

Release Notes

RSA Access Manager Web Agent 5.0 SP2



September 29, 2014

Introduction

This document lists what's new and changed in RSA Access Manager Web Agent 5.0 SP2. It includes additional installation information, as well as workarounds for known issues. Read this document before installing the software. This document contains the following sections:

- [What's New In This Release](#)
- [Fixed Issues](#)
- [Known Issues](#)
- [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>.

What's New In This Release

This section describes the major changes introduced in this release. For detailed information on each change, refer to the *RSA Access Manager 5.0 SP2 for Web Servers Installation and Configuration Guide*.

Microsoft Office SharePoint 2013 Claims-based Authentication Support. RSA Access Manager supports Single Sign-On (SSO), leveraging claims-based authentication for SharePoint 2013

Support to choose challenge method for Adaptive Authentication. RSA Access Manager provides the flexibility for the user to select the challenge method while being challenged for Adaptive Authentication.

Mobile browser support. RSA Access Manager Web Agent 5.0 SP2 supports Safari browser on iOS 5.1.x and Chrome browser on Android 4.4.2.

Microsoft Outlook Web Access (2013) Single Sign-On Support. RSA Access Manager Web Agent 5.0 SP2 supports Windows Single Sign-On (SSO) into Outlook Web Access (OWA) 2013 for IIS 8.0 web server.

New Supported Platforms

- IBM HTTP Server (IHS) 8.5 (64-bit) on AIX 7.1
- Apache 2.2.23 (64 bit) on Oracle Solaris 11.2 (SPARC 64)
- Apache 2.2.23 (32 bit) on Oracle Solaris 11.2 (SPARC 64)
- Oracle iPlanet Web Server 7.0 Update 15 (64-bit) on Oracle Solaris 11.2 (SPARC 64)
- Oracle iPlanet Web Server 7.0 Update 15 (32-bit) on Oracle Solaris 11.2 (SPARC 64)
- IIS Web Server 8.5 (64-bit) on Microsoft Windows Server 2012 R2 Standard (x86-64 bit)
- IIS Web Server 8.5 (32-bit) on Microsoft Windows Server 2012 R2 Standard (x86-64 bit)

Supported Platforms From Previous Releases

- IBM HTTP Server (IHS) 8.5 (64-bit)
 - Red Hat Enterprise Linux Edition 6.2 (x86-64 bit)
 - Red Hat Enterprise Linux Edition 6.4 (x86-64 bit)
 - AIX 6.1
- IBM HTTP Server (IHS) 8.5 (32-bit) for Microsoft Windows Server 2008 R2 SP1 Enterprise (x86-64 bit)
- IIS Web Server 8.0 (64-bit) on Microsoft Windows Server 2012 Standard (x86-64 bit).

RSA Access Manager Web Agents 5.0 SP2 Release Notes

- Apache 2.2.23 Web Server (32-bit)
 - SUSE Linux Enterprise Server 10 and SUSE Linux Enterprise Server 11(x86)
 - Oracle Solaris 10 (SPARC64)
 - Red Hat Enterprise Linux Edition 6.0 (x86)
- Apache 2.2.23 Web Server (64-bit)
 - SUSE Linux Enterprise Server 10 and SUSE Linux Enterprise Server 11 on (x86-64 bit)
 - Oracle Solaris 10 (SPARC64)
 - Red Hat Enterprise Linux Edition 6.0 (x86-64 bit)
 - HP-UX 11i v3 (IA64)
- Apache 2.2.22 Web Server (64-bit) on Microsoft Windows Server 2008 R2 SP1 (x86-64 bit).
- Apache 2.2.22 Web Server (32-bit) on Microsoft Windows Server 2008 R2 SP1(x86-64 bit).
- Apache 2.4.3 Web Server (64-bit)
 - Red Hat Enterprise Linux Edition 6.0 (x86-64 bit)
 - SUSE Linux Enterprise Server 11 (x86-64 bit)
- Oracle iPlanet Web Server 7.0 Update 15 (64-bit).
 - Oracle Solaris 10 (SPARC64)
 - Red Hat Enterprise Linux 5.5 on (x86-64 bit)
- Oracle iPlanet Web Server 7.0 Update 15 (32-bit).
 - Oracle Solaris 10 (SPARC64)
 - Red Hat Enterprise Linux 5.5 (x86)
- IBM HTTP Server (IHS) 7.0 (32-bit)
 - Microsoft Windows Server 2008 R2 SP1 Enterprise (x86-64 bit)
 - AIX 6.1
 - Red Hat Enterprise Linux 6.2 on (x86-64 bit)
- IBM HTTP Server (IHS) 8.5 (32-bit) on AIX 6.1
- IIS Web Server 7.0 (64-bit) on Microsoft Windows Server 2008 Enterprise SP2 (x86-64 bit).
- IIS Web Server 7.0 (32-bit) on Microsoft Windows Server 2008 Enterprise SP2 (x86) and (x86-64 bit).
- IIS Web Server 7.5 (64-bit) on Microsoft Windows Server 2008 Enterprise R2 SP1 (x86-64 bit).
- IIS Web Server 7.5 (32-bit) on Microsoft Windows Server 2008 Enterprise R2 SP1 (x86-64 bit).
- IBM Domino Web Server 8.5 (32-bit) on Oracle Solaris 10 (SPARC 64).
- Microsoft Forefront Threat Management Gateway (TMG) 2010 on Microsoft Windows Server 2008 Enterprise R2 SP1 (x86-64 bit).

