CA CloudMinder™

Troubleshooting Guide

1.53

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: Installation Issues

When installing CA CloudMinder, some common issues can prevent a successful installation.

This section contains the following topics:

Server Issues

The following server issues may occur during an installation.

Install All of the Components in the Correct Order

Before installing any CA CloudMinder components, install all required packages, including Linux patches.

After configuring the packages and permission, install the server components in the correct order. Review the listing of packages and permissions, and the component order installation located in the *Installation Guide*.

Correctly Configure the Firewall/iptable and SELinux Security Settings

Before running the installation, check the following firewall, iptable, and SELinux settings on all servers in the CA CloudMinder environment.

Follow these steps:

1. Set the state of the firewall/ip tables using the following commands:
   ```
   chkconfig iptables off
   service iptables stop
   ```
2. Check and set the state of SELinux using the following command:
   ```
   sestatus
   ```
3. If the response is permissive or disabled, perform no action. If the response is enforcing, change the state using the following commands:
   ```
   edit /etc/selinux/config
      SELINUX=permissive
   setenforce 0
   ```

MSGMNI kernel Installation Error

Symptom:

Install fails with message "MSGMNI kernel parameter set is not sufficient"

Solution:

1. Navigate to the server kit install file:

   /opt/CA/saas/repo/application/local_environment.sh

2. Edit the file as follows.

   Change the line that reads:

   REQUIRED_MSGMNI=" 32"

   to read:

   REQUIRED_MSGMNI=" 33"

3. Re-run the Provisioning Server installation process.

Network Issues

Problems with network setup can cause failures in the installation process. Consider the following actions to isolate the problem:

- Make sure all servers are able to ping each other.
- If DNS is not running in the environment, host files on each server need correct IP information.
- Firewall and load balancer ports need proper configuration. The list of required ports is available in the Port Communication Tables section of the *Installation Guide*.
- Import the complete certificate chain to the server connected to the Internet: Use the **SSLCertificateChainFile** parameter in the Apache configuration on the Secure Proxy Server.
- The IdentityMinder Server, Cloud IAM Connector Server, and SiteMinder Policy Server need an Outbound-Only Internet connection.
- If the internal and external hostnames are different for the Security Proxy Server, edit the **server.conf** file, found here:
  `/opt/CA/secure-proxy/proxy-engine/conf/server.conf`

  Set the following parameter:
  `redirectrewritablehostnames="<InternalHostName>, <ExternalHostName>"`

The properties.sh File

Verify that parameters are correct in the **properties.sh** file. Some common mistakes include providing incorrect server names, incorrect paths, and missed parameters.

Important! When your installation completes, save a backup copy of the **properties.sh** file to a secure location! Linux periodically removes files from the **/tmp** folder.

You will need this backup copy for future upgrades. Details for each parameter in the **properties.sh** file are in the *Installation Guide*.

Chapter 2: Tenant Deployment Issues

The section provides information to troubleshoot tenant deployment related issues.

This section contains the following topics:

Tenant Creation Issues

When creating tenants, several general recommendations exist:

- When experiencing tenant creation issues, check the JBoss log of the Cloud Service Provider (CSP) to see if the creation has started. For example, was the CSP able to contact the Hosting container? Depending on the content, it can helpful to view the JBoss log of the CA Identity Manager server and then the [assign the value for iamcs in your book] daily log.
  - The CSP JBoss log is located here:

    /opt/CA/siteminder/adminui/[JBOSS]/server/default/log/server.log

  - The Connector Server log is located here:

    /opt/CA/IdentityManager/ConnectorServer/jcs/logs/jcs_daily.log

  - The JBoss log is located here:

    IM JBoss log: /opt/[JBOSS]/server/all/log/server.log

  Note: [JBOSS] varies, depending whether you are using the JBoss EAP or Community version.

- Setting **com.ca.voyager** to DEBUG in JBoss of both CSP console and CA IdentityMinder can provide additional helpful information.
- When creating a new tenant, do not include the word **tenant** in its name.

Check the follow settings in the CSP Console:

- If the CA IAM Connector Server is installed on a separate server, then make sure that SiteMinder Provisioning Server Tenant Service Host is set to the CA IAM Connector Server host name in the Hosting Container.
- In the Hosting Container, list all host names for CA IdentityMinder, SiteMinder Provisioning Server, and the CA IAM Connector Server in the section for Tenant DSA Router Hostnames. If the CA IAM Connector Server is installed on the SiteMinder Provisioning Server, list the host names of the SiteMinder Provisioning Server instead.

