CA CloudMinder™

Service Provider Release Notes

1.53

This Documentation, which includes embedded help systems and electronically distributed materials (hereinafter referred to as the “Documentation”), is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

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:

1.53

This release of CA CloudMinder supports the Oracle 12c database.

Note:

- All customers should install CABI 3.2 SP2 with the patch.
- Customers can upgrade to CA CloudMinder 1.53 and continue to use Oracle 11g.

Important! CA Technologies has not tested migrating an existing and deployed CA CloudMinder Oracle 11g database to Oracle 12c. As a precaution, we recommend doing a fresh installation of CA CloudMinder when you intend to start using Oracle 12c.

1.52

Support for the SCIM Connector

CA CloudMinder supports the SCIM (System for Cross-domain Identity Management) connector. For more information, see How to Connect CA CloudMinder to SCIM:

https://wiki.ca.com/display/IMGC10/How+to+Connect+CA+CloudMinder+to+SCIM

Support for Social Sign-on

CA CloudMinder supports letting users log in using any of the top social IdPs such as Facebook, Google, Twitter, LinkedIn, WindowsLive, Sina Weibo, and RenRen.

Refer to the *SSO Partnership Federation Guide* for more information.

Support for Single Sign-on to Office 365

CA CloudMinder enables single sign-on between enterprise users and Office 365 services. Federating to Office 365 removes the burden of hosting services locally. For example, an enterprise user logs in to the desktop email client but is unaware that the service is in the cloud. The sign-in experience with Office 365 is the same as if they were connected to an on-premise application.

Refer to the *SSO Partnership Federation Guide* for more information.

Support for Disambiguation for SAML 2.0

CA CloudMinder now has support for disambiguation for SAML 2.0 local Identity Providers. this allows an IdP to configure multiple partnerships with remote Service providers that use the same Service provider ID.

Search for "Disambiguation ID", under "SAML 2 Local IdP Entity Dialog" in the CSP Console online Help.

Support for Dynamic ACS URL

The SAML 2.0 IdP->SP Partnership UI has a new check box in the "SSO and SLO tab" of the partnership wizard:

Accept Dynamic ACS URL (Only in Signed Authnrequest)

Selecting this option means the SSO Service will accept any valid URL for the AssertionConsumerServiceURL when the <AuthnRequest> is signed, as well as use it for delivering the Assertion post successful authentication at the Identity Provider.

Search the CSP Console Help for "SSO (SAML 2.0 IdP)" under "SSO and SLO Dialog".

New Wiki for Connectors Documentation

The documentation for connectors has moved to a wiki. The wiki is a collaborative environment that lets you:

- Find answers quickly with intuitive search
- Access up-to-date information on mobile devices
- Export content to PDF
- Rate or comment on any topic, and provide feedback to CA Technologies

CA Information Services monitors the wiki and makes regular updates.

Changes to Audit Reporting Table

In CA CloudMinder 1.52, the audit log table has moved from CLOUDMINDERACCESSLOG4 to SMACCESSLOG4. SMACCESSLOG4 is used to generate SSO reports.

The following changes are implemented in CA CloudMinder to support audit data in SMACCESSLOG4:

- A script to migrate data from CLOUDMINDERACCESSLOG4 to SMACCESSLOG4 runs automatically during SiteMinder Policy Server upgrade
- The BIAR file now points to SMACCESSLOG4

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

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 15)
Support for Two Step Authentication (see page 15)

1.1 SP2

Availability of Mobile Client for ArcotID PKI Authentication (see page 15)

Support for Two Step Authentication (see page 15)

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

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.ManagedConnectionFactoryDeploymen
t] (Thread-20) Exception during getSubject()Unauthenticated caller:null

java.lang.SecurityException: Unauthenticated caller:null
   at
org.jboss.security.integration.JBossSecuritySubjectFactory.createSubject(JBossSecurityS
ubjectFactory.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.

Rebooting the SMPS Generates a Tunnel Failure

Symptom:

If you reboot the SMPS without rebooting the Identity Manager deployment, you could get tunnel failures between Identity Manager and SMPS. This could affect tenant deployment.

Solution:

If you need to reboot the SMPS deployment, always make sure to also reboot the Identity Manager deployment.

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.

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.

General Issues

Signing out of Office 365 SLO Displays an Error Page

Symptom:

When the end user clicks Sign out in Office365, an error page appears.

