

Release Notes

RSA Authentication Agent 8.0.4 for Web for IIS 7.5, 8.0, 8.5, and 10



June 2020

Introduction

Read this document before installing the software. This document contains the following sections:

- [What's New in This Release](#)
- [Product Documentation](#)
- [Upgrading to Web Agent 8.0.4](#)
- [Content Security Policy Support](#)
- [Fixed Issues](#)
- [Known Issues](#)
- [Support and Service](#)

These *Release Notes* may be updated. The most current version of these *Release Notes*, and additional Web Agent documentation, can be found on RSA Link at

<https://community.rsa.com/community/products/secuid/authentication-agent-web-iis>.

What's New in This Release

RSA Authentication Agent 8.0.4 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](#).

Web Agent 8.0.4 includes the following changes.

Support for a Content Security Policy (CSP). Web Agent 8.0.4 supports using a content security policy (CSP) and CSP HTTP headers to prevent certain types of attacks on trusted web pages, such as cross-site scripting (XSS) and date injection attacks. By default, a CSP is enabled. For more information, see [Content Security Policy Support](#).

Recommendation to Open SharePoint Documents Online. RSA recommends opening SharePoint documents online using Office Online server configuration instead of in their native applications. For example, use Office Online (Office Web Apps), instead of opening Microsoft Word documents in Microsoft Office.

Windows Server 2019 Support. The Web Agent 8.0.4 adds support for the following:

- IIS 10 on Windows Server 2019
- Outlook Web Access (OWA) on Microsoft Exchange Server 2019 CU5 on Windows Server 2019 (Desktop Experience)
Web Agent 8.0.4 does not support OWA on Microsoft Exchange Server 2019 CU5 on Windows Server 2019 (Core)
- SharePoint 2019 on Windows Server 2019
- SharePoint 2019 on Windows Server 2016
- SharePoint 2016 on Windows Server 2019

To configure OWA on Exchange Server 2019 and SharePoint Server 2019, follow the instructions for the 2016 versions of these products. See the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

Outlook Web Access (OWA) Cumulative Updates on Windows Server 2012 R2. RSA qualified the following:

- OWA on Microsoft Exchange Server 2016 CU13
 - OWA on Microsoft Exchange Server 2013 CU23
-

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 8.0.4 for Web for IIS 7.5, 8.0, 8.5, and 10 is in the `\doc` directory.

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

Upgrading to Web Agent 8.0.4

You can upgrade to Web Agent 8.0.4 without uninstalling Web Agent 8.0, Web Agent 8.0.1, Web Agent 8.0.2, or Web Agent 8.0.3.

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*.
- When you upgrade to Web Agent 8.0.4, new HTML templates replace the default templates in the `/templates` directory. If you previously customized these templates, you need to store them in a different directory and specify the location in the web access authentication properties sheet.

To upgrade from Web Agent 8.0, 8.0.1, 8.0.2, or 8.0.3:

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, Web Agent 8.0.4 enables a Content Security Policy (CSP). You can disable the CSP for these reasons:
 - Your Web Agent HTML pages use custom JavaScript that the CSP cannot verify.
 - You use older browsers that do not support a CSP, for example, Internet Explorer 8.0.
 - You use RSA Authentication Manager risk-based authentication (RBA), which relies upon additional templates that are not controlled by the Web Agent.

To disable the CSP, do the following:

- a. On the Web Agent machine, set an environment variable by using the Windows GUI that manages environment variables. For example, go to **Control Panel > All Control Panel Items > System > Advanced system settings > Environment Variables**.

- b. In the System variables section, set NO_CONTENT_SECURITY to 1.
- c. In a Command Prompt window, run IISReset with administrator privileges.
- By default, Web Agent 8.0.4 and Web Agent 8.0.3 support UDP networking.

If you upgraded to Web Agent 8.0.4 from Web Agent 8.0, 8.0.1, or 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, Web Agent 8.0.1, or Web Agent 8.0.2, you must re-enable TCP/IP networking support after upgrading to Web Agent 8.0.4.

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 later 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 8.0.4 corrects an overly restrictive Web Agent 8.0.3 security change involving access to configuration data, which sometimes required an additional procedure after upgrading. After upgrading to Web Agent 8.0.4, the Web Agent 8.0.3 restrictions no longer apply.

Content Security Policy Support

Web Agent 8.0.4 includes a content security policy (CSP) and CSP headers to help prevent certain types of attacks, such as cross-site scripting (XSS) and date injection attacks, on the web pages that are used for RSA SecurID authentication. The Web Agent uses the CSP to prevent browsers from running JavaScript that is not provided by the Web Agent.

Note: This feature does not support RSA Authentication Manager risk-based authentication (RBA).