CA Directory Web Services Issues

If CA Directory errors occur, make sure that the CA Directory DSAs and DxAgent web service are running on all servers that have Directory installed.

Follow these steps:

1. Log in as the DSA user:
   ```
   su - dsa
   dxserver status
   ```
2. If any DSAs are stopped, enter the following command:
   ```
   dxserver start all
   ```
3. Check the DxAgent status:
   ```
   cd /opt/CA/Directory/dxserver/dsamgmt
   ./dxagent.sh status
   ```
4. If the DxAgent is not running, run the following command:
   ```
   ./dxagent.sh start
   ```

"Unable to process your Request now" Error Message When Accessing the User Console

Symptom

When accessing the User Console, the following error message appears: "Unable to process your Request now."

Consider the following three solutions.

Solution 1

This error can appear when the Credential Handling Service does not have the correct Tenant Web Services shared secret.

By default, CA CloudMinder is configured with the assumption that Tenant Web Services keeps the default shared secret.

During the installation of the SiteMinder Policy Server, if the **_aa_tws_shared_secret** property in **properties.sh** is set to another value, then you need to make Tenant Web Services and the Credential Handling Service aware of this shared secret using the following procedure:

Note: This is a multi-part procedure, with procedures for both editing and viewing the various shared secret configurations in two places.

Correct the Tenant Web Services shared secret

On the SiteMinder Policy Server and the Tenant Web Services shared secret configuration:

1. cd /opt/CA/AdvancedAuth/Tomcat/webapps/tenant-services/WEB-INF/classes/resources
2. (optional) dos2unix tenantconfiguration.xml
3. Edit tenantconfiguration.xml
4. Set **twssecret** to the value of **_aa_tws_shared_secret** from the **properties.sh** file, and make sure **isencrypted=false.**
5. Restart Advance Authentication Tomcat.
6. View **tenantconfiguration.xml** again.
7. Copy the now-encrypted shared secret.

Correct the SPS-Credential Handling Service shared:

Follow these steps:

1. Edit **/opt/CA/secure-proxy/Tomcat/webapps/chs/WEB-INF/classes/config/chsConfig.properties** file as follows:
2. Copy the encrypted value of **_aa_tws_shared_secret** from the tenantconfiguration.xml file and place it as the **sharedsecret** value in the **chsConfig.properties** file.
3. Restart SPS.

Check the Tenant Web Service Configuration

To obtain tenant information, CA CloudMinder invokes the CA IdentityMinder tenant Web Service. Check its configuration in the tenant user console.

1. Navigate to System, Web Services, Modify Web Service.
2. Search for and then select the Web Service object.
3. On the Security tab, make sure to clear the Require Secure Communication option.

Increase Logging Level

If after checking the configuration,the problem persists, follow these steps:

1. Increase Tenant Web Services logging level by completing the following steps:
   a. Connect to the system where the SiteMinder Policy Server and Advanced Authentication are installed.
   b. Edit **/opt/CA/AdvancedAuth/Tomcat/webapps/tenant-services/WEB-INF/classes/resources/webserviceslogger.properties** to set the log level to **DEBUG**.
   c. Restart the Advanced Authentication Tomcat server.
2. Repeat the use case.
3. Review the **twslogging.log** file, located by default in **/opt/CA**.

Credential Handling Service Login Issues

Symptom

After deploying a tenant, users cannot log into the CloudMinder tenant. Some symptoms could include:

- Invalid credential errors appear even after providing correct login information
- No response from the login page.

Solution

Use the following steps to temporarily change the Authentication Scheme) to Basic. This temporary change allows you log in to the User Console to fix problems with the application and authentication method configuration.

1. Login to the CSP Console.
2. Select the Policies tab.
3. Click Domains, and then select the **TenantDomain** name.
4. Select the Realms tab, and then modify (in step 6, below) the **tenantName_chsforms_realm_es**.
5. Make a note of the current authentication scheme. You will restore this value later.
6. In the Authentication Scheme drop-down, select Basic.
7. Save the changes.
8. You should now be able to login into the tenant User Console to update the configuration.
9. After logging in to the CloudMinder Tenant, review the configuration for the application and authentications methods.
10. After correcting any issues with the application and authentication method, go back to the CSP Console and restore the original authentication scheme.