Solution:

1. Create a custom JSP page for logout.

2. Add a custom JSP URI in Logout URI of CAM-AgentObj (ACO object in WAMUI Console) for removing the smsession cookie.

3. In partnership, we have not did any changes

4. In the custom JSP, after clearing the session, give the logout URL as http://login.microsoftonline.com/logout.srf

When the user clicks Sign-out, the user is redirected to the last ACO logout URL, until the logout page of Office365 appears without any error.

Unable to Set Bulk Load Approval Size

Users cannot view how many tasks are within a Bulk Load Approval Request so as to monitor how large a job is, as well as its impact on system resources.

AD Endpoint Explore Of Users Container Fails

Symptom:

When a creating a new AD endpoint, the ADSContainer objects are not added into the Provisioning Directory. When creating an Explore definition for the Users container, the object would be added to the Provisioning Repository. The Explore executes successfully as long as this object exists.

If this object does not exist in the Provisioning Directory, then an attempt is made to add it via the Connector Server, causing a failure.

Solution:

Create a new Explore definition for the Users container to trigger the creation of the object in the Provisioning Directory. You can then delete this new definition, and then use the original definitions.

Error when Synchronizing while modifying a DirSync Template Mapping

Symptom:

Synchronizing a DirSync Template Mapping that uses Javascript while you are in the process of modifying it generates an error.

Solution:

When you want to synchronize, make sure that you save the template, right-click the template, and then select Synchronize.

Import Server Certificate to Cloud CA IAM Connector Server

Symptom:

When I import the server certificate to the Cloud CA IAM connector server, it does not synchronize with the all connector servers in a high availability environment or connector servers at the disaster recovery site.

Solution:

Import the server certificate to all connector server instances in a high availability environment and at the disaster recovery site.

False Error from DR_mode.sh

Symptom:

The DR_mode.sh script assumes that the CA IAM Connector Server and Provisioning Server are always on the same machine. Using this script when the CA IAM Connector Server and Provisioning Server are on different systems causes errors. You can ignore these errors.

Solution:

Ensure that the Provisioning Server and CA IAM Connector Server services are running on both the primary and disaster recovery site.

Unable to Launch Security Token Service Page

Symptom:

The Security Token Service page does not display, and shows an error similar to "The website cannot display the page."

Solution:

Follow these steps:

1. Click the Back button in the browser. The Secure Proxy Server Administrative user interface displays correctly.
2. Click Web Services, Security Token Service. The Available Security Token Services page displays correctly.

Error Message after Deploying the Security Token Service

Symptom:

After deploying the Security Token Service, the Secure Proxy Server nohup.out log has an error message similar to the following:

```
INFO: Initializing Spring FrameworkServlet 'ssohub'
java.lang.IllegalArgumentException: InputStream cannot be null at
javax.xml.parsers.DocumentBuilder.parse(DocumentBuilder.java:117)
```

Solution:

You can ignore this message. It does not impact the functionality.

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.

Some Users Missing after Bulk Load

Symptom:

After Bulk Load, a few users are missing from the Provisioning Directory even though they exist in the Identity Management User Store.

Solution:

1. Create a policy on Modify User task completion. The add action is adding the user to a provisioning role. The add action is adding the user to a provisioning role. The default role is Empty Provisioning Role.
2. Make sure that the CSV file contains the password/confirmed password for each user. If the attributes are not given, you can change some user attributes.
3. Upload the original CSV file.

   On the second page, select the Modify User task for the action and the Create User task for the non-existent object.
4. Click Finish.

Tenant Management Issues

Unable to Set Tenant Quota Max

You can currently set the task quota on a per-tenant basis by logging into the Tenant environment: In the User Console, select System, Manage Task Quota.

You cannot set the maximum total task quota across all of the tenants being hosted on a single installation. A high number may system resources.

Tenant Creation Fails

Symptom:

Tenant creation fails with the handshake alert: unrecognised name.

Solution:

1. Edit the JBoss run.sh file on the Identity Management server.
2. Add the following Java option:

   ```
   jsse.enableSNIExtension=false
   ```
3. Edit the JBoss run.sh file on the CSP console.
4. Repeat step 2.

Deletion Fails

Symptom:

Under some circumstances, the CSP Console can indicate that a tenant deletion has failed.

Solution:

Follow these steps:

1. Verify the following setting on your SPS servers:

   In /opt/CA/secure-proxy/proxy-engine/proxyserver.sh:

   -Dhttp_connection_timeout=300000

   If needed, set this appropriately and restart SPS.
2. Regardless of the SPS setting, delete the tenant a second time.