Security is built into the Web Agent HTML templates and the HTML pages that rely upon them. The JavaScript functions on the HTML page can only run if they have a nonce value that matches the nonce value provided by the CSP. The nonce value is a long, pseudorandom combination of letters and numbers that is used only one time, similar in concept to an RSA SecurID tokencode, for example, zcoD67ms1BuX3kt9vuQmbtQeZA2. The nonce value changes each time the page loads. If an attacker inserts malicious JavaScript, refreshing the page changes the nonce value, and the script does not run.

You cannot apply a global web server policy containing a nonce value to these HTML pages. Global nonce values are not possible because the nonce value changes each time an individual HTML page loads.

You can verify that the CSP is being applied by viewing the source on your HTML pages. For example, in Internet Explorer, right-click the page and select **View source**. The HTML code displays a meta tag such as this one:

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self'
'nonce-zcoD67ms1BuX3kt9vuQmbtQeZA2' object-src 'self'">
```

JavaScript functions display a matching nonce value:

```
<script language="JavaScript" nonce="zcoD67ms1BuX3kt9vuQmbtQeZA2">
```

Fixed Issues

The following issues are fixed in this release.

AAIS-1511. Applications can retrieve the RSA username with an RSAUSER cookie, which replaces the HTTP_RSAUSER variable that was previously used. To configure the RSAUser cookie, set the following registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\RSAWebAgent\  
    RSAUSERCustomHeader = 1 (REG_DWORD)
```

AAIS-1518. Web Agent allows applications to use the Identity property ApplicationPoolIdentity for any application pool.

AAIS-1533. Updated the copyright information that displays as system information in the Web Agent binaries.

AAIS-1534. Resolved an issue in which the Web Agent might prompt for credentials or supply single-sign on credentials on URLs that are not meant to be protected. For example, OWA does not protect Active Sync URLs, and prompting for credentials caused unexpected behavior. This issue occurred on busy systems with a high volume of network traffic.

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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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: AAIS-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 8.0.4](#).

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

Tracking Number: AAIS-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: AAIS-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: AAIS-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: AAIS-1441, AAIS-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: AAIS-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: AAIS-1446, AAIS-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 Guide*, 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: AAIS-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.

SharePoint Server documents could not be opened in Microsoft Office 2013 when persistent cookies were set to expire only when the cookie lifetime expires

Tracking Number: AAIS-1488

Problem: In some cases, when the **PersistentCookieIdleTime** registry key is set to zero, which makes persistent cookies expire only when cookie lifetime expires, Microsoft Office 2013 could not open documents, but Microsoft Office 2010 could.

Workaround: .Make sure to configure the correct URLs for long-term persistent cookies. Follow the instructions in “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*, and configure the following URLs:

/shared documents/

/_vti_bin/cellstorage

/_vti_bin/sharedaccess

/_vti_bin/webs

Need to reauthenticate while actively editing a SharePoint Server 2013 or 2016 document with Microsoft Office 2013 or 2016

Tracking Number: AAIS-1489, AAIS-1492

Problem: Reauthentication is required at short intervals while actively editing a SharePoint Server 2013 or 2016 document with Microsoft Office 2013 or 2016. Persistent cookies are configured correctly, but SharePoint Server does not refresh the cookies, and so an idle timeout occurs. Microsoft Office 2010 does not experience this issue.

Workaround: Make persistent cookies expire only when cookie lifetime expires. Follow the instructions in “Remove the Idle Timeout Value for Persistent Cookies” in Chapter 4 of the of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

Unable to sign into an Office document after reauthenticating

Tracking Number: AAIS-1490

Problem: When editing SharePoint Server documents using Microsoft Office, if the cookie expires, after reauthenticating through browser, the Sign-In option does not work. To sign in, you must close the document and open it again.

Workaround: Make persistent cookies expire only when cookie lifetime expires. Follow the instructions in “Remove the Idle Timeout Value for Persistent Cookies” in Chapter 4 of the of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

Prompted twice for Windows credentials when opening a SharePoint Server 2016 document with Microsoft Office 2016

Tracking Number: AAIS-1491

Problem: When opening a SharePoint Server 2016 document with Microsoft Office 2016, a user is prompted for Windows credentials, then prompted for RSA SecurID authentication, and then prompted a second time for Windows credentials. SharePoint Server 2013 does not experience this issue.

Workaround: Make persistent cookies expire only when cookie lifetime expires. Follow the instructions in “Remove the Idle Timeout Value for Persistent Cookies” in Chapter 4 of the of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

Must register the SecurIDSSOModule before setting up single sign-on to the SharePoint Server

Tracking Number: AAIS-1497

Problem: On a new Windows server, you must register the SecurIDSSOModule before you can configure the Web Agent for single sign-on to the SharePoint Server 2013 or 2016.