Solution 2

In SiteMinder, review the Agent Config Object. Make sure that the parameter **ValidTargetDomain** has the correct value. For example, the value could be .ca.com instead of the correct external domain name for your system.

Solution 3

If the previous two solutions were not helpful, you can increase the CHS log level.

Follow these steps:

1. Edit the file **/opt/CA/secure-proxy/Tomcat/webapps/chs/WEB-INF/classes/config/chslog4j.properties**, as follows:
   a. Change all INFO parameters to DEBUG.
   b. Save the file.
2. Restart your secure proxy server.
3. Perform the operations that give you an error.
4. View the debug information in the log file, located here:

   /opt/CA/secure-proxy/proxy-engine/logs/chsLogin.log

Internal Error When Logging in with PKI with risk or with OTP with risk

Symptom

On a new tenant, when logging in with PKI with risk or OTP with risk authentication flows, the following message appears:

"An internal error has occurred. Please close and re-open your browser. If the problem persists, please contact your helpdesk".

Solution

Do the following:

1. Check the cm-aa.log log file on SPS machine. The default location is here: `/opt/CA/secure-proxy/proxy-engine/logs/`
2. Look for the following error: com.arcot.riskfortAPI.RiskException: Configuration not found
3. If the preceding error appears, complete the following steps:
   a. Login to the arcotadmin console as a global administrator.
   b. Manually refresh the cache refresh for the tenant and verify that risk evaluation rules are showing up.

Chapter 3: Runtime Issues

There can be several issues during product run-time.

This section contains the following topics:

Use Trace with Network Traffic Issues

Using a trace tool is very useful when troubleshooting network traffic issues.

Troubleshoot Issues from the User's Browser (HTTP Trace)

The only CA CloudMinder interface accessible by end users and tenant administrators is the console, so troubleshooting runtime issues starts from the browser. Fiddler2, HttpWatch, ieHTTPHeaders, Firefox TamperData, Chrome Developer Tools and other commercially available tools can be used to trace HTTP activities.

Using HTTP trace at the browser level helps to determine the CA CloudMinder task flow. HTTP trace can capture information such as HTTP actions (GET, POST, and so on), data (headers, cookies, and post data), and server and location values. HTTP status helps determine in which step the issue happens, and aiding the reviewer in identifying the next component to investigate.

Typical HTTP status codes include the following:

- 2xx (success) – the action was successfully received, understood and accepted
- 3xx (redirection) – further action must be taken to complete the request
- 4xx (client error) – the request contains bad syntax or cannot be fulfilled
- 5xx (server error) – the server fails to fulfill an apparently valid request

Network Trace

Tools such as Wireshark can assist Operations, Support, and Engineering teams analyze network traffic and expedite issue resolution. Some typical usage of network trace tools include:

- Ensure that the customer's proxy and firewall do not prevent traffic from connecting to the on-premise [assign the value for iamcs in your book].
- Ensure that the relevant layer in the CloudMinder stack (load balancer, proxy, Secure Proxy Server, [assign the value for iamcs in your book]) can be quickly isolated, such as where an http routing issue is occurring within CloudMinder.

Chapter 4: Identity Management Issues

Identity Management combines several components, each with their own locations for logging and configuration. Knowing how to activate trace, as well as knowing where the configuration and logging files are certainly helps in troubleshooting. Components include the Application Server, Provisioning Server, On-Premise and Cloud Connector Servers, and the CA Directory.

This section contains the following topics:

How to Troubleshoot from the User Console

You can use the User Console to search for the list of events you are looking for. You can View Submitted Tasks to drill down into each Task and the events that make up that task. This helps you to diagnose where, when, and why a failure occurred.

From the User Console, navigate to System, View Submitted Tasks.

Note: If View Submitted Tasks does not have the detailed information for the issue you are troubleshooting, it does provide the starting point for identifying which areas to further research.

How to Enable Logging and Trace Tools

Use the following procedures to enable the logging and trace tools on the system components for debugging purposes.

How to Enable Application Server Debugging

1. From the Identity Minder/JBoss server, navigate to:
   `/opt/<jboss directory>/server/all/deploy/iam_im.ear/config/com/netegrity/config`.
2. Edit log4j_jboss.properties, changing the value to DEBUG for each of the functions you want to trace.

How to Enable Provisioning Server Endpoint Debugging

You can enable transaction logging for the Provisioning Server or endpoint logging for a specific tenant.

