CA Adapter

Release Notes

r2.2.9

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 4: Defects Fixed 21

Chapter 5: Product Limitations 29

Chapter 1: General Release Information

Note: CA Adapter still contains the terms Arcot, WebFort, and RiskFort in some of its code objects and other artifacts. Therefore, you will find occurrences of Arcot, WebFort, and RiskFort in all CA Adapter documentation. In addition, some of the topics in this guide do not follow the standard formatting guidelines. These inconsistencies will be fixed in a future release.

This section contains the following topics:

Operating System Support

The prerequisites for CA Adapter are based on the server platform.

For detailed information about platform support and system requirements, see the *CA Adapter Installation and Configuration Guide* for your platform.

Documentation

Updated documentation for this product is available at http://ca.com/support.

The documentation, in bookshelf format, includes:

- CA Adapter Installation and Configuration Guide for UNIX Platforms
- CA Adapter Installation and Configuration Guide for Microsoft Windows
- CA Adapter for Cisco IPSec VPN Configuration Guide
- CA Adapter for Juniper SSL VPN Configuration Guide
- CA VPN Client User's Guide for Windows
- CA Adapter Release Notes
- CA VPN Client Release Notes

Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Chapter 2: New Features

This section contains the following topics:

Support for Oracle RAC

From this release onward, Oracle RAC version 11.2.0.1.0 has been added to the list of databases supported by CA AuthMinder and CA Adapter.

Support for MySQL

From this release onward, MySQL Enterprise Edition 5.1 has been added to the list of databases supported by CA Adapter.

Support for JBoss Application Server

CA Adapter now supports JBoss application server versions 5.1.x.

Support for CA SiteMinder 12.5

This release of CA Adapter extends support for CA SiteMinder version 12.5.

Compatibility with AuthMinder 7.1.01 and RiskMinder 3.1.01

This release of CA Adapter is compatible with AuthMinder 7.1.01 and RiskMinder 3.1.01.

Enhanced CA Adapter Configuration Wizard

The CA Adapter configuration wizard, which is a web-based application, has now been enhanced to configure authentication flows, save the configurations to the AFM_HOME location, load the configurations, and allow administrators to update the flows.

Support for Multiple Organizations

CA Adapter now supports multiple organizations through profiles. A profile is a set of configurations that define a flow for an organization. You can create multiple profiles for a single organization.

Multi-Byte Data Support for CA Adapter Components

Fields such as User identifier, Password, QnA, and so on, which are used for CA Adapter configurations, now accept multi-byte data.

Support for Multiple Primary Authentication Mechanisms

You can now configure multiple primary authentication mechanisms using profiles. Each profile enables one primary authentication mechanism and a set of secondary authentication mechanisms.

Profile Support for CA VPN Client

CA VPN Client now works with the profiles configured in the CA Adapter configuration wizard. End users see a drop-down list of the profiles that are supported by CA VPN Client, and they can select the profile to be used for authentication

Support for ArcotID OTP and OATH Synchronization

On behalf of the end user, CA Adapter can now perform synchronization of time-based and counter-based OATH OTP and ArcotID OTP credentials.

Support for ArcotID OTP as Primary Authentication Mechanism on Browser

CA Adapter now supports ArcotID OTP as the primary authentication mechanism on a browser. In addition, the ArcotID OTP Browser-Based Primary Authentication Flow also supports risk evaluation.

Support for ArcotID OTP Desktop Client

CA Adapter now supports the ArcotID OTP desktop client. Users can provision and download the ArcotID OTP credential on their desktop client and use that credential to generate OTPs for authentication

Support for Optional Personal Assurance Message (PAM)

In the CA Adapter configuration wizard, administrators are provided a Prompt User option. When this option is selected, end users are prompted to set their PAM during enrollment. The same is displayed to end users during authentication.

Support for Reading Information from the Installation Directory

You can now read various properties files and configuration files from the CA Adapter installation directory, AFM_HOME.

Support for All Flows in Juniper SSL VPN

CA Adapter now supports all possible flows for Juniper SSL VPN. Each flow consists of one primary authentication mechanism and a set of secondary authentication mechanisms.

