CA CloudMinder™

Installation Guide

1.51

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

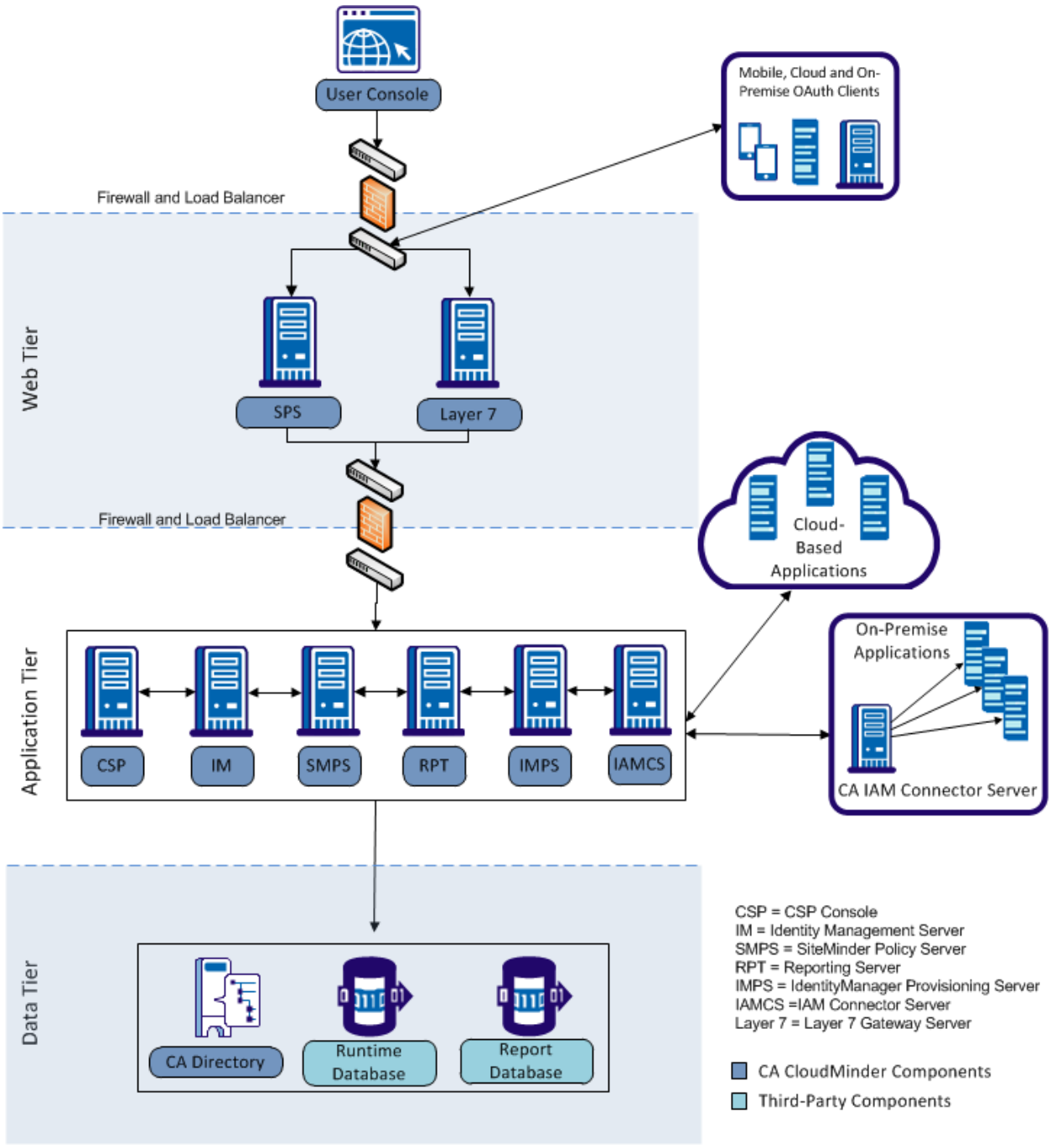
Contents

Chapter 1: Installation Overview

This section contains the following topics:

Standalone Architecture

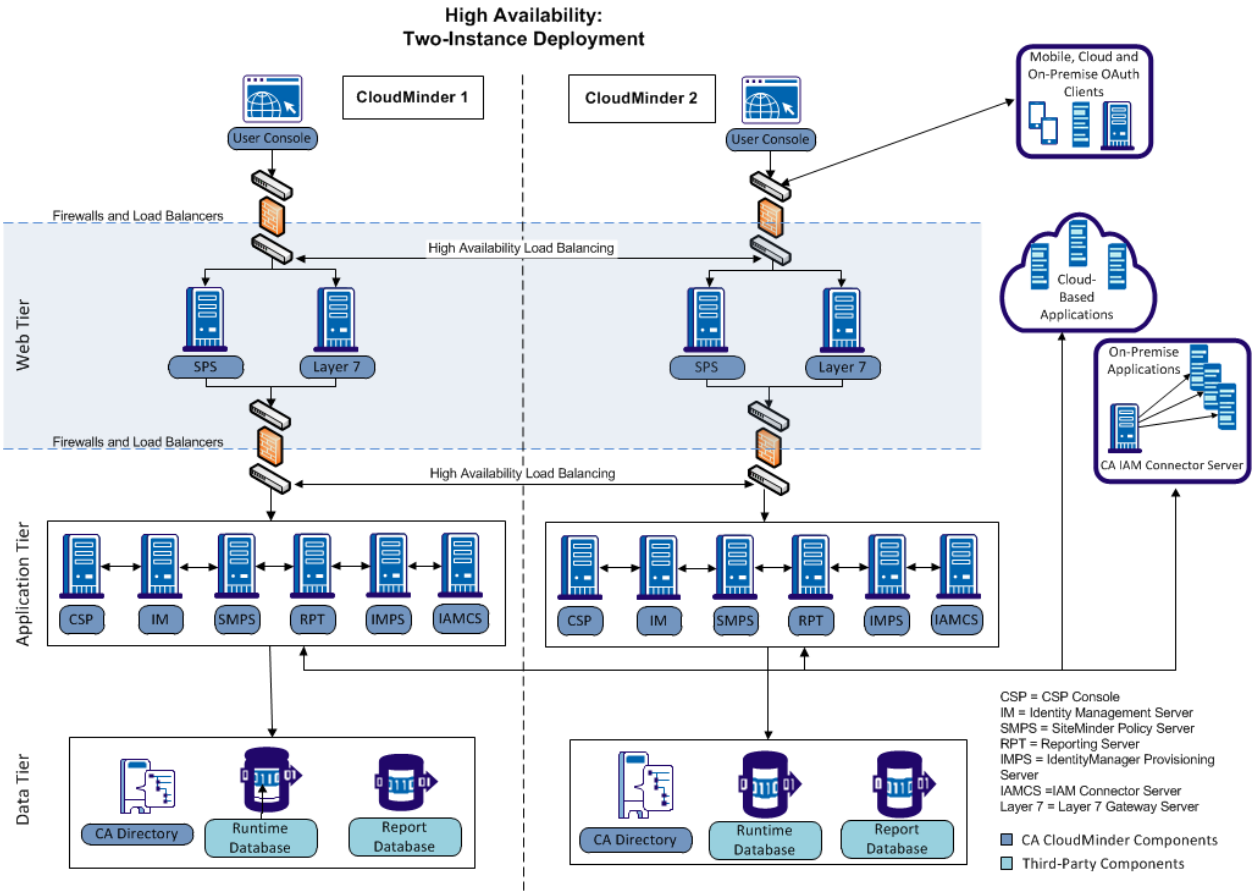
CA CloudMinder is deployed using a three-tier architecture. Components are separated into web interface, application, and data tiers. Web services connect these tiers. The deployment architecture for a standalone installation is as follows:



High Availability Architecture

In a production setting, we recommend that you use a high-availability deployment. You install two or more instances of each component, except for Oracle or PostgreSQL databases. If any server or other component becomes unavailable, a duplicate server operates in its place. This appoach minimizes the risk of service interruption.

Note: For the purposes of this document, we assume that a high-availability deployment has two instances of each component, except for the databases.



Order of Component Installation

You can deploy CA CloudMinder in a Linux environment only. Prepare your installation environment accordingly. These separate systems can be physical or virtual. Have the appropriate physical or virtual hardware available before you begin installation.

You install system components in a specific order, beginning with the data tier. You then move upward through the architecture, installing the application servers and components, ending with the web and interface components. You install each component on a separate system as follows:

- Oracle or PostgreSQL database software
- CA Directory server
- Provisioning Server
- CA IAM Connector Server CA IAM CS
- SiteMinder Policy server
- CSP console
- Secure Proxy server
- Identity Management server
- Business Objects server, if you plan to install CA Business Intelligence to enable reporting for your environment.
- Layer 7 Gateway

Install each component and confirm that it is running before you install the next component. For example, for a two-instance high-availability deployment, first you install two instances of CA Directory server. Then, you install two instances of Provisioning server as the next procedure.

Properties Files

Each server component has a properties file, with the exception of the Layer 7 Gateway servers. Before installing a component, complete the properties file with information such as system and database user names, passwords, and host names. During installation, the properties file distributes the information, enabling components to function properly and communicate with one another.

You need the properties.sh files during future upgrades and for general reference. The installation of the server backs up the properties.sh file to this location with an appropriate time stamp:

`/opt/CA/config/`

If you prefer to use a different location, set the TARGET environment variable to that location.

Important! For security purposes, the backed up file excludes all passwords; therefore, make separate arrangements to recall the passwords you need.

Database Installation

Install Oracle or PostgreSQL database software for Identity Management runtime data and for reporting data.

PostgreSQL

- You can download the PostgreSQL software from http://www.postgresql.org/

  Install the PostgreSQL client (postgresql-8.4.7-2.el6.x86_64) on the systems with the SiteMinder Policy Server and the Identity Management server.

- To use a PostgreSQL database for reporting, install SQLAnywhere for the Business Objects CMS and the audit database.

  For Business Objects, use the *CA Business Intelligence Installation Guide* to perform a custom installation and choose SQLAnywhere.

Oracle

- You can purchase the software from Oracle. Install an Oracle 11g database.
- Configure the database with all services (such as listener and DB) running.
- For good performance, the Oracle database requires the following settings:
  - Sessions=772
  - Processes=500
- Configure the Oracle database with a UTF-8 encoded character set. If you plan to enable Advanced Authentication for your environment, install the AL32UTF8 Oracle database character set.
- Create an Oracle user with the username "CamAdmin" and privileges to create tablespaces and users. Assign the CamAdmin user the DBA and Connect roles in Oracle. This CamAdmin user is used to create other base CA CloudMinder system users. Make a note of the password for CamAdmin for later use during installation.
- If you plan to install CA Business Intelligence for reporting, install and configure an additional Oracle 11g database to house reporting data.

Port Communication Tables

We recommend that you configure a firewall and load balancer between external internet traffic and the Secure Proxy Server. We also recommend that you configure a firewall and load balancer between the Secure Proxy Server and the system application tier.

The following table shows the ports to configure on your firewalls and load balancers. The load balancer receives inbound traffic from the originating component over the Port In. Traffic traveling outbound from the load balancer uses the Port Out.

Open the appropriate ports on your load balancers.

Component	Port In	Port Out	Traffic Flow	Description
Web Tier Load Balancer (LB1)	443	443	(ext)->LB1->SPS	External traffic distributed across all Secure Proxy Server (SPS) instances.
Web Tier Load Balancer	8443	8443	(ext)->LB1->L7	External calls to the Layer 7 Gateway (L7) distributed across all Gateway instances.
Web Tier Load Balancer	1812	1812	(ext)->LB1->SPS	External calls to the Radius Proxy server (Radius) distributed across all SPS instances.
Application Tier Load Balancer (LB2)	8443	8080	a) SPS->LB2->IM b) SPS->LB2-> IM.SMTP	a) Identity Management requests coming from SPS distributed across all IM instances. b) SMTP requests coming from SPS distributed across all IM instances.
Application Tier Load Balancer	8080	8080	a) IMPS->LB2->IM b) SMPS->LB2->IM	a)Identity Management requests coming from Provisioning Server distributed across all IM instances. b) Identity Managementrequests coming from SiteMinder Proxy Server (SMPS) distributed across all IM instances.
Application Tier Load Balancer	22002	22001	SPS->LB2->IAMCS	CA IAM CS (IAMCS) requests coming from SPS distributed across all IM instances.
Application Tier Load Balancer	443	20080	SPS->LB2->IAMCS	IAMCS management requests coming from SPS distributed across all IM instances.
Application Tier Load Balancer	44441	44441	a) SPS->LB2->SMPS b) IM->LB2->SMPS	a) SMPS requests coming from SPS distributed across all SMPS instances. b) SMPS requests coming from IM distributed across all SMPS instances.
Application Tier Load Balancer	9443	9090	a) SPS->LB2->SMPS b) SPS->LB2->SMPS	a) SMPS (authentication tenant web services) requests coming from SPS distributed across all SMPS instances. b) SMPS (authentication data service) requests coming from SPS distributed across all SMPS instances.

Application Tier Load Balancer	9090	9090	IM->LB2->SMPS	SMPS (authentication unified directory service) requests coming from the CSP console distributed across all SMPS instances.
Application Tier Load Balancer	9743	9742	SPS->LB2->SMPS	SMPS (AuthMinder) requests coming from SPS distributed across all SMPS instances.
Application Tier Load Balancer	9742	9742	IM->LB2->SMPS	SMPS (AuthMinder) requests coming from IM distributed across all SMPS instances.
Application Tier Load Balancer	9745	9745	IM->LB2->SMPS	SMPS (AuthMinder management service) requests coming from IM distributed across all SMPS instances.
Application Tier Load Balancer	7680	7680	IM->LB2->SMPS	SMPS (RiskMinder) requests coming from IM distributed across all SMPS instances.
Application Tier Load Balancer	1812	1814	SPS->LB2->Auth.Radius	Radius requests coming from the Radius Proxy running inside SPS. Port 1814 is used to respond back to the Radius Proxy.
Application Tier Load Balancer	20498	20498	L7->LB2->DXrouter	User Directory requests coming from the Layer 7 Gateway distributed across the application tier DXrouter instances.

IM = CA Identity Management

SPS = Secure Proxy Server

IMPS = Provisioning Server

SMPS = SiteMinder Policy Server

IAMCS = CA IAM Connector Server

L7 = Layer 7 Gateway Server

Radius = Radius Proxy Server

How to Deploy CA CloudMinder

As a hosting administrator, you need an understanding of the high-level procedures for installing and configuring CA CloudMinder. This overview describes the process for creating a CA CloudMinder environment and includes links to detailed instructions.

1. Install CA CloudMinder, including:
   - Installing all server components (see page 15)
   - Configuring load-balancing and high availability (see page 141)
   - Accessing logs (see page 165)
2. Replace default user accounts.

   For security reasons, we recommend that you replace default user account and passwords with your own secure administrator accounts.
3. Create and deploy tenants.
4. Configure the authentication method for the tenant.
   - Standard authentication
   - Advanced authentication, if applicable
5. Configure single sign-on, if applicable.
6. Configure your tenant user environment, including:
   - Assigning roles and adding administrators
   - Creating groups
   - Configuring managed endpoints to connect the system to external resources
   - Configuring provisioning to give users accounts in external resources
   - Configuring services to give users protected access to external resources
7. Add users to the tenant

In the *SSO Getting Started Guide*, the following topics describe how to configure common combinations of services:

- SSO Using Advanced Authentication and Provisioning
- SSO Using a Third-Party IdP and Self-Registration
- SSO Using an OAuth Authentication Scheme and Self-Registration

Chapter 2: Server Installation

This section contains the following topics:

CA CloudMinder ISO images

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

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

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

CA CloudMinder 1.51	ISO File Name	MD5SUM	File Size
CA Business Intelligence r3.3 for Linux - DVD	DVD06213531E.iso	2276e0786505e7ad3504b3a6ca77c864	5,415,825,408
CA CloudMinder 1.51 Cloud Components (DVD 1 of 2)	DVD03100038E.iso	d36c0a070079a21579574057d66b774c	2,519,728,128
CA CloudMinder 1.51 Cloud Components (DVD 2 of 2)	DVD03100448E.iso	daf29da07d4b91c00bfb16155858ee8a	2,883,780,608
CA CloudMinder 1.51 On-premise Components	DVD03095802E.iso	d759efe457d97722f6edd6cd84149b60	1,784,479,744

Directory Server

Standalone Directory Server

Use this procedure to install a CA Directory Server.

For a high-availability deployment, after you complete this procedure, continue with the Directory Server 2 procedure. Otherwise, after you complete this procedure continue with installing the Provisioning Server.

The Provisioning Directory is installed as part of CA Directory Kit.

CA Directory Pre-Installation Steps

To prepare for installation, confirm that your server environment is properly prepared. Then install the required packages.

Follow these steps:

1. Install 64-bit Linux RHEL 6.1.
2. Download, but do not install, a 64-bit JDK to your local system or to a file share. You can also use a JRE in place of a JDK.

   Note: The system installer can install the JDK automatically. We recommend that you download a JDK and allow the system to install it.
3. Verify that the systems where you plan to install CA Directory and the Provisioning Server can ping each other. For a high availability installation, make sure each system can ping the three other systems. I.e., each CA Directory system can ping the other, and can ping both Provisioning Server systems, and vice versa.
4. Be sure that this system has sufficient disk space for the number of tenants it will support.

   When you deploy a tenant, an LDIF file is uploaded through DSA Management. The upload process requires twice the amount of space. For example, if the DSA data store is 2.5 GB, the system needs 5 GB available while the LDIF is loading.
5. Obtain the Directory Server ISO image from the CA Support site and extract it.
6. Copy the kit (CAM-DIR_kit-*date*.zip) to / (the root folder).
7. Unzip the kit.
8. Install the following packages:
   - binutils-2*x86_64*
   - glibc-2*x86_64* nss-softokn-freebl-3*x86_64*

- glibc-2*i686* nss-softokn-freebl-3*i686*
- compat-libstdc++-33*x86_64*
- glibc-common-2*x86_64*
- glibc-devel-2*x86_64*
- glibc-devel-2*i686*
- glibc-headers-2*x86_64*
- elfutils-libelf-0*x86_64*
- elfutils-libelf-devel-0*x86_64*
- gcc-4*x86_64*
- gcc-c++-4*x86_64*
- ksh-*x86_64*
- libaio-0*x86_64*
- libaio-devel-0*x86_64*
- libaio-0*i686*
- libaio-devel-0*i686*
- libgcc-4*x86_64*
- libgcc-4*i686*
- libstdc++-4*x86_64*
- libstdc++-4*i686*
- libstdc++-devel-4*x86_64*
- make-3.81*x86_64*
- numactl-devel-2*x86_64*
- sysstat-9*x86_64*
- compat-libstdc++-33*i686*
- compat-libcap*
- unixODBC*
- libstdc++*
- compat-libstdc++-33.i686
- compat-libstdc++-296.i686
- glibc.i686

- ksh.x86_64
- libgcc.i686
- libidn.i686
- libstdc++.i686
- libX11.x86_64
- libXau.x86_64
- libxcb.x86_64
- libXext.i686
- libXi.i686
- libXtst.i686
- ncurses-devel.i686
- nss-softokn-freebl.i686
- dos2unix
- telnet

9. Run the following commands to set the state of the firewall/ip tables:

```
chkconfig iptables off
service iptables stop
```

10. Run the following commands to check and set the state of SELinux:
    a. Check the status:
    ```
    sestatus
    ```
    b. If the response is "permissive" or "disabled", do nothing
    c. If the response is "enforcing", change the state:
    ```
    sudo vi /etc/selinux/config
    setenforce 0
    ```

Configure the CA Directory Properties File

Set the parameters for the CA Directory server installation. Parameters pass information required to enable successful communication and function among system components.

You need the following information to complete the CA Directory parameters.

- The host names of the systems where you plan to install the CA Directory Servers
- The host names of the systems where you plan to install the IdentityMinder Provisioning Servers

Follow these steps:

1. Navigate to /tmp/properties.sh.
2. In the properties.sh file, set the following parameters.

   _Environment

   Leave as the default, CHANGE_ME_LATER.

   _SoftwareVersion

   Leave as the default, STATIC.

   _impd_fips_mode

   Leave as the default, false.

   _DomainSuffix

   Set this to your network domain.

   _impd_shared_secret

   A password shared by the Provisoning Directory and Provisioning Server. Use any password, but it must match the password for _impd_shared_secret in the properties file you will create during Provisioning Server installation.

   Make a note of this password so you can use it later during the installation process.

   _imps_hostname

   Enter the host names of systems where you plan to install the Provisioning Server, separated by commas.

_ha_host_list

For a high-availability deployment, enter the host names of other systems where you plan to install CA Directory (other than the system on which you are currently installing CA Directory).

In a single-instance deployment, leave this parameter blank.

_ha_primary_host

For a high-availability deployment, enter the host name of the system where you install the first CA Directory. Use the same value for the second CA Directory installation.

In a single-instance deployment, leave this parameter blank.

_dir_webservice_details

Leave as default, true.

_dir_webservices_port

Port used by Web Services. Leave as the default, 9080, unless you cannot use this port in your environment. If you must change the web services port, enter a new port number.

Note: If you must change the web services port, use the same port for web services on all servers.

_dir_webservices_secure_port

Port used by Web Services. Leave as the default, 9443, unless you cannot use this port in your environment. If you must change the web services port, enter a new port number.

Note: If you must change the web services port, use the same port for web services on all servers.

_dir_webservices_username

User name for Web Services. Leave as the default, dsaweb.

_dir_webservices_password

The password for Web Services. Create any password, but it must match the password for _impd_shared_secret in the properties file you will create during Provisioning Server installation.

Make a note of this password so you can use it later during the installation process.

_COMP_CLASS

Leave as the default, ca_cam.directory.

_COMP_NAME

Leave as the default, main.directory.

_APP_NAME

Leave as the default, directory_server.

JAVA64_LOCATION

Location of an existing 64-bit JRE if preinstalled. Set this parameter if you choose to install your JRE separately. In this case, symbolically link /opt/java64 to your JRE.

However, instead of installing a JRE separately, the system installer can do this automatically. We recommend that you download a JRE and allow the system to install it.

See the JAVA64_KIT parameter.

JAVA64_KIT

Location of a 64-bit JRE that you download to the local system or to a file share. If this parameter is set, the server kit will install this JRE automatically.

USER_JAVA64

Leave blank for installation. This parameter is intended for upgrades, not installation.

_ntp_server

IP address or host name of the NTP server to use to synchronize the server time.

3. Back up the properties.sh file. Rename it to a logical name, for example, directory1properties.sh.

   Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

   Important! The original properties.sh file resides in a temp folder. If the server is shut down, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further installation or use of the system.

Install and Verify the CA Directory Server

After you set the CA Directory parameters and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```

2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, verify the installation as follows.

