CA CloudMinder™

Service Provider Release Notes

1.51

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.

CA Technologies Product References

This document references the following CA Technologies products:

- CA CloudMinder™ Identity Management
- CA CloudMinder™ Advanced Authentication
- CA CloudMinder™ Single Sign-On
- CA Directory
- CA IdentityMinder™
- CA AuthMinder™
- CA RiskMinder™
- CA SiteMinder®
- CA SiteMinder® for Secure Proxy Server
- CA Layer 7

Contents

Chapter 1: New and Changed Features

This section contains the following topics:

1.51

This release of CA CloudMinder includes these new and changed features.

Support for PostgreSQL as Runtime and Report Databases

New CA CloudMinder installations can use PostgreSQL as an alternative to Oracle.

For information on how to install PostgreSQL, see Order of Component Installation in the *Installation Guide*.

Note: Upgrades from Oracle to PostgreSQL are not supported.

Automatic Backup of Property Files by the Installer

Most CA CloudMinder server components use a properties file during installation. The properties file includes information, such as user names, passwords, and host names, that enables components to communicate with one another.

In previous versions, administrators had to back up the properties file to a /tmp directory manually.

The automated backup removes passwords to increase security.

For more information about property file backups, see Properties Files.

Simplified Tenant Deployment Procedures

In previous releases, host administrators had to complete additional configuration steps after creating a tenant environment. In this release, manual configuration steps have been eliminated to simplify the deployment process.

Changes to CA SiteMinder Realms and SSO Authentication Methods

To automate steps in tenant deployment, the resource URLs in the following table have changed.

Important! The changes to CA SiteMinder realms and SSO authentication methods only affect new installations. If you are upgrading existing environments, you do not need to change your deployment.

Current Resource	New Resource
/affwebservices/<tenant-name>/forms.jsp	/chs/redirectservlet/<tenant-name>/forms
/affwebservices/<tenant-name>/arcotidrisk.jsp	/chs/ redirectservlet/<tenant-name>/arcotidrisk
/affwebservices/<tenant-name>/arcototprisk.jsp	/chs/ redirectservlet/<tenant-name>/arcototprisk
/affwebservices/<tenant-name>/arcotid.jsp	/chs/ redirectservlet/<tenant-name>/ arcotid
/affwebservices/<tenant-name>/arcototp.jsp	/chs/ redirectservlet/<tenant-name>/arcototp

Changes to the resource URLs are reflected in the documentation in this release.

WorkPoint 3.5 Support

WorkPoint 3.5 requires eXtended Architecture (XA).

If you are upgrading to this release, see Database Upgrade in the *Upgrade Guide* for instructions on how to configure the database to support XA.

1.5

Two-Factor Authentication for VPN Systems with RADIUS (see page 9)

Simplified Activation for ArcotID OTP Mobile Authentication (see page 9)

Multiple User Selection for ArcotID OTP Activation Emails (see page 9)

SSO Using CA CloudMinder as an OAuth Authorization Server (see page 9)

Home Realm Detection (see page 10)

Two-Factor Authentication for VPN Systems with RADIUS

CA CloudMinder 1.5 supports RADIUS. RADIUS offers two-factor authentication for VPN systems protected by CA CloudMinder.

RADIUS is enabled by default in this release. The administrator must add a RADIUS client and assign a RADIUS credential configuration. For more information, see Configure CA CloudMinder for RADIUS.

Simplified Activation for Arcot OTP Mobile Authentication

Users can activate a CA ArcotID OTP credential and set a PIN directly from the mobile or desktop application after requesting a self-activation email. Users are not required to complete the web-based enrollment process or authenticate with their CA CloudMinder password before using the application.

Administrators can enable this feature by enabling the Advanced Authentication Self Manager role. Once enabled, all users have this role. If administrators do not want all users to have this role, they can copy the role, adjust the membership policy, and enable the copied role.

Multiple User Selection for ArcotID OTP Activation Emails

Administrators can select multiple users to receive activation emails and codes for ArcotID OTP mobile devices. Previously, administrators could only select one user at a time. This release allows administrators to search for users by organization. The search displays all users in the organization with individual checkboxes. The administrator selects all the necessary users in bulk instead of individually. Users activate their devices with information from the instructions in their email.