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.

Use the following procedure to delete a tenant.

Note: For High Availability Systems: You need to follow the steps for each leg. You should only need to delete the tenant and directory from IM manage on the first leg.

For Disaster Recovery Systems: You need to follow the same steps at both sites. You should only need to delete the tenant and directory for IM manage at the first site.

1. Delete IME from IM Manage (only from one IM server) by accessing the IM Management Console:

   a. Got to http://<IM Host>:8080/iam/immanage/

   b. Go to Home, Environments.

   c. Select the environment for the tenant to delete.

   d. Select Delete.

2. Delete the Directory from IM Manage (only from one IM server) by accessing the IM Management Console:

   a. Go to http://<IM Host>:8080/iam/immanage/

   b. Go to Home, Directories.

   c. Select the check box for the directory corresponding to your tenant.

   d. Click Delete.

   This will not have any effect,

   e. In the SMPS, navigate to /opt/CA/siteminder./ og and in smps.log find any entry similar to the following:

```
"[Delete.cpp:338][Reduce][ERROR][sm-xpsxps-03340] Cannot delete a related record.
(CA.SM::UserDirectory@0e-000621de-79d1-1485-8f37-38450a82d0cb(cm3Tenant
Directory):CA.SM::IMSDirectory@32-00074f6b-79d1-1485-8f37-38450a82d0cb(cm3 Tenant
Directory).CA.SM::IMSDirectory.UserDirectoryLink)"
```

   The failure was because the tenant user directory couldn't be deleted because it had a related entry which is CA.SM::IMSDirectory@32-00074f6b-79d1-1485-8f37-38450a82d0cb.

   f. Delete the related entry from SMPS by using the following steps:

   i) Run XPSExplorer.

   ii) Type F to find by XID.

   iii) Paste the XID obtained from log (CA.SM::IMSDirectory@32-00074f6b-79d1-1485-8f37-38450a82d0cb) and then press enter.   The related object appears.

iv) Press D to delete the object.

g. Now that the related entry is deleted, delete the user directory from the IM Manage by following steps a, b, c, and d above.

3. If the domain and the directory are still in SiteMinder, restart or reboot SiteMinder services (All SMPS and Admin UI servers) as follows:

   On SMPS:

   a. service S98sm stop

   b. Service S98sm start

   On the CSP Console:

   c. service S98smAdminUI stop

   d. Service S98smAdminUI start

4. Update tenant dsa router on each IM, JCS, IMPS, SMPS to remove tenant

   a. su – dsa

   b. cd /opt/CA/Directory/dxserver/config/knowledge
   vi <hostname>-cam-tenant-router

   c. Delete for example: cm3 is the tenant

```
# CA DXserver/config/knowledge/
#
# Knowledge configuration file written by dxagent
#
# Refer to the Admin Guide for the format of the set dsa command.

set dsa "s010130009046-cam-tenant-cm3" =
{
prefix =   <o ca><ou cam><ou cm3>
dsa-name =   <o ca><ou cam><ou cm3><cn s010130009046-cam-tenant-cm3>
dsa-password            = "secret"
address         = ipv4 "s010130009046" port 50006
disp-psap               = DISP
snmp-port               = 50006
console-port            = 50007
auth-levels             = clear-password
dsp-idle-time           = 50
multi-write-group               = primary
dsa-flags               = multi-write, no-service-while-recovering,
multi-write-group-hub
trust-flags             = allow-check-password, trust-conveyed-originator
link-flags              = ssl-encryption-remote
};
```

   d. Update the dxc file using the following commands:

   i) cd /opt/CA/Directory/dxserver/config/settings

ii) vi <hostname>-cam-tenant-router.dxc

iii) remove tenant for example if tenant is cm3 change:
set write-precedence = s010130009046-cam-tenant-cm1, s010130009046-cam-tenant-cm3, s010130009046-cam-tenant-cm4; to set write-precedence = s010130009046-cam-tenant-cm1, s010130009046-cam-tenant-cm4;

5. Restart the dxa router on each IM, IMPS, JCS, SMPS, and Directory system:
   a. su – dsa
   b. dxserver stop all
   c. dxserver start all
6. Remove the provisioning directory on each IMPS
   a. cd /opt/CA/Directory/dxserver/config/knowledge
   b. vi -imps-router.dxc and remove tenant info

