CA CloudMinder™

Service Provider Release Notes

1.5

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: Changed Features

This section contains the following topics:

1.5

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.

1.1 SP2

Availability of Mobile Client for ArcotID PKI Authentication (see page 9)

Support for Two Step Authentication (see page 9)

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

Downloading CA CloudMinder ISO images

You receive instructions for downloading CA CloudMinder files when you receive your license.

To help ensure that the files download successfully, consider the following notes:

- Use Download Manager to download the files.
- Check the MD5SUM and size for each file after you download them.

CA CloudMinder 1.5	ISO File Name	MD5SUM	File Size
CA Business Intelligence r3.3 for Linux - DVD	DVD06213531E.iso	2276e0786505e7ad3504b3a6ca77c864	5,415,825,408
CA CloudMinder 1.5Cloud Components (DVD 1 of 2)	DVD11174406E.iso	9f852fe9c63fdb6dc3eba45ca26af9a2	3,399,155,712
CA CloudMinder 1.5 Cloud Components (DVD 2 of 2)	DVD11174458E.iso	4778a00f4e0e60b7e8187a4d1f5f8214	2,136,473,600
CA CloudMinder 1.5 On-premise Components	DVD11174121E.iso	399814261e47c4b41989c8500f5d0a92	1,783,365,632

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.

An Error Occurs When I Upgrade the CA SiteMinder® Policy Server

Symptom:

The following error message appears when I upgrade the CA SiteMinder® Policy Server:

Arcot arrfserver Watchdog Service initializing ...
Operation stop being performed on Server <*servername*> Server
Operation failed.
Could not get failure details.TransportException. while connecting to [http://localhost:9743/] Err : create: No Transports AvailableOperation start being performed on Server servername Server
All environment variables are set

Solution:

This error message is benign and does not indicate an issue with the upgrade process on the CA SiteMinder® Policy Server. You can ignore this message.

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.

OpenID Images do not Display After Upgrade

Symptom:

In upgrade environments, images in the OpenID provider may not appear. Functionality is not impacted.

Solution:

During the upgrade, copy the contents of:

/opt/CA/secure-proxy/proxy-engine/examples/forms

to:

/opt/CA/secure-proxy/proxy-engine/examples/siteminderagent/forms

General Issues

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.

Devices May Display Certificate Security Warnings During Authentication

Symptom:

Some devices may show an error for untrusted certificates when users authenticate. This means intermediate certificates are missing from the trust store.

Solution:

Verify that the Apache httpd configuration in the SPS machine has the complete certificate chain configured. Visit Apache.org for configuration information.

Issues with CA ArcotID OTP Enrollment Task in Internet Explorer 9 or 10

Symptom:

If you are using Internet Explorer 9 or 10, the self service task, CA ArcotID OTP Enrollment, does not generate an activation code.

The task successfully creates the activation code in other supported browsers.

Solution:

Turn on Compatibility View in Internet Explorer 9 or 10.

Note: For more information, see the Microsoft Support site for details.

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.

Do Not Delete Applications That Are Assigned To Active Services

Do not delete applications that are assigned to active services. If you delete an application from an active service, CA CloudMinder throws a null pointer exception.

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.

Application Names And Authentication Names Are Case Sensitive

Application names and authentication names are case-sensitive. For example, TestApplication and testapplication are treated as two different names. Do not capitalize the same application names and authentication names differently. If you do capitalize the names differently, CA CloudMinder treats them as different names.

Forgotten User Times Out

Symptom:

On a slower system, the forgotten user ID task times out as Task Pending before the user name appears.

Solution:

Configure the email option for the forgotten user ID task so that the user receives the user name by email.

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.

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.

Tenant Name and Tag Cannot Contain String "Tenant"

Symptom:

When a tenant name contains the string "tenant", reports that are run on the tenant data can fail or reports can contain an empty data set. Other unexpected behaviors can also occur.

Solution:

Do not include the string "tenant" in the name or tag of a tenant. When you create a tenant, select both a Name and a Tag for the tenant that do not include the string "tenant". See the following examples:

Correct:

Tenant Name: Forward Incorporated

Tenant Tag: forward_incorporated

Incorrect:

Tenant Name: Forward Tenant

Tenant Tag: forward_tenant

Security Code over Voice Message Does Not Support Certain Codes

Symptom:

Users do not receive security codes that have more than eight characters when the Security Code over Voice Message option is selected.

Users see the following error message:

```
Error: An error has occurred while sending the Security Code. Please
try again later.
```

Solution:

To avoid this issue, use one of the following workarounds:

- Set the security code length to eight characters or less in Security Code Profile
- Select an option other than Security Code over Voice Message. For example, Security Code over Email supports security codes that include more than eight characters.

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.

Error: Launch Task Does Not Contain URL

Symptom:

The launch task for accessing an endpoint does not work after refreshing the CA CloudMinder build. When users try to use the task, the following error occurs:

`Error: External task <endpoint> Launch Task Does Not Contain URL`

Users are not redirected to the endpoint URL.

Solution:

1. Log in to the User Console.
2. Search for and select the launch task by using Modify Admin Task.

   The task that you selected opens.
3. Click Submit without changing anything.

The launch task works properly after completing these steps.

Minimum Password Length Error Message Does not Display

Symptom:

If password length is too short when resetting a password, the error message explaining minimum password length displays incorrectly. This behavior also occurs if the user leaves the password fields empty. Users receive the following message:

Error: $(PARAM_NAME)$ is less than the minimum length.

Solution:

Make sure that the Advanced Authentication password policy is the same as the <stmdr> password policy.

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.

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.

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.

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.

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 3: Fixed Issues

This section contains the following topics:

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
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
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

Support Ticket	Problem Reported
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
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.