3. On the CA Directory server system, check that Java is running:

   ```
   ps -ef | grep java
   ```

   The output shows the following:

   ```
   java -Xms256m -Xmx1024m -cp ./lib/*
   com.ca.directory.dxagent.service.DxAgentService
   ```

4. Log in as the DSA user:

   ```
   su – dsa
   ```

5. Check the Directory Server status by issuing the dxserver command:
   ```
   dxserver status
   ```

   The output shows that the four impd processes have started:
   ```
   <dir1 host>-impd-notify started
   <dir1 host>-impd-main started
   <dir1 host>-impd-inc started
   <dir1 host>-impd-co started
   ```

6. For a high-availability deployment, continue with installing a second CA Directory server. For a single-instance deployment, continue with installing the Provisioning Server.

High-Availability: Directory Server 2

Prepare a second system that is separate from the one on which you installed the first CA Directory instance.

Confirm that your server environment is properly prepared and install the required packages. Follow the same steps (see page 16) as you did for the first instance.

Configure the Second CA Directory Properties File

Set the parameters for the second CA Directory server instance.

Copy the properties file from the first CA Directory Server instance and change only the parameters that are different for the second instance. Remember to rename and back up the new properties file after you complete the parameters.

You need the following information to complete the CA Directory parameters.

General Information:

The host names of the systems where you plan to install the CA Directory Servers.

Follow these steps:

1. On the **first** CA Directory Server system, copy the properties.sh file that you just configured.
2. Navigate to /tmp/properties.sh on the **second** CA Directory Server system. Replace the properties.sh file with the configured copy from the first CA Directory Server system.
3. Change the following parameter values:

   _ha_host_list

   Enter the host names of other CA Directory systems in your environment, other than the system on which you are currently installing. In a two-instance high-availability deployment, enter the host name of the system where you installed the first CA Directory instance.

   In a single-instance deployment, leave this parameter blank.

   _ha_primary_host

   Enter the host name of the system where you installed the first CA Directory instance.

   For example, Directory1 (where the system on which you are currently installing is Directory2)

   Note: The primary host is always the system where you installed the first CA Directory instance.

4. Leave all other parameter values as you set them for the first CA Directory Server.
5. Back up the properties.sh file. Rename it to a logical name, for example, directory2properties.sh.

   Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

Important! The original properties.sh file resides in a temp folder. If the server is restarted, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further use of this component and the system on which it is installed.

Install and Verify the Second CA Directory Server

After you set the parameters for the second CA Directory instance and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```

2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, verify the installation as follows.

3. On the CA Directory server system, check that Java is running:

   ```
   ps -ef | grep java
   ```

   The output shows the following:

   ```
   java -Xms256m -Xmx1024m -cp ./lib/*
   com.ca.directory.dxagent.service.DxAgentService
   ```

4. Log in as the DSA user:

   ```
   su – dsa
   ```

5. Check the Directory Server status by issuing the dxserver command:
   ```
   dxserver status
   ```

   The output shows that the four impd processes have started:
   ```
   <dir2 host>-impd-notify started
   <dir2 host>-impd-main started
   <dir2 host>-impd-inc started
   <dir2 host>-impd-co started
   ```

Continue with installing the Provisioning Server.

Provisioning Server

Standalone Provisioning Server

Use this procedure to install a Provisioning Server.

For a high-availability deployment, after you complete this procedure, continue with the Provisioning Server 2 procedure. Otherwise, after you complete this procedure continue with installing the CA IAM CS.

More Information:

Provisioning Server Pre-Installation Steps (see page 25)
Configure the Provisioning Server Properties File (see page 27)
Install and Verify the Provisioning Server (see page 32)
Provisioning Server Troubleshooting (see page 33)

Provisioning Server Pre-Installation Steps

To prepare for installation, confirm that your server environment is properly prepared. Then install the required packages.

Follow these steps:

1. Install 64-bit Linux RHEL 6.1.
2. Download, but do not install, a 64-bit JDK to your local system or to a file share. You can also use a JRE in place of a JDK.

   Note: The system installer can install the JDK automatically. We recommend that you download a JDK and allow the system to install it.
3. Verify that the systems where you previously installed CA Directory, and the systems where you plan to install the Provisioning Server, can ping each other. For a high availability installation, make sure each system can ping the three other systems. I.e., each Provisioning Server system can ping the other, and can ping both CA Directory systems, and vice versa.
4. Obtain the Provisioning Server ISO image from the CA Support site and extract it.
5. Copy the kit (CAM-IMPS_kit-*date*.zip) to / (the root folder).
6. Unzip the kit.
7. Install the following packages:

- binutils-2*x86_64*
- glibc-2*x86_64* nss-softokn-freebl-3*x86_64*
- glibc-2*i686* nss-softokn-freebl-3*i686*
- compat-libstdc++-33*x86_64*
- glibc-common-2*x86_64*
- glibc-devel-2*x86_64*
- glibc-devel-2*i686*
- glibc-headers-2*x86_64*
- elfutils-libelf-0*x86_64*
- elfutils-libelf-devel-0*x86_64*
- gcc-4*x86_64*
- gcc-c++-4*x86_64*
- ksh-*x86_64*
- libaio-0*x86_64*
- libaio-devel-0*x86_64*
- libaio-0*i686*
- libaio-devel-0*i686*
- libgcc-4*x86_64*
- libgcc-4*i686*
- libstdc++-4*x86_64*
- libstdc++-4*i686*
- libstdc++-devel-4*x86_64*
- make-3.81*x86_64*
- numactl-devel-2*x86_64*
- sysstat-9*x86_64*
- compat-libstdc++-33*i686*
- compat-libcap*
- unixODBC*
- libstdc++*
- compat-libstdc++-33.i686
- compat-libstdc++-296.i686

- glibc.i686
- ksh.x86_64
- libgcc.i686
- libidn.i686
- libstdc++.i686
- libX11.x86_64
- libXau.x86_64
- libxcb.x86_64
- libXext.i686
- libXi.i686
- libXtst.i686
- ncurses-devel.i686
- nss-softokn-freebl.i686
- dos2unix
- telnet

8. Run the following commands to set the state of the firewall/ip tables:

```
chkconfig iptables off
service iptables stop
```

9. Run the following commands to check and set the state of SELinux:

   a. Check the status:
   ```
   sestatus
   ```

   b. If the response is "permissive" or "disabled", do nothing

   c. If the response is "enforcing", change the state:
   ```
   sudo vi /etc/selinux/config
   setenforce 0
   ```

Configure the Provisioning Server Properties File

Set the parameters for the Provisioning Server installation.

You need the following information to complete the Provisioning Server parameters.

General Information:

- Your CA Directory host names

From the CA Directory properties file:

- _impd_shared_secret
- _dir_webservices_password

Follow these steps:

1. Navigate to /tmp/properties.sh.
2. In the properties.sh file, set the following parameters.

   _Environment

   Leave as the default, CHANGE_ME_LATER.

   _SoftwareVersion

   Leave as the default, STATIC.

   _DomainSuffix

   Set this to your network domain.

   _impd_shared_secret

   Enter the same password you entered for _impd_shared_secret in the properties files for CA Directory.

   _impd_hostname

   Host name of the system where you installed the primary CA Directory instance.

   _impd_bind_pwd

   A password which the Provisioning Server uses to connect to the Provisioning Directory. Create any password.

   Make a note of this password so you can use it later during the installation process.

   _impd_ha_hosts

   For a high-availability deployment, enter the host name of the alternate CA Directory server.

   For example, Directory2 (where the primary CA Directory server is Directory1)

   Note: If you have three or more instances of CA Directory, separate the entries with commas. For example: Directory2, Directory3.

   In a single-instance deployment, leave this parameter blank.

   _impd_root_domain_pwd

   Enter the same password you entered for _impd_shared_secret in the properties files for CA Directory.

_impd_parent_domain_pwd

Enter the same password you entered for _impd_shared_secret in the properties files for CA Directory.

_impd_etaadmin_pwd

Enter the same password you entered for _impd_shared_secret in the properties files for CA Directory.

_provisioning_server_pwd

The Provisioning Server password. Create any password. Use the same password on all Provisioning Servers.

Make a note of this password so you can use it later during the installation process.

_provisioning_repository_pwd

Enter the same password you entered for _impd_shared_secret in the properties files for CA Directory.

_connector_server_pwd

The password used to access the CA IAM CS. Create any password. This must match the password for _connector_server_pwd in the properties file you will create during CA IAM CS installation.

Make a note of this password so you can use it later during the installation process.

_provisioning_domain

Leave as the default value.

Important! The following six parameters are required only during CA IAM CS installation. If you are currently installing the Provisioning Server, leave the following six parameters blank.

_http_proxy_enabled

Addresses whether you need a proxy to connect to the internet. Set to True if you need to enable a proxy to connect to the internet, for example, if the Provisioning Server is on a protected intranet. Set to False if the Provisioning Server has direct access to the internet and no proxy is enabled.

_http_proxy_user

The Proxy User required for authentication.

_http_proxy_pwd

The password for the Proxy User.

_http_proxy_domain

The proxy domain required for authentication.

_http_proxy_port

The proxy port required for authentication.

_http_proxy_server

The proxy server required for authentication.

_install_imps

Set to True to install the Provisioning Server.

Note: This parameter allows you to install a Provisioning Server through this installer. Set this to False to prevent a Provisioning Server from installing.

Also see the _install_jcs parameter.

_impd_skip_snapshot

Leave as the default value, false. This setting allows tenant deployment to succeed.

_dir_webservices_port

Port used by Web Services. Leave as the default, 9080, unless you cannot use this port in your environment. If you must change the web services port, enter a new port number.

Note: If you must change the web services port, use the same port for web services on all servers.

_dir_webservices_username

User name for Web Services. Leave as the default, dsaweb.

_dir_webservices_password

Enter the same password you entered for _dir_webservices_password in the properties file for the first CA Directory instance.

_dir_webservices_secure_port

Port used by Web Services. Leave as the default, 9443, unless you cannot use this port in your environment. If you must change the web services port, enter a new port number.

Note: If you must change the web services port, use the same port for web services on all servers.

_imps_fips_keyfile

Leave as the default, false.

_COMP_CLASS

Leave as the default, ca_cam.directory.

_COMP_NAME

Leave as the default, main.directory.

_APP_NAME

Leave as the default, directory_server.

JAVA64_LOCATION

Location of an existing 64-bit JRE if preinstalled. Set this parameter if you choose to install your JRE separately. In this case, symbolically link /opt/java64 to your JRE.

However, instead of installing a JRE separately, the system installer can do this automatically. We recommend that you download a JRE and allow the system to install it.

See the JAVA64_KIT parameter.

JAVA64_KIT

Location of a 64-bit JRE that you download to the local system or to a file share. If this parameter is set, the server kit will install this JRE automatically.

USER_JAVA64

Leave blank for installation. This parameter is intended for upgrades, not installation.

_install_jcs

Set to False to install the Provisioning Server.

Note: This parameter allows you to install either an CA IAM CS through this installer. Set this to False to prevent an CA IAM CS from installing.

Also see the _install_imps parameter.

_ntp_server

IP address or host name of the NTP server to use to synchronize the server time.

_remote_imps_hostname

Enter the host name of the primary Provisioning Server system.

Note: This parameter is not needed when the Provisioning Server and CA IAM CS are on the same system.

3. Back up the properties.sh file. Rename it to a logical name, for example, provisioning1properties.sh.

   Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

   Important! The original properties.sh file resides in a temp folder. If the server is shut down, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further installation or use of the system.

Install and Verify the Provisioning Server

After you set the Provisioning Server parameters and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```

2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, verify the installation as follows.

3. On the CA Directory Server system, check that Java is running:

   ```
   ps -ef | grep java
   ```

   The output shows the following:

   ```
   /opt/CA/Directory/dxserver/dsamgmt/jvm/bin/java -Xms256m
   -Xmx1024m -cp /opt/CA/Directory/dxserver/dsamgmt/lib/*
   com.ca.directory.dxagent.service.DxAgentService
   jvm/bin/java -ea
   -Dkaraf.home=/opt/CA/IdentityManager/ConnectorServer -server
   -Xms128M -Xmx1024M -XX:MaxPermSize=384m -Djava.awt.headless=true
   -Dcom.sun.management.jmxremote
   -Dderby.system.home=/opt/CA/IdentityManager/ConnectorServer/dat
   a/der
   by -Dderby.storage.fileSyncTransactionLog=true
   -Djava.endorsed.dirs=/opt/CA/IdentityManager/ConnectorServer/li
   b/endorsed
   -Djava.ext.dirs=/opt/CA/IdentityManager/ConnectorServer/jvm/lib
   /ext:/opt/CA/IdentityManager/ConnectorServer/lib/ext
   -Dkaraf.instances=/opt/CA/IdentityManager/ConnectorServer/insta
   nces
   ```

```
-Dkaraf.base=/opt/CA/IdentityManager/ConnectorServer
-Dkaraf.data=/opt/CA/IdentityManager/ConnectorServer/data
-Djava.util.logging.config.file=/opt/CA/IdentityManager/Connect
orSer
ver/etc/java.util.logging.properties
-Dkaraf.startLocalConsole=false -Dkaraf.startRemoteShell=true
-Djcsroot=/opt/CA/IdentityManager/ConnectorServer/jcs
-Dlog4j.configuration=/opt/CA/IdentityManager/ConnectorServer/e
tc/org.ops4j.pax.logging.cfg
-Dsun.lang.ClassLoader.allowArraySyntax=true -classpath
/opt/CA/IdentityManager/ConnectorServer/conf:/opt/CA/IdentityMa
nager/ConnectorServer/lib/karaf-jaas-boot.jar:/opt/CA/IdentityM
anager/ConnectorServer/lib/karaf.jar:/opt/CA/IdentityManager/Co
nnectorServer/lib/servicemix-version.jar:/opt/CA/IdentityManage
r/ConnectorServer/lib/smix4SecurityWrapper.jar:/opt/CA/Identity
Manager/ConnectorServer/j
cs/tools/lib/cacommons.jar
smix.security.wrapper.Smix4SecurityWrapper
```

4. Log in as the DSA user:

   ```
   su – dsa
   ```

5. Enter the following command:

   ```
   dxserver status
   ```

   The output shows that the server has started:

   ```
   <Provisioning-Server-host>-imps-router started
   ```

6. Log in as the IMPS user:

   ```
   su - imps
   ```

7. Navigate to /opt/CA/IdentityManager/ProvisioningServer/bin.

8. Enter the following command:

   ```
   ./imps status
   ```

   The output shows the following:

   ```
   im_ps is running
   ```

9. For a high-availability deployment, continue with installing a second Provisioning Server. For a single-instance deployment, continue with installing the CA IAM CS.

Provisioning Server Troubleshooting

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.

High-Availability: Provisioning Server 2

Prepare a second system that is separate from the one on which you installed the first Provisioning Server instance.

Confirm that your server environment is properly prepared and install the required packages. Follow the same steps (see page 25) as you did for the first instance.

Configure the Second Provisioning Server Properties File

Set the parameters for the second Provisioning Server instance.

Copy the properties file from the first Provisioning Server instance and change only the parameters that are different for the second instance. Remember to rename and back up the new properties file after you complete the parameters.

You need the following information to complete the Provisioning Server parameters.

From the properties file of your first Provisioning Server instance:

- _impd_bind_pwd

Follow these steps:

1. On the **first** Provisioning Server system, copy the properties.sh file that you just configured.
2. Navigate to /tmp/properties.sh on the **second** Provisioning Server system. Replace the properties.sh file with the configured copy from the first Provisioning Server system.
3. Change the following parameter values:

   _impd_bind_pwd

   Enter the same password you entered for _impd_bind_pwd in the properties file for the first Provisioning Server instance.

4. Leave all other parameter values as you set them for the first Provisioning Server.
5. Back up the properties.sh file. Rename it to a logical name, for example, provisioning2properties.sh.

   Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

   Important! The original properties.sh file resides in a temp folder. If the server is shut down, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further installation or use of the system.

Install and Verify the Second Provisioning Server

After you set the parameters for the second Provisioning Server instance and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```

2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, verify the installation as follows.

3. On the CA Directory Server system, check that Java is running:

   ```
   ps -ef | grep java
   ```

   The output shows the following:

   ```
   /opt/CA/Directory/dxserver/dsamgmt/jvm/bin/java -Xms256m
   -Xmx1024m -cp /opt/CA/Directory/dxserver/dsamgmt/lib/*
   com.ca.directory.dxagent.service.DxAgentService
   jvm/bin/java -ea
   -Dkaraf.home=/opt/CA/IdentityManager/ConnectorServer -server
   -Xms128M -Xmx1024M -XX:MaxPermSize=384m -Djava.awt.headless=true
   -Dcom.sun.management.jmxremote
   -Dderby.system.home=/opt/CA/IdentityManager/ConnectorServer/dat
   a/der
   by -Dderby.storage.fileSyncTransactionLog=true
   -Djava.endorsed.dirs=/opt/CA/IdentityManager/ConnectorServer/li
   b/endorsed
   -Djava.ext.dirs=/opt/CA/IdentityManager/ConnectorServer/jvm/lib
   /ext:/opt/CA/IdentityManager/ConnectorServer/lib/ext
   -Dkaraf.instances=/opt/CA/IdentityManager/ConnectorServer/insta
   nces
   ```

```
-Dkaraf.base=/opt/CA/IdentityManager/ConnectorServer
-Dkaraf.data=/opt/CA/IdentityManager/ConnectorServer/data
-Djava.util.logging.config.file=/opt/CA/IdentityManager/Connect
orSer
ver/etc/java.util.logging.properties
-Dkaraf.startLocalConsole=false -Dkaraf.startRemoteShell=true
-Djcsroot=/opt/CA/IdentityManager/ConnectorServer/jcs
-Dlog4j.configuration=/opt/CA/IdentityManager/ConnectorServer/e
tc/org.ops4j.pax.logging.cfg
-Dsun.lang.ClassLoader.allowArraySyntax=true -classpath
/opt/CA/IdentityManager/ConnectorServer/conf:/opt/CA/IdentityMa
nager/ConnectorServer/lib/karaf-jaas-boot.jar:/opt/CA/IdentityM
anager/ConnectorServer/lib/karaf.jar:/opt/CA/IdentityManager/Co
nnectorServer/lib/servicemix-version.jar:/opt/CA/IdentityManage
r/ConnectorServer/lib/smix4SecurityWrapper.jar:/opt/CA/Identity
Manager/ConnectorServer/j
cs/tools/lib/cacommons.jar
smix.security.wrapper.Smix4SecurityWrapper
```

4. Log in as the DSA user:

   ```
   su – dsa
   ```

5. Enter the following command:

   ```
   dxserver status
   ```

   The output shows that the server has started:

   Provisioning-Server-host>-imps-router started

6. Log in as the IMPS user:

   ```
   su - imps
   ```

7. Navigate to /opt/CA/IdentityManager/ProvisioningServer/bin.

8. Enter the following command:

   ```
   ./imps status
   ```

   The output shows the following:

   ```
   im_ps is running
   ```

Continue with installing the CA IAM CS.

CA IAM CS

Standalone CA IAM CS

Use this procedure to install a CA IAM CS.

For a high-availability deployment, after you complete this procedure, continue with the CA IAM CS 2 procedure. Otherwise, after you complete this procedure continue with installing the SiteMinder Policy Server.

Note: You install the CA IAM CS using the same server kit as you used to install the Provisioning Server. However, several steps and parameters are different from the Provisioning Server installation. Follow the instructions in this section carefully.

CA IAM CS Pre-Installation Steps

To prepare for installation, confirm that your server environment is properly prepared. Then install the required packages.

Follow these steps:

1. Install 64-bit Linux RHEL 6.1.
2. Download, but do not install, a 64-bit JDK to your local system or to a file share. You can also use a JRE in place of a JDK.

   Note: The system installer can install the JDK automatically. We recommend that you download a JDK and allow the system to install it.
3. Obtain the Provisioning Server ISO image from the CA Support site and extract it.
4. Copy the kit (CAM-IMPS_kit-*date*.zip) to / (the root folder).
5. Unzip the kit.
6. Install the following packages:
   - binutils-2*x86_64*
   - glibc-2*x86_64* nss-softokn-freebl-3*x86_64*
   - glibc-2*i686* nss-softokn-freebl-3*i686*
   - compat-libstdc++-33*x86_64*
   - glibc-common-2*x86_64*
   - glibc-devel-2*x86_64*
   - glibc-devel-2*i686*
   - glibc-headers-2*x86_64*

- elfutils-libelf-0*x86_64*
- elfutils-libelf-devel-0*x86_64*
- gcc-4*x86_64*
- gcc-c++-4*x86_64*
- ksh-*x86_64*
- libaio-0*x86_64*
- libaio-devel-0*x86_64*
- libaio-0*i686*
- libaio-devel-0*i686*
- libgcc-4*x86_64*
- libgcc-4*i686*
- libstdc++-4*x86_64*
- libstdc++-4*i686*
- libstdc++-devel-4*x86_64*
- make-3.81*x86_64*
- numactl-devel-2*x86_64*
- sysstat-9*x86_64*
- compat-libstdc++-33*i686*
- compat-libcap*
- unixODBC*
- libstdc++*
- compat-libstdc++-33.i686
- compat-libstdc++-296.i686
- glibc.i686
- ksh.x86_64
- libgcc.i686
- libidn.i686
- libstdc++.i686
- libX11.x86_64
- libXau.x86_64

- libxcb.x86_64
- libXext.i686
- libXi.i686
- libXtst.i686
- ncurses-devel.i686
- nss-softokn-freebl.i686
- dos2unix

7. Run the following commands to set the state of the firewall/ip tables:

```
chkconfig iptables off
service iptables stop
```

8. Run the following commands to check and set the state of SELinux:
   a. Check the status:
      `sestatus`
   b. If the response is "permissive" or "disabled", do nothing
   c. If the response is "enforcing", change the state:
      ```
      sudo vi /etc/selinux/config
      setenforce 0
      ```

Configure the CA IAM CS Properties File

Set the parameters for the CA IAM CS installation.

You need the following information to complete the CA IAM CS parameters.

General Information:

- Your CA Directory host names
- Your Provisioning Server host names
- The IP address or host name of your NTP server

From the CA Directory properties file:

- _impd_shared_secret
- _dir_webservices_password

From your Provisioning Server properties file:

- _impd_bind_pwd
- _provisioning_server_pwd
- _connector_server_pwd

Follow these steps:

1. Navigate to /tmp/properties.sh.
2. In the properties.sh file, set the following parameters.

   _Environment

   Leave as the default, CHANGE_ME_LATER.

   _SoftwareVersion

   Leave as the default, STATIC.

   _DomainSuffix

   Set this to your network domain.

   _impd_shared_secret

   Enter the same password you entered for _impd_shared_secret in the properties files for CA Directory.

   _impd_hostname

   Host name of the system where you installed the primary CA Directory instance.

   _impd_bind_pwd

   Enter the same password you entered for _impd_bind_pwd in the properties file for the Provisioning Servers.

   _impd_ha_hosts

   For a high-availability deployment, enter the host name of the alternate CA Directory server.

   For example, Directory2 (where the primary CA Directory server is Directory1)

   Note: If you have three or more instances of CA Directory, separate the entries with commas. For example: Directory2, Directory3.

   In a single-instance deployment, leave this parameter blank.

   _impd_root_domain_pwd

   Enter the same password you entered for _impd_shared_secret in the properties files for CA Directory.

   _impd_parent_domain_pwd

   Enter the same password you entered for _impd_shared_secret in the properties files for CA Directory.