1. From JXPlorer, connect to the provisioning server machine using the following parameters:
   - Port: 20389
   - Base Distinguished Name: dc=eta
   - User Distinguished Name: eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=im,dc=eta
   - Password: <Use the password set in the **impd_etaadmin_pwd** property in the Provisioning Server's properties.sh file at installation time>
2. Navigate to eta, im, CommonObjects, Configuration, Parameters, Transaction Log, Level.
3. If the parameter “eTConfigParamValue” is set to 0, set the parameter to 7.
4. Submit.

Enable endpoint logging for a specific tenant

1. Connect to the provisioning server machine using the following parameters:
   - Port: 20389
   - Base Distinguished Name: dc=im,dc=TENANTKEY:<tenantname>,dc=eta
   - User Distinguished Name: eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=im,dc=eta
   - Password: <Use the password set in the **impd_etaadmin_pwd** property in the IMPS Server properties.sh file at installation time>

2. Navigate to eta, TENANTKEY:<tenantname>, im, <Endpoint Type>, <Endpoint ID>. The parameter “eTLog” is set to 0 by default.
3. Set the parameter to 1.
4. Submit.

Locations for the Configuration, Log, and Trace Files for Identity Management Components

Note: Enabling trace may impact performance. Only enable trace during troubleshooting process.

The log files for the components appear in the following locations.

Application Server Logs

The JBoss server.log file contains information about all activity that occurs in the CloudMinder IdentityMinder application, including startup, access, and debugging activities.

The server.log file is located on each IdentityMinder/JBoss server, under **/opt/<jboss directory>/server/all/log**.

Directory Server Logs

These logs contain information about activity that occurs in the user and provisioning directories. This includes information about adding, updating, and deleting users, groups, and other objects from these directories. These logs are tenant-specific and named with the tenant id.

These logs can be found on each of the CloudMinder Directory servers, under **/opt/CA/Directory/dxserver/logs**.

Provisioning Server Logs

These logs contain information about the creation of endpoints, explore/correlate activities, global user creation, transactions that occur between the provisioning server and endpoint accounts, and notifications that occur between the provisioning server and the IdentityMinder server.

These logs are located on the CloudMinder Provisioning Server machine under **/opt/CA/IdentityManager/ProvisioningServer/logs**.

Connector Server Logs

The connector server logs contain information about the provisioning activity that occurs between the provisioning server and the endpoints. They also contain information about the On-Premise CA IAM Connector connection to the Cloud CA IAM Connector . These logs can be accessed directly from the CA IAM Connector console, both on-premise and in the cloud from the logs tab.

These logs can also be accessed from the file system in the following locations:

- Cloud CA IAM Connector logs:
  /opt/CA/IdentityManager/ConnectorServer/jcs/logs

- On Premise CA IAM Connector logs: **C:\Program Files (x86)\CA\Identity Manager\Connector Server\jcs\logs**
- On Premise CCS logs: **C:\Program Files (x86)\CA\Identity Manager\Connector Server\ccs\logs**

Troubleshooting from the Management Console

The hosting administrator uses the Management Console to configure all the Identity Management Directories and Environments. Each tenant has an environment and a directory. Each tenant also uses the Provisioning Directory. From the immanage console, you can review and modify:

- Corporate Directory Attribute Mapping
- Provisioning Directory Attribute Mapping
- Validation Rule Sets
- Auditing
- Business Logic Task Handlers, Logical Attribute Handlers, and Event Listeners
- User Console Settings
- System Manager Settings
- Web Services
- Workflow
- Miscellaneous Attributes: This section of Management Console contains many new settings pertaining to the tenant for CloudMinder, including several attributes for Arcot Advanced Authentication.

Note: Be very careful when making changes to these settings.

The Management Console also provides you with the ability to Export and Import your Environments and Directories, as well as to individually stop and start each tenant environment.

How to Troubleshoot the Provisioning Server

The CloudMinder Provisioning Server does not have a provisioning manager. You must perform all troubleshooting from the directory itself, using an LDAP editor such as JXPlorer.

The provisioning server manages all communication and modifications to every endpoint. All information collected from the endpoints is stored in the provisioning store, which is an LDAP directory. JXPlorer is an LDAP browser tool used to view and update the LDAP store.

From JXPlorer, point to the Provisioning server to use the following parameters:

- Port: 20389
- Base Distinguished Name: dc=eta
- User Distinguished Name: eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=im,dc=eta
- Password: < Password set in the impd_etaadmin_pwd property in the IMPS Server properties.sh file at installation time>

From JXPlorer, you can troubleshoot issues by reviewing settings under im, Common Objects, Configuration, Parameters.