SSO using CloudMinder as an OAuth Authorization Server

A user can log in to an OAuth client application using their CA CloudMinder credentials. An administrator configures CA CloudMinder to act as an OAuth Authorization Server, and optionally an OpenID user info endpoint, in this partnership. The user can then use single-sign on to access these browser-based applications, including mobile implementations.

The new Layer 7 Gateway component provides this service. The Layer 7 Gateway is a Java application that runs within a dedicated Tomcat instance and uses the Tomcat HTTP listener. The Layer 7 Gateway uses MySQL as its internal database.

Note: For more information, see SSO using CloudMinder as an OAuth Authorization Server.

Home Realm Detection

Home realm detection enables users who have authenticated with their domain credentials to log into a target application without needing to select an identity provider on the CA CloudMinder login page.

For example, Salesforce.com is a software resource outside of your network environment. Users who have logged into the network with domain credentials should be able to access Salesforce.com without having to select an IdP in the CA CloudMinder login page.

Note: For more information, see Enable Domain Users to Access Applications Without Re-Authenticating.

(new related group 1)

Availability of Mobile Client for ArcotID PKI Authentication (see page 10)
Support for Two Step Authentication (see page 10)

1.1 SP2

Availability of Mobile Client for ArcotID PKI Authentication (see page 10)

Support for Two Step Authentication (see page 10)

Availability of Mobile Client for ArcotID PKI Authentication

In the current release, in addition to the native client and JavaScript client, CA CloudMinder also supports the use of a mobile client for ArcotID PKI authentication. End users can use this client application on their mobile devices to authenticate using an ArcotID PKI credential. The ArcotID PKI credential configuration is enhanced to include an option to enable the mobile client.

Support for Two Step Authentication

Secondary authentication is typically invoked when performing sensitive tasks, such as when authenticating roaming users or resetting passwords. To enhance the level of security of a protected resource during secondary authentication, CA CloudMinder now enables you to chain two secondary authentication methods. When the two-step authentication feature is enabled, both the configured authentication methods are invoked one after the other.

Chapter 2: Known Issues

This section contains the following topics:

Install and Upgrade Issues

Install the CA SiteMinder® Policy Server

Symptom:

When I attempt to install the CA SiteMinder® Policy Server manually, an error message indicates that the installation failed. The version is correct and the CA SiteMinder® install logs show no errors, but the CA SiteMinder® services are not started.

Solution:

Check that the DISPLAY environment variable is not set in the Linux shell. If it is set, unset the DISPLAY environment variable before you run the CA SiteMinder® Policy Server. To do unset the variable, use the unset DISPLAY command in the Linux shell.

Repeated Message in JBoss Log

Symptom:

After I install Identity Management manually, the following error is continually logged in the JBoss log:

"2014-03-20 04:01:36,058
WARN [org.jboss.resource.connectionmanager.ManagedConnectionFactoryDeployment] (Thread-20) Exception during getSubject()Unauthenticated caller:null

java.lang.SecurityException: Unauthenticated caller:null
at
org.jboss.security.integration.JBossSecuritySubjectFactory.createSubject(JBossSecuritySubjectFactory.java:92)
at
org.jboss.resource.connectionmanager.ManagedConnectionFactoryDeployment$1.run(ManagedConnectionFactoryDeployment.java:738).....

Solution:

This message is benign and does not affect Identity Management functionality.

Upgrade the CSP console

Symptom:

I see an exception when I access Rules using the path Policies>Domain>Rules when I upgrade the CSP console. Rules appear correctly when I use the path Policies>Domain>Domains<*select Tenant Domain*>Realms <*select Realm*>Rules.

Solution:

This issue can be caused when the database contains rules with the same name but different cases that were created before the 1.51 upgrade. Use the XPSExplorer tool to edit these rules. Rules that you need to delete from the database to resolve this issue appear in XPSExplorer without a parent object associated with them.