   _impd_etaadmin_pwd

   Enter the same password you entered for _impd_shared_secret in the properties files for CA Directory.

_provisioning_server_pwd

Enter the same password you entered for _provisioning_server_pwd in the properties files for the Provisioning Servers.

_provisioning_repository_pwd

Enter the same password you entered for _impd_shared_secret in the properties files for CA Directory.

_connector_server_pwd

Enter the same password you entered for _connector_server_pwd in the properties files for the Provisioning Servers.

_provisioning_domain

Leave as the default value.

Note: The following six parameters are required only if you need a proxy between the CA IAM CS and the internet. Otherwise, leave them blank.

_http_proxy_enabled

Addresses whether you need a proxy to connect to the internet. Set to True if you need to enable a proxy to connect to the internet, for example, if the Provisioning Server is on a protected intranet. Set to False if the Provisioning Server has direct access to the internet and no proxy is enabled.

_http_proxy_user

The Proxy User required for authentication.

_http_proxy_pwd

The password for the Proxy User.

_http_proxy_domain

The proxy domain required for authentication.

_http_proxy_port

The proxy port required for authentication.

_http_proxy_server

The proxy server required for authentication.

_install_imps

Set to False to install the CA IAM CS.

Note: This parameter allows you to install a Provisioning Server through this installer. Set this to False to prevent a Provisioning Server from installing.

Also see the _install_jcs parameter.

_impd_skip_snapshot

Leave as the default value, false. This setting allows tenant deployment to succeed.

_dir_webservices_port

Port used by Web Services. Leave as the default, 9080, unless you cannot use this port in your environment. If you must change the web services port, enter a new port number.

Note: If you must change the web services port, use the same port for web services on all servers.

_dir_webservices_username

User name for Web Services. Leave as the default, dsaweb.

_dir_webservices_password

Enter the same password you entered for _dir_webservices_password in the properties file for the first CA Directory instance.

_dir_webservices_secure_port

Port used by Web Services. Leave as the default, 9443, unless you cannot use this port in your environment. If you must change the web services port, enter a new port number.

Note: If you must change the web services port, use the same port for web services on all servers.

_imps_fips_keyfile

Leave as the default, false.

_COMP_CLASS

Leave as the default, ca_cam.directory.

_COMP_NAME

Leave as the default, main.directory.

_APP_NAME

Leave as the default, directory_server.

JAVA64_LOCATION

Location of an existing 64-bit JRE if preinstalled. Set this parameter if you choose to install your JRE separately. In this case, symbolically link /opt/java64 to your JRE.

However, instead of installing a JRE separately, the system installer can do this automatically. We recommend that you download a JRE and allow the system to install it.

See the JAVA64_KIT parameter.

JAVA64_KIT

Location of a 64-bit JRE that you download to the local system or to a file share. If this parameter is set, the server kit will install this JRE automatically.

USER_JAVA64

Leave blank for installation. This parameter is intended for upgrades, not installation.

_install_jcs

Set to True to install the CA IAM CS.

Note: This parameter allows you to install an CA IAM CS through this installer. Set this to False to prevent an CA IAM CS from installing.

Also see the _install_imps parameter.

_ntp_server

IP address or host name of the NTP user to use to synchronize the server time.

_remote_imps_hostname

Enter the host name of the primary Provisioning Server system.

Note: This parameter is not needed when the Provisioning Server and CA IAM CS are on the same system.

3. Back up the properties.sh file. Rename it to a logical name, for example, connectorserver1properties.sh.

Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

Important! The original properties.sh file resides in a temp folder. If the server is shut down, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further installation or use of the system.

Install and Verify the CA IAM CS

After you set the CA IAM CS parameters and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```

2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, verify the installation as follows.

3. Check that Java is running:

   ```
   ps -ef | grep java
   ```

   The output shows the following:

   ```
   /opt/CA/Directory/dxserver/dsamgmt/jvm/bin/java -Xms256m
   -Xmx1024m -cp /opt/CA/Directory/dxserver/dsamgmt/lib/*
   com.ca.directory.dxagent.service.DxAgentService
   jvm/bin/java -ea
   -Dkaraf.home=/opt/CA/IdentityManager/ConnectorServer -server
   -Xms128M -Xmx1024M -XX:MaxPermSize=384m -Djava.awt.headless=true
   -Dcom.sun.management.jmxremote
   -Dderby.system.home=/opt/CA/IdentityManager/ConnectorServer/dat
   a/der
   by -Dderby.storage.fileSyncTransactionLog=true
   -Djava.endorsed.dirs=/opt/CA/IdentityManager/ConnectorServer/li
   b/endorsed
   -Djava.ext.dirs=/opt/CA/IdentityManager/ConnectorServer/jvm/lib
   /ext:/opt/CA/IdentityManager/ConnectorServer/lib/ext
   -Dkaraf.instances=/opt/CA/IdentityManager/ConnectorServer/insta
   nces
   -Dkaraf.base=/opt/CA/IdentityManager/ConnectorServer
   -Dkaraf.data=/opt/CA/IdentityManager/ConnectorServer/data
   -Djava.util.logging.config.file=/opt/CA/IdentityManager/Connect
   orSer
   ver/etc/java.util.logging.properties
   -Dkaraf.startLocalConsole=false -Dkaraf.startRemoteShell=true
   -Djcsroot=/opt/CA/IdentityManager/ConnectorServer/jcs
   -Dlog4j.configuration=/opt/CA/IdentityManager/ConnectorServer/e
   tc/org.ops4j.pax.logging.cfg
   -Dsun.lang.ClassLoader.allowArraySyntax=true -classpath
   ```

```
/opt/CA/IdentityManager/ConnectorServer/conf:/opt/CA/IdentityMa
nager/ConnectorServer/lib/karaf-jaas-boot.jar:/opt/CA/IdentityM
anager/ConnectorServer/lib/karaf.jar:/opt/CA/IdentityManager/Co
nnectorServer/lib/servicemix-version.jar:/opt/CA/IdentityManage
r/ConnectorServer/lib/smix4SecurityWrapper.jar:/opt/CA/Identity
Manager/ConnectorServer/j
cs/tools/lib/cacommons.jar
smix.security.wrapper.Smix4SecurityWrapper
```

4. Log in as the root user.

   ```
   su - root
   ```

5. Enter the following command:

   ```
   service im_jcs status
   ```

   The output shows the following:

   ```
   jcs is running
   ```

6. For a high-availability deployment, continue with installing a second CA IAM CS. For a single-instance deployment, continue with installing the SiteMinder Policy Server.

High-Availability: CA IAM CS 2

Prepare a second system that is separate from the one on which you installed the first CA IAM CS instance.

Confirm that your server environment is properly prepared and install the required packages. Follow the same steps (see page 37) as you did for the first instance.

Configure the Second CA IAM CS Properties File

Set the parameters for the second CA IAM CS instance.

Copy the properties file from the first CA IAM CS instance and change only the parameters that are different for the second instance. Remember to rename and back up the new properties file after you complete the parameters.

You need the following information to complete the CA IAM CS parameters.

General Information:

- Your Provisioning Server host names

Follow these steps:

1. On the **first** CA IAM CS system, copy the properties.sh file that you just configured.
2. Navigate to /tmp/properties.sh on the **second** CA IAM CS system. Replace the properties.sh file with the configured copy from the first CA IAM CS system.
3. Change the following parameter values:

   _remote_imps_hostname

   Enter the host name of the failover (second) Provisioning Server system.

   Note: This parameter is not needed when the Provisioning Server and CA IAM CS are on the same system.
4. Leave all other parameter values as you set them for the first CA IAM CS.
5. Back up the properties.sh file. Rename it to a logical name, for example, connectorserver2properties.sh.

   Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

   Important! The original properties.sh file resides in a temp folder. If the server is shut down, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further installation or use of the system.

Install and Verify the Second CA IAM CS

After you set the parameters for the second CA IAM CS instance and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```
2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, verify the installation as follows.
3. Check that Java is running:

   ```
   ps -ef | grep java
   ```

   The output shows the following:

   ```
   /opt/CA/Directory/dxserver/dsamgmt/jvm/bin/java -Xms256m
   -Xmx1024m -cp /opt/CA/Directory/dxserver/dsamgmt/lib/*
   com.ca.directory.dxagent.service.DxAgentService
   ```

```
jvm/bin/java -ea
-Dkaraf.home=/opt/CA/IdentityManager/ConnectorServer -server
-Xms128M -Xmx1024M -XX:MaxPermSize=384m -Djava.awt.headless=true
-Dcom.sun.management.jmxremote
-Dderby.system.home=/opt/CA/IdentityManager/ConnectorServer/dat
a/der
by -Dderby.storage.fileSyncTransactionLog=true
-Djava.endorsed.dirs=/opt/CA/IdentityManager/ConnectorServer/li
b/endorsed
-Djava.ext.dirs=/opt/CA/IdentityManager/ConnectorServer/jvm/lib
/ext:/opt/CA/IdentityManager/ConnectorServer/lib/ext
-Dkaraf.instances=/opt/CA/IdentityManager/ConnectorServer/insta
nces
-Dkaraf.base=/opt/CA/IdentityManager/ConnectorServer
-Dkaraf.data=/opt/CA/IdentityManager/ConnectorServer/data
-Djava.util.logging.config.file=/opt/CA/IdentityManager/Connect
orSer
ver/etc/java.util.logging.properties
-Dkaraf.startLocalConsole=false -Dkaraf.startRemoteShell=true
-Djcsroot=/opt/CA/IdentityManager/ConnectorServer/jcs
-Dlog4j.configuration=/opt/CA/IdentityManager/ConnectorServer/e
tc/org.ops4j.pax.logging.cfg
-Dsun.lang.ClassLoader.allowArraySyntax=true -classpath
/opt/CA/IdentityManager/ConnectorServer/conf:/opt/CA/IdentityMa
nager/ConnectorServer/lib/karaf-jaas-boot.jar:/opt/CA/IdentityM
anager/ConnectorServer/lib/karaf.jar:/opt/CA/IdentityManager/Co
nnectorServer/lib/servicemix-version.jar:/opt/CA/IdentityManage
r/ConnectorServer/lib/smix4SecurityWrapper.jar:/opt/CA/Identity
Manager/ConnectorServer/j
cs/tools/lib/cacommons.jar
smix.security.wrapper.Smix4SecurityWrapper
```

4. Log in as the root user.

   ```
   su - root
   ```

5. Enter the following command:

   ```
   service im_jcs status
   ```

   The output shows the following:

   ```
   jcs is running
   ```

Continue with installing the SiteMinder Policy Server.

SiteMinder Policy Server

Standalone Policy Server

Use this procedure to install a SiteMinder Policy Server.

For a high-availability deployment, after you complete this procedure, continue with the SiteMinder Policy Server 2 procedure. Otherwise, after you complete this procedure continue with installing the CSP console.

SiteMinder Policy Server Pre-Installation Steps

To prepare for installation, confirm that your server environment is properly prepared. Then install the required packages.

Follow these steps:

1. Install 64-bit Linux RHEL 6.1.
2. Download, but do not install, a 32-bit JDK and a 64-bit JDK to your local system or to a file share.

   Note: The system installer can install the JDK automatically. We recommend that you download a JDK and allow the system to install it.

   Important! The SiteMinder Policy Server installation requires a JDK, rather than a JRE.
3. Download, but do not install, JBoss 5.1.0 to your local system or to a file share.

   Note: The system installer JBoss automatically.
4. Verify Oracle is configured as follows:
   - The Oracle Database server is available with all Oracle services (listener, DB, and so on) running
   - Oracle has a user with username "CamAdmin" with the privileges to create tablespace and user. CamAdmin has the DBA and Connect Oracle roles. Make a note of the password for CamAdmin for later use during installation.
   - The Oracle Database uses a UTF-8 encoded character set. If you plan to enable Advanced Authentication for your environment, install the AL32UTF8 Oracle database character set.

5. Obtain the SiteMinder Policy Server ISO image from the CA Support site and extract it.
6. Copy the kit (CAM-SMPS_kit-*date*.zip) to / (the root folder).
7. Unzip the kit.
8. Install the following packages required for Advanced Authentication
   - binutils-2*x86_64*
   - glibc-2*x86_64* nss-softokn-freebl-3*x86_64*
   - glibc-2*i686* nss-softokn-freebl-3*i686*
   - compat-libstdc++-33*x86_64*
   - glibc-common-2*x86_64*
   - glibc-devel-2*x86_64*
   - glibc-devel-2*i686*
   - glibc-headers-2*x86_64*
   - elfutils-libelf-0*x86_64*
   - elfutils-libelf-devel-0*x86_64*
   - gcc-4*x86_64*
   - gcc-c++-4*x86_64*
   - ksh-*x86_64*
   - libaio-0*x86_64*
   - libaio-devel-0*x86_64*
   - libaio-0*i686*
   - libaio-devel-0*i686*
   - libgcc-4*x86_64*
   - libgcc-4*i686*
   - libstdc++-4*x86_64*
   - libstdc++-4*i686*
   - libstdc++-devel-4*x86_64*
   - make-3.81*x86_64*
   - numactl-devel-2*x86_64*
   - sysstat-9*x86_64*

- compat-libstdc++-33*i686*
- compat-libcap*
- unixODBC*
- libstdc++*
- compat-libstdc++-33.i686
- compat-libstdc++-296.i686
- glibc.i686
- ksh.x86_64
- libgcc.i686
- libidn.i686
- libstdc++.i686
- libX11.x86_64
- libXau.x86_64
- libxcb.x86_64
- libXext.i686
- libXi.i686
- libXtst.i686
- ncurses-devel.i686
- nss-softokn-freebl.i686
- dos2unix
- telnet

9. Issue the following command:

   ```
   rpm –i compat-libtermcap-2.0.8-49.el6.i686.rpm
   ```

10. Install the Korn shell packages at /bin/ksh.
11. Run the following commands to set the state of the firewall/ip tables:

```
chkconfig iptables off
service iptables stop
```

12. Run the following commands to check and set the state of SELinux:
    a. Check the status:
    ```
    sestatus
    ```
    b. If the response is "permissive" or "disabled", do nothing
    c. If the response is "enforcing", change the state:
    ```
    sudo vi /etc/selinux/config
    setenforce 0
    ```

Configure the SiteMinder Policy Server Properties File

Set the parameters for the SiteMinder Policy Server installation.

You need the following information to complete the SiteMinder Policy Server parameters.

General Information:

- Your Provisioning Server host names
- The host names of the systems where you plan to install the SiteMinder Policy Servers
- Fully Qualified Domain Name of your SiteMinder Policy Server system, or in a high-availability deployment, the SiteMinder Policy Server load balancer
- Fully Qualified Domain Name of your Secure Proxy Server system, or in a high-availability deployment, the Secure Proxy Server load balancer
- The file path to your JBoss kit. The kit should be in zip file format.
- License.dat file for SiteMinder. Contact customer support to download this file from the CA Support site.
- The IP address or host name of your NTP server

From your Oracle installation:

- Password for your CamAdmin user
- The host name of your Oracle Server or RAC
- Your Oracle SID, or if a RAC configuration, your Oracle Service name

From your CSP DSA installation:

- _csp_dir_host

From the CA Directory properties file:

- _dir_webservices_password

Follow these steps:

1. Navigate to /tmp/properties.sh.
2. In the properties.sh file, set the following parameters.

   _Environment

   Leave as the default, VMWare

   _db_schema_user

   Database user with DBA privileges for Oracle and Postgres. The default is caadmin. For an upgrade on Oracle, _oracle_schema_user is used if db_schema_user is not set.

   _db_schema_password

   Password for user defined by db_schema_user. If this property is blank on an upgrade from Oracle, _Oracle_schema_password is used.

   _oracle_schema_user

   An Oracle database user with DBA and Connect privileges. This property remains for backwards compatibility with CA CloudMinder 1.5. If it is set and db_schema_user is not set, db_schema_user uses this value.

   For upgrade, you can leave this unchanged or set it to the value used for _db_schema_user.

   _oracle_schema_password

   The password for the oracle_schema_user. This property remains for backwards compatibility with CA CloudMinder 1.5. If it is set and db_schema_password is not set, db_schema_password uses this value.

   For upgrade, you can leave this unchanged or set it to the value used for _db_schema_password.

   _db_server

   Hostname of Oracle and Postgres database server. For an Oracle RAC setup, use the RAC host name.

   _database_name

   For Oracle, the SID or Service name (use the Service name for an Oracle RAC setup); for PostgreSQL, the default database name..

_ps_tablespace_filename

For Oracle,enter the path to the tablespace file as follows:

<path_to_PS_tablespace_file>/<name_of_PS_tablespace_file.dbf>

This property is not used for PostgreSQL. Make a note of this value so you can use it later during the installation process.

_ps_tablespace_filesize

For Oracle, the size of the table space for the SiteMinder Policy Server database. We recommend an initial size of 1000MB. This property is not used for PostgreSQL.

_ps_ha_hosts

For a high-availability deployment, enter the host name where you plan to install the second SiteMinder Policy Server.

Note: If you have three or more instances of SiteMinder Policy Server, separate the entries with commas. For example: PolicyServer2, PolicyServer3. Do not include the host name on which you are currently installing.

In a single-instance deployment, leave this parameter blank.

_ps_db_user

A user name for the Oracle or PostgreSQL database user for the Policy Server database. Create any user name.

Make a note of this user name so you can use it later during the installation process.

_ps_db_password

A password for the Oracle or PostgreSQL database user for the SiteMinder Policy Server database. Create any password.

Make a note of this password so you can use it later during the installation process.

_ps_tablespace_name

Table space name for the Policy Server database. Create any table space name.

Make a note of this name so you can use it later during the installation process. This property is not used for PostgreSQL.

_aa_db_user

A user name for the Advanced Authentication Oracle or PostgreSQL database. Create any user name.

Make a note of this user name so you can use it later during the installation process. Use the same value for _im_webfort_user when you install the Identity Management Server.

_aa_db_password

A password for the aa_db_user. Create any password.

Make a note of this password so you can use it later during the installation process. Use the same value for _im_webfort_password when you install the Identity Management Server.

_aa_tablespace_filename

Enter a name for the Oracle tablespace file for the Advanced Authentication database, in one of the following formats. This property is not used for PostgreSQL.

- For an Oracle RAC setup, enter only the tablespace file name. Do not include the file name extension:

  <name_of_AA_tablespace_file>

- For a non-RAC setup, enter the full path to the tablespace file. Include the file name extension:

  <path_to_AA_tablespace_file>/<name_of_AA_tablespace_file.dbf>

_aa_tablespace_filesize

The size of the file for the table space for the Advanced Authentication database. We recommend an initial size of 1000MB. This property is not used for PostgreSQL.

_aa_tablespace_name

The name of the Advanced Authentication table space.This property is not used for PostgreSQL.

_aa_tomcat_user

The name of a user who starts the Advanced Authentication Tomcat service. Leave as the default, root.

_ps_encryption_key

An encryption key for the Policy Server. Enter any string for the encryption key.

Note: This key is used in encryption processes by the SiteMinder policy server. Choose a string that fulfills typical password best practices.

_ps_admin_password

A password for the default SiteMinder user. Create any password.

Make a note of this password so you can use it later during the installation process. Use the same value for _generic_password when you install the Identity Management Server.

_sm_audit_cleanup_days

Leave as the default, 10.

_ps_license_data

Enter the path on your local system or in a file share to the license.dat file for your SiteMinder Policy Server. Enter the path in the following format:

<*path_to_license.dat_file*>/license.dat

_dir_webservices_username

User name for Web Services. Leave as the default, dsaweb.

_dir_webservices_password

Enter the same password you entered for _dir_webservices_password in the properties file for the first CA Directory instance.

_csp_console

Set to false if you are installing a SiteMinder Policy Server.

Note: This parameter allows you to install a CSP Console through this installer. Set this to False to prevent a CSP Console from installing.

Important! Set this to true only once for your entire deployment. You only need one CSP Console instance, even in a high-availability deployment.

We recommend that you install a CSP console on a system separate from your SiteMinder Policy Server.

_csp_deploy_dsa

Set to false if you are installing a SiteMinder Policy Server.

Note: This parameter allows you to install a CSP DSA through this installer. Set this to False to prevent a CSP Console from installing.

Important! Set this to true only once for your entire deployment. You only need one CSP DSA instance, even in a high-availability deployment.

We recommend that you install a CSP DSA on the same system on which you install the CSP Console. Install the CSP Console and CSP DSA on a system separate from your SiteMinder Policy Server.

_csp_dir_webservices_port

Port used by Web Services. Leave as the default, 9080, unless you cannot use this port in your environment. If you must change the web services port, enter a new port number.

Note: If you must change the web services port, use the same port for web services on all servers.

_csp_dir_webservices_username

User name for Web Services. Leave as the default, dsaweb.

_csp_dir_webservices_password

Enter the same password you entered for _dir_webservices_password in the properties file for the first CA Directory instance.

_csp_id

Leave as the default, cacsp.

_csp_dir_host

Enter the host name of the system where you plan to install the CSP DSA.

_csp_dir_port

Port used for CSP DSA. Leave as the default, 50000, unless you cannot use this port in your environment. If you must change the web services port, enter a new port number.

Note: If you must change the CSP DSA port, use the same port for the CSP DSA on all SiteMinder Policy Servers.

_csp_dir_password

The administrator password for the default user cspadmin in the CSP DSA. Create any password.

Make a note of this password for future use.

Note: The installation automatically creates the cspadmin user name. You choose the password to apply to this account.

_csp_webservice_cfg_id

Leave as the default, cspwebservice.

_csp_webservice_cfg_secret

Leave as the default. Internal use, do not change.

_aa_dsn_name

Required. The ODBC data source name. Enter any name for the data source.

_aa_tws_base_url

Required. Enter the URL for Tenant Web Sevices, using the following format:

http://<*internal_host:internal_tomcat_port*>/tenant-services/cm/tenantws

- For a non-high-availability deployment, the internal host is the fully-qualified domain name of the SiteMinder Policy Server.
- For a high-availability deployment, use the fully-qualified domain name of the SiteMinder Policy Server load balancer.
- The port number is 9090 by default.

aa_im_base_url

Required. Enter the base URL for the Identity Management Server, using the following format:

https://<*external_host*>/iam/im/

- For a non-high-availability deployment, the external host is the fully-qualified domain name of the Secure Proxy Server.
- For a high-availability deployment, use the fully-qualified domain name of the Secure Proxy Server load balancer.
- If your Secure Proxy Server is not using the https protocol, begin the base URL with http://

This information is used for browser redirect.

_aa_tws_config_id

Required. The configuration id for Tenant Web Services. The default value, tenantwebservices, is pre-populated.

If you want to use a different value, you must update the value here and in the Identity Management Server properties file.

_aa_tws_shared_secret

Required. The plain shared secret used by Tenant Web Services. The default value, firewall, is pre-populated.

We recommend that you change this value. Enter any value.

Note: You must update the value here and in the Identity Management Server properties file.

_aa_tomcat_host_address

Required. Enter the internal host address.

- For a non-high-availability deployment, the internal host is the fully-qualified domain name of the SiteMinder Policy Server.
- For a high-availability deployment, use the fully-qualified domain name of the SiteMinder Policy Server load balancer.