Device ID Cookie Set Based on User Input

CA Adapter provides end users the option to select whether they are using a public or private computer. The DeviceID cookie is now set based on the end users selection.

Chapter 3: Known Issues

This section contains the following topics:

Log Files Do Not Roll Over to Backup Files in IBM WebSphere

Symptom:

On IBM WebSphere, the log files for the State Manager and AFM applications do not roll over to the backup files automatically.

Solution:

Edit the AFM and State Manager log properties files as follows:

1. Navigate to the *AFM_HOME*\conf\afm directory, and open arcotafm-log4j.properties and arcotsm-log4j.properties in a text editor.
2. Search for the following entries in the files and comment it out by preceding it with a hash symbol (#):
   - In the AFM log properties file:
     log4j.appender.afmout=org.apache.log4j.DailyRollingFileAppender
   - In the State Manager log properties file:
     log4j.appender.smlog=org.apache.log4j.DailyRollingFileAppender
3. Add the following entry after the line you commented out in the previous step:

   In the AFM log properties file:

   log4j.appender.afmout=com.arcot.logger.log4j.appender.ArcotDailyRollingFileAppender

   In the State Manager log properties file:

   log4j.appender.smlog=com.arcot.logger.log4j.appender.ArcotDailyRollingFileAppender
4. Save and close the files.
5. Restart the WebSphere application server.

ArcotID PKI Authentication and Enrollment Fail When Using an ActiveX Client

Symptom:

If ArcotID PKI ActiveX client is used for authentication and enrollment, and this client is not installed on the end user's system, then at runtime the client is downloaded to the end user's system but authentication and enrollment operations fail.

Solution:

End users must restart the browser and authenticate again.

Authentication Using Internet Explorer 8 Displays a Warning

Symptom:

If you have configured an ArcotID PKI key size of 2048, when an end user tries to authenticate using Internet Explorer 8, the following warning message appears:

A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer might become unresponsive.

Solution:

Use an ArcotID PKI key size of 1024.

Blank Page Displayed During ArcotID PKI Download

Symptom:

If an end user is using Internet Explorer 9 on a Windows 7 system and has enabled certain advanced settings in Internet Explorer, and if ArcotID PKI authentication is used, then the end user might see a blank page when downloading the ArcotID PKI credential.

Solution:

The end user must reset Internet Explorer advanced settings by navigating to Tools, Internet Options, Advanced, and then Reset.

Risk-Based Workflows Fail if Network Speed is Low

Symptom:

If the speed of your network is very low, then risk-based authentication might fail.

Solution:

Check your network settings, and if required, specify a higher value for the ArcotSMResponseWait parameter in the adaptershim.ini file.

ArcotID OTP Credential Creation or Download Requests Fail if the Desktop Client and AFM Share a Browser Session

Symptom:

If an end user has the ArcotID OTP Desktop Client and AFM open in the same browser session, and if an ArcotID OTP OATH credential creation or download request is sent from the Desktop Client to AFM, the request is processed the first time and the credential is downloaded. However, subsequent requests to AFM in the same browser session are rejected and the end user is informed that the session has expired.

Solution:

Use different browser sessions for AFM and the ArcotID OTP Desktop Client.

ArcotID OTP Authentication Fails if the Organization Name Contains a Space

Symptom:

If an organization name contains a space, primary authentication flows that use ArcotID OTP do not work.

Solution:

Ensure that organization names do not include spaces in them.

All Application Logs Redirected to the AFM Log File in JBoss

Symptom:

In JBoss application server, after deploying the AFM, State Manager, and sample application-specific WAR files, the application server logs are all redirected to the AFM log file, arcotafm.log.

Solution:

Create a new file, jboss-web.xml, and do the following:

1. Copy the following into the jboss-web.xml file:

```
<jboss-web>
  <class-loading java2ClassLoadingCompliance="false">
    <loader-repository>
      com.arcot:loader=<UniquenameforClassLoader>
      <loader-repository-config>
        java2ParentDelegation=false
      </loader-repository-config>
    </loader-repository>
  </class-loading>
</jboss-web>
```

   UniquenameforClassloader must be unique for each application. For example, you can use ArcotAFMClassloader for AFM, ArcotSMClassloader for State Manager, and so on.