      For example:

```
# CA DXserver/config/knowledge/
#
# Knowledge configuration file written by dxagent
#
# Refer to the Admin Guide for the format of the set dsa command.

set dsa "tenant-cm3-s010130009046" =
{
prefix =   <dc cm3>
dsa-name =   <dc etadb><cn tenant-cm3-s010130009046>
dsa-password            = "secret"
address         = ipv4 "s010130009046" port 20904
disp-psap               = DISP
snmp-port               = 20904
console-port            = 20905
auth-levels             = clear-password
dsp-idle-time           = 50
dsa-flags               = multi-write, no-service-while-recovering,
multi-write-group-hub
trust-flags             = allow-check-password, trust-conveyed-originator
link-flags              = ssl-encryption-remote
};
```

7. Update the dxc file on each IMPS server for the imps router
   a. cd /opt/CA/Directory/dxserver/config/settings
   b. vi <hostname>-imps-router.dxc

c. change set write-precedence = s010130009046-impd-main, s010130009046-impd-inc, s010130009046-impd-co, s010130009046-impd-notify, tenant-cm1-s010130009046, tenant-cm3-s010130009046, tenant-cm4-s010130 to set write-precedence = s010130009046-impd-main, s010130009046-impd-inc, s010130009046-impd-co, s010130009046-impd-notify, tenant-cm1-s010130009046, tenant-cm4-s010130

8. Restart the dsa's on each IMPS:

   a. su – dsa

   b. dxserver stop all

   c. dxserver start all

9. Stop the DSA's for tenants on all DIR servers:

   a. su – dsa

   b. dxserver stop <host name>-cam-tenant-<tenant tag> (ie s010130009046-cam-tenant-cm3)

   c. dxserver stop tenant-<tenant tag>-<host name> stop (ie tenant-cm17-s010130009046)

10. Remove the tenant data files from each DIR server:

    a. su – dsa

    b. cd /opt/CA/Directory/dxserver/data

    c. ls *<tenant tag>*

    d. delete all files returned from B (for example: cam-tenant-cm3.ldif tenant-cm3-s010130009046.db tenant-cm3-s010130009046.tx, tenant-cm3-s010130009046.db tenant-cm3-s010130009046.tx)

       a. cam-tenant-<tenant tag>.ldif

       b. tenant-<tenant tag>-<hostname>.db

       c. tenant-<tenant tag>-<hotname>.tx

       d. <host name>-cam-tenant-<tenant tag>-.db

       e. <hostname-cam>--tenant-<tenant tag>-.tx

11. Remove knowledge files from Directory server

    a. su – dsa

    b. cd /opt/CA/Directory/dxserver/config/knowledge

    c. delete tenant-<tenant tag>-<hostname> .dxc (ie tenant-cm3-s010130009046.dxc)

    d. delete <host name> -cam-tenant-<tenant tag>.dxc (ie s010130009046-cam-tenant-cm3.dxc)

12. Remove the settings files on each directory server for the tenant
    a. su – dsa
    b. cd /opt/CA/Directory/dxserver/config/settings
    c. delete tenant-<tenant tag>-<hostname>.dxc (ie tenant-cm3-s010130009046.dxc)
    d. delete <host-name>-cam-tenant-<tenant tag>.dxc (ie s010130009046-cam-tenant-cm3.dxc)
13. Remove the dxi file from each directory server
    a. cd /opt/CA/Directory/dxserver/config/servers
    b. remove   tenant-<tenant tag>-<hostname>.dxi (ie tenant-cm3-s010130009046.dxi)
    c. remove <host name>-cam-tenant-<tenant tag>.dxi (ie s010130009046-cam-tenant-cm3.dxi)
14. Remove the pem files on each directory server:
    a. su – dsa
    b. cd /opt/CA/Directory/dxserver/config/ssld/personalities
    c. remove <host-name>-cam-tenant-<tenant tag>.pem (ie s010130009046-cam-tenant-cm3).pem
    d. remove tenant-<tenant tag>-<hostname>.pem (ie tenant-cm11-s010130009046.pem
15. Remove the auto start file on each directory server:
    a. su – dsa
    b. cd /opt/CA/Directory/dxserver/config/autostart
    c. remove <host name>-cam-tenant-<tenant tag> tenant-<tenant tag>-<hostname> (ie s010130009046-cam-tenant-cm3 tenant-cm3-s010130009046)
16. Remove the limits file on each directory sever
    a. su – dsa
    b. cd /opt/CA/Directory/dxserver/config/limits
    c. remove <host name>-cam-tenant-<tenant tag>.dxc (ie s010130009046-cam-tenant-cm3.dxc)
    d. tenant-<tenant tag>-<host name>.dxc (ie tenant-cm3-s010130009046.dxc)
17. Remove ssld files on each directory server
    a. su – dsa
    b. cd /opt/CA/Directory/dxserver/config/ssld