Update Realm and Rule Names

For tenants created before CA CloudMinder 1.1 SP1 (Refresh), confirm that the SiteMinder Realms for the Advanced Authentication are correctly named including case.

In that release, the administrator created rules and realms for Advanced Authentication using the User Console. This process is now automated. However, those realms and rules did not follow the standard naming convention. Therefore, when you export the tenant before or after an upgrade, the export fails. To correct this problem, rename those realms and rules using the following procedure.

Follow these steps:

1. Log in to the CSP console.
2. Click Policies, Domain, Domain.
3. Select *tenant-tag*domain.
4. Got to the Realms tab.
5. Modify any realm which does not begin with the *tenant-tag_* and end with _realm_es.
6. For each realm, make sure the rules follow the naming convention of *tenant-tag_name*_rule _es and make sure the case matches.

   For example, if your *tenant-tag* is **west**, you would use:

   ```
   west_arcototp_withrisk_realm_es
   west_arcototp_realm_es
   west_arcotid_withrisk_realm_es
   west_arcotid_realm_es
   west_arcotid_rule_es
   west_arcotid_withrisk_rule_es
   west_arcototp_withrisk_rule_es
   west_arcototp_rule_es
   ```

Special Characters in Passwords

Using the following special characters in a password causes the CA IAM CS and CSP Console installs to fail:

@, #, !, $

To prevent installation issues, use passwords that do not contain @, #, !, or $ characters.

Unable To Access SSO Reports

Symptom:

I cannot access my SSO reports after I upgrade to CA CloudMinder 1.5.

Solution:

Set the default connection type to JDBC for SSO reports after an upgrade to 1.5.

Follow these steps:

1. Use Modify Admin Tasks to search for the following report tasks:

   SSO-Authentications by Authentication Type Report

   SSO-Unique User Authentications Detail Report

   SSO-Unique User Authentications Summary Report

   SSO-Authentications by Auth type per Application Report

   SSO-User Accesses per Application Report

   SSO-User Access Detail Report

   SSO-User Authentication Detail Report
2. Select a report to edit (you can only select one report at a time).
3. Click the Search tab.
4. Click Browse to locate the search screen for each task.

   Default: The search screen is selected in the list.
5. Edit the search screen for the report task and select the JDBC connection name under Connection Object for the report.
6. Click OK.
7. Repeat steps 2 through 6 for each report you need to edit.

Restart SiteMinder Secure Proxy Server (SPS) after Upgrade

Symptom:

After upgrading CA CloudMinder, SPS does not start automatically.

Solution:

Manually start the SPS.

Policy Server Fails Against Load Balancer

Symptom:

When a load balancer is part of the installation, Siteminder validation fails against the load balancer IP address.

Solution:

1. Log into the CSP console.
2. Click Infrastructure, Agent, Agent Configuration Objects.
3. Modify the AgentConfigurationObject being configured for the Secure Proxy Server.
4. Set the CustomIpHeader to HTTP_ORIGINAL_IP.
5. Click Save.

Chapter 3: General Issues

This section contains the following topics:

Incorrect Reference to WS-Federation Metadata Exchange

The SSO Partnership Federation Guide incorrectly includes documentation on WS-Federation Metadata Exchange. This feature is not supported in the current CA CloudMinder version.

The Secure Proxy Server Is Not Responsive After a Network Disconnection

Symptom:

When I try to log in to a Secure Proxy Server after being disconnected from the network, the log in fails. I see the following message:

Server Error. The server was unable to process your request.

Solution:

Configure a 5-minute delay on the load balancer to allow the Secure Proxy Server to recover after disconnecting from the network. See the documentation for your load balancer for information about how to configure the 5-minute delay.

An Error Occurs When I Stop the SSG Services On a Layer 7 Appliance

Symptom:

When I stop the SSG services on a Layer 7 appliance, the following error sometimes appears:

iptables-restore: line 20 failed

Solution:

This error message is benign and does not indicate an issue on the Layer 7 appliance. You can ignore this error message.

Missing Search Screens for Web Services Configuration

The various search screens needed to set member rules for a web service configuration object are missing. This procedure corrects the problem.