Common Provisioning Errors

The following provisioning errors may appear.

Cannot Provision to Salesforce

Symptom

When provisioning to Salesforce, the following message appears:

Error: Salesforce CRM Content User is not allowed for this License Type

Solution

Do the following:

1. Login to Salesforce.
2. Navigate to the user setup menu.
3. In the quick find section, type CRM.
4. In the search results, click the **Settings** link, and then clear the **Enable Salesforce CRM Content** option.

Unable to Acquire an Active Directory Endpoint

Symptom

When acquiring an Active Directory endpoint, the operation fails with a Confidentiality required error message.

Solution

This error can occur when the Active Directory SSL certificate was not imported correctly to the on-premise CA IAM Connector Server.

Do the following:

1. Launch the Microsoft Management Console.
2. Add the Certificates snap-in.
3. Select Computer Account on Local Computer
4. Verify that your Active Directory certificate is listed in the Trusted Root Certification Authorities..

On Premise CA IAM Connector Server Cannot Connect to the Cloud CA IAM Connector Server

Symptom

The on-premise JCA IAM Connector Server cannot connect to the Cloud CA IAM Connector Server.

Solution

- Import all CloudMinder web server certificates, including the Certificate Authority chain, into the On-Premise Connector server
- Check that port 443 is available on the Cloud CA IAM Connector server.
- Ensure that the clocks on both Cloud and On-Premise servers are synchronized to an NTP server. Only a few seconds difference can exist, unless you have configured the time offset accordingly. Time offset can be configured from the Cloud Connector server console.

CA Directory

The following CA Directory errors may appear:

Directory DSA Will Not Start

If a Directory DSA will not start, you can attempt to start it in debug mode using the following command:

```
dxserver –d start <dsaname>
```

This command provides you with any error messages resulting from the failed start. These messages are also available in the log files in the following directory:

/opt/CA/Directory/dxserver/logs.

How to Enable Tracing

To enable tracing, edit the configuration files in the following directory:

/opt/CA/Directory/dxserver/config/logging

Note: For more details about tracing, refer to CA Directory documentation.

How to Review the Most Common DSA Settings

To review the most common DSA settings, view the files pertaining to the DSA in the following directory:

/opt/CA/Directory/dxserver/config/knowledge

How to Review any Schema Issues

To review any schema issues, view the files in the following directory:

/opt/CA/Directory/dxserver/config/schema

Chapter 5: Federation Single Sign-On Issues

To assist in troubleshooting, you should know how to activate trace, and the location of the configuration and logging files.

This section contains the following topics:

How to Use the Cloud Service Provider Administration Console to Troubleshoot

The Cloud Service Provider team uses the CSP Console to configure authentication schemes, domain policies, federation entities and partnerships.

If an **authentication** issue is reported, log in to the Cloud Service Provider Administration Console, and then check that the following items are correctly configured:

- User directory
- Realms: agent, effective resource, authentication scheme, and authentication level
- Rules
- Policies
- Responses

If a **federation single sign-on** issue is reported, check the following:

- The SAML signing certificate
- The Identity Provider entity configuration
- The Service Provider entity configuration
- The partnership configuration

How to Enable Logging and Trace Tools for Federation Single-Sign-On

Use the following procedures to enable the logging and trace tools on the system components for debugging purposes.

Note: Enabling trace may impact performance, so trace should only be turned on during troubleshooting process.

How to Enable Logging and Trace for the Secure Proxy Server

All requests for CloudMinder services go through the Secure Proxy Server. You can enable the Secure Proxy Server web agent logging and tracing using either Agent Configuration Object or local configuration.

For most cases, CA Technologies recommends editing Agent Configuration Object settings, because changes there automatically take place; local configuration requires restarting the Secure Proxy Server.

Follow these steps:

1. For the Agent Configuration Object, launch the Cloud Service Provider Administrative User Interface.
2. Navigate to Infrastructure, Agent Configuration Objects
3. Edit the Agent Configuration Object for the the Security Proxy Server web agent. The following parameters need to be configured:
   - LogFile
   - LogFileName
   - TraceFile
   - TraceFileName
   - TraceConfigFile.

Note: If necessary to debug proxy rules, locate the **proxyrules.xml** file, and set the **nete:proxyrules** element's debug attribute to **yes**.

