Release Notes
RSA Access Manager 6.1

August 14, 2009

Introduction

This document lists what's new and changed in RSA Access Manager 6.1. It includes additional installation information, as well as workarounds for known issues. RSA recommends that you read this document before installing and using RSA Access Manager 6.1. This document contains the following sections:

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

To view product documentation delivered in PDF format, you need the Adobe Acrobat Reader. To download the latest version of the Reader, go to www.adobe.com.

Note

The 3.5 RSA ClearTrust Web Server Agents and version 1 tokens are not supported from this release.

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 appropriate *RSA Access Manager guide*.

Secure Delegated Impersonation. You can now delegate administrators to act as impersonators and access the applications used by other users and troubleshoot the issues that the users face. For more information, see the *Servers Installation and Configuration Guide*.

Unique User Session. You can now enable the user session to be active on only one IP address. For more information, see the *Servers Installation and Configuration Guide*.

Dynamic Debugging. You can now enable or disable debugging without restarting the Access Manager Servers. For more information, see the *Servers Installation and Configuration Guide*.

User Self-Service Console. RSA Access Manager provides a web-based User Self-Service Console to let your users change or reset their passwords and update attributes such as first name, email, and other custom properties. For more information, see the *Servers Installation and Configuration Guide*.

RSA enVision Integration. You can integrate RSA Access Manager with RSA enVision to manage your logs. For more information, see the *Planning Guide*.

Support for Additional Data Stores. RSA Access Manager now supports the use of the following new or updated data stores:

- Oracle 10g Release 2 (10.2) RAC
- Microsoft SQL 2005 SP3
- Microsoft SQL 2008
- Microsoft Active Directory (AD) on Microsoft Windows Server 2008
- Microsoft Active Directory (AD) in combination with Active Directory Application Mode (ADAM) on Microsoft Windows Server 2008
- Sun Java System Directory Server 6.3
- Novell eDirectory 8.8.0

For more information, see the *Servers Installation and Configuration Guide*.

Support for JDBC Driver. RSA Access Manager now supports the use of Oracle driver version 10g (10.2.0.1 or later) JDBC driver.

Custom Password Restrictions. In addition to the password policy in Access Manager, you can write your own listener classes to enforce any extra validation for the passwords of the users that are created or modified. For more information, see the *Servers Installation and Configuration Guide*.

Enhanced Java Runtime Environment (JRE) Support. To scale up better for large deployments, you can now run RSA Access Manager Servers using a 64-bit Java Virtual Machine. RSA Access Manager Servers now inculde JRE 1.6 and also supports IBM JRE5 and JRE6 for AIX . For more information, see the *Servers Installation and Configuration Guide*.

Utility to Secure Configuration Files. RSA Access Manager provides an encryption utility called manage-config that lets you protect the Access Manager configuration files. For more information, see the *Servers Installation and Configuration Guide*.

Other Enhancements

Default Bind Credentials for LDAP Referrals. LDAP server can now be configured using the **ldap.conf** file to bind to other directory servers, whose referral locations are unknown while following referrals.

Handling LDAP Exceptions. LDAP exceptions created due to authentication failures, such as disabled account/password, expired account/password, and user failed to change the password on first logon can now be logged with appropriate messages in the log files for the administrator to view. For more information, see the *Servers Installation and Configuration Guide*.

New Bad Token Cache Support. Similar to token cache of the Authorization Server, bad token cache is supported and is configurable. Simple network management protocol (SNMP) can be used to get statistics of bad token errors and bad token cache. For more information, see the *Servers Installation and Configuration Guide*.

Enhanced Logging. RSA Access Manager now provides more detailed log messages in the respective Access Manager Server log files. For more information, see the *Servers Installation and Configuration Guide*.

Increase efficiency of LDAP queries. The number of reduntant LDAP queries that are executed by Access manager is reduced to improve the LDAP performance.

JVM statistics through SNMP. You can now monitor the statistics of the functioning of JVM for the Access Manager Servers. For more information, see the *Servers Installation and Configuration Guide*.