Follow these steps:

1. Execute Modify Admin task and select Create Web Service Configuration.
2. Click on the Tabs Tab.
3. Select the Members Tab and enter the missing screens:
   - Group Search Screen, Default Group Search.
   - Organization Search Screen, Default Organization Search.
   - Admin Role Search Screen, Default Admin Role Search.
4. Save.
5. Execute Modify Admin task and select Modify Web Service Configuration.
6. Click on the Tabs Tab.
7. Select the Members Tab and enter the missing screens:
   - Group Search Screen, Default Group Search.
   - Organization Search Screen, Default Organization Search
   - Admin Role Search Screen, Default Admin Role Search
8. Save.

Now you can execute the Create/Modify Web Service configuration task and set the member rules.

References to Provisioning Manager

References to Provisioning Manager in this bookshelf apply to customers who also purchase the on-premise product, CA IdentityMinder.

Error Using Wizard to Create WSFED RP to IP Partnership

Symptom:

In the CSP Console, an error occurs when you use the partnership creation wizard to create a WSFED RP->IP Federation partnership. The error occurs when you try to import a certificate.

Note: This issue does not occur when you use the wizard to create other types of partnership.

Solution:

Import the certificate in Infrastructure, X509 Certificate Management instead. After you create the certificate, you can use the partnership creation wizard to successfully create a WSFED RP->IP Federation partnership.

Intermittent Issue When Revoking a Service

Occasionally, revocation rules are not applied correctly when you remove a service from a user. In some cases, revocation rules do not correctly clear attributes. In other cases, users are not removed from a role.

This issue occurs intermittently.

Chapter 4: Tenant Management Issues

This section contains the following topics:

Delete a Tenant

Before you delete a tenant, delete partnerships that use this tentant's user directory or modify such partnerships to use a different directory.

Create a New Authentication Method in the Tenant Console

Symptom:

When I create a new authentication method in the tenant console, the authentication URL points to default jsp file. Example: /affwebservices/redirectjsp/forms.jsp'.

Solution:

Set the URL to:

/chs/redirect/tenantKey/forms

Or

/chs/redirect/tenantKey/arcotid

Tenant Deletion Fails Initially

Symptom:

No error is reported in the CSP Console. After trying to delete the tenant two or three times, the deletion succeeds.

Solution:

Set the following value in /opt/CA/secure-proxy/proxy-engine/proxyserver.sh:

```
-Dhttp_connection_timeout=300000
```

Then, restart the SPS.

Recreating a Tenant After Deletion Fails

Symptom:

If you deploy a tenant, delete the tenant, and then attempt to deploy the tenant again with the same name, the deployment fails. The following error message occurs:

Failed to register tenant directory with AuthMinder: OrgRegistryError

with Error: "Failed to register tenant directory with AuthMinder: OrgRegistryError"

Solution:

To prevent the error, rename the tenant in the Advanced Authentication Administration Console.

Chapter 5: Authentication Issues

This section contains the following topics:

Error With AcrotID PKI Authentication With Desktop Client 1.6

Symptom:

When I try to authenticate with AcrotID PKI with OTP Desktop Client 1.6, an error message appears similar to the following:

Page Title: Website restore error
Page Heading: We were unable to return you to ca.com
URL: res://ieframe.dll/acr_error.htm#

The URL in the message depends on your configuration.

Solution:

Upgrade to OTP Desktop Client 2.2.2.

Error Configuring Credential Types

Symptom:

After creating a tenant organization, the organization may not be available when configuring authentication credentials.

Solution:

Restart the RiskFort and WebFort servers and continue your authentication configuration task.

Unable to Select Security Code When Configuring an Advanced Authentication Flow

Symptom:

You have enabled the Security Code credential type but cannot select it when configuring an advanced authentication flow.

Solution:

Disable and re-enable the Security Code credential type. You can then use it in advanced authentication flows.

Chapter 6: Connector Issues

This section contains the following topics:

Error Logging into Connector Server

Symptom:

Only a user with the role of tenant administrator can access the CA IAM Connector Server administrative user interface. Requests from other user roles are looped without an error message explaining the problem.

Solution:

Log in connector server exclusively as a tenant administrator.