   c. remove <host name>-cam-tenant-<tenant tag>.dxc   (ie s010130009046-cam-tenant-cm3.dxc)

   d. remove tenant-<tenant tag>-<hostname>.dxc (ie tenant-cm3-s010130009046.dxc)

18. Remove the log configuration files on each directory server

    a. su – dsa

    b. cd /opt/CA/Directory/dxserver/config/logging/

    c. remove tenant-<tenant Name>-<DIR Server>.dxc

    d. remove <DIR Server>-cam-tenant-<Tenant Name>.dxc

19. Restart all DSA on all Directory machines

    a. su – dsa

    b. dxserver stop all

    c. dxserver start all

20. Verify that the DSA no longer show via a dxserver status on each directory server

    a. su – dsa

    b. dxserver status

    c. Verify that the dsa for the tenant are not there:

       ■ <host name>-cam-tenant-<tenant tag> (ie s010130009046-cam-tenant-cm3)

       ■ tenant-<tenant tag>-<host name> stop (ie tenant-cm17-s010130009046)

21. Remove the Provisioning association:

    a. Use LDAP tool like JXplorer

    b. Connect to your IMPS machine using user name and password

       1) Use port 20391

       2) User DN eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,dc=etadb

       3) Password <your password for Provisioning DSA>

       4) Goto etadb, im, CommonObjects, Configuration, Parameters, Tenant Data, Tenant Identifiers.

       5) Delete eTConfigPramValue for the tenant tag.

22. Delete the tenant from the CSP console:
    Iin DR need to export and import Derby – Refer to the DR documentation for steps to delete a tenant for DR.

23. Inactivate the tenant from the Arcot Admin Console:

    a. Go to http://<smps host>.ca.com:9090/arcotadmin/mabamlogin.htm

    b. Search active tenants and find your tenant.

    c. Note the GUID this will help with the next step.

    d. Inactivate the tenant.

24. Delete tenant from Arcot Admin console

    a. Go to http://<smps host>.ca.com:9090/arcotadmin/mabamlogin.htm

    b. Search inactive tenants and find your tenant – the tenant was renamed by the inactive to the GUID. So you need to find the GUID which is for you tenant. If you don't have this from the last step, look at each tenant and go to the next page and look at the DN.

    c. Delete the tenant.

Tips for Re-Deploying a Deleted Tenant

- If you get a message from a tenant deployment that the tenants is already registered with IMPS, verify that the IMPD has been updated to remove the tenant. See IMPD.
- If a tenant deployment says DSA ports are in use, make sure ports are not in use on the Directory server. See Port or verify that all the steps were done on the directory server. If needed, restart the directory servers.
- If tenant deployment says AA org exists. Then see AA.
- If tenant deployment gets errors on SMOID or duplicate records on the SiteMinder side, then run XPSExport, find the record id, and then user XPSExplorer to delete the duplicate.

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

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.

Authentication Issues

Connector Server Network Peers Connectivity Problems

Symptom:

When using network peer On Premise CA IAM Connector Server and you stop one CA IAM Connector Server, it may not be detected, and previsioning may fail.

Solution:

When you stop one CA IAM Connector Server, force a synchronization between the two on-premise nodes.

User With Expired Credentials Must Perform Extra Step

Symptom:

When authenticating with PKI, you use your password to unlock your PKI credentials. If you are forced to change your password (such as when a temporary password is generated, or the admin sets the user to change password) and authenticate with PKI, Advanced Authentication sends you correctly to the enrollment task, where you can change your password and reissue your PKI credentials in one task.

However, if you authenticate with PKI and you are in violation of password policies (such as inactivity, not changing your password in required time) Advanced Authentication does not detect this. The system then sends you to the Password Change task.

Solution:

Users must first go to the Password Change task, and then the Enrollment task. Users must change their password, and then perform a secondary authentication to reissue their credentials.