_shim_aaui_host_port

Required. Enter the external host address, i.e., the domain exposed to the outside world. Supply the host name even though the parameter name ends with _port.

- For a non-high-availability deployment, the external host is the fully-qualified domain name of the Secure Proxy Server.
- For a high-availability deployment, use the fully-qualified domain name of the Secure Proxy Server load balancer.

_shim_sm_webagent_host_port

Required. Enter the external host address, i.e., the domain exposed to the outside world. Supply the host name even though the parameter name ends with _port.

- For a non-high-availability deployment, the external host is the fully-qualified domain name of the Secure Proxy Server.
- For a high-availability deployment, use the fully-qualified domain name of the Secure Proxy Server load balancer.

_tws_imdb_user

Required. A user name in the Identity Management data store. Enter any user name.

Make a note of this user name so you can use it later during the installation process. Use the same value for _im_db_user when you install the Identity Management Server. This user is created during Identity Management installation.

_tws_imdb_pwd

A password for the user defined in _tws_imdb_user. Enter any password.

Make a note of this password so you can use it later during the installation process. Use the same value for _im_db_password when you install the Identity Management Server.

_tws_im_ws_host

Enter the host name of the system where you plan to install the Identity Management Server. This is used in TWS for accessing the web services deployed in the Identity Management Server.

_haprefimps

Enter the host name of the primary IdentityMinder Provisioning Server. This is the first Provisioning Server you installed.

_hafoimps

Enter the host name of the secondary or failover IdentityMinder Provisioning Server. This is the second Provisioning Server you installed.

_advanced_auth

Set to true to enable advanced authentication.

USER_INSTALL_DIR

Default location of your SiteMinder installation. For example: /opt/CA.

JAVA64_LOCATION

Location of an existing 64-bit JRE if preinstalled. Set this parameter if you choose to install your JRE separately. In this case, symbolically link /opt/java64 to your JRE.

However, instead of installing a JRE separately, the system installer can do this automatically. We recommend that you download a JRE and allow the system to install it.

See the JAVA64_KIT parameter.

JAVA64_KIT

Location of a 64-bit JRE that you download to the local system or to a file share. If this parameter is set, the server kit will install this JRE automatically.

USER_JAVA64

Leave blank for installation. This parameter is intended for upgrades, not installation.

JAVA32_LOCATION

Location of an existing 32-bit JRE if preinstalled. Set this parameter if you choose to install your JRE separately. In this case, symbolically link /opt/java32 to your JRE.

However, instead of installing a JRE separately, the system installer can do this automatically. We recommend that you download a JRE and allow the system to install it.

See the JAVA32_KIT parameter.

JAVA32_KIT

Location of a 32-bit JRE that you download to the local system or to a file share. If this parameter is set, the server kit will install this JRE automatically.

USER_JAVA32

Leave blank for installation. This parameter is intended for upgrades, not installation.

JBOSS_KIT

Enter the file path, on the local system or a file share, of the JBoss to install. The JBoss kit should be in zip file format. JBOSS can be either the community version or the Enterprise Application Platform (EAP).

_ntp_server

IP address or host name of the NTP server to use to synchronize the server time.

_aa_report_tablespace_filename

Required. The path for the orcl_aa_report.dbf file, in the following format:

<*Path on Oracle Server*>/orcl_aa_report.dbf

_aa_report_tablespace_filesize

Required. The size of the file for the table space for Advanced Authentication reports. Leave as the default, 20M.

AA_CATALINA_LOG_DIR

Leave as the default, $USER_INSTALL_DIR/AdvancedAuth/Tomcat/logs

This is the location of catalina.log.

3. Back up the properties.sh file. Rename it to a logical name, for example, policyserver1properties.sh.

   Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

   Important! The original properties.sh file resides in a temp folder. If the server is shut down, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further installation or use of the system.

Install and Verify the SiteMinder Policy Server

After you set the Policy Server parameters and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```

2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, verify the installation as follows.

3. Issue this command to check if Java is running:

   ```
   ps –ef|grep java
   ```

   The response is as follows:

   ```
   "java -Xms256m -Xmx1024m -cp ./lib/*
   com.ca.directory.dxagent.service.DxAgentService"
   "/opt/32/jdk1.6.0_31/jre/bin/java -Xrs
   -Dnete.ps.root=/opt/CA/siteminder -classpath
   /opt/CA/siteminder/lib/smconapi.jar:/opt/CA/siteminder/monitor/
   smmon.jar com.netegrity.smmonagent.SmMonAgentRun"
   ```

```
"/opt/CA/siteminder/adminui/runtime/bin/java
-Dprogram.name=run.sh -server -Xms128m -Xmx1024m
-XX:MaxPermSize=256m -Dorg.jboss.resolver.warning=true
-Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000 -disableassertions
-Djboss.platform.mbeanserver=true
-Dderby.system.home=/opt/CA/siteminder/adminui/server/default/d
ata/derby
-Djavax.net.ssl.keyStore=/opt/CA/siteminder/adminui/server/defa
ult/conf/keyStore.jks -Djavax.net.ssl.keyStoreType=jks
-Djavax.net.ssl.keyStorePassword=changeit
-Djavax.net.ssl.trustStore=/opt/CA/siteminder/adminui/server/de
fault/conf/trustStore.jks -Djavax.net.ssl.trustStoreType=jks
-Djavax.net.ssl.trustStorePassword=changeit
-Djava.net.preferIPv4Stack=true
-Djava.endorsed.dirs=/opt/CA/siteminder/adminui/lib/endorsed
-classpath
/opt/CA/siteminder/adminui/bin/run.jar:/opt/CA/siteminder/admin
ui/runtime/lib/tools.jar org.jboss.Main"
```

4. Inspect the /opt/CA/siteminder/registry/sm.registry file.

   It should have the following highlighted entry (usually at second line in file):

```
HKEY_LOCAL_SYSTEM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion=
813012936
ImsInstalled=                                  8.0;  REG_SZ
InstallKey=
{RC2}Xemlc/LaIcFzZdUpcR+CSlR9A6SNgg0YDQOwEsqfvKk=;      REG_SZ
Label=                                          758;  REG_SZ
Language=                                        EN;  REG_SZ
Location=                      /opt/CA/siteminder;  REG_SZ
MasterKeyFile=         /opt/CA/siteminder/bin/EncryptionKey.txt;
REG_SZ
Update=                                      00.00;  REG_SZ
Version=                                     12.51;  REG_SZ
```

5. Issue this command to confirm that SiteMinder is running:

```
ps –ef|grep sm
```

   The response is as follows:

```
"/opt/CA/siteminder/bin/smexec"
"smpolicysrv"
"/opt/32/jdk1.6.0_31/jre/bin/java -Xrs
-Dnete.ps.root=/opt/CA/siteminder -classpath
/opt/CA/siteminder/lib/smconapi.jar:/opt/CA/siteminder/monitor/
smmon.jar com.netegrity.smmonagent.SmMonAgentRun"
```

6. For a high-availability deployment, continue with installing a second SiteMinder Policy Server. For a single-instance deployment, continue with installing the CSP Console.

High-Availability: SiteMinder Policy Server 2

Prepare a second system that is separate from the one on which you installed the first SiteMinder Policy Server instance.

Confirm that your server environment is properly prepared and install the required packages. Follow the same steps (see page 48) as you did for the first instance.

Configure the Second SiteMinder Policy Properties File

Set the parameters for the second SiteMinder Policy Server instance.

Copy the properties file from the first SiteMinder Policy Server instance and change only the parameters that are different for the second instance. Remember to rename and back up the new properties file after you complete the parameters.

You need the following information to complete the SiteMinder Policy Server parameters.

General Information:

- The host names of the systems where you plan to install the SiteMinder Policy Servers
- License.dat file for SiteMinder. Contact customer support to download this file from the CA Support site

Follow these steps:

1. On the **first** SiteMinder Policy Server system, copy the properties.sh file that you just configured.
2. Navigate to /tmp/properties.sh on the **second** SiteMinder Policy Server system. Replace the properties.sh file with the configured copy from the first SiteMinder Policy Server system.
3. Change the following parameter values:

   _ps_ha_hosts

   For a high-availability deployment, enter the host name where you installed the first SiteMinder Policy Server.

   Note: If you have three or more instances of SiteMinder Policy Server, separate the entries with commas. For example: PolicyServer1, PolicyServer3. Do not include the host name on which you are currently installing.

   In a single-instance deployment, leave this parameter blank.

   _ps_license_data

   Enter the path on your local system or in a file share to the license.dat file for your SiteMinder Policy Server. Enter the path in the following format:

   <*path_to_license.dat_file*>/license.dat

4. Leave all other parameter values as you set them for the first SiteMinder Policy Server.
5. Back up the properties.sh file. Rename it to a logical name, for example, policyserver2properties.sh.

   Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

   Important! The original properties.sh file resides in a temp folder. If the server is shut down, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further installation or use of the system.

Install and Verify the Second SiteMinder Policy Server

After you set the parameters for the second Policy Server instance and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```

2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, verify the installation as follows.

3. Issue this command to check if Java is running:

   ```
   ps –ef|grep java
   ```

   The response is as follows:

   ```
   "java -Xms256m -Xmx1024m -cp ./lib/*
   com.ca.directory.dxagent.service.DxAgentService"
   "/opt/32/jdk1.6.0_31/jre/bin/java -Xrs
   -Dnete.ps.root=/opt/CA/siteminder -classpath
   /opt/CA/siteminder/lib/smconapi.jar:/opt/CA/siteminder/monitor/
   smmon.jar com.netegrity.smmonagent.SmMonAgentRun"
   "/opt/CA/siteminder/adminui/runtime/bin/java
   -Dprogram.name=run.sh -server -Xms128m -Xmx1024m
   -XX:MaxPermSize=256m -Dorg.jboss.resolver.warning=true
   -Dsun.rmi.dgc.client.gcInterval=3600000
   -Dsun.rmi.dgc.server.gcInterval=3600000 -disableassertions
   -Djboss.platform.mbeanserver=true
   -Dderby.system.home=/opt/CA/siteminder/adminui/server/default/d
   ata/derby
   ```

```
-Djavax.net.ssl.keyStore=/opt/CA/siteminder/adminui/server/defa
ult/conf/keyStore.jks -Djavax.net.ssl.keyStoreType=jks
-Djavax.net.ssl.keyStorePassword=changeit
-Djavax.net.ssl.trustStore=/opt/CA/siteminder/adminui/server/de
fault/conf/trustStore.jks -Djavax.net.ssl.trustStoreType=jks
-Djavax.net.ssl.trustStorePassword=changeit
-Djava.net.preferIPv4Stack=true
-Djava.endorsed.dirs=/opt/CA/siteminder/adminui/lib/endorsed
-classpath
/opt/CA/siteminder/adminui/bin/run.jar:/opt/CA/siteminder/admin
ui/runtime/lib/tools.jar org.jboss.Main"
```

4. Inspect the /opt/CA/siteminder/registry/sm.registry file.

   It should have the following highlighted entry (usually at second line in file):

```
HKEY_LOCAL_SYSTEM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion=
813012936
ImsInstalled=                                  8.0;  REG_SZ
InstallKey=
{RC2}Xemlc/LaIcFzZdUpcR+CSlR9A6SNgg0YDQOwEsqfvKk=;      REG_SZ
Label=                                          758;  REG_SZ
Language=                                        EN;  REG_SZ
Location=                    /opt/CA/siteminder;  REG_SZ
MasterKeyFile=        /opt/CA/siteminder/bin/EncryptionKey.txt;
REG_SZ
Update=                                     00.00;  REG_SZ
Version=                                    12.51;  REG_SZ
```

5. Issue this command to confirm that SiteMinder is running:

```
ps –ef|grep sm
```

   The response is as follows:

```
"/opt/CA/siteminder/bin/smexec"
"smpolicysrv"
"/opt/32/jdk1.6.0_31/jre/bin/java -Xrs
-Dnete.ps.root=/opt/CA/siteminder -classpath
/opt/CA/siteminder/lib/smconapi.jar:/opt/CA/siteminder/monitor/
smmon.jar com.netegrity.smmonagent.SmMonAgentRun"
```

Continue with installing the CSP Console.

CSP Console

Use this procedure to install a CSP Console.

You only need to install one instance of the CSP console, even if you are installing a high-availability deployment. After you complete this procedure continue with installing the Secure Proxy Server.

CSP Console Pre-Installation Steps

To prepare for installation, confirm that your server environment is properly prepared. Then install the required packages.

Important! The host name of the machine where you install the CSP Console must contain lower case letters only. If the host name includes upper case letters, the CSP Console does not open, and a looping error occurs in the log.

Follow these steps:

1. Install 64-bit Linux RHEL 6.1.
2. Download, but do not install, a 32-bit JDK and a 64-bit JDK to your local system or to a file share.

   Note: The system installer can install the JDK automatically. We recommend that you download a JDK and allow the system to install it.

   Important! The CSP console installation requires a JDK, rather than a JRE.
3. Download, but do not install, JBoss 5.1.0 to your local system or to a file share.

   Note: The system installer JBoss automatically.
4. Verify Oracle is configured as follows:
   - The Oracle Database server is available with all Oracle services (listener, DB, and so on) running
   - Oracle has a user with username "CamAdmin" with the privileges to create tablespace and user. CamAdmin has the DBA and Connect Oracle roles. Make a note of the password for CamAdmin for later use during installation.
   - The Oracle Database uses a UTF-8 encoded character set. If you plan to enable Advanced Authentication for your environment, install the AL32UTF8 Oracle database character set.
5. Obtain the SiteMinder Policy Server ISO image from the CA Support site and extract it.
6. Copy the kit (CAM-SMPS_kit-*date*.zip) to / (the root folder).
7. Unzip the kit.
8. Install the following packages required for Advanced Authentication
   - yum install -y binutils-2*x86_64*
   - yum install -y glibc-2*x86_64* nss-softokn-freebl-3*x86_64*
   - glibc-2*i686* nss-softokn-freebl-3*i686*
   - compat-libstdc++-33*x86_64*
   - glibc-common-2*x86_64*
   - glibc-devel-2*x86_64*

- glibc-devel-2*i686*
- glibc-headers-2*x86_64*
- elfutils-libelf-0*x86_64*
- elfutils-libelf-devel-0*x86_64*
- gcc-4*x86_64*
- gcc-c++-4*x86_64*
- ksh-*x86_64*
- libaio-0*x86_64*
- libaio-devel-0*x86_64*
- libaio-0*i686*
- libaio-devel-0*i686*
- libgcc-4*x86_64*
- libgcc-4*i686*
- libstdc++-4*x86_64*
- libstdc++-4*i686*
- libstdc++-devel-4*x86_64*
- make-3.81*x86_64*
- numactl-devel-2*x86_64*
- sysstat-9*x86_64*
- compat-libstdc++-33*i686*
- compat-libcap*
- unixODBC*
- libstdc++*
- compat-libstdc++-33.i686
- compat-libstdc++-296.i686
- glibc.i686
- ksh.x86_64
- libgcc.i686
- libidn.i686
- libstdc++.i686

- libX11.x86_64
- libXau.x86_64
- libxcb.x86_64
- libXext.i686
- libXi.i686
- libXtst.i686
- ncurses-devel.i686
- nss-softokn-freebl.i686
- dos2unix
- telnet

9. Execute the following command:
   ```
   rpm –i compat-libtermcap-2.0.8-49.el6.i686.rpm
   ```
10. Make sure that the following soft link still exists. Reverting a virtual machine snapshot removes this link.

    ```
    mv /dev/random /dev/random.orig
    ln -s /dev/urandom /dev/random
    ```
11. Install the Korn shell packages at /bin/ksh.
12. Run the following commands to set the state of the firewall/ip tables:

    ```
    chkconfig iptables off
    service iptables stop
    ```
13. Run the following commands to check and set the state of SELinux:
    a. Check the status:
       ```
       sestatus
       ```
    b. If the response is "permissive" or "disabled", do nothing
    c. If the response is "enforcing", change the state:
       ```
       sudo vi /etc/selinux/config
       setenforce 0
       ```

Configure the CSP Console Properties File

Set the parameters for the CSP console installation.

The SiteMinder Policy Server installation and the CSP console installation are very similar. Copy the properties file from the first SiteMinder Policy Server instance and change only the parameters that are different for CSP console installation. Remember to rename and back up the new properties file after you complete the parameters.

You need the following information to complete the CSP console parameters.

General Information:

- The host names of the systems where you plan to install the SiteMinder Policy Servers
- License.dat file for SiteMinder. Contact customer support to download this file from the CA Support site

Follow these steps:

1. On the first SiteMinder Policy Server system, copy the properties.sh file that you recently configured.
2. Navigate to /tmp/properties.sh on the CSP console system. Replace the properties.sh file with the configured copy from the first SiteMinder Policy Server system.
3. Change the following parameter values:

   _ps_ha_hosts

   For a high-availability deployment, enter the host name where you installed the first SiteMinder Policy Server.

   Note: If you have three or more instances of SiteMinder Policy Server, separate the entries with commas. For example: PolicyServer1, PolicyServer3. Do not include the host name on which you are currently installing.

   In a single-instance deployment, leave this parameter blank.

_ps_license_data

Enter the path on your local system or in a file share to the license.dat file for your SiteMinder Policy Server. Enter the path in the following format:

<*path_to_license.dat_file*>/license.dat

_csp_console

Required. Set to true to install the CSP console.

Note: This parameter allows you to install a CSP console through this installer. Set this to False to prevent a CSP console from installing.

Important! Set this to true only once for your entire deployment. You only need one CSP console instance, even in a high-availability deployment.

We recommend that you install a CSP console on a system that is separate from your SiteMinder Policy Server.

_csp_deploy_dsa

Required. Set to true to install the CSP DSA.

Note: This parameter allows you to install a CSP DSA through this installer. Set this to False to prevent a CSP DSA from installing.

Important! Set this to true only once for your entire deployment. You only need one CSP DSA instance, even in a high-availability deployment.

We recommend that you install a CSP DSA on the same system on which you install the CSP Console. Install the CSP Console and CSP DSA on a system that is separate from your SiteMinder Policy Server.

4. Leave all other parameter values as you set them for the first SiteMinder Policy Server.
5. Back up the properties.sh file. Rename it to a logical name, for example, cspconsoleproperties.sh.

   Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

   Important! The original properties.sh file resides in a temp folder. If the server is shut down, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further installation or use of the system.

Install and Verify the CSP Console

After you set the CSP console parameters and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```

2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, verify the installation as follows.

3. Issue this command to check if Java is running:

   ```
   ps –ef|grep java
   ```

   The response is as follows:

   ```
   "java -Xms256m -Xmx1024m -cp ./lib/*
   com.ca.directory.dxagent.service.DxAgentService"
   "/opt/32/jdk1.6.0_31/jre/bin/java -Xrs
   -Dnete.ps.root=/opt/CA/siteminder -classpath
   /opt/CA/siteminder/lib/smconapi.jar:/opt/CA/siteminder/monitor/
   smmon.jar com.netegrity.smmonagent.SmMonAgentRun"
   "/opt/CA/siteminder/adminui/runtime/bin/java
   -Dprogram.name=run.sh -server -Xms128m -Xmx1024m
   -XX:MaxPermSize=256m -Dorg.jboss.resolver.warning=true
   -Dsun.rmi.dgc.client.gcInterval=3600000
   -Dsun.rmi.dgc.server.gcInterval=3600000 -disableassertions
   -Djboss.platform.mbeanserver=true
   -Dderby.system.home=/opt/CA/siteminder/adminui/server/default/d
   ata/derby
   -Djavax.net.ssl.keyStore=/opt/CA/siteminder/adminui/server/defa
   ult/conf/keyStore.jks -Djavax.net.ssl.keyStoreType=jks
   -Djavax.net.ssl.keyStorePassword=changeit
   -Djavax.net.ssl.trustStore=/opt/CA/siteminder/adminui/server/de
   fault/conf/trustStore.jks -Djavax.net.ssl.trustStoreType=jks
   -Djavax.net.ssl.trustStorePassword=changeit
   -Djava.net.preferIPv4Stack=true
   -Djava.endorsed.dirs=/opt/CA/siteminder/adminui/lib/endorsed
   -classpath
   /opt/CA/siteminder/adminui/bin/run.jar:/opt/CA/siteminder/admin
   ui/runtime/lib/tools.jar org.jboss.Main"
   ```

4. Inspect the /opt/CA/siteminder/registry/sm.registry file.

   It should have the following highlighted entry (usually at second line in file):

   ```
   HKEY_LOCAL_SYSTEM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion=
   813012936
   ImsInstalled=                                  8.0;  REG_SZ
   InstallKey=
   {RC2}Xemlc/LaIcFzZdUpcR+CSlR9A6SNgg0YDQOwEsqfvKk=;      REG_SZ
   Label=                                        758;  REG_SZ
   Language=                                      EN;  REG_SZ
   Location=                    /opt/CA/siteminder;  REG_SZ
   MasterKeyFile=         /opt/CA/siteminder/bin/EncryptionKey.txt;
   REG_SZ
   Update=                                    00.00;  REG_SZ
   Version=                                   12.51;  REG_SZ
   ```

5. Issue this command to confirm that SiteMinder is running:

   ```
   ps –ef|grep sm
   ```

   The response is as follows:

   ```
   "/opt/CA/siteminder/bin/smexec"
   "smpolicysrv"
   "/opt/32/jdk1.6.0_31/jre/bin/java -Xrs
   -Dnete.ps.root=/opt/CA/siteminder -classpath
   /opt/CA/siteminder/lib/smconapi.jar:/opt/CA/siteminder/monitor/
   smmon.jar com.netegrity.smmonagent.SmMonAgentRun"
   ```

Continue with installing the Secure Proxy Server.

Secure Proxy Server

Standalone Secure Proxy Server

Use this procedure to install a Secure Proxy Server.

For a high-availability deployment, after you complete this procedure, continue with the Secure Proxy Server 2 procedure. Otherwise, after you complete this procedure continue with installing the Identity Management Server.

Secure Proxy Server Pre-Installation Steps

To prepare for the installation, confirm that your server environment is properly prepared. Then install the required packages.

Follow these steps:

1. Install 64-bit Linux RHEL 6.1.
2. Download, but do not install, a 32-bit JDK and a 64-bit JDK to your local system or to a file share. You can also use a JRE in place of a JDK.