New Administrative Privileges. RSA Access Manager provides two new administrative privileges in the Administrative Console called Config Admin and Audit Admin. You can use this administrative privileges to modify parameter in an encrypted server configuration file. For more information, see the *Administrator's Guide*.

^Top

Hotfixes

The following list includes the hotfixes made since RSA Access Manager 6.0 that have been integrated into RSA Access Manager 6.1.

Issue	Hotfix	Description
41084	6.0.0.01	First roll-up hotfix for AXM 6.0
41378	6.0.0.02	The Admin GUI is not able to get new LDAP connections since the LDAP Server has multiple TCP connections in CLOSE_WAIT state
42051	6.0.0.03	Logging enhancements
43928	6.0.0.04	Support IBM JRE 1.5 and IBM JSSE
44662	6.0.0.05	55 to 60 Schema Upgrade for delegated admin is broke
44986	6.0.0.06	Hotfix 3 breaks creating group with user through admin API
45354	6.0.0.07	JRE for CT 6.0 does not handle 2007 DST changes
45441	6.0.1.01	Iserver CPU usage increase after failover
46028	6.0.1.02	Connections to LDAP are being dropped/restored continually
46208	6.0.1.03	Weblogic 9.0 license is not unlimited
46227	6.0.2.01	Allow to set windows flags on account creation even when windows_lockout is set to false
45941	6.0.2.02	Build cleartrust.jar with synchronization fix
45867	6.0.2.03	Protected URL cache flush can cause thread leaks
46074	6.0.2.04	Oracle cursors are not closed when adding users to groups
46322	6.0.2.05	The ct_runtime_api.h documentation is incomplete
46359	6.0.2.06	LDAP failover not working when an LDAP server abruptly becomes unreachable
46405	6.0.2.07	Concurrent mod exception in logs
46492	6.0.2.08	OutOfMemoryError on Dispatcher when an Agent has an expired cert
46682	6.0.2.09	Admin API IUser.setProperty is case sensitiive when caching is enabled
46753	6.0.2.10	With a large number of connections JRE runs out of heap
53468	6.0.2.11	ldap.auxuser.scope parameter not working
55550	6.0.2.12	aserver throws "not connected (80); Unknown error" after certain LDAP searches
55846	6.0.2.13	Performance issue when adding a user to a group with eserver.log.verbose=true
56121	6.0.2.14	Any type of persistent connection to dispatcher port will eventually cause denial of service for dispatcher process
56024	6.0.2.15	ctws.war doesn't work in weblogic 9.0
56181	6.0.2.16	DAL passwords visible via SNMP
56431	6.0.2.17	Request Latest JNetDirect JSQLConnect Release 5.5
57513	6.0.2.18	Restricted Java Runtime API
58039	6.0.2.19	Unable to remove admin rights and change User ID in the same transaction
58838	6.0.2.20	Different log levels required for server verbose output
58765	6.0.2.21	ArrayIndexOutOfBoundsException with RoundRobin + SSL + Dispatchers array
60093	6.0.2.22	Creating a new user is slow in production
59541	6.0.2.23	Admin Group member list is corrupted
60153	6.0.2.24	Enforce dedicated DS for .authentication_store in failover configuration