Special Characters Not Allowed In Username During Arcot OTP Enrollment

Symptom:

If a user’s name or other account information uses special characters (such as an umlaut: ü), trying to enroll a user with Arcot One Time Password generates an error message.

Solution:

If possible, do not use special characters when entering user information. Special characters include Chinese and Japanese characters, as well as the following characters: À, Á, Â, Ã, Ä, È, É, Ê, Ë, Ò, Ó, Ô, Õ, Ö, Û, Ü, à, á, â, ã, ä

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.

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.

Connector Issues

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.

Reporting Issues

Cannot View Scheduled Reports

Reports that were previously scheduled for recurrence do not appear in the Modify Report Recurrences task.

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.

Disaster Recovery Known Issues

Missing Emails During Failover

Symptom:

If a failover occurs during the use of a Bulk load create user task, some emails are not sent to notify the user about the new account. View Submitted Tasks shows the users who were not notified.

Solution:

Notify users that are identified in the View Submitted Tasks that accounts exist for them.

Incomplete Tasks During Failover

Symptom:

If failover occurs during a Report Snapshot, Explore and Correlate, or Bulk Load task, the task remains in an in progress state. The task never completes.

Solution:

For an incomplete task (Report Snapshot, Explore and Correlate or Bulk Load), resubmit the task.

Missing Primary Directory DSAs

Symptom:

Missing DSA errors occur in this situation:

1. Fail over to the DR site.
2. Shutdown the primary site systems.
3. Log in to the CSP console at the DR site.

   In the hosting container, make the following changes:

   a. Remove all primary site systems.

   b. Change the DR site systems to be primary site systems.
4. Add a tenant.
5. Logged into DR site CSP console, which is now the primary site.

   In the hosting container, make the following changes:

   a. Change the primary site systems back to DR site systems.

   b. Change the DR site systems back to primary site systems.

Errors messages report that Provisioning Directory DSAs are missing at the primary site.

Solution:

If you remove primary site systems from the hosting container, add them back as DR site systems.

No Account Synchronization During Shutdown

Symptom:

Active Directory accounts are not synchronized when the Identity Management server and the CA IAM Connector Server are shut down. During the shutdown period, accounts that are created and deleted are not synchronized to the tenant directory.

Solution:

If directory synchronization was in progress when the shutdown occurred, restart directory synchronization.

Chapter 3: Fixed Issues

This section contains the following topics:

Fixed Issues in 1.53

The following issues are fixed in CA CloudMinder 1.53:

Support Ticket	Problem Reported
21807842-01 00013793	Policy Express policy causing a never ending loop on Submitted Task Failed
21958599-01	Arcot Webfortcrashed
22046436-01	Identity Manager servers OutOfMemoryExceptions
21965747-01 22030482-01	Patches For Poodle Vulnerability
21848425-01	Email Addresses tab on Create Active dir account: Clicking any tab besides the EmailAddresses tab for the Create Active Dir. account task grays out the Email Addresses tab
21934175-01	Update doc to say you should not use bulk load to set relationships like groups, admin roles, and provisioning roles
21990930-01 22003412-01	HTTP 500 error with SPS and CloudMinder Integration
21934625-01	When Configuring resources with IWA Authentication Scheme and Password Policies on the Active Directory User Store with a disabled user, the Policy Server redirects the user to the default Password Services page, and not the one from the Password Policies.
	SAML 2.0 implementation: The Assertion Generator doesn't set the Destination attribute when generating a failure response.
21860928-01	Logo size appears large in email

Support Ticket	Problem Reported
21843738-01	The SiteMinder Audit Extension (SMAE) module of CA CloudMinder seems to require clear-text database password in its configuration file.
21793450-01	Using $ in passwords for install scripts causes the installation to fail.
21769638-01 21875453-01	Executing a Modify Email task from email causes an error.

Fixed Issues in 1.52

The following issues are fixed in CA CloudMinder 1.52:

Support Ticket	Problem Reported
21859486-1 21880560-1	When creating a multi-value attribute for an assertion, CA CloudMinder separates each value with a caret.
21856059-1	ProviderID is not URLDecoded in usage in CA CloudMinder 1.51 affwebserves, so does not match entry in policy server.
21751265-1	Audience problems with AWS as the service provider and CA CloudMinder as the identity provider.

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.

Support Ticket	Problem Reported
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.
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
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

Support Ticket	Problem Reported
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
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

Support Ticket	Problem Reported
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.