   Note: The system installer can install the JDK automatically. We recommend that you download a JDK and allow the system to install it.
3. Obtain the Secure Proxy Server ISO image from the CA Support site and extract it.
4. Copy the kit (CAM-SPS_kit-*date*.zip) to / (the root folder).
5. Unzip the kit.
6. Install the following packages:
   - binutils-2*x86_64*
   - glibc-2*x86_64* nss-softokn-freebl-3*x86_64*
   - glibc-2*i686* nss-softokn-freebl-3*i686*
   - compat-libstdc++-33*x86_64*
   - glibc-common-2*x86_64*
   - glibc-devel-2*x86_64*
   - glibc-devel-2*i686*
   - glibc-headers-2*x86_64*
   - elfutils-libelf-0*x86_64*
   - elfutils-libelf-devel-0*x86_64*
   - gcc-4*x86_64*
   - gcc-c++-4*x86_64*
   - ksh-*x86_64*
   - libaio-0*x86_64*
   - libaio-devel-0*x86_64*
   - libaio-0*i686*
   - libaio-devel-0*i686*
   - libgcc-4*x86_64*
   - libgcc-4*i686*

- libstdc++-4*x86_64*
- libstdc++-4*i686*
- libstdc++-devel-4*x86_64*
- make-3.81*x86_64*
- numactl-devel-2*x86_64*
- sysstat-9*x86_64*
- compat-libstdc++-33*i686*
- compat-libcap*
- unixODBC*
- libstdc++*
- compat-libstdc++-33.i686
- compat-libstdc++-296.i686
- glibc.i686
- ksh.x86_64
- libgcc.i686
- libidn.i686
- libstdc++.i686
- libX11.x86_64
- libXau.x86_64
- libxcb.x86_64
- libXext.i686
- libXi.i686
- libXtst.i686
- ncurses-devel.i686
- nss-softokn-freebl.i686
- dos2unix
- telnet

7. Run the following commands:

```
rpm –i compat-expat1-1.95.8-8.el6.i686.rpm
rpm –i libuuid-2.17.2-12.el6.i686.rpm
rpm –i apr-1.3.9-3.el6.i686.rpm
rpm –i db4-4.7.25-16.el6.i686.rpm
rpm –i expat-2.0.1-9.1.el6.i686.rpm
rpm –i apr-util-1.3.9-3.el6_0.1.i686.rpm
```

8. Run the following commands to set the state of the firewall/ip tables:

```
chkconfig iptables off
service iptables stop
```

9. Run the following commands to check and set the state of SELinux:

   a. Check the status:
   ```
   sestatus
   ```

   b. If the response is "permissive" or "disabled", do nothing

   c. If the response is "enforcing", change the state:
   ```
   sudo vi /etc/selinux/config
   setenforce 0
   ```

Configure the Secure Proxy Server Properties File

Set the parameters for the Secure Proxy Server installation.

You need the following information to complete the CSP console parameters.

General Information:

- Your primary SiteMinder Policy Server host name
- Your primary CA IAM CS host name
- The host name of the system where you plan to install the primary Identity Management Server
- The domain name for your installation, for example, forwardinc.com
- The path to your Secure Proxy Server certificate file and key file, if it already exists

From the SiteMinder Policy Server properties file:

- _ps_admin_password

Follow these steps:

1. Navigate to /tmp/properties.sh.
2. In the properties.sh file, set the following parameters.

   _Environment

   Leave as the default, VMWare.

   _policy_server_hostname

   Enter the host name for the first SiteMinder Policy Server you installed.

_im_hostname

Enter the host name of the system where you plan to install the first Identity Management Server.

_jcs_hostname

Enter the host name for the first CA IAM CS you installed.

policy_server_password

Password for the default SiteMinder Policy Server user. Enter the same password you entered for _ps_admin_password in the properties file for the Policy Server.

_DomainSuffix

Enter the domain name for your installation, for example, forwardinc.com

JAVA64_LOCATION

Location of an existing 64-bit JRE if preinstalled. Set this parameter if you choose to install your JRE separately. In this case, symbolically link /opt/java64 to your JRE.

However, instead of installing a JRE separately, the system installer can do this automatically. We recommend that you download a JRE and allow the system to install it.

See the JAVA64_KIT parameter.

JAVA64_KIT

Location of a 64-bit JRE that you download to the local system or to a file share. If this parameter is set, the server kit will install this JRE automatically.

USER_JAVA64

Leave blank for installation. This parameter is intended for upgrades, not installation.

JAVA32_LOCATION

Location of an existing 32-bit JRE if preinstalled. Set this parameter if you choose to install your JRE separately. In this case, symbolically link /opt/java32 to your JRE.

However, instead of installing a JRE separately, the system installer can do this automatically. We recommend that you download a JRE and allow the system to install it.

See the JAVA32_KIT parameter.

JAVA32_KIT

Location of a 32-bit JRE that you download to the local system or to a file share. If this parameter is set, the server kit will install this JRE automatically.

USER_JAVA32

Leave blank for installation. This parameter is intended for upgrades, not installation.

_ntp_server

Required. IP address or host name of the NTP user to use to synchronize the server time.

SSL_ENABLE

Required. Set to yes to run the Secure Proxy Server in SSL mode.

CERT_SPS

Enter the path to your Secure Proxy Server certificate file. Leave this value blank if you want the installer to create a self-signed certificate.

Note: A production installation should not use a self-signed certificate.

An example for an existing certificate file could be:

/opt/mycerts/MySPS.crt

KEY_SPS

Enter the path to your Secure Proxy Server key file. Leave this value blank if you want the installer to create a key.

_cert_passwd

The password of the Secure Proxy Server self-signed certificate that the install will generate. Create any password.

The value is required only if you want the installer to create a self-signed certificate. If your certificate already exists, leave this value blank.

SSL_SUBJECT

The subject of the certificate that the install will generate. The value is required only if you want the installer to create a self-signed certificate. The following shows an example format:

/C=IN/ST=AP/L=HYD/CN=XYZ

Where C = country name, ST = state, L = City, and CN = common name

3. Back up the properties.sh file. Rename it to a logical name, for example, secureproxyserver1properties.sh.

Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

Important! The original properties.sh file resides in a temp folder. If the server is shut down, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further installation or use of the system.

Install and Verify the Secure Proxy Server

After you set the Secure Proxy Server parameters and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```

2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, verify the installation as follows.

3. Make sure that services are running. Enter this command:

   ```
   ps –ef | grep httpd
   ```

   The response should be instances of the following line:

   ```
   /opt/CA/secure-proxy/httpd/bin/httpd -d
   /opt/CA/secure-proxy/httpd -k start
   ```

4. Check that Java is running. Enter the following command:

   ```
   ps –ef | grep java
   ```

   The response should be similar to the following, ending with server.conf:

   ```
   /opt/jdk1.6.0_31/32/bin/java -ms256m -mx512m -server
   -Dcatalina.base=/opt/CA/secure-proxy/Tomcat
   -Dcatalina.home=/opt/CA/secure-proxy/Tomcat
   -Djava.io.tmpdir=/opt/CA/secure-proxy/Tomcat/temp
   -DHTTPClient.log.mask=0
   -DHTTPClient.Modules=HTTPClient.RetryModule|org.tigris.noodle.N
   oodleCookieModule|HTTPClient.DefaultModule
   -Dlogger.properties=/opt/CA/secure-proxy/Tomcat/properties/logg
   er.properties -DNETE_WA_ROOT=/opt/CA/webagent
   -DPWD=/opt/CA/secure-proxy -classpath
   /opt/CA/secure-proxy/Tomcat/bin/proxybootstrap.jar:/opt/CA/secu
   re-proxy/Tomcat/properties:/opt/jdk1.6.0_31/32/lib/tools.jar:/o
   pt/CA/secure-proxy/Tomcat/bin/bootstrap.jar:
   com.netegrity.proxy.ProxyBootstrap -config
   /opt/CA/secure-proxy/proxy-engine/conf/server.conf
   ```

5. Start the Secure Proxy Server as follows:
   a. Navigate to /opt/CA/secure-proxy/proxy-engine
   b. Issue these commands:

```
./sps-ctl stop
./sps-ctl startssl
```

   The Secure Proxy Server starts.
6. For a high-availability deployment, continue with installing a second Secure Policy Server. For a single-instance deployment, continue with installing the Identity Management Server.

High-Availability: Secure Proxy Server 2

Prepare a second system that is separate from the one on which you installed the first Secure Proxy Server instance.

Confirm that your server environment is properly prepared and install the required packages. Follow the same steps (see page 72) as you did for the first instance.

Configure the Second Secure Proxy Server Properties File

Set the parameters for the second Secure Proxy Server instance.

Copy the properties file from the first Secure Proxy Server instance and change only the parameters that are different for the second instance. Remember to rename and back up the new properties file after you complete the parameters.

You need the following information to complete the Secure Proxy Server parameters.

General Information:

- Your second (failover) SiteMinder Policy Server host name
- Your second (failover) CA IAM CS host name
- The host name of the system where you plan to install the second (failover) Identity Management Server

From the SiteMinder Policy Server properties file:

- _ps_admin_password

Follow these steps:

1. On the **first** Secure Proxy Server system, copy the properties.sh file that you just configured.
2. Navigate to /tmp/properties.sh on the **second** Secure Proxy Server system. Replace the properties.sh file with the configured copy from the first Secure Proxy Server system.
3. Change the following parameter values:

   _policy_server_hostname

   Enter the host name for the second SiteMinder Policy Server you installed.

   _im_hostname

   Enter the host name of the system where you plan to install the second Identity Management Server.

   _jcs_hostname

   Enter the host name for the second CA IAM CS you installed.

4. Leave all other parameter values as you set them for the first SiteMinder Policy Server.
5. Back up the properties.sh file. Rename it to a logical name, for example, secureproxyserver2properties.sh.

   Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

   Important! The original properties.sh file resides in a temp folder. If the server is shut down, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further installation or use of the system.

Install and Verify the Second Secure Proxy Server

After you set the parameters for the second Secure Proxy Server and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```

2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, verify the installation as follows.

3. Make sure that services are running. Enter this command:

   ```
   ps –ef | grep httpd
   ```

   The response should be instances of the following line:

   ```
   /opt/CA/secure-proxy/httpd/bin/httpd -d
   /opt/CA/secure-proxy/httpd -k start
   ```

4. Check that Java is running. Enter the following command:

   ```
   ps –ef | grep java
   ```

   The response should be similar to the following, ending with server.conf:

   ```
   /opt/jdk1.6.0_31/32/bin/java -ms256m -mx512m -server
   -Dcatalina.base=/opt/CA/secure-proxy/Tomcat
   -Dcatalina.home=/opt/CA/secure-proxy/Tomcat
   -Djava.io.tmpdir=/opt/CA/secure-proxy/Tomcat/temp
   -DHTTPClient.log.mask=0
   -DHTTPClient.Modules=HTTPClient.RetryModule|org.tigris.noodle.N
   oodleCookieModule|HTTPClient.DefaultModule
   -Dlogger.properties=/opt/CA/secure-proxy/Tomcat/properties/logg
   er.properties -DNETE_WA_ROOT=/opt/CA/webagent
   -DPWD=/opt/CA/secure-proxy -classpath
   /opt/CA/secure-proxy/Tomcat/bin/proxybootstrap.jar:/opt/CA/secu
   re-proxy/Tomcat/properties:/opt/jdk1.6.0_31/32/lib/tools.jar:/o
   pt/CA/secure-proxy/Tomcat/bin/bootstrap.jar:
   com.netegrity.proxy.ProxyBootstrap -config
   /opt/CA/secure-proxy/proxy-engine/conf/server.conf
   ```

5. Start the Secure Proxy Server as follows:
   a. Navigate to /opt/CA/secure-proxy/proxy-engine
   b. Issue these commands:

```
./sps-ctl stop
./sps-ctl startssl
```

   The Secure Proxy Server starts.

Continue with installing the Identity Management Server.

Identity Management Server

Standalone Identity Management Server

Use this procedure to install an Identity Management Server.

For a high-availability deployment, after you complete this procedure, continue with the Identity Management Server 2 procedure. Otherwise, after you complete this procedure continue with installing the Report Server.

Identity Management Server Pre-Installation Steps

To prepare for installation, confirm that your server environment is properly prepared. Then install the required packages.

Note: For installation a high-availability JBoss cluster, all nodes on the cluster must be on the same subnet.

Follow these steps:

1. Install 64-bit Linux RHEL 6.1.
2. Download, but do not install, a 64-bit JDK to your local system or to a file share.

   Note: The system installer can install the JDK automatically. We recommend that you download a JDK and allow the system to install it.

   Important! The Identity Management installation requires a JDK, rather than a JRE.

3. Download, but do not install, JBoss 5.1.0 to your local system or to a file share.

   Note: The system installer JBoss automatically.

4. Verify that Oracle is configured as follows:
   - The Oracle Database server is available with all Oracle services (listener, DB, and so on) running
   - Oracle has a user with username "CamAdmin" with the privileges to create tablespace and user. CamAdmin has the DBA and Connect Oracle roles. Make a note of the password for CamAdmin for later use during installation.
   - The Oracle Database uses a UTF-8 encoded character set. If you plan to enable Advanced Authentication for your environment, install the AL32UTF8 Oracle database character set.
5. From the Oracle web site, download the JCE policy zip file, jce_policy-6.zip. Copy the file to the /tmp folder on your Identity Management server.
6. Obtain the Identity Management Server ISO image from the CA Support site and extract it.
7. Copy the kit (CAM-IM_kit-*date*.zip) to / (the root folder).
8. Unzip the kit.
9. Install the following packages:
   - binutils-2*x86_64*
   - glibc-2*x86_64* nss-softokn-freebl-3*x86_64*
   - glibc-2*i686* nss-softokn-freebl-3*i686*
   - compat-libstdc++-33*x86_64*
   - glibc-common-2*x86_64*
   - glibc-devel-2*x86_64*
   - glibc-devel-2*i686*
   - glibc-headers-2*x86_64*
   - elfutils-libelf-0*x86_64*
   - elfutils-libelf-devel-0*x86_64*
   - gcc-4*x86_64*
   - gcc-c++-4*x86_64*
   - ksh-*x86_64*
   - libaio-0*x86_64*
   - libaio-devel-0*x86_64*
   - libaio-0*i686*
   - libaio-devel-0*i686*

- libgcc-4*x86_64*
- libgcc-4*i686*
- libstdc++-4*x86_64*
- libstdc++-4*i686*
- libstdc++-devel-4*x86_64*
- make-3.81*x86_64*
- numactl-devel-2*x86_64*
- sysstat-9*x86_64*
- compat-libstdc++-33*i686*
- compat-libcap*
- unixODBC*
- libstdc++*
- compat-libstdc++-33.i686
- compat-libstdc++-296.i686
- glibc.i686
- ksh.x86_64
- libgcc.i686
- libidn.i686
- libstdc++.i686
- libX11.x86_64
- libXau.x86_64

- libxcb.x86_64
- libXext.i686
- libXi.i686
- libXtst.i686
- ncurses-devel.i686
- nss-softokn-freebl.i686
- dos2unix
- telnet

10. Run the following commands to set the state of the firewall/ip tables:

```
chkconfig iptables off
service iptables stop
```

11. Run the following commands to check and set the state of SELinux:

    a. Check the status:
    ```
    sestatus
    ```

    b. If the response is "permissive" or "disabled", do nothing

    c. If the response is "enforcing", change the state:
    ```
    sudo vi /etc/selinux/config
    setenforce 0
    ```

Configure the Identity Management Server Properties File

Set the parameters for the Identity Management Server installation.

General Information:

- The host names of the systems where you installed the CA Directory servers
- The host names of the systems where you installed the SiteMinder Policy servers
- The host names of the systems where you installed the Provisioning servers
- The host names of the systems where you plan to install the Identity Management servers
- The JBoss ID for the Identity Management Server you are installing.
- The name of the mail server that you want the Identity Management server to use for email notifications
- The return address that you want the Identity Management server to use for email
- The full file path to the JCE policy zip file, jce_policy-6.zip

From your Oracle installation:

- Password for your CamAdmin user
- The host name of your Oracle Server or RAC
- Your Oracle SID, or if a RAC configuration, your Oracle Service name

From the CA Directory properties file:

- impd_shared_secret
- _dir_webservices_username
- _dir_webservices_password
- _dir_webservices_port

From the SiteMinder Policy Server properties file:

- _ps_db_user
- _ps_db_password
- _ps_tablespace_name
- _ps_admin_password
- _aa_db_user
- _aa_db_password
- _csp_dir_host
- _csp_dir_port
- _csp_dir_password

From the Provisioning Server properties file:

- _provisioning_server_pwd
- _connector_server_pwd

Follow these steps:

1. Navigate to /tmp/properties.sh.
2. In the properties.sh file, set the following parameters.

_Environment

Leave as the default, VMWare.

_db_server

Hostname of Oracle and PostgreSQL database server. For an Oracle RAC setup, use the RAC host name.

db_schema_user

Database user with DBA privileges for Oracle and PostgreSQL. The default is caadmin. For an upgrade on Oracle, _oracle_schema_user is used if db_schema_user is not set.

db_schema_password

Password for user defined by db_schema_user. If this property is blank on an upgrade from Oracle, _oracle_schema_password is used.

_oracle_schema_user

An Oracle database user with DBA and Connect privileges. This property remains for backwards compatibility with CA CloudMinder 1.5. If it is set and db_schema_user is not set, db_schema_user uses this value.

For upgrade, you can leave this unchanged or set it to the value used for _db_schema_user.

_oracle_schema_password

The password for the oracle_schema_user. This property remains for backwards compatibility with CA CloudMinder 1.5. If it is set and db_schema_password is not set, db_schema_password uses this value.

For upgrade, you can leave this unchanged or set it to the value used for _db_schema_password.

_database_name

For Oracle, the SID or Service name (use the Service name for an Oracle RAC setup); for PostgreSQL, the default database name.

_im_db_user

A user name for the Identity Management database. Create any user name.

_im_db_password

A password you for the Identity Management Oracle or PostgreSQL database user. Create any password.

_im_tablespace_name

Table space name for the Identity Management Oracle or PostgreSQL database. Create any table space name.

_im_tablespace_filename

Enter a name for the Oracle tablespace file for the Identity Management server, in one of the following formats.

- For an Oracle RAC setup, enter only the tablespace file name. Do not include the file name extension:

  <name_of_IM_tablespace_file>

- For a non-RAC setup, enter the full path to the tablespace file. Include the file name extension:

  <path_to_IM_tablespace_file>/<name_of_IM_tablespace_file.dbf>

_im_tablespace_filesize

The size of the table space for the Identity Management database. We recommend an initial size of 1000MB. This property is not used for PostgreSQL.

_ps_db_user

Enter the same user name you entered for _ps_db_user in the properties file for the first SiteMinder Policy Server instance. This property is used for Oracle and PostgreSQL.

_ps_db_password

Enter the same password you entered for _ps_db_password in the properties file for the first SiteMinder Policy Server instance. This property is used for Oracle and PostgreSQL.

_ps_tablespace_name

Enter the same name you entered for _ps_tablespace_name in the properties file for the first SiteMinder Policy Server instance. This property is not used for PostgreSQL.

_generic_username

The default SiteMinder Policy Server user name.

_generic_password

Enter the same password you entered for _ps_admin_password in the properties file for the first SiteMinder Policy Server installation. This is the password for the default SiteMinder Policy Server user.

_agent_name

The name of the agent which the Identity Management Server uses to communicate with the SiteMinder Policy Server. For internal use. Leave as the default, camadmin.

_agent_password

A password you create for the agent used by the Identity Management Server to communicate with the SiteMinder Policy Server.

_sm_host

Enter the host address of the SiteMinder Policy Server load balancer VIP.

_use_siteminder

Set to the value "True" so that the Identity Management Server is installed with SiteMinder integration enabled.

_use_clustering

Set to the value "True" to enable high availability installation of the Identity Management servers.

Set to the value "False" to disable high availability installation, for example, in a test environment.

_mail_server

Enter the name of the mail server that you want the Identity Management server to use for email notifications.

_sendmail_smart_relay_host

This is used for the sendmail configuration of the relay host. Leave blank or specify the local host.

_email_return_address

Enter the return address that you want the Identity Management server to use for email.

_cluster_sucker_password

A password used by JBoss cluster. Leave as the default setting or create any password.

_cluster_peer_host

Enter the host name of the server on which you are currently installing Identity Management.

_jboss_server_id

Enter a JBoss ID for the Identity Management Server you are installing. Create any unique ID. We recommend a value of "1" for your first Identity Management instance, "2" for your second instance, etc.

_uarm_user_id

Internal use only. Do not change.

_uarm_password

Internal use only. Do not change.

_uarm_dev_user_id

Internal use only. Do not change.

_multicast_groupname

Enter a unique name you create for this Identity Management cluster. Choose a different multicast groupname for each cluster you run.

All the Identity Management Servers in the cluster share the same value for this parameter. This can be any text string, but we recommend a short name, because it is included in every message sent around the cluster.

_multicast_address

Enter a unique multicast address you create for this Identity Management cluster. Choose a different multicast address for each cluster you run.

All the Identity Management servers in the cluster share the same value for this parameter. By default, JBoss AS uses UDP multicast for most intra-cluster communication. Consider a multicast address of the form 239.255.x.y. See JBoss documentation for additional guidelines.

_im_fips_mode

Set to the value "False" to install without FIPS mode. CA CloudMinder 1.5 does not currently support FIPS mode.

_im_fips_key_location

"/tmp"

Location of the FIPS key.

Leave as the default. CA CloudMinder 1.5 does not currently support FIPS mode.

_im_webfort_user

Enter the same name you entered for _aa_db_user in the properties file for the first SiteMinder Policy Server instance. This is the advanced authentication database user name. If webfort is not used, set this property to the same value as _im_db_user. This property applies for both Oracle and PostgreSQL.

_im_webfort_password

Enter the same name you entered for _aa_db_password in the properties file for the first SiteMinder Policy Server instance. This is the advanced authentication database user password. If webfort is not used, set this property to the same value as _im_db_password. This property applies for both Oracle and PostgreSQL.

_TenantProvDirPassword

Enter the same value you entered for impd_shared_secret in the properties file for the first Directory Server instance.

_TenantProvServerSecret

Enter the same value you entered for _provisioning_server_pwd in the properties file for the first Provisioning Server instance.

_TenantProvDirectorySecret

Enter the same value you entered for impd_shared_secret in the properties file for the first Directory Server instance.

_TenantProvJCSPassword

Enter the same value you entered for _connector_server_pwd in the properties file for the first Provisioning Server instance.

_cspHostName

Enter the host name where you installed the first (primary) SiteMinder Policy Server.

_cspHostPort

Enter 8080, or enter the CSP console Port if it is installed on a non-default port.

_cspContextPath

Internal use. Do not change.

_cspAlias

Internal use. Do not change.

_cspSecure

Set to the value "True" to enable SSL on the CSP console (use HTTPS).

Set to the value "False" to disable SSL on the CSP console (use HTTP).

_cspConfigurationId

Internal use. Do not change.

_cspConfigurationSecret

Internal use. Do not change.

_envBaseURL

Enter your the base URL for your CA CloudMinder environment, in the following format:

<SPS>.<YOURDOMAIN>/iam/im

Where SPS is your Secure Proxy Server, and YOURDOMAIN is the domain address for your environment.

For example:

cloudminderspsvip1.forwardinc.com/iam/im

_dirHosts

Enter all CA Directory host names in your environment, separated by commas.

_internalBaseURL

Set this Hosting Container to specify Internal Base URL when you do not want the notifications from Provisioning Server to go to the Environment Base URL.

An internal Identity Management Server load balancer can be specified here. This load balancer will be used as the Provisioning Server notification URL for any tenants deployed. Tenants deployed when no Internal Base URL has been specified will have a Provisioning Server notification URL that is derived from the Environment Base URL.

_dirDsaMgmtUser

Enter the same value as you entered for _dir_webservices_username in the properties file for the first CA Directory instance. Be sure to uncomment this parameter (remove # from the parameter name).