60574	6.0.2.25	Groups Save in group with large number of members is slow
60770	6.0.2.26	Impact of upcoming DST changes in New Zealand
40500	6.0.2.27	Additional properties made available in runtime API
61384	6.0.2.28	Authserver fails to initialize if one dispatcher name fails DNS check
62642	6.0.2.29	normalizeDN forces lowercase to getUserByName, incompatible with IA5 attribute type
60991	6.0.2.30	RTAPI can leak connections
62955	6.0.2.31	java.lang.Error: Log event dispatcher has not been initialized - Exception throw within Admin API Application
63164	6.0.2.32	List entitlements when adding to a group with a large number of entitlements take a long time
63553	6.0.2.33	JRE for Solaris provided with 6.0.2 is lacking 64-bit binaries
69710	6.0.2.34	AuthorizationLRU Cache is cleared on every data event processed by Auth Server
70267	6.0.2.35	Customer receives 'No Such Entry' exception during userToAdministrativeGroupCache.loadAddedKey call
71424	6.0.2.36	Connection leak in for Oracle with ORA-17008 connection errors
72188	6.0.2.37	Keyserver does not log client address in log file errors
72403	6.0.2.38	Cannot debug token errors because tokens are not logged
72726	6.0.2.39	randomize_dispatchers doesn't randomize 1st dispatcher in array
72984	6.0.2.40	Log message appears in batches in customer setup
98333	6.0.2.41	JCIFS needs to be updated in order to fix a critical issue
98391	6.0.2.42	Cannot find bad client from log entry.
100146	6.0.2.43	Aserver not retry to connect to DB
104299	6.0.2.44	Admingui (6.0.2) error with the password policy screen
105104	6.0.2.45	Admin functionality over web services
105377	6.0.2.46	Three more operations to be included in the admin web service
105351	6.0.2.47	Saving a new administrative user with required properties fails with objectclass violation
106174	6.0.2.48	Authorization server hangs under certain conditions
106117	6.0.2.49	Interoperability issue with runtime web services
107651	6.0.2.50	The parameter databasefatalcode in sql.conf doesn't work with MSSQL
103375	6.0.2.51	SQL/Cannot manually map IWA/UserMappingExample.java against current cleartrust.jar in 6.02
109304	6.0.2.52	failed_count does not reset after successful logon
109374	6.0.2.53	aserver.log shows authentication failed when post auth hook
112827	6.0.2.54	Enabling "extended_results=smartrule-deny,cleartext" causes many unneeded LDAP queries"
117408	6.0.2.55	Possible memory leak introduced in 5.5.3.151
109048	6.0.3.01	Not authorized RC_NOT_AUTHORIZED error when updating properties of a user
109064	6.0.3.02	RC_TRANSPORT_ERROR error when trying to delete an Admin Group
428665	6.0.4.01	Dispatcher thead lockup on startup with large number of clients
114433	6.0.4.02	Admin group lookups not necessary
115151	6.0.4.03	Deadlock in JCIFS
114568	6.0.4.04	Admingui lists users in aux store multiple times

113000	6.0.4.05	Enabling "extended_results=smartrule-deny,cleartext" causes many unneeded LDAP queries"
113009	6.0.4.06	Aserver and Eserver exiting when ldap timeout occurs
116418	6.0.4.07	"SNMP no such object" error for some items in aserver cache
115246	6.0.4.08	Exception thrown in Datastore connection manager
117332	6.0.4.09	Possible memory leak introduced in 5.5.3.151
117038	6.0.4.10	Multiple aservers on one machine to not register correctly with iserver.
117490	6.0.4.11	SNMP dispatcherActiveAuthServersEntry does not track all aservers
118250	6.0.4.12	AxM 6.0.4 missing latest JCIF.jar from 6.0.2.41
118288	6.0.4.13	Upgrade ldap_55_to_60.bat and ldap_55_to_60.sh from 6.0.2 missing from 6.0.4
118428	6.0.4.14	Transport error (RC_TRANSPORT_ERROR): ORA-01000: maximum open cursors exceeded
117918	6.0.4.15	SNMP get does not return data for row after aserver is restarted
118707	6.0.4.16	ADMINGUI, cannot save password policy with blank exclusion list
118963	6.0.4.17	Value of user property including "(double quotation) is not displayed completely on AdminGUI
119345	6.0.4.18	SSL connection to entitlement server fails
118091	6.0.4.19	Difference in LDAP searches between aserver and eserver
119162	6.0.4.20	ctscFailedLoginCount does not increment normally when ctscLockoutExpirationDate is disabled
120711	6.0.4.21	UPN Dynamic Creation feature fails
121898	6.0.4.22	Package Auth Manager Java API hotfix as Access Manager 6.0.4 hotfix
121860	6.0.4.23	Corruption of Protected URL cache
122278	6.0.4.24	6.0.4 cumulative patch missing files in sdk
123833	6.0.4.25	AdminAPI Web Services cannot log to local file
123532	6.0.4.26	IllegalArgumentException in connection manager
124494	6.0.4.27	Admin Webservices issues

^Top

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.

