the URLs that are used to edit documents. For instructions, see “Configure Long-Term Persistent Cookies for Microsoft Office” in Chapter 7 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.
3. You can disable the RSA Response Interceptor module that monitors web site activity and triggers a modal popup privacy screen when cookies expire. For instructions, see “Disable the RSA Response Interceptor Module” in Chapter 8 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

Modal popup window displayed immediately after authenticating to the Microsoft SharePoint Server site

Tracking Number: AAIIS-1437

Problem: The modal popup window is displayed immediately after logging on to the Microsoft SharePoint Server site.

Workaround: On the RSA SecurID web access authentication properties sheet, select the **Session Logoff** option, instead of the **Modal Popup** option. For more information, see “Configure Advanced Settings” in Chapter 4 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

RSA SecurID Logon page displayed instead of the modal popup window on a Microsoft SharePoint Server site

Tracking Number: AAIIS-1438

Problem: After a cookie expires, the Microsoft SharePoint Server site displays an RSA SecurID Logon page instead of the Modal Popup window.

Workaround: On the RSA SecurID web access authentication properties sheet, select the **Session Logoff** option, instead of the **Modal Popup** option. For more information, see “Configure Advanced Settings” in Chapter 4 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

After an upgrade to Web Agent 8.0.1 in an environment with back end servers, session logoff no longer occurs or users are redirected to a different page following a session logoff

Tracking Number: AAIIS-1441, AAIIS-1442

Problem: After upgrading to Web Agent 8.0.1 in an environment with back end servers, the Microsoft SharePoint Server site does not automatically log off following an idle timeout, or if a session logoff occurs, users are directed to a different page after re-authenticating.

Workaround: If the upgrade did not update the RSAResponseInterceptorModule entry in the **web.config** file for the back end servers, you can copy the front end RSAResponseInterceptorModule entry from **C:\Program Files\RSA Security\RSAWebAgent\WebID\ web.config**. The RSAResponseInterceptorModule entry is in the <modules> tag, which is before the </system.webServer> tag. Paste the following entry into the **web.config** file for the back end servers:

```
<add name="RSAResponseInterceptorModule" type="SecurityModules.ResponseInterceptor,
RSAResponseInterceptorModule, Version=version_number, Culture=neutral,
PublicKeyToken=3b8ca08bdac1d008" />
</modules>
```

Where *version_number* is the correct version number for the Web Agent, for example, **8.0.1.*x***.

If your Web Agent deployment uses Microsoft SharePoint Server, but does not use Microsoft Exchange Server with Outlook Web App (OWA), you can disable the RSA Response Interceptor module to avoid generating network traffic. For instructions, see “Disable the RSA Response Interceptor Module” in Chapter 8 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

Session logoff continues to occur on a SharePoint Server site after persistent cookies are set to never expire

Tracking Number: AAIIS-1444

Problem: Session logoff occurs on a protected SharePoint Server web site, even persistent cookies are set to never expire, as described in “Remove the Idle Timeout Value for Persistent Cookies” in Chapter 4 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

Workaround: You can prevent session logoff by disabling the RSA Response Interceptor module. For instructions, see “Disable the RSA Response Interceptor Module” in Chapter 8 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

SharePoint Server 2013 administrators must set the RSA SecurID Pool to .NET 4.x before enabling Web Agent

Tracking Number: AAIIS-1446, AAIIS-1447

Problem: For SharePoint Server 2013, enabling the Web Agent before setting the RSA SecurID Pool to .NET Framework 4.x results in Web Agent configuration error messages and Windows System Runtime error messages.

Workaround: For SharePoint Server 2013, follow the instructions in “Prerequisites for Using Web Agent with SharePoint Server 2013” in Chapter 7 of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Gu*ide, and then enable the Web Agent, as described in “Protect the Site, Application, Files, or Folders” in Chapter 4. This issue does not affect SharePoint Server 2010 or 2016.

Upgrade to version 8.0.2 might display an error message that can be safely ignored

Tracking Number: AAIIS-1474

Problem: During an upgrade to version 8.0.2, the installer might display the error message “The installer has encountered an unexpected error installing this package. This may indicate a problem with the package. The error code is 2803.” After you click **OK**, the upgrade succeeds.

Workaround: The error message appears to be machine specific. You can safely ignore the error message.

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.

Before You Call Customer Support

Please have your build number available when you call. To locate the build number, do the following:

1. Log on to the machine on which Web Agent is installed.
2. Click **Start > Control Panel > Programs and Features**.
3. Locate the **RSA Authentication Agent for Web for IIS** in the list. The build number follows “8.0.2.”

Trademarks

Intellectual Property Notice