Issue Adding Additional On Premise CA IAM Connector Servers

Symptom:

You can successfully install an additional on-premise CA IAM Connector Server and create a connection to the cloud CA IAM Connector Server. However, in the cloud CA IAM Connector Server you cannot create a route using the newly added on-premise CA IAM Connector Server.

Note: This issue occurs *only* when you add an additional on-premise CA IAM Connector Server for a tenant.

Only tenants who support two on-premise connectors in different data centers on different networks need to install multiple on-premise CA IAM Connector Servers. In this case, specifying the second Tenant Host ID causes the issue with creating routes.

Solution:

To create a route for the second on-premise CA IAM Connector Server, restart the cloud CA IAM Connector Server service.

Multiple cloud CA IAM Connector Servers are installed for high availability. Restarting one server should not negatively affect performance. However, do not restart the cloud CA IAM Connector Server when long running events, such as an Explore and Correlate or directory synchronization, is in progress.

Chapter 7: Reporting Issues

This section contains the following topics:

Failure to connect to Snapshot Database for PostgreSQL

Symptom:

When you try to create a snapshot database connection or you attempt to establish a connection, CA CloudMinder is unable to connect to the object store. The issue occurs when a PostgreSQL database is the object store and the default snapshot database. The cause is that the firewall does not allow traffic on the PostgreSQL database port (5432).

Solution:

Disable the firewall and allow traffic on port 5432, the database port.

Schedule Reports Task not Invoking Workflow

The Schedule Reports task is not invoking workflow if the Identity Management reports need to capture snapshots.

Follow these steps:

1. Use Modify Admin Task to select the Schedule Reports task.
2. Click the Events tab.

   Select the one with the event name Capture Snapshot Event.
3. Select Single Step Approval from the drop down box of Non-Policy Based entry.
4. Locate the Default Approver section.
5. Select Approve Capture Snapshot in the Approval Task drop down.

6. Locate the Participant Resolver drop down.
7. Choose Admin Role Members.

   Search for CSP Administrator and select that role.
8. Repeat the steps 4 through 7 for the Primary Approver section.
9. Save.

Chapter 8: Fixed Issues

This section contains the following topics:

Fixed Issues in 1.51

The following issues are fixed in CA CloudMinder 1.51.

Support Ticket	Problem Reported
21398571-1	Remove AppLogic warning message from the CA CloudMinder kit installer.
21405244-1	Icons go missing when logging out of Identity Management.
21420488-1	Identity Management button styles are inconsistent.
21423543-1	Issues with Web service and public user accounts.
21424021-1	Exception (tews6.wsdl.lmsException) is generating stubs with Axis.
21459422	Metadata is not updated in IAM CS.
21477905-1	Google Oauth gives the error "Unable t get the attributes for the user" intermittently.
21522100-1	Connector installation fails if a password contains a special character.
21532475-1	CA SiteMinder® authentication for TEWS has issues.
21586286-1	The WCTX parameter is not preserved when using WS-Fed to access SharePoint.
21592346-1	Internet Explorer behaves incorrectly when resizing a screen.
21620829-1	[Connector] Socket Closed #2 message.
21634496	Error message is not displayed when wrong credentials are entered.
21634502	Re-login is denied even when a user submits valid credentials on the second attempt to log in.

Support Ticket	Problem Reported
21634505	User account is not locked even after three invalid password attempts.
21636087-1	The customer cannot achieve an active partnership running CA CloudMinder, and sees an error in the Administration user interface.
21655098-1	Imported services do not display in the Service Wizard.
21656651	An error occurs without ArcotID PKI application installed.
21668496-1	Policy server upgrade fails with core dump: *** glibc detected *** /opt/CA/siteminder/bin/XPSDDInstall: double free or corruption (fasttop): 0xf7500468.
21716142	Problems with Shell\Wipro partnership: Unable to view and modify.
21730077-1	"User Authentication Details" report does not capture the required data.
N\A	On a slow running machine, the Forgot Username task times out to the Task Pending screen before the username is displayed on the page. Note: This issue was addressed by creating templates using email policies.