2. Copy the jboss-web.xml file to *App_Exploded_Location**App_Name*\WEB-INF

   where,

   App_Exploded_Location is the location where JBoss has extracted the application

   App_Name is the name of the application, for example, arcotafm or arcotsm.

   If jboss-classloading.xml file is present in this location, then delete the file.

3. Restart the application server.

Repeat this procedure for the AFM, State Manager, and SAML sample applications.

Risk Evaluation from State Manager Fails Due to Class Loading Issues

Symptom:

In JBoss application server, after deploying the AFM, State Manager, and sample application-specific WAR files, the WAR files are not extracted based on how the applications are deployed. This might cause risk evaluation from State Manager to fail due to class loading issues.

Solution:

Follow these steps:

1. Explode one of the WAR files to a local directory.
2. Create a new file, jboss-web.xml in *App_Exploded_Location**App_Name*\WEB-INF

   where,

   App_Exploded_Location is the location where JBoss has extracted the application

   App_Name is the name of the application, for example, arcotafm or arcotsm..
3. Copy the following into the jboss-web.xml file:

```
<jboss-web>
  <class-loading java2ClassLoadingCompliance="false">
    <loader-repository>
      com.arcot:loader=<UniquenameforClassLoader>
      <loader-repository-config>
        java2ParentDelegation=false
      </loader-repository-config>
    </loader-repository>
  </class-loading>
</jboss-web>
```

   UniquenameforClassloader must be unique for each application. For example, you can use ArcotAFMClassloader for AFM, ArcotSMClassloader for State Manager, and so on.
4. If a jboss-classloading.xml file is present in the *App_Exploded_Location**App_Name*\WEB-INF directory, then delete the file.
5. Restart the application server.

Repeat this procedure for the AFM, State Manager, and SAML sample applications.

Application Does Not Detect Backup Data Source Availability in JBoss

Symptom:

If both primary and backup data sources are configured in JBoss application server, and if both databases are down, the application throws an error. However, even after the backup database is up, the application does not work as it does not detect the availability of the backup data source.

Solution:

Refresh the backup data source. The application starts working.

Incorrect Parameter Added for Time-Based Rollover in the adaptershim.ini File

Symptom:

After configuring CA Adapter using the wizard, the adaptershim.ini configuration file contains the wrong parameter name and value in the section for time-based rollover of the log file, as shown in the following example:

# "LOG_FILE_ROLLOVER_INTERVAL" property specifies how often you want the log file to
# rollover to the backup file. The values recognized are HOURLY, DAILY,
# WEEKLY, and MONTHLY. DAILY results in the file rolling over when the first
# log message is received after midnight. The time check is
# based on the logged time. By default, the local time zone is used for
# logging.
Param2=**MAX_LOG_FILE_SIZE**=10000000

The value of Param2 must be LOG_FILE_ROLLOVER_INTERVAL and not MAX_LOG_FILE_SIZE.

Solution:

In the LOG_FILE_ROLLOVER_INTERVAL property section in the adaptershim.ini file, change the following line:

Param2=MAX_LOG_FILE_SIZE= 10000000

to

Param2=LOG_FILE_ROLLOVER_INTERVAL=DAILY

Issue with Custom Uninstallation of CA Adapter

Symptom:

If no components are selected for uninstallation, the installer still displays a message stating that components have been successfully uninstalled.

Solution:

This issue has no functional impact. When you perform uninstallation, select the components that you want to uninstall.

Chapter 4: Defects Fixed

This section contains the following topics:

Certain Special Characters Not Allowed in the ArcotID PKI Password

Symptom:

CA Adapter did not allow special characters <, >, and & in the ArcotID PKI password.

Solution:

This release of CA Adapter allows special characters <, >, and & in the ArcotID PKI password.