_dirDsaMgmtPassword

Enter the same value as you entered for _dir_webservices_password in the properties file for the first CA Directory instance. Be sure to uncomment this parameter (remove # from the parameter name).

_dirDsaMgmtPort

Enter the same value as you entered for _dir_webservices_port in the properties file for the first CA Directory instance. Be sure to uncomment this parameter (remove # from the parameter name).

_tenantDsaRouterHosts

Enter the host names for all hosts with a DSA router in your installation, separated by commas.

For Example:

Identity Management Server1, Identity Management Server2, SiteMinder Policy Server1, SiteMinder Policy Server2, Provisioning Server1, Provisioning Server2

_tenantDsaRouterMgmtUser

Leave as default, blank.

_tenantDsaRouterMgmtPassword

Leave as default, blank.

_tenantDsaRouterMgmtPort

Leave as default, blank.

_impsHosts

Enter the host names for all Provisioning Servers, separated by commas.

For Example:

Provisioning Server1, Provisioning Server2

_impsDsaMgmtUser

Leave as default, blank.

_impsDsaMgmtPassword

Leave as default, blank.

_impsDsaMgmtPort

Leave as default, blank.

_impsTenantServiceHost

Enter the host name of the first (primary) Provisioning Server.

Note: If the CA IAM CS is on a separate server, enter the host name of the CA IAM CS instead.

_impsTenantServicePassword

Enter the same password as you entered for _connector_server_pwd in the properties file for the first instance of the Provisioning Server. This is the password used to access the CA IAM CS.

_haprefimps

Enter the host name of the first (primary) Provisioning Server.

_hafoimps

Enter the host name of the second (failover) Provisioning Server.

_CSPDeployDir

Internal use. Do not change.

_CSPID

Internal use. Do not change.

_CSPName

Internal use. Do not change.

_CSPDirPassword

Enter the same password you entered for _csp_dir_password in the properties file for the first SiteMinder Policy Server instance.

_CSPDirHost

Enter the same host name you entered for _csp_dir_host in the properties file for the first SiteMinder Policy Server instance.

_CSPDirPort

Enter the same password you entered for _csp_dir_port in the properties file for the first SiteMinder Policy Server instance.

_authMinderHost

Enter the host name for the first (primary) SiteMinder Policy Server.

JAVA64_LOCATION

Location of an existing 64-bit JRE if preinstalled. Set this parameter if you choose to install your JRE separately. In this case, symbolically link /opt/java64 to your JRE.

However, instead of installing a JRE separately, the system installer can do this automatically. We recommend that you download a JRE and allow the system to install it.

See the JAVA64_KIT parameter.

JAVA64_KIT

Location of a 64-bit JRE that you download to the local system or to a file share. If this parameter is set, the server kit will install this JRE automatically.

JBOSS_KIT

Enter the file path, on the local system or a file share, of the JBoss to install. The JBoss kit should be in zip file format. JBOSS can be either the community version the or Enterprise Application Platform (EAP).

_ntp_server

IP address or host name of the NTP server to use to synchronize the server time.

_jce_zip_file

Enter the full file path to the JCE policy zip file. You downloaded the jce_policy-6.zip file from the Oracle web site during the Identity Management pre-installation steps.

_secure_session_cookie

The server kit configures JBoss to use session cookies with secure and httpOnly attributes if two conditions are met:

1. property _secure_session_cookie is set to true in properties.sh:

_secure_session_cookie=true; export _secure_session_cookie

2. property _envBaseURL starts with https in properties.sh:

_envBaseURL=https://webserver.ca.com; export _envBaseURL

If both conditions are not met, the session cookie will be left as is. The server kit contains a script that can be used to reconfigure the session cookie based on these conditions at any time:

configSessionCookie.sh

This script reads the properties and either enables the attributes in the JBoss session cookie or disables them depending on the values of the two properties. A JBoss restart is then required for the settings to take effect.

The User Console does not work properly without HTTPS if configured with secure session cookies.

3. Back up the properties.sh file. Rename it to a logical name, for example, identitymanager1properties.sh.

   Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

   Important! The original properties.sh file resides in a temp folder. If the server is shut down, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further installation or use of the system.

Install and Verify the Identity Management Server

After you set the Identity Management Server parameters and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```

2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, set up JBoss. Then verify the installation as follows.

Setup Using JBoss EAP

If you are using JBoss EAP, do the following:

1. Edit the file /opt/jboss-eap-5.1.2/jboss-as/server/all/conf/props/jmx-console-users.properties
2. Uncomment the line "#admin=admin"
3. Run the following command:
   ```
   dos2unix ../conf/props/jmx-console-users.properties
   ```
4. Stop and Start the Identity Management Server using JBoss, using the following steps:
   ```
   cd /etc/init.d/im stop
   ```
   ```
   cd /etc/init.d/im start
   ```

JBoss Configuration

The recommended memory for the Identity Management Server on JBoss is 6GB (6144). This is physical memory rather than swap space.

During installation, the system allocates memory to JBoss. The installation process calculates the memory allocation based on the physical memory of the system, as follows:

- Less than 8G, *memory* minus 2G is allocated
- More than 8G, *memory* divided by 2 is allocated
- The minimum memory allocated is 1G

After installation is complete, check your overall system memory and check the memory allocated to JBoss. The JBoss memory allocation is found in the run.sh file on the Identity Management Server.

If you do not have sufficient memory on the system, increase the max memory used by JBoss as follows:

1. Edit the file /opt/jboss-5.1.0.GA/bin/run.sh as follows:
   ```
   JAVA_OPTS="$IDM_OPTS $DEBUG_OPTS
   -Djava.security.policy=workpoint_client.policy -Xms256m
   –Xmx6144m -XX:MaxPermSize=256m -XX:ReservedCodeCacheSize=50m"
   ```
   In this example, the memory allocated is 6GB (6144).
2. Restart JBoss.

Verify the Server Installation

1. Issue this command to check if Java is running:
   ```
   ps –ef|grep java
   ```

The response includes the following:

```
java -Xms256m -Xmx4096m -cp ./lib/*
com.ca.directory.dxagent.service.DxAgentService
```

2. Verify that the /opt/jboss-5.1.0.GA/bin/run.sh file has the multicast_address and multicast_groupname that were set in /tmp/properties.sh file.
3. Verify that the following folders are present.

   For the community edition of JBoss:

   ```
   /opt/jboss-5.1.0.GA/server/all/deploy/iam_im.ear/user_console.w
   ar/META-INF/csp
   /opt/jboss-5.1.0.GA/server/all/deploy/iam_im.ear/user_console.w
   ar/META-INF/tenant
   ```

   For JBoss EAP:

   ```
   /opt/jboss-eap-5.1.2/jboss-as//server/all/deploy/iam_im.ear/use
   r_console.war/META-INF/csp
   /opt/jboss-eap-5.1.2/jboss-as//server/all/deploy/iam_im.ear/use
   r_console.war/META-INF
   ```

4. Verify that the following files are present.

   For the community edition of JBoss:

   ```
   /opt/jboss-5.1.0.GA/server/all/deploy/iam_im.ear/user_console.w
   ar/META-INF/csp/CSP.properties
   /opt/jboss-5.1.0.GA/server/all/deploy/iam_im.ear/user_console.w
   ar/META-INF/tenant/Container.properties
   ```

   For JBoss EAP:

   ```
   /opt/jboss-eap-5.1.2/jboss-as//server/all/deploy/iam_im.ear/use
   r_console.war/META-INF/csp/CSP.properties
   /opt/jboss-eap-5.1.2/jboss-as//server/all/deploy/iam_im.ear/use
   r_console.war/META-INF/tenant/Container.properties
   ```

5. For a high availability installation, edit the following file:

   For the community edition of JBoss:

   `/opt/jbos-5.1.0.GA/server/all/deploy/iam_im.ear/policyserver.rar/META-INF/ra.xml`

   For JBoss EAP:

   `/opt/jboss-eap-5.1.2/jboss-as//server/all/deploy/iam_im.ear/policyserver.rar/META-INF/ra.xml`

   This requires the following line:

   `<config-property-value>Your SiteMinder Policy Server1 Hostname,44441,44442,44443</config-property-value>`

6. For a high-availability deployment, continue with installing a second Identity Management Server. For a single-instance deployment, continue with installing the Report Server.

High-Availability: Identity Management Server 2

Prepare a second system that is separate from the one on which you installed the first Identity Management Server instance.

Confirm that your server environment is properly prepared and install the required packages. Follow the same steps (see page 82) as you did for the first instance.

Configure the Second Identity Management Server Properties File

Set the parameters for the second Identity Management Server instance.

Copy the properties file from the first Secure Proxy Server instance and change only the parameters that are different for the second instance. Remember to rename and back up the new properties file after you complete the parameters.

You need the following information to complete the Secure Proxy Server parameters.

General Information:

- The host names of the systems where you are installing the Identity Management servers
- The JBoss ID for the Identity Management Server you are installing.

Follow these steps:

1. On the **first** Identity Management server system, copy the properties.sh file that you just configured.
2. Navigate to /tmp/properties.sh on the **second** Identity Management server system. Replace the properties.sh file with the configured copy from the first Identity Management system.
3. Change the following parameter values:

   _cluster_peer_host

   Enter the host name of the server on which you are currently installing Identity Management.

   _jboss_server_id

   Enter a JBoss ID for the Identity Management Server you are installing. Create any unique ID. We recommend a value of "1" for your first Identity Management instance, "2" for your second instance, etc.
4. Leave all other parameter values as you set them for the first Identity Management server.
5. Back up the properties.sh file. Rename it to a logical name, for example, identitymanager2properties.sh.

   Note: This file is critical for upgrades. We recommend that you back up this file. This file contains passwords, so be sure to save it in a secure location.

   Important! The original properties.sh file resides in a temp folder. If the server is shut down, the properties.sh file is discarded. Therefore, rename and back up this file before proceeding with any further installation or use of the system.

Install and Verify the Second Identity Management Server

After you set the parameters for the Identity Management Server and back up the properties.sh file, run the installation program.

Verify the installation before proceeding with further installation steps.

Follow these steps:

1. Navigate to:

   ```
   /opt/CA/saas/repo/application/
   ```

2. Run:

   ```
   ./appliance_local.sh config
   ```

   When installation is complete, set up JBoss. Then verify the installation as follows.

Setup Using JBoss EAP

If you are using JBoss EAP, do the following:

1. Edit the file
   /opt/jboss-eap-5.1.2/jboss-as/server/all/conf/props/jmx-console-users.properties
2. Uncomment the line "#admin=admin"
3. Run the following command:
   `dos2unix ../conf/props/jmx-console-users.properties`
4. Stop and Start the Identity Management Server using JBoss, using the following steps:
   `cd /etc/init.d/im stop`

   `cd /etc/init.d/im start`

JBoss Configuration

The recommended memory for the Identity Management Server on JBoss is 6GB (6144). This is physical memory rather than swap space.

During installation, the system allocates memory to JBoss. The installation process calculates the memory allocation based on the physical memory of the system, as follows:

- Less than 8G, *memory* minus 2G is allocated
- More than 8G, *memory* divided by 2 is allocated
- The minimum memory allocated is 1G

After installation is complete, check your overall system memory and check the memory allocated to JBoss. The JBoss memory allocation is found in the run.sh file on the Identity Management Server.

If you do not have sufficient memory on the system, increase the max memory used by JBoss as follows:

1. Edit the file /opt/jboss-5.1.0.GA/bin/run.sh as follows:
   ```
   JAVA_OPTS="$IDM_OPTS $DEBUG_OPTS
   -Djava.security.policy=workpoint_client.policy -Xms256m
   –Xmx6144m -XX:MaxPermSize=256m -XX:ReservedCodeCacheSize=50m"
   ```
   In this example, the memory allocated is 6GB (6144).
2. Restart JBoss.

Verify the Server Installation

1. Issue this command to check if Java is running:
   ```
   ps –ef|grep java
   ```
   The response includes the following:
   ```
   java -Xms256m -Xmx4096m -cp ./lib/*
   com.ca.directory.dxagent.service.DxAgentService
   ```
2. Verify that the /opt/jboss-5.1.0.GA/bin/run.sh file has the multicast_address and multicast_groupname that were set in /tmp/properties.sh file.
3. Verify that the following folders are present.

   For the community edition of JBoss:
   ```
   /opt/jboss-5.1.0.GA/server/all/deploy/iam_im.ear/user_console.w
   ar/META-INF/csp
   /opt/jboss-5.1.0.GA/server/all/deploy/iam_im.ear/user_console.w
   ar/META-INF/tenant
   ```
   For JBoss EAP:
   ```
   /opt/jboss-eap-5.1.2/jboss-as//server/all/deploy/iam_im.ear/use
   r_console.war/META-INF/csp
   /opt/jboss-eap-5.1.2/jboss-as//server/all/deploy/iam_im.ear/use
   r_console.war/META-INF
   ```

4. Verify that the following files are present.

   For the community edition of JBoss:

   ```
   /opt/jboss-5.1.0.GA/server/all/deploy/iam_im.ear/user_console.war/META-INF/csp/CSP.properties
   /opt/jboss-5.1.0.GA/server/all/deploy/iam_im.ear/user_console.war/META-INF/tenant/Container.properties
   ```

   For JBoss EAP:

   ```
   /opt/jboss-eap-5.1.2/jboss-as//server/all/deploy/iam_im.ear/user_console.war/META-INF/csp/CSP.properties
   /opt/jboss-eap-5.1.2/jboss-as//server/all/deploy/iam_im.ear/user_console.war/META-INF/tenant/Container.properties
   ```

5. For a high availability installation, edit the following file:

   For the community edition of JBoss:

   ```
   /opt/jbos-5.1.0.GA/server/all/deploy/iam_im.ear/policyserver.rar/META-INF/ra.xml
   ```

   For JBoss EAP:

   ```
   /opt/jboss-eap-5.1.2/jboss-as//server/all/deploy/iam_im.ear/policyserver.rar/META-INF/ra.xml
   ```

   This requires the following line:

   ```
   <config-property-value>Your SiteMinder Policy Server1 Hostname,44441,44442,44443</config-property-value>
   ```

Continue with installing the Report Server.

Report Server

Standalone Report Server

If you do not need high availability for the Report Server, use the following procedure for a standalone installation.

Prerequisites

If you are planning to use RHEL 6 for the Business Objects installation, these prerequisites exist:

- Minimum patch requirements for RHEL 6: compat-libstdc++-33-3.2.3-69.el6.i686 (compatibility standard C++ library from GCC 3.3.4); glibc-2.12-1 (RedHat advisory RHBA-2007:0619-3); libXext.i386; libncurses.so.5, libXext-devel-1.1-3.el6.i686, libXext-devel-1.1-3.el6.x86_64

  Note: Install both X86_64 & i636 patches for the above. We recommend using yum install *package_name*.

  The hostname cannot have special characters such as '-' (a hyphen). It can be only alpha-numeric.

- Oracle Client 32Bit (or you can use Instant Client. To download OracleLinuxClient.zip)
- Open your Oracle server Enterprise Management Console or SQL console and create Tablespaces for CMS ("BO_CMS_TS") and Auditing ("BO_AUDIT_TS"). Also create 2 users, one for CMS ("BO_CMS_USER") and other for Auditing ("BO_AUDIT_USER") and give them dba privileges on respective Tablespaces.
- locale en_US.utf8 (to be default locale for BO installation)
- export LANG=en_US.utf8

Follow these steps:

1. Create a UNIX group (for example: bobje) to be used as a CA Business Intelligence User:
   ```
   # groupadd -g 400 bobje
   ```
2. Create a folder to be used as home folder for CA Business Intelligence User:
   ```
   # mkdir /home/bobje
   ```

3. Create a UNIX user (for example: bobje) to be used by the CA Business Intelligence installer for administrators:

   ```
   # useradd -d /home/bobje -g bobje bobje
   ```

4. Set the password for the user created in step 3.

   ```
   # passwd bobje
   ```

5. Change the ownership of the home directory as follows:
   ```
   # chown -R bobje:bobje /home/bobje
   ```

6. Download and copy the CABI3.3 to /home/bobje (or home folder created in step #2)

7. Extract the installer GZ file as follows:
   `gunzip cabi-`*`version_number`*`-linux.tar.gz`

8. Extract the TAR file as follows:
   `tar -xvf cabi-`*`version_number`*`-linux.tar`

9. Give necessary permissions on CABI install folder and Installer media
   `copy OracleLinuxClient.zip to /tmp`

10. Extract zip file and all other zip files in it

11. Rename the folder "instantclient_11_2" to "oracle" and move "oracle" folder to /opt/.

12. Go to /opt/oracle and create softlinks as below

    ```
    ln -s libclntsh.so.11.1 libclntsh.so
    ln -s libocci.so.11.1 libocci.so
    ```

13. Create a file "tnsnames.ora" with following content. Remember to replace parameters (specified between < and >) according to your setup

    ```
     <your Oracle SID> =
       (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = <Oracle Hostname>)(PORT =
    1521))
      (CONNECT_DATA =
     (SERVER = DEDICATED)
     (SERVICE_NAME = <your Oracle Service/SID name>)
    ```

14. Edit .bash_profile of both "root" (/root/.bash_profile) and "bobje" (/home/bobje/.bash_profile) (or CA Business object user created in step #3) and add the following.

Note: If /home/bobje/.bash_profile does not exist for bobje user, create one and change owner to bobje using command "chown bobje:bobje /home/bobje/.bash_profile"

```
export ORACLE_HOME=/opt/oracle
export PATH=$PATH:$ORACLE_HOME
export TNS_ADMIN=/opt/oracle
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/oracle
```

15. Go to the user home folder (/home/bobje).
16. Run the Cabi installer.

    ```
    cabiinstall.sh
    ```

    Note: CABI installation is console installation. Provide the necessary details in the screen, keeping note of the passwords, ports and usernames provided during the installation

    See the following section for a few important parameters to be given during installation.

Non-Root Credentials

The BusinessObjects Enterprise installation program needs to run as a non-root user. The installer is running as the 'root' user, enter credentials for a valid non-root user.

- User Name: bobje
- Group Name: bobje
- For Installation Type, Select New (Install a new Enterprise system) for Oracle, orr Custom for PostgreSQL)
- Select 1 - Use an existing database (Oracle/DB2/Sybase/MySQL,SQLAnywhere)" for CMS Repository
- Select 2 - Oracle for Database Type
- Provide CMS user details for the CMS Database
- Provide Audit user details for the Audit Database
- Select Yes to initialize the database
- Select 1 - Install Tomcat, deploy web applications"

  Note: In case of any database error during install, check the latest "/opt/CA/SharedComponents/CommonReporting3/setup/logs/dbcheck" for details. All installation logs exist here: "/opt/CA/SharedComponents/CommonReporting3/setup/logs/"

Install verification

After installation, you should be able to access the CMS console (http://<hostname>:8080/CmcApp)

Post Installation for the Report Server

Starting and Stopping the Report Server

1. To start the server, SSH to the Business Objects system:

```
cd /opt/CA/SharedComponents/CommonReporting3/bobje/setup
source env.sh
cd ..
./startservers
./tomcatstartup.sh
```

2. To stop the server, SSH to Business Objects system:

```
cd /opt/CA/SharedComponents/CommonReporting3/bobje/setup
source env.sh
cd ..
./stopservers
./tomcatshutdown.sh
```

To Check the Installed Business Objects Server Version:

1. Log in to CMS Console.
2. On the Home page, click Settings under the Manage section.
3. Check the Product Version is 12.5.0.1265, which applies to CA Business Intelligence 3.3.

Customize the mergeconnections script

1. Update Registry Entries as follows:

   For reports, such as JDBC/XML, set the registry key to use the Crystal Enterprise/Report Application Server

   For the Identity Management Server to change data sources for reports in the Report Server, run the mergeConnection script.

2. Check for Windows control characters in the mergeconnections script.

   If you downloaded the software using FTP in binary mode, these characters do not appear in this script. If you used another download method, use the dos2unix command to remove these characters.

3. Copy the mergeconnections_3.0.cf script from the system with the Identity Management Admin toolkit to the Report Server. On the system with the toolkit, the default location for this script is as follows:

   ```
   /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/Report
   ServerTools
   ```

4. On the Report Server system, place the script in this location:

   installation-directory`/bobje/enterprise120/generic`

5. Source in the environment variables for BusinessObjects Enterprise, as follows:

   `source` *installation-directory*`/bobje/setup/env.sh`

6. Run the following script:

   ```
   ./configpatch.sh mergeconnections_3.0.cf
   ```

7. Select 1 as the option when prompted.

   Note: Set the environment variable as follows before you run the script:

   ```
   export _POSIX2_VERSION=199209
   ```

8. Restart crystal processing servers as follows:

9. Log in as the non-root user you used to install the Report Server.

10. Issue these commands:

    ```
    cd /opt/CA/SharedComponents/CommonReporting3/bobje
    ./stopservers
    ./startservers
    ```

Copy the JDBC JAR Files

Follow these steps:

1. Navigate to the jdbcdrivers folder where the Identity Management Server Admin toolkit is installed. The default location is as follows:

   ```
   [set the alternate Installation Path
   variable]/tools/lib/jdbcdrivers
   ```

2. Copy ojdbc14.jar (for Oracle) or sqljdbc.jar (for SQL Server) or postgresql-9.3-1101.jdbc3.jar (for PostgreSQL) *to* the following location:

   ```
   /opt/CA/SharedComponents/CommonReporting3/bobje/java/lib/extern
   al
   ```

   The ojdbc14.jar and the sqljdbc.jar files are in the following location:

   ```
   /opt/CA/IdentityManager/IAM_Suite/IdentityManager/tools/ReportS
   erverTools/
   ```

   The postgresql-9.3-1101.jdbc3.jar is available at the following location:

   ```
   /opt/reports
   ```

3. Open the jdbc.sbo file in this directory:

   ```
   $CABI_HOME/bobje/enterprise120/linux_x86/dataAccess/RDBMS/conne
   ctionServer/jdbc
   ```

4. If you are using an Oracle Database, add the path for the location of jar file under the section for Oracle 11.

   Replace this section:

```
<JDBCDriver>
   <!--  Uncomment and edit the following lines
     to define java classes required by JDBC driver
&lt;ClassPath&gt;
    &lt;Path&gt;your jar or class files directory&lt;/Path&gt;
&lt;/ClassPath&gt;
 -->
        <Parameter Name="JDBC
Class">oracle.jdbc.OracleDriver</Parameter>
       <Parameter Name="URL
Format">jdbc:oracle:thin:@$DATASOURCE${:$DATABASE$}</Parameter>
</JDBCDriver>
With this section
<JDBCDriver>
        <ClassPath>

<Path>/opt/CA/SharedComponents/CommonReporting3/bobje/java/lib/
external/ojdbc14.jar</Path>
          </ClassPath>
       <Parameter Name="JDBC
Class">oracle.jdbc.OracleDriver</Parameter>
       <Parameter Name="URL
Format">jdbc:oracle:thin:@$DATASOURCE${:$DATABASE$}</Parameter>
</JDBCDriver>
```

5. If you are using a PostgreSQL database, add the path for location of jar file under the section for PostgreSQL 8.

   Replace this section

```
<JDBCDriver>
  <!--  Uncomment and edit the following lines
     to define java classes required by JDBC driver
&lt;ClassPath&gt;
    &lt;Path&gt;your jar or class files directory&lt;/Path&gt;
&lt;/ClassPath&gt;
 -->
        <Parameter Name="JDBC
Class">org.postgresql.Driver</Parameter>
        <Parameter Name="URL
Format">jdbc:postgresql://$DATASOURCE$/$DATABASE$</Parameter>
</JDBCDriver>
With this section:
<JDBCDriver>
        <ClassPath>

<Path>/opt/CA/SharedComponents/CommonReporting3/bobje/java/lib/
external/postgresql-9.3-1101.jdbc3.jar</Path>
        </ClassPath>
        <Parameter Name="JDBC
Class">org.postgresql.Driver</Parameter>
        <Parameter Name="URL
Format">jdbc:postgresql://$DATASOURCE$/$DATABASE$</Parameter>
      </JDBCDriver>
```

6. Save and close jdbc.sbo file.

7. Open the CRConfig.xml file, found in the following location:

   ```
   /opt/CA/SharedComponents/CommonReporting3/bobje/java
   ```

8. Add the location of the JDBC JAR files to the Classpath.

   - PostgreSQL - ${BOBJEDIR}/java/lib/external/postgresql-9.3-1101.jdbc3.jar
   - Oracle - ${BOBJEDIR}/java/lib/external/ojdbc14.jar

   For example:

```
<Classpath>${BOBJEDIR}/java/lib/external/postgresql-9.3-1101.jd
bc3.jar:${BOBJEDIR}/java/lib/sqljdbc.jar:${BOBJEDIR}/java/lib/o
jdbc14.jar:…</Classpath>
```

9. Save the file.

10. Restart the Report Server as follows:

```
cd /opt/CA/SharedComponents/CommonReporting3/bobje
./stopservers
./startservers
```

Run the Registry Script

For the Identity Management Server to change data sources for reports in the Report Server, run the mergeConnection script.