How to Enable Logging and Trace for the Federation Web Services

You can enable trace to extract detailed message about federation transactions. For example, you can look at the **FWSTrace.log** to see the generated SAML assertion. Changes to the **LoggerConfig.properties** file require restarting the Secure Proxy Server.

Follow these steps:

1. Configure the following parameters:
   - LoggingOn
   - LogFileName

- TracingOn
- TraceFileName
- TraceConfig

How to Enable Logging and Trace for the Policy Server

By default, the SiteMinder Policy Server logs information in the **smps.log** file. This file is typically the starting point to troubleshoot policy server side issues. If you need additional trace information, turn on trace from the Policy Server Management Console.

Note: You can invoke the Policy Server Management Console from here: **/opt/CA/siteminder/bin/smconsole**

Follow these steps:

1. From the Profiler tab, set the Enable Profiling option to enable profiling.
2. Click Configuration Settings, and then move selected components to the right.
3. To troubleshoot federation related issues, make sure to select the Fed_Server component. This component monitors activity for the assertion generator and the SAML authentication scheme. For example, you can view the generated assertion in the smtracedefault.log file.

Note: Changes to the Profile settings take effect automatically.

How to Enable Logging and Trace for the Extensible Policy Store (XPS)

Enable XPS validation and federation object tracing to monitor federation database activities. Use the XPSConfig utility to make changes.

Note: CA Technologies recommends restarting the Policy Server after the change.

SiteMinder logs these activities to the smps.log file.

Locations for the Configuration, Log, and Trace Files for Federation Single-Sign-On Components

The following list shows the default configuration and log/trace file locations for Federation Single Sign-On Components:

Note: Use the relevant value for [JBOSS] below, depending on your version. For instance, the path with EAP is /opt/CA/siteminder/adminui/jboss-as/server/...

For the community version, it is

/opt/CA/siteminder/adminui/server/...

- Cloud Service Provider Admin Console log configuration: **/opt/CA/siteminder/adminui/[JBOSS]/server/default/deploy/iam_siteminder.ear/user_console.war/META-INF/SiteMinderLog4j.properties**
- Cloud Service Provider Admin Console log file: **/opt/CA/siteminder/adminui/[JBOSS]/server/default/log/server.log**
- Secure Proxy Server web agent name: **CAM-Agent**
- Secure Proxy Server agent configuration object: **CAM-AgentObj**
- Apache error log file: **/opt/CA/secure-proxy/httpd/logs/error.log**
- Secure Proxy Server log file: **/opt/CA/secure-proxy/proxy-engine/logs/sps.log**
- Secure Proxy Servertrace file: **/opt/CA/secure-proxy/proxy-engine/logs/sps_trace.log**
- FWS logging/tracing configuration file: **/opt/CA/secure-proxy/Tomcat/webapps/affwebservices/WEB-INF/classes/LoggerConfig.properties**
- FWS trace file: **/opt/CA/secure-proxy/proxy-engine/logs/FWSTrace.log**
- Policy server log file: **/opt/CA/siteminder/log/smps.log**
- Policy server trace file: **/opt/CA/siteminder/log/smtracedefault.log**

Common Federation Single-Sign-On Issues

The following Federation Single-Sign-On Issues may occur.

Initial SAML Request Succeeds, but the Browser Loops

Symptom

The initial SAML request goes through, but then the browser goes into infinite redirects (or loops).

Solution

There could be multiple solutions, including:

- Check that the user exists in both the Identity Provider and Service Provider sides.
- If CloudMinder is the Identity Provider, make sure that the CloudMinder SAML signing certificate - and not the web server SSL certificate - is provided to the Service Provider.
- Confirm that other correct metadata information is exchanged between the Identity Provider and Service Provider.
- Confirm that the Security Proxy Server Agent Configuration Object's **ValidTargetDomain** parameter has the correct value. The default setting is .ca.com.
- If CloudMinder is the Identity Provider and Credential Handling Service is used as the delegated authentication method, make sure the partnership's minimum authentication level is no more than the authentication level of authentication methods provided by the Credential Handling Service.

SAML Request Returns Message that RelayState is Invalid

Symptom

A SAML request returns a message that the RelayState is invalid.

Solution

Point the RelayState to the destination in encoded URL.

OAuth Authentication Does Not Work

Symptom

OAuth authentication, such as Google or Facebook, does not work.