No Support for Microsoft SQL Server Replication

Symptom:

Microsoft SQL Server replication was not supported in earlier releases of AuthMinder.

Solution:

In this release, primary keys have been added in all tables to support database replication.

No Configuration in CA Adapter to Specify the SiteMinder API Version to Be Used

Symptom:

There was no configuration in CA Adapter to specify the SiteMinder API version to be used by Adapter.

Solution:

This issue has been resolved. CA Adapter now provides the configuration parameter, SmApiVersion, in the adaptershim.ini file to specify the SiteMinder API version to be used. For example, to configure Adapter to use the SiteMinder API version 0x300, set the parameter as follows under the arcot/integrations/smadapter section in the adaptershim.ini file:

```
SmApiVersion=300
```

Non-Reentrant System Calls Used In CA Adapter

Symptom:

CA Adapter used the non-reentrant system calls, localtime, ctime, gmtime, and asctime.

Solution:

This issue is resolved. These non-reentrant system calls have been replaced with the following equivalent reentrant system calls:

- localtime is replaced with localtime_r
- ctime is replaced with ctime_r
- gmtime is replaced with gmtime_r
- asctime is replaced with asctime_r

Authentication Transactions Were Very Slow

Symptom:

Authentication transactions were taking a very long time when the load was heavy.

Solution:

The reason for this issue was that the putenv() function was getting called for each call to SmAuthQuery API, consequently corrupting environment variables for the process. This issue is fixed now and the putenv() function is getting called only once as expected.

Time-Based Rollover of Log Files Caused Performance Issues

Symptom:

In the earlier release, the default log file rollover policy was time-based, which resulted in large log file sizes. This caused performance issues.

Solution:

This issue has been addressed in the current release by enabling the configuration of size-based rollover policies. The default logging configuration in adaptershim.ini has been changed to roll over the Adapter SHIM log file after reaching the configured file size instead of rolling over based on time. Log rollover policy can be configured as shown in the following examples:

To configure a time-based rollover policy with a rollover time interval of one day, make the following settings under the section [arcot/integrations/smadapter/LogLibrary1] in adaptershim.ini:

```
DLLName=ArcotLog2FileSC
HandleLevel=3
EntryPoint=CreateFileLogHandler
ParamSupported=3
Param1=LOG_FILE_NAME=ARCOT_HOME/logs/arcotadaptershim.log
Param2=LOG_FILE_ROLLOVER_INTERVAL=DAILY
Param3=BACKUP_LOG_FILE_LOCATION=ARCOT_HOME/logs/backup
#Param4=LOG_LINE_FORMAT=$$TS1L$$ $$SEV$$ pid $$PID$$ tid $$TID$$: $$MID$$
$$MSG$$ ($$LID$$)
```

To configure a size-based rollover policy with a maximum log file size limit of 10000000 bytes, make the following settings under the section [arcot/integrations/smadapter/LogLibrary1] in adaptershim.ini:

```
DLLName=ArcotLog2FileSC
HandleLevel=3
EntryPoint=CreateFileLogHandler
ParamSupported=3
Param1=LOG_FILE_NAME=ARCOT_HOME/logs/arcotadaptershim.log
Param2=MAX_LOG_FILE_SIZE=10000000
Param3=BACKUP_LOG_FILE_LOCATION=ARCOT_HOME/logs/backup
#Param4=LOG_LINE_FORMAT=$$TS1L$$ $$SEV$$ pid $$PID$$ tid $$TID$$: $$MID$$
$$MSG$$ ($$LID$$)
```

JavaScript Error When User Changed LDAP Password

Symptom:

SiteMinder Policy Server can be configured to force users to change their LDAP password the next time they login. If this configuration was enabled and a resource was protected with Arcot authentication, a JavaScript error was displayed informing the user that the LDAP password could not be changed.

Solution:

This release of CA Adapter supports the required configuration changes in SiteMinder Policy Server. You can set PasswdSvcUserAtt to a valid LDAP attribute of string type in the adaptershim.ini file. The fix will work only in controllers that use LDAP authentication. This property has to be configured under the sections as required.