Follow these steps:

1. Install and startup a X-server on your client operating system. (You can download X-Win32 from http://www.starnet.com/products/xwin32/download.php)
2. Log on to Linux by BOE installation account and run bash as below:

```
bash$ export DISPLAY=$YOURXWin32ClientSYSTEMNAME:0.0
bash$ echo &DISPLAY
bash$ cd $INSTALLDIR/bobje/setup/
bash$ source env.sh
bash$ regedit
```

   where $INSTALLDIR is where BOE is installed.

3. Switch to X-win32 client system and there will be a prompt Registry Editor if the configuration is successful in step 2.
4. Create a registry category under HKEY_LOCAL_SYSTEM: HKEY_LOCAL_SYSTEM\Software\Business Objects\Suite 12.0\Crystal Reports\DatabaseOptions
5. Add a key named MergeConnectionProperties under DatabaseOptions category and set the String value to Yes.
6. Add a key also named MergeConnectionProperties under HKEY_CURRENT_USER\Software\Business Objects\Suite 12.0\Crystal Reports\DatabaseOptions category and set String value Yes as it's Data.
7. Refresh or schedule report in Infoview and now it works.

Deploy Default Reports

The Identity Management Server comes with default reports you can use for reporting. BIConfig is a utility that uses a specific XML format to install these default reports for the Identity Management Server.

Important! This process updates all default reports. If you customized any default reports, be sure to back them up before performing the update.

Follow these steps:

1. Gather the following information about the Report Server:
   - Hostname
   - Administrator name

- Administrator password
- Snapshot database type

2. Download the CA Business Intelligence 3.3 BIConfig utility (biconfig_3_3_1_0.zip) from the CABI FTP site.
3. Copy all content from the *installer-root-directory*/disk1/cabi/biconfig folder to the *im_admin_tools_dir*/ReportServerTools folder.
4. Set the JAVA_HOME variable to the 64-bit version of the JDK 6 update45 you installed.
5. Run the following command

   For Oracle:

   ```
   ./biconfig.sh -h "hostname" -u "administrator_name" -p
   "administrator_password" -f "oracle-biar.xml"
   ```

   For PostgreSQL:

   ```
   ./biconfig.sh -h "hostname" -u "administrator_name" -p
   "administrator_password" -f "postgres-biar.xml"
   ```

   Note: Be sure that biconfig.sh has execute permissions.
6. View the biconfig.log file found in the location where you ran the biconfig command.
7. Verify that the default reports installed successfully. Inspect the end of the log file for status; a successful installation appears as follows:

   ```
   ReportingDeployUtility - Reporting utility program terminated and
   return code = 0
   ```

Secure the Report Server with SSL

The Identity Management Server and Report Server communicate over a non-secure connection. Secure Sockets Layer (SSL) connection can be used to secure the connection between Report Server and The Identity Management Server.

An SSL connection ensures that the communication is encrypted when data is accessed from the Report Server. Before configuring the SSL, verify that the BO (Business Objects) Server has HTTPS enabled. To secure the connection with SSL, self-signed certificate or the certificate from the Certified Authority (CA) can be used.

The following procedure describes how to configure an SSL certificate using self-signed certificate.

Follow these steps:

1. Export the certificate from the keystore used in the BO Server, using any tool which generates a certificate.
2. Copy the certificate to a directory where the Identity Management Server is installed.
3. Import the Certificate in to the Java trust store (cacerts). Also, verify that the certificate is imported in to the java version which is currently used by CA IdentityMinderIdentity Management Server.
4. Restart the Application Server for the changes to take effect.
5. In The User Console, go to System, Reporting, Report Server Connection. Select the Secure Connection option.
6. Click Test Connection to verify the connectivity.

The following procedure is an example on how to export and import a certificate using the Keytool utility.

1. In the Business Objects Report Server, open the command prompt and enter the following command to export the certificate from the keystore:

   ```
   ../jvm/bin/keytool -export -alias testcert -file certificate.cer
   -keystore /root/.keystore  –storepass <keystore password>
   ```

2. Copy the certificate to a directory where the Identity Management Server is installed.
3. In the Identity Management Server, open the command prompt and enter the following command to import the certificate into the keystore:

   ```
   ../jvm/bin/Keytool -import - trustcacerts –file
   /root/certificater.cer –alias testcert -keystore
   JAVA_HOME/jre/lib/security/cacerts -storepass password
   ```

   The certificate is successfully installed.

Note: We recommend that you refer to the vendor-specific documentation to configure SSL on the Report Server. The Report Server supports Tomcat and IIS servers.

Uninstallation

To uninstall BusinessObjects Enterprise, run the uninstallBOBJE.sh script. The uninstallBOBJE.sh script is installed to the bobje directory of your installation.

This script stops all BusinessObjects Enterprise servers and processes, and then deletes the files copied from the product CD during your original installation of BusinessObjects Enterprise. Installing BusinessObjects Enterprise creates a number of additional files on your system. The uninstallBOBJE.sh script will not remove the files created during the installation process, or files created by the system or by users after installation. The files that remain include log files created by BusinessObjects Enterprise. These log files can be useful in diagnosing problems with previous installations.

To remove all BusinessObjects Enterprise files, perform an rm -rf command on the bobje directory.

Note: If you performed the “system” installation type, you will also need to delete the run control scripts from the appropriate /etc/rc# directories.

Additional Information

MergeConnectionProperties registry key

To be able to change server or database information at runtime for reports that are based on command objects. A registry key named "HKEY_CURRENT_USER\Software\Business Objects\Suite 11.0\Crystal Reports\DatabaseOptions\MergeConnectionProperties (Yes/No)" was introduced to allow the option of merging old connection properties to new connection properties; however, the problem continues, because the provider is not included in the query definition.

For reports,such as JDBC/XML, users must set the registry key to 'Yes" use the Crystal Enterprise/Report Application Server.

- ojdbc.jar or ojdbc14.jar
- Ojdbc6.jar is for java 1.6 since it supports the new JDBC 4.0 specification (it has a dependency on JDK 1.6).
- Whereas CABI 3.3 runs with JDK 1.5. We have to copy ojdbc14.jar to work with the reports.

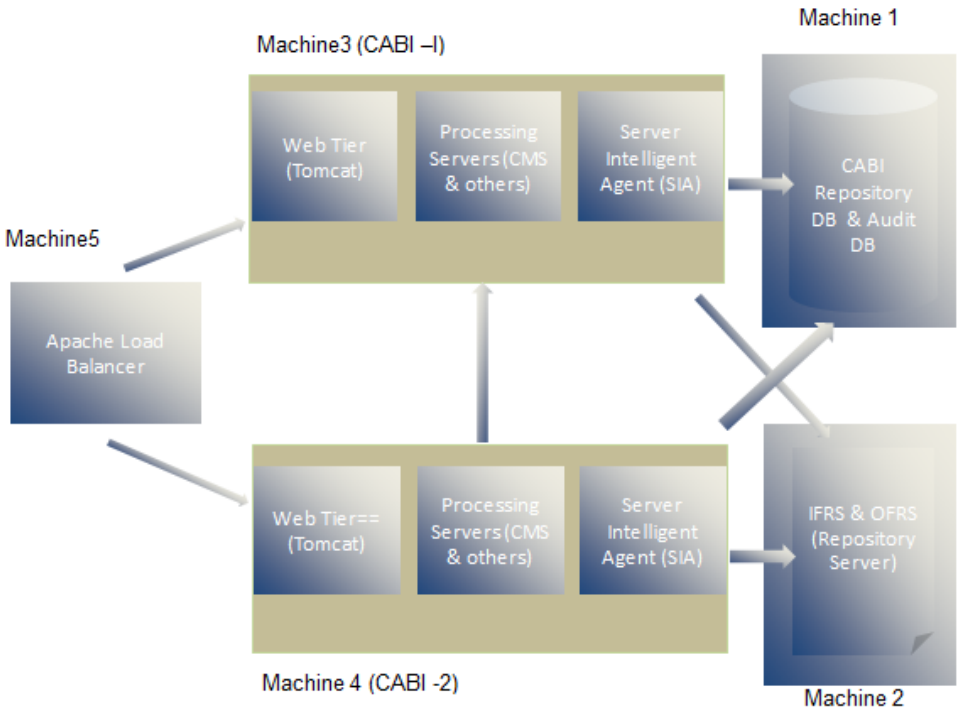
Debugging/Logs

If the CMS does not start, check the /var/log/messages file for the information. This is equivalent to event viewer in windows.

High Availability Report Server

To support a high availability report server, this chapter describes installing CA Business Intelligence on Linux platform using Apache Tomcat as the application server. The Apache HTTP Server is used as a load balancer. See the following diagram for details on this architecture.

Equation 1: High Availability Report Server



Prerequisites

Complete the following prerequisites:

1. Install the required Linux prerequisite patches to install CA Business Intelligence on System3 and System4.
2. Install the required Linux prerequisite patches to install Oracle Client on System3 and System4.

3. Install the required Linux prerequisite patches to install Oracle Server on System1.
4. Make sure NFS Server is installed on System2.
5. Make sure NFS Client is installed on System3 and System4.

System1 (Database Server)

Install the Oracle server and create two databases, one for CMS and one for Auditing. See the Oracle documentation for instructions on how to install Oracle on Linux and how to create databases on Linux after installing Oracle.

System2 (File Repository Server)

Perform the following steps on the File Repository Server system to configure and to start the NFS Server.

1. Log in to the system as root.
2. Open a terminal window and execute the following command:

```
service nfs start
service nfs status
mkdir -p /home/nfs/cabi
useradd -s /bin/bash cabiuser
chown cabiuser /home/nfs/cabi
id cabiuser
```

3. Reflect the cabiuser id and gid in the following line:

```
append /home/nfs/cabi
System*(rw,all_squash,anonuid=501,anongid=501) to /etc/exports
file
exportfs -a
showmount -e System2
su cabiuser
mkdir frsinput frsoutput
```

System3

1. Install the Oracle client.
2. Create a non-root user with the name cabiuser.

   This non-root user creation is mandatory to install CA Business Intelligence on Linux.
3. Create a group with the name cabiuser.
4. Add this user to group cabiuser.
5. Install CA Business Intelligence as follows:

   a. Use the New install option.

   b. Provide the System1 database details in the CMS and Audit DB section.

   c. Choose Tomcat as application server.

   See the CA Business Intelligence implementation guide for more information about the installation process.

Once the installation is complete, make sure that you are able to log in to CMC through the web URL.
`http://System3:8080/CmcApp`

System 4

1. Install the Oracle client.
2. Create a non-root user with the name cabiuser.
3. Create a group with the name cabiuser.
4. Add this user to group cabiuser.
5. Install CA Business Intelligence as follows:

   a. Choose the Custom or Expand Install option. In the next screen, clear MySQL from Server Components to make this server the second node in the cluster.

   b. Provide the System 3 details as the primary CMS in the next screen.

   c. Provide the System1 database details in the CMS and Audit DB section.

   d. Choose Tomcat as application server.

   See the CA Business Intelligence implementation guide for more information about the installation process.

Make sure that you can log in to the CMC through the web URL:
`http://System4:8080/CmcApp`

Setup NFS client on both CA Business Intelligence systems:

Perform the following steps on both CA Business Intelligence systems (System3 and System4) to set up the NFS client, which is required to access a shared location in the file repository server.

1. Log in as root.
2. Open a terminal window and execute the following:

```
mkdir -p /home/nfs/cabi

useradd -s /bin/bash -m cabiuser

chown cabiuser /home/nfs/cabi

add bansr02-I53529:/home/nfs/cabi /home/nfs/cabi nfs defaults 0 0
to /etc/fstab

mount -a

mount

su -cabiuser

cd /home/nfs/cabi

touch a

rm a

ls –alrt

cd /opt/CA/SharedComponents/CommonReporting3/bobje

./stopservers
cd data/frsinput
cp –r * /home/nfs/cabi/frsinput
cd ../frsoutput
cp –r * /home/nfs/cabi/frsoutput
cd ../..
./startservers
./ccm.sh –disable all –username Administrator –password
adminpassword
```

After completing the preceding steps on any system, perform the following steps:

1. Log in to the CMC URL as Administrator.
2. Click Servers, Core Services and double click System3.InputFileRepository.
3. In the Input FileStore Service section, set /home/nfs/cabi/frsinput to File Store Directory and /home/nfs/cabi/frsinput/temp to Temporary Directory.
4. Do the similar activity for Output FileStore Service.
5. Restart the services.
6. Run this command in terminal as a cabiuser ./ccm.sh –enable all –username Administrator –password adminpassword

System 5

Perform the following steps to configure nodes in the cluster environment on the load balancer server (System5) as a root user. Be sure that the Apache httpd server is installed.

1. Login as a root and open terminal.
2. /etc/init.d/httpd start
3. View the test page at http://system5/
4. Change directory to /etc/httpd.
5. Go to the CA Support site to obtain the mod_jk.so file.
6. Copy the mod_jk.so file to the modules folder.
7. Insert the following lines in the conf/httpd.conf file before the Listen 80 line.

```
LoadModule jk_module /etc/httpd/modules/mod_jk.so
JkWorkersFile "/etc/httpd/conf/workers.properties"
JkMountFile conf/uriworkermap.properties
JkMount /servlet/* balancer
JkMount /*.jsp balancer
JkMount /jkmanager/* jkstatus
```

8. Create a conf/worker.properties file with following contents:

```
worker.list=balancer,jkstatus
worker.jkstatus.type=status

worker.worker1.port=8009
worker.worker1.host=System3
worker.worker1.type=ajp13
worker.worker1.lbfactor=1
```

```
worker.worker2.port=8009
worker.worker2.host=System4
worker.worker2.type=ajp13
worker.worker2.lbfactor=1

worker.balancer.type=lb
worker.balancer.balance_workers=worker1,worker2
worker.balancer.sticky_session=true
```

9. Create conf/uriworkermap.properties file with the following contents:

```
/jmx-console=balancer
/jmx-console/*=balancer
/web-console=balancer
/web-console/*=balancer
/*=balancer
/=balancer
/etc/init.d/httpd stop
/etc/init.d/httpd start
```

Load balancing configuration on both CA Business Intelligence systems:

Configure both nodes in the cluster to accept requests from the load balancer server. Perform the following steps in CA Business Intelligence servers (System3 and System4).

Open /opt/CA/SharedComponents/CommonReporting3/bobje/tomcat/conf/server.xml.

1. Comment out all Connector tags and add the following line:

   ```
   <Connector port="8009" enableLookups="false" redirectPort="8443"
   tomcatAuthentication="false" maxThreads="400"
   minSpareThreads="25" maxSpareThreads="100" protocol="AJP/1.3" />
   ```

   An Engine tag exists below this line. Append the extra attribute jvmRoute="worker1" to this tag. (In the second CABI server, make the value"worker2").

2. Restart servers on both Report Server systems.
3. Restart the HTTP server in the load balancer.

Now you can access CMC using the following URL:

http://system5/CmcApp

You can also access Infoview using the following URL:

http://system5/InfoViewApp

Layer 7 Gateway Server

Use this procedure to install the Layer 7 Gateway servers.

Note: These instructions assume you are installing two Gateway servers in a high-availability deployment.

For additional information, see the complete Layer 7 Installation and Maintenance Manual in the CA CloudMinder bookshelf.

Layer 7 Gateway Server Pre-Installation Steps

To prepare for installation, confirm that your server environments are properly prepared.

Follow these steps:

1. Install 64-bit Linux RHEL 5.9 on your Layer 7 gateway systems.
2. Obtain all required installation files for the Layer 7 Gateway server, as follows. Download these files to ~/download on your Gateway systems:

   From CA Support:

   - add_slave_user.sh
   - create_slave.sh
   - harden.sh
   - my.cnf
   - ssg
   - ssg-7.1.1-3_noDB.noarch.rpm

   From Oracle:

   - jdk-7u21-linux-x64.tar.gz
   - UnlimitedJCEPolicyJDK7.zip

   From MySQL:

   - mysql-connector-java-5.1.20.tar.gz
   - mySQL-client-5.5.30-1.rhel5.x86_64.rpm
   - mySQL-server-5.5.30-1.rhel5.x86_64.rpm

Deploy the First Layer 7 Gateway

These steps describe how to deploy the first gateway server.

Important! Delete any previous installations or data before deploying the gateway. Residual test installations or MySQL data can cause installation problems.

Follow these steps:

1. Log in to the system as the root user.
2. Perform base system configuration:
   a. Configure the network card for IPv4 with the following values:
      - Machine name
      - IP Address
      - Default gateway
      - DNS nameserver
   b. Disable IPv6:

      ```
      NETWORKING_IPV6=no in /etc/sysconfig/network
      ```

   c. Configure the timezone:

      ```
      /etc/sysconfig/clock
      ```

   d. Install the NTP server, if you have not already done so:

      ```
      yum install ntp
      ```

   e. Enable NTP autostart:

      ```
      /sbin/chkconfig ntpd on
      ```

   f. Start the NTP Service:

      ```
      service ntpd start
      ```

3. Reboot the machine:

   ```
   sync;sync;reboot
   ```

4. Log in to the system as the root user.
5. Install the MySQL packages with the following commands:

   ```
   cd ~/download
   rpm -ivh MySQL-client-5.5.30-1.rhel5.x86_64.rpm
   rpm -ivh MySQL-server-5.5.30-1.rhel5.x86_64.rpm
   cp -p my.cnf /etc
   service mysql start
   ```

   Note: If the first RPM attempt fails, the base RedHat system may already have another version of MySQL installed. Use rpm -e to remove any conflicts.

6. /usr/bin/mysql_secure_installation and set the following values:
   - Enter current password for root (enter for none): Press <enter> for none
   - Set root password?: Y
   - New password: 7layer
   - Re-enter new password: 7layer
   - Remove anonymous users?: Y
   - Disallow root login remotely?: Y
   - Remove test database and access to it? : Y
   - Reload privilege tables now?:Y

7. Install the JDK under /opt/SecureSpan/JDK with the following commands:

   Note: System scripts reference the JDK files in this location. Install the JDK in this specific subdirectory only.

```
cd ~/download
mkdir tmp
cd tmp
tar xvzf ../jdk-7u21-linux-x64.tar.gz
mkdir /opt/SecureSpan/
mv jdk1.7.0_21 /opt/SecureSpan/JDK
unzip ../UnlimitedJCEPolicyJDK7.zip
cp -p UnlimitedJCEPolicy/*jar
/opt/SecureSpan/JDK/jre/lib/security/
Set the following values for the preceding command:
   cp: overwrite
`/opt/SecureSpan/JDK/jre/lib/security/local_policy.jar'?: Y
   cp: overwrite
`/opt/SecureSpan/JDK/jre/lib/security/US_export_policy.jar'?: Y

Install the ssgnodb rpm and the required dependencies with the
following commands:
cd ~/download
rpm -ivh ssg-7.1.1-3_noDB.noarch.rpm
mkdir tmp
cd tmp
tar xvzf ../mysql-connector-java-5.1.20.tar.gz
cp -p
mysql-connector-java-5.1.20/mysql-connector-java-5.1.20-bin.jar
/opt/SecureSpan/Gateway/runtime/lib/mysql-connector-java-5.1.20
.jar
chown layer7:layer7
/opt/SecureSpan/Gateway/runtime/lib/mysql-connector-java-5.1.20
.jar
chmod 444
/opt/SecureSpan/Gateway/runtime/lib/mysql-connector-java-5.1.20
.jar
```

8. Add ssg service with the following commands:

```
cd ~/download
chmod +x ssg
cp -p ssg /etc/init.d/ssg
/sbin/chkconfig --add ssg
```

Deploy the Second Layer 7 Gateway

These steps describe how to deploy the second gateway server.

Important! Delete any previous installations or data before deploying the gateway. Residual test installations or MySQL data can cause installation problems.

Follow these steps:

1. Log in to the system as the root user.
2. Perform base system configuration:
   a. Configure the network card for IPv4 with the following values:
      - Machine name
      - IP Address
      - Default gateway
      - DNS nameserver
   b. Disable IPv6:

      ```
      NETWORKING_IPV6=no in /etc/sysconfig/network
      ```

   c. Configure the timezone:

      ```
      /etc/sysconfig/clock
      ```

   d. Install the NTP server, if you have not already done so:

      ```
      yum install ntp
      ```

   e. Enable NTP autostart:

      ```
      /sbin/chkconfig ntpd on
      ```

   f. Start the NTP Service:

      ```
      service ntpd start
      ```

3. Reboot the machine:

   ```
   sync;sync;reboot
   ```

4. Log in to the system as the root user.

5. Download the following files to ~/download:

   From CA Support:

   - add_slave_user.sh
   - create_slave.sh
   - harden.sh
   - my.cnf
   - ssg
   - ssg-7.1.1-3_noDB.noarch.rpm

   From Oracle:

   - jdk-7u21-linux-x64.tar.gz
   - UnlimitedJCEPolicyJDK7.zip

   From MySQL:

   - mysql-connector-java-5.1.20.tar.gz
   - mySQL-client-5.5.30-1.rhel5.x86_64.rpm
   - mySQL-server-5.5.30-1.rhel5.x86_64.rpm

6. Install the MySQL packages with the following commands:

   ```
   cd ~/download
   rpm -ivh MySQL-client-5.5.30-1.rhel5.x86_64.rpm
   rpm -ivh MySQL-server-5.5.30-1.rhel5.x86_64.rpm
   cp -p my.cnf /etc
   service mysql start
   ```

   Note: If the first RPM attempt fails, the base RedHat system may already have another version of MySQL installed. Use rpm -e to remove any conflicts.

