

# Release Notes

## RSA Access Manager Web Agent 5.0 SP3



July 21, 2015

---

### Introduction

This document lists what's new and changed in RSA Access Manager Web Agent 5.0 SP3 (Access Manager Web Agent). 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](#)
- [Platform Information](#)
- [Related Products](#)
- [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 about each feature, refer to the *RSA Access Manager Web Agent 5.0 SP3 Installation and Configuration Guide*.

- Support for Silent upgrade and re-installation.  
Access Manager Web Agent patch installer now supports upgrade and re-installation in Silent Mode.
- Support for SecurID as an Adaptive Authentication credential type.  
Access Manager Web Agent supports SecurID as an Adaptive Authentication credential type to provide enhanced security by authenticating a user using RSA Authentication Manager

### New Supported Platforms

- Apache™ HTTP Server 2.2.29 (32-bit)
  - Microsoft® Windows® Server 2012 R2 Standard (x86\_64)
- Apache HTTP Server 2.2.29 (64-bit)
  - Microsoft Windows Server 2012 R2 Standard (x86\_64)
- IBM® HTTP Server 8.5 (32-bit)
  - Microsoft Windows Server 2012 R2 Standard (x86\_64).

---

### Platform Information

This section lists the platform and operating systems supported by Access Manager Web Agent at the time of release.

#### Supported Platforms

- Apache HTTP Server 2.4.12 (64-bit)
  - Red Hat® Enterprise Linux 6.6 (x86\_64)
  - Novell® SUSE® Linux Enterprise Server 11 (x86\_64).

- Apache HTTP Server 2.2.29 (32-bit)
  - Microsoft Windows Server 2008 R2 Enterprise SP1 (x86\_64)
  - Novell SUSE Linux Enterprise Server 11 (x86)
  - Novell SUSE Linux Enterprise Server 10 (x86)
  - Oracle® Solaris 11.2 (SPARC64™)
  - Oracle Solaris 10 (SPARC64)
  - Red Hat Enterprise Linux 6.6 (x86)
- Apache HTTP Server 2.2.29 (64-bit)
  - HP-UX 11i v3 (IA64)
  - Microsoft Windows Server 2008 R2 Enterprise SP1 (x86\_64)
  - Novell SUSE Linux Enterprise Server 11 (x86\_64)
  - Novell SUSE Linux Enterprise Server 10 (x86\_64)
  - Oracle Solaris 11.2 (SPARC64)
  - Oracle Solaris 10 (SPARC64)
  - Red Hat Enterprise Linux 6.6 (x86\_64).
- IBM Domino® Web Server 8.5 (32-bit)
  - Oracle Solaris 10 (SPARC64).
- IBM HTTP Server 8.5 (64-bit)
  - AIX® 7.1 (PowerPC)
  - AIX 6.1 (PowerPC)
  - Red Hat Enterprise Linux 6.6 (x86\_64).
- IBM HTTP Server 8.5 (32-bit)
  - AIX 6.1 (PowerPC)
- IBM HTTP Server 7.0 (32-bit)
  - AIX 6.1 (PowerPC)
  - Microsoft Windows Server 2008 R2 Enterprise SP1 (x86\_64)
  - Red Hat Enterprise Linux 6.6 (x86\_64).
- Microsoft Internet Information Services (IIS) 8.5 (32-bit)
  - Windows Server 2012 R2 Standard (x86\_64).
- Microsoft IIS 8.5 (64-bit)
  - Windows Server 2012 R2 Standard (x86\_64).
- Microsoft IIS 8.0 (64-bit)
  - Windows Server 2012 Standard (x86\_64).
- Microsoft IIS 7.5 (32-bit)
  - Windows Server 2008 R2 Enterprise SP1 (x86\_64).
- Microsoft IIS 7.5 (64-bit)
  - Windows Server 2008 R2 Enterprise SP1 (x86\_64).