For example, if controller4.jsp is used, then PasswdSvcUserAtt property must be configured as follows under the section arcot/integrations/smadapter/OnePage:

```
[arcot/integrations/smadapter/OnePage]
PasswdSvcUserAtt=description
```

Note:The LDAP attribute must not be used by any other application and also read-write access must be allowed.

Unable to Change Password for LDAP-Based Authentication Workflows

Symptom:

For LDAP-based authentication workflows (used in controller3.jsp and controller4.jsp), users could not change their password under the following conditions:

- Password services are enabled in SiteMinder Policy Server.
- The user enters the correct old password, but provides an invalid new password.

  Note: If the user provides a password that does not match the password policy settings, then the system considers the password as invalid.

  On the next attempt to change the password, users were not allowed to do so even after providing the correct old password and a valid new password.

Solution:

In this release, the Authentication Shim has been modified to allow the user to change their password. Even if the user fails to provide a valid password in the first attempt, they can still change their password in the subsequent attempt by providing a valid password.

No Support for Updating SiteMinder Policy Server Registry Configuration

Symptom:

If password services are enabled in SiteMinder Policy Server for the LDAP-based authentication workflows (used in controller3.jsp and controller4.jsp), and if the user entered an old incorrect password, then the system incorrectly redirected the user to the following pages:

- For controller3.jsp, users were redirected to the shim2.fcc page.
- For controller4.jsp: users were redirected to the shim.fcc page.

The SiteMinder Policy Server registry configuration could not be changed to modify this behavior.

Solution:

This issue has now been resolved. This release of CA Adapter supports the required configuration changes in SiteMinder Policy Server.

SMUSRMSG is not RFC Compliant

Symptom:

Values set in the SMUSRMSG cookie were not RFC compliant.

Solution:

This issue has now been resolved.

Chapter 5: Product Limitations

This section contains the following topics:

Any Plugged-In USB Device Is Associated with the ArcotID PKI at the Time of Download

If a USB device is plugged-in to the system at the time of downloading the ArcotID PKI, then the USB device is also associated with the ArcotID PKI. During ArcotID PKI authentication, if the USB device is not plugged in to the system, then the user authentication fails.

CA Adapter Supports Only Unique Login IDs Across Domains

CA Adapter currently does not support non-unique Login IDs, even when the same Login ID is mapped to different domain names in LDAP.

Special Characters in LDAP Password Result in AFM Authentication Errors

If LDAP-based authentication is used, and if the LDAP password contains the \ or " characters, then authentication errors occur even though these characters are supported by LDAP.

End User Associated with Public Device If It was Used for Risk Evaluation Earlier

In an end user risk evaluation workflow, if the device being used for login already has a Device ID cookie but the user is not associated with the device, then even if the user selects the Public Computer option during authentication, the user is associated with the device. For subsequent transactions, the user is not prompted for secondary authentication.

ArcotID OTP Credential Provisioned to the Browser Cannot Be Used in an ArcotID OTP Application

If the ArcotID OTP credential algorithm is HOTP and if the credential is provisioned on the browser, the end user will not be able to use it on the ArcotID OTP application installed on their mobile device or desktop.

European Union Cookie Legislation Does Not Apply to ArcotID OTP Browser-Based Controllers

In ArcotID OTP browser-based controllers, the ArcotID OTP credential is downloaded to the end user's system even if the end user did not select European Union Cookie Legislation.

Uninstalling CA Adapter Does Not Delete the Registry File

When you uninstall CA Adapter, the zerog registry XML file, .com.zerog.registry.xml, is not removed. Only entries related to Adapter are removed from the XML file. If Adapter is the only product that was installed, then after uninstallation, the XML file will be empty with only a high-level element.

Registry Entries Not Removed After Uninstallation

Symptom:

After uninstallation, some of the registry entries related to the product are not removed.

Solution:

This issue has no functional impact. The registry entries are overwritten during the next installation.

Silent Mode of Installation Not Supported

The silent mode of installation is not supported.