Fixed Issues in 1.5

The following issues are fixed in CA CloudMinder 1.5.

Support Ticket	Problem Reported
21404829-1 and 21614500-1	Errors while deactivating a partnership
21469835	Credential enrollment exception
21483582-1	Need to change database passwords
21475947-1	On-premise dirsync monitors fail after twenty minutes
21495946-1	403 Request Forbidden Error
21508676-1	CA CloudMinder SPS installs some files and directories as world-writable
21513477-3	Issue with session expiration

Support Ticket	Problem Reported
21513477-4	Enumeration issue when authenticating using ArcotID PKI
21520677-1	Socket closed error
21528069-1	After upgrading to SP2, the Enable Password Changes from Endpoint Accounts is reset from enabled to disabled
21529727-1	CA CloudMinder is not reached after the SAML assertion is consumed by the CA CloudMinder SP side
21546422-3	Changing the Federation partnership name in CA CloudMinder SP2 is not working
21546422-4	Unable to activate remote SP partnership when the same SP is used in two partnerships. The first partnership is in an "Inactive" status.
21546422-9	After upgrading CA CloudMinder, there are issues with the Partnership Modify, Delete, and Activate features

Fixed Issues in 1.1 SP2

The following issues are fixed in CA CloudMinder 1.1 SP2.

Support Ticket	Problem Reported
21257766	IBM Rational Scan shows vulnerability with SPS
21277334-2	The max length of ETGLOBALUSERNAME is 256 characters
21324931-1	In SAML partnership configuration, selection of AES-256 Algorithm for encryption assertion throws http 500 error
21356958-1	An error occurs when loading flows for Forgot Username, Forgot Password, Submit OTP, and Register the Device
21364818-1	Advanced Authentication install failed--unable to find catalina.out
21364824-1	Log and monitoring configuration in run.sh are overwritten during IdentityMinder upgrade
21365665-1	User doesn’t get redirected after self-registration
21372274-1	Problem with Advanced Authentication Reset Password Screen

Support Ticket	Problem Reported
21374033-1	DATETIME format in WebService trust
21374151-1	Incorrect SAML version shown in CloudMinder response
21380133	SLO NullPointerException
21390224	Ater CloudMinder upgrade, Siteminder Admin UI license was replaced with an evaluation copy
21394902-1	Wrong task name for CAMSelfRegistrationWorkflow
21396738-1	Newly created endpoint is not listed in tenant User Console
21396863-1	Tenant environment URL loads slowly
21396988-1	Issue with ACS URL in partnership
21398500-1	Login page doesn't come up
21399204-1	Updating a logo requires an SPS restart
21400006-4 21400006-5	Running XPSExport and XPSSweeper commands resulted in a core dump
21407341-1	Install script fails when database passwords in properties.sh include the period (.) character
21407358-1	SMPS install script uses hard-coded password for createarcotauthscheme.sh
21408309-1	Clicking the link on Forget Username and Forget Password causes 500 error
21409260-1	Only one tenant can access Office 365 at a time
21415269-1	Missing File In SPS Server
21420028	Dxagent password in clear text in default-realm.properties file
21420499-1	Inconsistent button style - "Register Now" button
21420645-1	Requested Resource Error
21425298-1	IE security warning appears for "ArcotID PKI with Risk Authentication".
21435133-1	Wrong redirection in Forgotten Password task
21436678-1	Secondary authentication screen does not show SMS or email
21462257	Not able to export environments created in previous releases

Support Ticket	Problem Reported
21472889-1	User name display incorrect during PIN reset task (truncated)
21473758-1	Insecure content warning
21476134-1	Authentication Context Templates not displayed in Siteminder WAMUI
21487520-1	External URL tab redirects to wrong location
CQ 166303	Emails sent to users who use the Forgot My Pin task are sent from cloudminder@ca.com instead of the email address configured in the tenant settings.
CQ 167505	Duplicate links appear on the Home page after restarting the JBoss application server
CQ 168479	An HTTP 500 error occurs when you specify AES-256 as the encryption algorithm for a SAML 2.0 partnership. An error is also written to the FWStrace.log.