Workaround: For instructions, Chapter 7, “Configuring the Web Agent to Microsoft SharePoint Server” in the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

Mozilla FireFox users are prompted a second time for RSA SecurID authentication when they open a document with Microsoft Office 2016 on a SharePoint Server 2016 website

Tracking Number: AAIS-1499

Problem: Mozilla FireFox users are prompted for RSA SecurID authentication when they access a SharePoint Server 2016 website. When they open a SharePoint Server document with Microsoft Office 2016, they are again prompted for RSA SecurID authentication. Only FireFox is affected. Other browsers, such as Chrome and Internet Explorer, do not experience this issue.

Workaround: Make persistent cookies expire only when cookie lifetime expires. Follow the instructions in “Remove the Idle Timeout Value for Persistent Cookies” in Chapter 4 of the of the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

RSA Archer web site requires additional configuration to enable RSA SecurID authentication

Tracking Number: AAIS-1525

Problem: Instead of prompting for RSA SecurID authentication, the RSA Archer web site displayed the runtime error “Server Error in ‘/WebID’ Application.”

Workaround: Do the following:

1. Change the application pool for Archer (Default Website) to Classic mode.
2. Verify that `runAllManagedModulesForAllRequests` is set to `false`:

```
<modules runAllManagedModulesForAllRequests="false" />
```

For example, in the Internet Information Services (IIS) Manager, in the left pane, click **Web Site**, and then in the middle pane, after Management, double-click **Configuration Editor**.

3. Edit the Archer (root) **web.config** file:
 - a. In the config section, remove `preCondition="managedHandler"`:

```
<add name="AntiRequestForgeryModule"
type="ArcherTech.Web.HttpHandlers.AntiRequestForgeryModule, ArcherTech.Web"
preCondition="managedHandler" />
```

- b. Remove `requireAccess="Script"` from the sections shown below:

```
<add path="*.htm" verb="*"
type="ArcherTech.Web.HttpHandlers.FileAuthenticationHandler, ArcherTech.Web"
validate="false" requireAccess="Script" />
```

```
<add path="*.html" verb="*"
type="ArcherTech.Web.HttpHandlers.FileAuthenticationHandler, ArcherTech.Web"
validate="false" requireAccess="Script" />
```

```
<add path="*.pdf" verb="*"
type="ArcherTech.Web.HttpHandlers.FileAuthenticationHandler, ArcherTech.Web"
validate="false" requireAccess="Script" />
```

Internal URL unable to redirect to an external URL after RSA SecurID authentication

Tracking Number: AAIS-1531

Problem: An internal URL that is protected by RSA SecurID authentication is configured to redirect to an external URL. Users who access the internal URL are prompted to authenticate, but after they successfully authenticate, some users receive an error instead of redirecting to the external URL.

Session cookies are not being used for the redirect. Security scanner software might be removing these cookies.

Workaround: Configure persistent cookies. For instructions, see “Configure Long-Term Persistent Cookies for Microsoft Office” in the *RSA Authentication Agent 8.0 for Web for IIS Installation and Configuration Guide*.

Both session cookies and persistent cookies use the idle timeout value that is specified by the “Cookies expire if not used within the specified time” advanced setting in the RSA SecurID web access authentication properties sheet. However, unlike session cookies, which expire, persistent cookies are available after an idle timeout, but they require the user to authenticate again.

SharePoint Server 2019 web site displays the runtime error “Server Error in ‘WebID’ Application”

Tracking Number: AAIS-1532

Problem: After configuring SharePoint Server 2019 for RSA SecurID authentication, if you try to access the protected website, the runtime error “Server Error in ‘WebID’ Application” displays.

Workaround: SharePoint Server 2019 includes an automatic startup feature that is not compatible with the Web Agent. To disable this feature, use a text editor to open the following file:

c:\inetpub\wwwroot\wss\VirtualDirectories\80\web.config

Change the value of owin:AutomaticAppStartup to “false,” as shown below:

```
<appSettings>
  <add key="owin:AutomaticAppStartup" value="false" />
</appSettings>
```

Outlook Web Access requires RSA SecurID authentication on multiple tabs after a session times out

Tracking Number: AAIS-1541

Problem: When a session times out, Outlook Web Access (OWA) on Exchange Server 2016 and Exchange Server 2019 requires users to authenticate again on each open tab. Users might expect to perform RSA SecurID authentication one time.

Workaround: None. The need to re-authenticate on each open tab is a feature of OWA on Exchange Server 2016 and Exchange Server 2019. Other versions of OWA behave differently.

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 "8.0.4."

Copyright © 2015-2020 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

Dell, RSA, the RSA Logo, EMC and other trademarks are either registered trademarks or trademarks of Dell, Inc. or its subsidiaries. All other trademarks may be trademarks of their respective owners. For a list of RSA trademarks, go to <http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa>.

Intellectual Property Notice

This software contains the intellectual property of Dell Inc or it is licensed to Dell Inc from third parties. Use of this software and the intellectual property contained therein is expressly limited to the terms and conditions of the License Agreement under which it is provided by or on behalf of Dell Inc. or its subsidiaries.