- Microsoft IIS 7.0 (32-bit)
  - Windows Server 2008 Enterprise SP2 (x86)
  - Windows Server 2008 Enterprise SP2 (x86\_64).
- Microsoft IIS 7.0 (64-bit)
  - Windows Server 2008 Enterprise SP2 (x86\_64).
- Microsoft Forefront® Threat Management Gateway 2010 (64-bit)
  - Windows Server 2008 R2 Enterprise SP1 (x86\_64).
- Oracle iPlanet® Web Server 7.0 Update 15 (32-bit)
  - Solaris 11.2 (SPARC64)
  - Solaris 10 (SPARC64)
  - Red Hat Enterprise Linux 6.6 (x86).
- Oracle iPlanet Web Server 7.0 Update 15 (64-bit)
  - Solaris 10 (SPARC64)
  - Solaris 11.2 (SPARC64)
  - Red Hat Enterprise Linux 6.6 (x86\_64).

---

**Note:** Unless mentioned otherwise, 32-bit support means that all the 32-bit Access Manager Web Agents are supported on 32-bit web servers installed on 32-bit operating systems. On Solaris, both 32-bit and 64-bit installation of web servers are supported.

---

---

## Related Products

This section lists the supported related products.

### Supported Access Manager Servers

- Access Manager Server 6.2
- Access Manager Server 6.2 SP1
- Access Manager Server 6.2 SP2
- Access Manager Server 6.2 SP3.

### Supported Browsers

- Google® Chrome®
- Microsoft Internet Explorer® version 8, 9, 10, and 11
- Mozilla® Firefox®
- Apple® Safari® 6.0.5
- Mobile browsers:
  - Apple Safari browser on iOS 8.x
  - Google Chrome on Android® 5.x.

## Fixed Issues

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

- [Issues Fixed in this Release](#)
- [Enhancements for this Release](#)
- [Hotfixes Incorporated in this Release](#)

### Issues Fixed in this Release

---

Issue ID	Description
CTAG-4899	Access Manager Web Agent on Apache is Filling Swap Space.
CTAG-4645	Grammatical error in warning message.
CTAG-4142	In Apache Access Manager Web Agent, the Apache short property names that correspond to the latest Access Manager parameters are missing.
CTAG-3994	Add 32 bit or 64 bit designation to Access Manager Web Agent version information in log file.

---

### Enhancements for this Release

---

Issue ID	Description
CTAG-4775	For IWA Authentication, Access Manager Web Agent uses the CT_ORIG_URL query string based redirection when cookie based URL retention is enabled.

---

### Hotfixes Incorporated in this Release

---

Hotfix	Issue ID	Description
5.0.2.04	CTAG-5022	While TMG Access Manager Web Agent updates the cookie, illegal characters are appended to the response.
5.0.2.03	CTAG-5018	Access Manager Web Agent incorrectly logs SSL message at <Critical> log level.
5.0.2.02	CTAG-4985	Access is denied for unprotected resources after trying to login with non-existent user name.
5.0.2.01	CTAG-4968	Access Manager Web Agent incorrectly logs SSL message at <Critical> log level.
5.0.1.10	CTAG-4886	

---

## 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 Access Manager Web 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 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 Access Manager Web Agent for Apache web server on UNIX is configured with Rules.xml

**Tracking Number:** CTAG-2096

**Problem:** When Access Manager Web 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 [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 Access Manager Web Agent not restarting successfully. The Access Manager Web Agent does not log any information or error.

**Workaround:** In Windows 2008, the IIS Access Manager Web Agent installer creates the empty Logs folder with Write and Modify permissions to all Users of that machine. This allows the IIS Access Manager Web Agent to log information in any file under the 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 Access Manager Web Agent JSP Pages deployed on Tomcat 7 or WAS 7

**Tracking Number:** CTAG-3896

**Problem:** For Access Manager Web 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 Access Manager Web 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	<a href="https://knowledge.rsasecurity.com">https://knowledge.rsasecurity.com</a>
Customer Support Information	<a href="http://www.emc.com/support/rsa/index.htm">http://www.emc.com/support/rsa/index.htm</a>
RSA Ready Community	<a href="https://community.emc.com/community/connect/rsaxchange/rsa-ready?view=overview">https://community.emc.com/community/connect/rsaxchange/rsa-ready?view=overview</a>

---

Copyright © 2015 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 <http://www.emc.com/legal/emc-corporation-trademarks.htm>