Solution

Do the following:

- Make sure that the oauth related realm, response, and policy are configured correctly as part of tenant domain from the Cloud Service Provider Administration Console.
- Confirm that the Secure Proxy Server Agent Configuration Object's **SecureURL**s parameter is set to **yes;** also ensure that **?SMQUERYDATA=Sample** is added to the **oauthproviders.xml** application URL as well as the callback URL in Facebook/Google configuration.
- Make sure that the configuration for reading user attributes from the session store or context is consistent in the system.

  Check the following places:

  - authentication scheme
  - realm
  - openformatexpression.conf
  - oauth.properties.

OAuth Authentication Works, but OAUTH-Based Self-Registration Fails

Symptom

OAuth authentication works, but OAuth-based self-registration fails.

Solution

Do the following:

Check the IdentityMinder server to confirm that OpenFormatCookie-related configurations has been set for the tenant from the User Console.

External Task Error in the User Console

Symptom

You fail to Single Sign-On into the Service Provider using the launch task, and receive the following error from the User Console:

External task x Launch Task does not contain URL

Solution

Do the following:

1. From the User Console, use Modify Admin Tasks to check the launch task configurations.
2. If spaces exist in the task's tag or tab's tag, remove the spaces, and then submit the change.

Chapter 6: Advanced Authentication Issues

To assist in troubleshooting, you should know how to activate trace, and the location of the configuration and logging files.

This section contains the following topics:

How to Use the CA Arcot Administration Console to Troubleshoot

Typically, the CA Arcot Administration Console in CloudMinder manages risk rules and credential profiles. Many of the Arcot administration tasks, such as creating and managing organizations and credentials, are automated and closely integrated with the other CloudMinder components.

As such, you should avoid using the Console for general Arcot administration purposes.

In the case of Advanced Authentication failures, these failures may be resolved by refreshing cache in the Administration Console. Typical errors can include the following:

- When you observe errors in logs
- When configuring Advanced Authentication credentials for a tenant from the IM console about a configuration or an organization not found

Follow these steps:

1. Login to the CA Arcot Administration Console as a global administrator.
2. Navigate to the Organizations tab.
3. Perform a search.
4. Select the organization affected, and then click the Refresh Cache button.
5. Navigate to Services and Server Configurations tab, Administration Console, and then click Refresh Cache.
6. Select both Refresh System Configuration and Refresh Organization Configuration, and then click OK.

How to Enable Logging and Trace Tools for Advanced Authentication

Use the following procedures to enable the logging and trace tools on the system components for debugging purposes.

AuthMinder/RiskMinder

By default, log level is set to INFO.

To set a different log level or to enable trace:

1. Log in to the Arcot Administration Console at http://<smps_aa_hostname>:9090/arcotadmin/masteradminlogin.htm as masteradmin.
2. Navigate to Services and Server Configurations tab, WebFort or RiskFort, Instance Management, Select the instance
3. In the Logging Configuration section, change the log level or enable trace.

Tenant Web Service

By default, the log level is set to INFO.

Log configuration can be found here:

/opt/CA/AdvancedAuth/Tomcat/webapps/tenant-services/WEB-INF/classes/resources/webserviceslogger.properties

Advanced Authentication Server

By default, log level is set to WARN.

Log configuration can be found here:

/opt/CA/AdvancedAuth/Tomcat/lib/log4j.properties

Advanced Authentication UI/Flow Service

By default, log level is set to WARN.

Log configuration can be found here:

/opt/CA/secure-proxy/Tomcat/properties/log4j.properties

Locations for the Advanced Authentication Configuration, Log, and Trace files

Note: Enabling trace may impact performance. Only enable trace during troubleshooting process.

The log files for the components appear in the following locations.

- AuthMinder startup log: **/opt/CA/AdvancedAuth/logs/arcotwebfortstartup.log**
- AuthMinder log: **/opt/CA/AdvancedAuth/logs/arcotwebfort.log**
- RiskMinder startup log: **/opt/CA/AdvancedAuth/logs/arcotriskfortstartup.log**
- RiskMinder log: **/opt/CA/AdvancedAuth/logs/arcotriskfort.log**
- Tenant Web Service log: /**opt/CA/AdvancedAuth/logs/twslogging.log**
- Advanced Authentication Server log: **/opt/CA/AdvancedAuth/logs/cm-aads.log**
- Advanced Authentication UI/Flow log: **/opt/CA/secure-proxy/proxy-engine/logs/cm-aa.log**

Common Advanced Authentication Errors

The following advanced authentication errors may appear.