Certificate Tool does not accept an underscore character
Tracking Number: 9443
Problem: The Certificate Tool (certool) does not accept any certificate authority common name that includes an underscore character. When attempting to generate a keystore file, the certool prints the error message, "Error generating PKCS#12 file".
Workaround: There is no fix for this problem at this point of time.

Runtime API TOKEN_ERRORs can contain insufficient information
Tracking Number: 9448
Problem: If an API client program passes a broken token to the Runtime API, the API returns insufficient error details. The return values depend on the method called:

- isUserInGroup() and getGroupsForUser() returns an empty map.
- createToken(), getTokenValue(), getTokenValues(), setTokenValue(), setTokenValues(), and validateToken() throws a sirrus.runtime.TokenException.
- All other methods of sirrus.runtime.RuntimeAPI, which take a user argument, return the map with a single entry: { "EXCEPTION_MESSAGE", "<SOME TOKEN ERROR MESSAGE>" }. These methods are authenticate(), authorize(), getUserProperty(), and getUserProperties().

Workaround: There is no fix for this problem at this point of time.

Token problems can occur when running under Linux on VMware

Tracking Number: 20017
Problem: When running the Authorization Server under a Linux guest operating system on top of VMware, the RSA Access Manager token may not be updated as expected in response to Runtime API or Agent requests, even though the interval specified by .notouch_window has elapsed. This is due to a problem in VMware.
Workaround: For information, see this support page on the VMware web site, Clock in a Linux 2.6 Guest Runs Slowly Until Suspended and Resumed.

Special characters in User ID can cause loss of administrative privileges

Tracking Number: 39631
Problem: Administrators with special characters in their User IDs (for example, tom#22) can lose administrative privileges when their profiles are edited.
Workaround: Avoid special characters in User IDs.

Administrative Console fails to work when deployed on WebSphere 6.1

Tracking Number: 116577
Problem: The Administrative Console is not supported on WebSphere 6.1, when the **axm-admin-gui.war** file is deployed with anonymous SSL enabled. This is due to a limitation of Sun JRE 1.5.
Workaround: There is no fix for this problem at this point of time.

Administrative Console and User Self-Service Console is not working

Tracking Number: 121565
Problem: If the Access Manager Application Server Agent and the Administrative Console or the User Self-Service Console is installed on the same application server, the Administrative Console or the User Self-Service console does not work.
Workaround: There is no fix for this problem at this point of time.

User Self-Service Application fails to work when deployed on WebSphere 6.1

Tracking Number: 122735
Problem: The User Self-Service application, when deployed on WebSphere 6.1 does not work if the connection mode is set to Anonymous.
Workaround: There is no fix for this problem at this point of time.

User Self-Service Application fails to work when configured in Authentication mode

Tracking Number: 124935
Problem: If the User Self-Service application is configured in Authentication mode with self-signed PKCS #12 certificates, the WebLogic application server console displays an exception.
Workaround: Perform the following:

1. Go to your ***<domain name>*/bin** directory, where you have installed the User Self-Service application.
2. Open the **setDomainEnv.cmd** file.
3. In the POST_CLASSPATH variable, provide the location of the **cert.jar** file that comes packaged with the User Self-Service application.
4. Restart the WebLogic server.

^Top

Getting Support and Service

RSA SecurCare Online: https://knowledge.rsasecurity.com

Customer Support Information: www.rsa.com/support

RSA Secured Partner Solutions Directory: www.rsasecured.com

^Top

Trademarks

^Top