Supported Browsers

- Mozilla Firefox
- Microsoft Internet Explorer version 8, 9, 10, and 11.
- Google Chrome
- Safari 6.0.5
- Mobile browsers
 - Safari browser on iOS 5.1.x

- Chrome browser on Android 4.4.2

Fixed Issues

This section lists the issues that have been fixed in this release along with the following items:

- [Fixed Issues in Web Agent 5.0 SP2 Release](#)
- [Hotfixes Rolled up in Web Agent 5.0 SP2 Release](#)
- [Enhancements for Web Agent 5.0 SP2 Release](#)

Fixed Issues in Web Agent 5.0 SP2 Release

Tracking Number	Description
CTAG-4782	Support for deviceprint javascript shipped with AA 7.x
CTAG-4795	AXM-AA integration fails when using same user id (with different cases) are used.

Hotfixes Rolled up in Web Agent 5.0 SP2 Release

Bug Number	HotFix Number	Description
CTAG-4842	4.9.1.23	With IIS7 agent, Username and password are echoed back to the browser as part of the response header.
CTAG-4696	5.0.1.05	Touch time is not updated after idle/session timeout, if user tries to authenticate by accessing the logon page directly.
CTAG-4792	5.0.1.04	User properties are not published when cleartrust.agent.userprops_level is set to AuthN.
CTAG-4794	5.0.1.03	In new pin mode, SecurID authentication fails when cleartrust.agent.use_query_string is set to True.
CTAG-4734	5.0.1.02	Add support for WSFed wreply parameter in AxM-STS.
CTAG-4517	5.0.1.01	IIS agent does not report whether agent is configured as HTTP module or ISAPI filter in the agent log file.
CTAG-4691 CTAG-4692	5.0.0.05	AxM-STS sends duplicate requests when configured for claims based authentication. AxM-STS fails to encrypt the claims.
CTAG-4657	5.0.0.04	While attempting CERTIFICATE authentication after idle/session timeout, AxM agent reports CT_AUTH_UNKNOWN_ERROR
CTAG-4748	4.9.3.13	Apache agent while attempting certificate authentication crashes with Segmentation fault.

Enhancements for Web Agent 5.0 SP2 Release

Enhancements	Description
CTAG-4776	Support for configuring other non-AA methods such as BASIC, NT, Custom, SECURID before AA.

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. For many of the workarounds in this section, you must have administrative privileges. If you do not have the required privileges, contact your administrator.

Cookie Cache does not differentiate between authorization server pools.

Tracking Number: CTAG-1734

Problem: The RSA Access Manager agent maintains a single cache for user tokens, and does not differentiate between Authorization Server connection pools.

Workaround: If the Authorization Server pools for web server virtual hosts are configured to point to different RSA Access Manager Authorization Servers, you must assign a unique cleartrust.agent.cookie_name to each group of virtual hosts, so that cached credentials are maintained locally for each server. Note that Single Sign On (SSO) does not work in this configuration.

Lock rule does not work as intended when RSA Access Manager agent for Apache web server on UNIX is configured with Rules.xml

Tracking Number: CTAG-2096

Problem: When RSA Access Manager Agent for Apache web server on UNIX platform is configured with Rules.xml, the IP lock rule does not work as expected.

Workaround: None.

Post-form is posting with empty data, even after successful NTLM authentication.

Tracking Number: CTAG-2734

Problem: After a successful Windows NT LAN Manager (NTLM) authentication using Microsoft Internet Explorer 6.0 or later versions, posting data to the web server fails. When a user tries to post data to the web server after successful NTLM authentication, Internet Explorer requires the user to submit the domain credentials again and post data is lost in the process.

Workaround: Microsoft has confirmed this to be a problem with Microsoft Internet Explorer 6.0 and later versions, and has provided a workaround. For more information about the workaround, see this [Microsoft article](#).

When ctagent.log file is Deleted, it does not Allow Restart Without Changes.

Tracking Number: CTAG-1703

Problem: In Windows 2008, deleting the "logs" folder to remove all log files results in the IIS Agent not restarting successfully. The agent does not log any information or error.

Workaround: In Windows 2008, the IIS Agent installer creates the empty Logs folder with Write and Modify permissions to all Users of that machine. This allows the IIS agent to log information in any file under Logs folder. To avoid this problem:

- You must only delete ct_agent.log file.
- If you delete the "logs" folder, grant write and modify permissions to <machine>/USERS along with read and other default permissions

When the Access Manager session times out, saving an edited document fails.

Tracking Number: CTAG-3569

Problem: When the Access Manager session times out and if update polling intervals and opening document management pane at startup is not enabled in the Microsoft Office client, saving an edited document fails.

Workaround: You must save the document locally and then upload it to the SharePoint site.

French Characters not getting displayed correctly for RSA Access Manager Agent JSP Pages deployed on Tomcat 7 or WAS 7

Tracking Number: CTAG-3896

Problem: For RSA Access Manager Agent JSP pages deployed on Tomcat 7 or WAS 7, user's enrolled information is getting displayed in "ISO-8859-1" encoding instead of "UTF-8" encoding format. As a result, the french characters are displayed incorrectly during user challenge or editing the enrollment data.

Workaround: None.

Special Symbols get displayed on Licence Agreement when Agent is installed in Console Mode.

Tracking Number: CTAG-4439

Problem: When you read through the license agreement in the installers, you will find some special symbols.

Workaround: None.

Support and Service

RSA SecurCare Online	https://knowledge.rsasecurity.com
Customer Support Information	www.rsa.com/support
RSA Secured Partner Solutions Directory	https://gallery.emc.com/community/marketplace/rsa?view=overview

Copyright © 2014 EMC Corporation. All Rights Reserved. Published in the USA.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.rsa.com/legal/trademarks_list.pdf.