Advanced Authentication Feature Not Available for a Tenant

Ensure that the Advanced Authentication Manager admin role is enabled in the tenant console.

Startup Errors

If you have errors that may be preventing the servers from starting normally, check the AuthMinder/RiskMinder startup logs for database or other errors. If the servers started successfully, there should be a message indicating that the server is READY.

Configuration or Organization Not Found in cm-aads.log

Symptom

Error message indicates a configuration or organization is not found in the **cm-aads.log** file.

Solution

Do the following:

1. Login to the CA Arcot Administration Console as a global administrator.
2. Navigate to Organizations tab and perform a search.
3. Select the organization affected, and then click the Refresh Cache button.
4. Navigate to the Services and Server Configurations tab, Administration Console, and then click Refresh Cache.
5. Select the following options:
   - Refresh System Configuration
   - Refresh Organization Configuration
6. Click OK.

Error When Starting Advanced Authentication Flows

Symptom

When starting Advanced Authentication flows from the Credential Handler Service page, an error message similar to the following appears in the in **twslogging.log** file:

Timestamp - ERROR – RequestHandler – Authentication failed received authToken=…, CalculatedToken=…

Solution

This message may indicate that Advanced Authentication does not have the correct shared secret configured to communicate with Tenant Web Services.

Do the following:

Reset the shared secret, and ensure that the value set for **tws.shared.secret** in the AOK_OVERLOADED_PROPS database table matches with the shared secret in clear text.

During the installation of SiteMinder Policy Server, if the **_aa_tws_shared_secret** property in **properties.sh** is set to another value, then you need to make Tenant Web Services and the Credential Handling Service aware of this shared secret:

For the SiteMinder Policy Server, configure the Tenant Web Services shared secret:

1. cd /opt/CA/AdvancedAuth/Tomcat/webapps/tenant-services/WEB-INF/classes/resources
2. (optional) dos2unix tenantconfiguration.xml
3. Edit tenantconfiguration.xml.
4. Set **twssecret** to **_aa_tws_shared_secret value** and make sure **isencrypted=false.**
5. Restart Advanced Authentication Tomcat.
6. Edit tenantconfiguration.xml again.
7. Copy the now-encrypted shared secret.

Configure the SPS-Credential Handling Service shared secret:

1. Edit **/opt/CA/secure-proxy/Tomcat/webapps/chs/WEB-INF/classes/config/chsConfig.properties**.
2. Put the encrypted shared secret that yoiu copied in the step 7 above) from Siteminder policy server :tenantconfiguration.xml in the sharedsecret property.
3. Restart SPS.

Check the tenant Web Services

To obtain tenant information, Tenant Web Services invokes the Identity Minder tenant Web Service. Check its configuration in the tenant user console.

Follow these steps:

1. Navigate to System, Web Services, Modify Web Service.
2. Search for and then select the Web Service object.
3. On the Security tab, make sure to clear the Require Secure Communication option.

Increase the Log Level

If after checking the configuration, the problem persists, perform the following steps:

1. Increase Tenant Web Services logging level by completing the following steps:
   a. Connect to the siteMinder Policy Server/Advanced Authentication server.
   b. Edit **/opt/CA/AdvancedAuth/Tomcat/webapps/tenant-services/WEB-INF/classes/resources/webserviceslogger.properties** to set the log level to **DEBUG**.
   c. Restart the Advanced Authentication Tomcat server.
2. Replay the use case.
3. Review **twslogging.log**, located by default in **/opt/CA**.

ArcotID OTP Authentication Failures

Symptom

You entered the correct PIN for ArcotID OTP, but the generated OTP does not allow you to authenticate successfully.

Solution

Make sure that the time is correct and synchronized with all servers in CloudMinder.

Check if the server is correctly updating time from the configured NTP server.

Error Sending E-Mail During Authentication Flows

Symptom

You experience an error sending e-mail during authentication flows.

Solution

Do the following:

Check the following SMTP parameters in the **AOK_SYSTEM_DATA** table to ensure that they are set correctly:

- smtp.host
- smtp.host.port
- smtp.username
- smtp.password

Chapter 7: Report Issues to CA

To open a support ticket with CA, go to http://support.ca.com and log in using your account credentials.

After you open a support ticket, CA Support will request background information about your implementation. Depending on the specific issue, CA will typically request log and trace files for analysis. Please use the instructions in previous sections to collect the needed information.