7. /usr/bin/mysql_secure_installation and set the following values:

   - Enter current password for root (enter for none): Press <enter> for none
   - Set root password?: Y
   - New password: 7layer
   - Re-enter new password: 7layer
   - Remove anonymous users?: Y
   - Disallow root login remotely?: Y
   - Remove test database and access to it? : Y
   - Reload privilege tables now?:Y

8. Install the JDK under /opt/SecureSpan/JDK with the following commands:

   Note: System scripts reference the JDK files in this location. Install the JDK in this specific subdirectory only.

```
cd ~/download
mkdir tmp
cd tmp
tar xvzf ../jdk-7u21-linux-x64.tar.gz
mkdir /opt/SecureSpan/
mv jdk1.7.0_21 /opt/SecureSpan/JDK
unzip ../UnlimitedJCEPolicyJDK7.zip
cp -p UnlimitedJCEPolicy/*jar
/opt/SecureSpan/JDK/jre/lib/security/
Set the following values for the preceding command:
   cp: overwrite
`/opt/SecureSpan/JDK/jre/lib/security/local_policy.jar'?: Y
   cp: overwrite
`/opt/SecureSpan/JDK/jre/lib/security/US_export_policy.jar'?: Y

Install the ssgnodb rpm and the required dependencies with the
following commands:
cd ~/download
rpm -ivh ssg-7.1.1-3_noDB.noarch.rpm
mkdir tmp
cd tmp
tar xvzf ../mysql-connector-java-5.1.20.tar.gz
cp -p
mysql-connector-java-5.1.20/mysql-connector-java-5.1.20-bin.jar
/opt/SecureSpan/Gateway/runtime/lib/mysql-connector-java-5.1.20
.jar
chown layer7:layer7
/opt/SecureSpan/Gateway/runtime/lib/mysql-connector-java-5.1.20
.jar
chmod 444
/opt/SecureSpan/Gateway/runtime/lib/mysql-connector-java-5.1.20
.jar
```

9. Add ssg service with the following commands:

```
cd ~/download
chmod +x ssg
cp -p ssg /etc/init.d/ssg
/sbin/chkconfig --add ssg
```

Configure Database Replication

Configure database replication on your Layer 7 Gateway servers by creating a Master-Master configuration.

Follow these steps:

1. SSH into both Gateways.
2. Stop the Gateway process on both servers by entering the following command:

   ```
   service ssg stop
   ```

   Note: You may see the following message:

   Shutting down Gateway Services: [FAILED]

   This simply means that the Gateway service were not started. Continue with database replication.
3. Enter the following command on both Gateways:

   ```
   cd ~/download; chmod +x add_slave_user.sh; chmod +x
   create_slave.sh
   ```
4. On Gateway 1, run the following command:

   ```
   ./add_slave_user.sh
   ```

   a. For the slave hostname, enter the fully qualified system name of Gateway 2.

   b. For the replication user, enter the MySQL database account that is used for replication. The default name is repluser.

   c. For the root user password, enter 7layer.

   Important! Enter known or default values for configurations that are not specified in this section.

   d. For the slave hostname, enter the fully qualified system name of Gateway 2.

   e. Set the node to primary (1).
5. On Gateway 2, run the following command:

   ```
   ./add_slave_user.sh
   ```

   Respond to the questions as follows:

   a. For the slave hostname, enter the fully qualified system name of Gateway 1.

   b. For the replication user, enter the MySQL database account that is used for replication. The default name is repluser.

   c. For the root user password, enter 7layer.

   Important! Enter known or default values for configurations that are not specified in this section.

   d. For the slave hostname, enter the fully qualified system name of Gateway 1.

e. Set the node to secondary (2).

6. On Gateway 1, run the following command:

   ```
   ./create_slave.sh
   ```

   Note: This script uses port 3306. If required, change the port to 3307.

   a. For the replication user, enter the MySQL database account that is used for replication. The default name is repluser.

   b. Enter the hostname of Gateway 2 for MASTER

      Important! Do not clone the database.

7. On Gateway 2, run the following command:

   ```
   ./create_slave.sh
   ```

   Note: This script uses port 3306. If required, change the port to 3307.

   a. For the replication user, enter the MySQL database account that is used for replication. The default name is repluser.

   b. Enter the hostname of Gateway 1 for MASTER.

      Important! Do not clone the database.

8. Verify replication with the following command:

   ```
   mysql -p -e "show slave status\G"
   ```

   Note: -p is required to prompt for root password.

   Enter 7layer for the password.

   - For Gateway 1, MASTER is Gateway 2.
   - For Gateway 2, MASTER is Gateway 1.

Create an Internal Database

In a clustered configuration, you create an internal database on only Gateway 1. This database is replicated automatically to Gateway 2. The Gateway 1 database is the primary, while the Gateway 2 database is used for failover.

Follow these steps:

1. On Gateway 1, enter the following commands:
   `/opt/SecureSpan/Gateway/runtime/bin/setup.sh --jdk /opt/SecureSpan/JDK`
2. Select 2 Configure the Layer 7 Gateway.
3. Press Enter to accept the default Java VM Path.
4. Press Enter to accept the Java VM Memory Allocation [512].

5. Set the following configuration values:
   - Database Connection: Yes
     - Database Host: enter "localhost" or the Gateway hostname

       For example, enter L7host.forewardinc.com.
     - Database Port: 3306
     - Database Name: ssg
     - Database Username: any username
     - Database Password: any password

     Note: If you modify the database username and password, record these values for later use.
   - Administrative DB User: root
   - Administrative DB Password: 7layer

     Important! Do not modify the default administrative database user and password values. They reference existing default values.
   - Configure Failover Connection: No
   - SSM Username: admin
   - SSM Password: your password
   - Administrative HTTPS Listener?: No
   - Cluster Hostname: Enter the URL of the load balancer.
   - Cluster Password: your password

     Note: Record this password for use when configuring Gateway 1 and 2.
   - Enabled: Yes
   - Press Enter to return to the menu
6. Type X to return to the UNIX shell.

Configure the Gateway 1 Database

This section covers connecting Gateway 1 to the internal database.

Follow these steps:

1. SSH into Gateway 1.
2. Enter /opt/SecureSpan/Gateway/runtime/bin/setup.sh --jdk /opt/SecureSpan/JDK.
3. Select 2 - Configure the Layer 7 Gateway.

4. Select 2 - Database Connection.
5. Enter the username and password you set when you created the database.
6. Set the following configuration values:
   - Database Connection: Yes
     - Database Host: The fully qualified system name for the Gateway 1
     - Database Port: 3306
     - Database Name: ssg
     - Database Username: any username
     - Database Password: any password

       Record these values for later use.
     - Administrative DB User: root
     - Administrative DB Password: 7layer

     Important! Use the default administrative database user and password values. They reference existing default values.
   - Configure Failover Connection: Yes
     - Database Failover Host: This is the failover MySQL database. Enter the fully qualified system name for the Gateway 2.
     - Database Failover Port: 3306
   - SSM Username: admin
   - SSM Password: Any password
   - Administrative HTTPS Listener?: No
   - Cluster Hostname: The URL of the load balancer
   - Cluster Password: The password you created for the cluster.
7. Select S - Save and Exit.
8. Press [Enter] to continue.
9. Enter the following commands:

   ```
   /sbin/chkconfig ssg on
   /sbin/chkconfig --list ssg
   ```

   The system responds with:

   ```
   ssg  0:off  1:off   2:on   3:on   4:on   5:on   6:off
   ```

Configure the Gateway 2 Database

This section describes how to connect Gateway 2 to the internal database.

Follow these steps:

1. SSH into Gateway 2.
2. Enter /opt/SecureSpan/Gateway/runtime/bin/setup.sh --jdk /opt/SecureSpan/JDK
3. Select 2 - Configure the Layer 7 Gateway.
4. Press Enter to accept the default Java VM Path.
5. Press Enter to accept the Java VM Memory Allocation [512].
6. Set the following configuration values:
   - Database Connection: Yes
     - Database Host: The fully qualified system name for the Gateway 1 even though this is gateway 2.
     - Database Port: 3306
     - Database Name: ssg
     - Database Username: any username.
     - Database Password: any password

       Record these values for later use.
     - Administrative DB User: root
     - Administrative DB Password: 7layer

     Important! Use the default administrative database user and password values. They reference existing default values.
   - Configure Failover Connection: Yes
     - Database Failover Host: This is the failover MySQL database. Enter the fully qualified system name for the Gateway 2.
     - Database Failover Port: 3306
   - SSM Username: admin
   - SSM Password: The password used for gateway one
   - Administrative HTTPS Listener?: No
   - Cluster Hostname: The URL of the load balancer
   - Cluster Password: The password used for gateway one.
7. Select S - Save and Exit.
8. Press [Enter] to continue.

9. Enter the following commands:

```
/sbin/chkconfig ssg on
/sbin/chkconfig --list ssg
```

The system responds with:

The system responds with:

```
ssg  0:off  1:off   2:on   3:on   4:on   5:on   6:off
```

Reboot Both Gateways

Reboot both Gateways by running the following command on both machines:

```
synch;synch;reboot
```

Harden the Gateway Servers

This section describes how to harden the Gateways. Perform the steps and commands on both systems.

Follow these steps:

1. SSH into the Gateway server as root user and enter the following commands:

```
useradd -m ssgconfig
passwd ssgconfig
```

Provide the password of your choice for the user ssgconfig.

```
cd ~/download
chmod +x harden.sh
cp -p harden.sh ~/harden.sh
cd ~
```

```
./harden.sh -h vmware
```

2. If ./harden.sh -h vmware fails, review error messages and manually resolve any conflicts. For example, you many need to run the following commands:

```
yum erase subscription-manager
yum erase yum-updatesd
yum erase yum-security
yum erase rhn-client-tools
echo "SINGLE=/sbin/sulogin" >> /etc/sysconfig/init
```

3. Review ~/harden.sh.log for hardening results, manually resolve conflicts, and re-run the hardening process as needed.

Once the harden.sh script has been run successfully, you can no longer log in as root. If you wish to gain root access to the system, log in as user ssconfig and run the su command to change your login ID to root. Typically, you must run the harden.sh script multiple times even if the script shows no error messages upon execution.

Install the PostgreSQL JDBC Driver

If any tenant OTK/OIDC database are PostgreSQL-driven, use this procedure on all Gateways in the cluster.

Follow these steps:

1. Connect with SSH.
2. Stop the service by running the following command:

   ```
   service ssg stop
   ```

3. Install the JDBC driver by running the following commands:

   ```
   cp postgresql-9.3-1100.jdbc41.jar
   /opt/SecureSpan/Gateway/runtime/lib/ext/.
   chown layer7:layer7
   /opt/SecureSpan/Gateway/runtime/lib/ext/postgresql-9.3-1100.jdb
   c41.jar
   ```

4. Expose the JDBC driver to the Gateway by modifying system properties. Edit this file:
   `/opt/SecureSpan/Gateway/node/default/etc/conf/system.properties`
5. Add this line:

   ```
   com.l7tech.server.jdbcDriver=com.mysql.jdbc.Driver\ncom.l7tech.
   jdbc.mysql.MySQLDriver\
   ncom.l7tech.jdbc.db2.DB2Driver\ncom.l7tech.jdbc.oracle.OracleDr
   iver\
   ncom.l7tech.jdbc.sqlserver.SQLServerDriver\norg.postgresql.Driv
   er
   ```

6. Save and exit.
7. Start the service by running the following command:

   ```
   service ssg start
   ```

Install Mobile Access Gateways (MAG) and Siteminder Assertion Packages

The steps for this procedure are different on the two Gateways of your high-availability deployment. Follow the instructions carefully.

On Gateway 1:

1. Connect with SSH.
2. Run the following commands:
   - service ssg stop
   - rpm -Uvh --nodeps ssg-mag-cloudminder_1.51-2.0-3.noarch.rpm
   - rpm -Uvh ssg-sm12-7.0-1.x86_64.rpm
3. Register the agent by running the following commands:
   - cd /opt/SecureSpan/siteminder/bin/
   - ./smreghost.sh -i <SITEMINDER-IP> -u <SITEMINDER-USER> -p <SITEMINDER-PASS> -hn <CLUSTER-HOSTNAME> -hc <SITEMINDER-CONFIG-SETTING> -cf <SITEMINDER-FIPS-MODE>

     Note: The SiteMinder values refer to the existing SiteMinder deployment for this environment.

     This command builds the SmHost.conf file.

     An example of this command is as follows:

     ./smreghost.sh -i SMPSVIP -u siteminder -p <pwd> -hn layer7 -hc DefaultHostSettings -cf COMPAT
4. Restart the service by running the following command:

   ```
   service ssg start
   ```

On Gateway 2:

1. Connect with SSH.
2. Run the following commands:
   - service ssg stop
   - rpm -Uvh --nodeps ssg-mag-2.0-1-cloudminder.noarch.rpm
   - rpm -Uvh ssg-mag-cloudminder_1.51-2.0-3.noarch.rpm
3. Restart the service by running the following command:

   ```
   service ssg start
   ```

After installing the MAG and SiteMinder assertion packages, perform the remaining configuration steps on Gateway one only. No further configuration is necessary on Gateway 2.

Install the Layer 7 License File

Note: In a high-availability environment where you have installed two gateways, perform these steps on Gateway 1 only.

Upon initial login to the Gateway, the Layer 7 Policy Manager prompts you to install your license file.

Follow these steps:

1. Navigate to the Layer 7 Policy Manager web interface at the following URL:

   https://<GATEWAY_ONE_HOSTNAME>:8443/ssg/webadmin

2. Log in using the credentials you created during installation for the Gateway admin user.

   These are the credentials you entered for SSM username and SSM password.

   Note: The Gateway includes a login security feature to prevent unauthorized access. After several failed login attempts, the system locks. After 20 minutes, the lockout timer expires and you may attempt login again.

   The Cluster License window appears.

3. Click Install License.

4. Navigate to the location where you unpacked the Layer 7 tarball and select the following license file:

   `CA_Cloudminder_MSP_SSGv7_5yr.xml`

5. Click I Agree to start the license installation.

   The Cluster License window reappears.

   Note: Installation is proceeding at this time. The system may seem unresponsive for several minutes while the installation completes. Do not attempt to interact with the system until installation is confirmed.

6. Verify that the license is valid and close the window.

Import the Certificate for the Gateway

Note: In a high-availability environment where you have installed two gateways, perform these steps on Gateway 1 only.

Import the digital certificate for the Layer 7 Gateway.

Follow these steps:

1. Select Manage, then Manage Certificates.

2. Click Add.

The Add Certificate Wizard opens.

3. Select Retrieve via SSL Connection and enter the HTTPS URL of the certificate as follows:

   `https://localhost:8443`

4. Click Next.
5. Click to Accept hostname mismatch, if applicable.
6. Leave the Certificate Name unchanged. Click Next.
7. Select the following usage options:

   Outbound SSL Connections

   Signing Certificated for Outbound SSL Connections

   Signing Client Certificates

8. Confirm that the certificate is a Trust Anchor.
9. Leave Revocation Checking as the default.
10. Click Finish.
11. Click Close.

Create Cluster Property: siteminder12.agent.configuration

Note: In a high-availability environment where you have installed two gateways, perform these steps on Gateway 1 only.

Configure the siteminder12.agent.configuration property settings for your Layer 7 Gateway node. This cluster property helps manage the interaction of the Gateway with the SiteMinder component.

If your node is part of a cluster, all other nodes in the cluster inherit the new settings as well.

Follow these steps:

1. Select Manage, then Manage Cluster-Wide Properties.
2. Click Add.

3. In the Key field, enter:

   `siteminder12.agent.configuration`

4. Navigate to the Layer 7 Gateway tarball and locate the following file in a text editor:

   `siteminder12.agent.configuration.txt`

5. Save a copy of this file. Rename the copy to reflect the name of the tenant for which you are configuring OAuth. For example:

   `siteminder12.agent.configuration.forwardinc.txt`

6. Open the file in a text editor.

7. Navigate to the following file:

   `SmHost.conf`

   Note: The SmHost.conf file is found in the same location as the smreghost script. The smreghost script runs during installation and creates the SmHost.conf file. You can find it on Gateway 1 in /opt/SecureSpan/siteminder/bin.

8. Open the file in a text editor.

9. In the SiteMinder agent configuration file, perform the following operations:

   a. Replace <SITEMINDER-AGENT> with the configured Agent ID from SiteMinder.

      This is the agent associated with all realms.

   b. Replace <SITEMINDER-IP> with the VIP or host name for the SiteMinder Policy Server listed in SmHost.conf.

   c. Replace <SITEMINDER-SECRET> with the secret listed in SmHost.conf.

      Copy and paste the secret, excluding the quotation marks (").

   d. Replace <SITEMINDER-FIPSMODE> with the FIPS mode listed in SmHost.conf.

   e. Replace <CLUSTER-HOSTNAME> with the host name listed in SmHost.conf.

   f. If required, modify other parameters. If not, leave the parameters as the default values.

      Note: The *agent.ipcheck* parameter must remain set to True.

   g. Save the SiteMinder agent configuration file, then copy the contents of the file to your clipboard.

10. In the Policy Manager, in the Value field for the siteminder12.agent.configuration property, paste the updated contents of the siteminder12.agent.configuration.txt file.

11. Click Ok.

Create Cluster Property: token.salt

Note: In a high-availability environment where you have installed two gateways, perform these steps on Gateway 1 only.

Configure the token.salt property settings for your Layer 7 Gateway node. If your node is part of a cluster, all other nodes in the cluster inherit the new settings as well.

Salt enhances the security of the token store. It is a random string that the system uses to encrypt the token store.

Follow these steps:

1. Select Manage, then Manage Cluster-Wide Properties.
2. Examine the list of properties. If token.salt already exists, skip the remainder of this process.

   If the property does not already exist, click Add.
3. In the Key field, enter:

   `token.salt`
4. In the Value field, enter a random string that will act as salt for the token store. Generate a random string by running the following on the command line:

   openssl rand -base64 32
5. Copy the output and paste it into the Value field.
6. Click Ok.

Restart Gateways

To complete the Layer 7 Gateway installation, restart the service on both Gateways by running the following command:

```
service ssg start
```

You have now completed the Layer 7 Gateway installation.

The Layer 7 Gateway is used to enable CloudMinder to act as an OAuth Authorization Server for an OAuth client. For example, if a tenant wants their users to access an OAuth client application through single sign-on, you can configure CloudMinder to validate the request for user authorization. Perform the necessary configuration for each tenant and each OAuth client application by following the steps in SSO with CloudMinder as an OAuth Authorization Server.

Chapter 3: Configuration

This section contains the following topics:

Initial Configuration

Follow these steps after you have installed all components and have confirmed that all servers are running.

Follow these steps:

1. Perform the following steps on all Oracle and PostgreSQL servers:
   a. Edit the /etc/ntp.conf file

      Add "server <*_ntp_server*>" to the list of servers

      Where <_ntp_server> is the IP address of your NTP server.

   b. Restart the ntpd service as follows:

      ```
      service ntpd restart
      ```

   c. Enable the ntpd service as follows:

      chkconfig ntpd on

2. Increase the processes and sessions for the Oracle database servers as follows:
   a. Launch SQL Plus and connect as the Oracle system database administrator.

   b. Under SQL Plus, run the following commands:

      ```
      alter system set processes=500 scope=spfile;
      alter system set sessions=824 SCOPE=spfile;
      ALTER SYSTEM SET EVENT='44951 TRACE NAME CONTEXT FOREVER, LEVEL
      1024' scope=spfile;
      shutdown immediate
      startup
      ```

3. To enable on the Oracle database transactions for Workpoint 3.5, execute the following commands, substituting an appropriate value for *Identity Management user*:

```
ALTER SYSTEM SET JAVA_POOL_SIZE=120M scope=spfile;
ALTER SYSTEM SET SHARED_POOL_SIZE=240M scope=spfile;
create pfile from spfile;
shutdown immediate;
startup;
@$ORACLE_HOME\javavm\install\initjvm.sql;
@$ORACLE_HOME\javavm\install\initxa.sql;
grant select,insert,update,delete on DBA_PENDING_TRANSACTIONS to
Identity Management user;
grant select,insert,update,delete on DBA_PENDING_TRANSACTIONS to
system;
shutdown immediate;
startup;
```

   Note:You can ignore errors such as "ORA-29539: Java system classes already installed." However, you may receive a disconnect message from the database, This error is mostly observed while executing the following command:

   ```
   @$ORACLE_HOME\javavm\install\initjvm.sql;
   ```

   If you receive this error, continue with the next SQL command:

   ```
   @$ORACLE_HOME\javavm\install\initjvm.sql;
   ```

4. To enable on the PostgreSQL database transactions for Workpoint 3.5, perform the following steps:

   a. Execute the following commands:

      ```
      export POSTGRES_HOME=PostgreSQL Installation directory
      cd $POSTGRES_HOME/data
      ```

   b. Set max_connections to a value based on the number of users to be updated with the bulk loader task. The value should be greater than the number of connections you enable in your connection pool.

   c. Update postgresql.conf to set max_prepared_transactions to the max_connections value or higher.

      If you set max_prepared_transactions to 0, you disable transactions.

   d. Restart the database as follows:

      ```
      cd $POSTGRES_HOME/bin
      ./pg_ctl restart -D $POSTGRES_HOME/data -m fast
      ```

5. For high-availability deployments, on the second SiteMinder Policy Server system only, perform these steps:

   a. Edit the following file:

      /opt/CA/AdvancedAuth/conf/arcotcommon.ini

   b. Search for InstanceId=1

c. Change the line to InstanceId=2

6. On all SiteMinder Policy Servers, restart Tomcat as follows:
   a. Navigate to /opt/CA/AdvancedAuth/Tomcat/bin
   b. (If Tomcat is already started) ./shutdown.sh
   c. ./startup.sh
7. Bootstrap the AuthMinder/RiskMinder/Advanced Authentication UDS service
   a. Connect to http://<*SiteMinder Policy Server*>:9090/arcotadmin/mabamlogin.htm using the default password: master1234!
   b. Change the default password to avoid any security loopholes.
   c. Create a global administrator for use later for configurations that are currently unavailable from the CSP console.

      Choose defaultorg as the organization and an appropriate username/password.

      Select the global administrator role, and the manages all organizations setting.

d. Log out.

e. Start webfort and riskfort, if they are not currently running, using the following commands. In a high-availability deployment, start these servers on both SiteMinder Policy Server systems.

```
cd /opt/CA/AdvancedAuth/bin
./riskfortserver start
./webfortserver start
```

8. If you restarted the database in Step 1, restart webfort and riskfort on both SIteMinder Policy Servers.

```
cd /opt/CA/AdvancedAuth/bin
./riskfortserver stop
./webfortserver stop
./riskfortserver start
./webfortserver start
```

9. For each Identity Managementserver running JBoss EAP, perform these steps:

a. Edit the jmx-console-users.properties in this location:

```
/opt/boss-eap-5.1.2/jboss-as/server/all/conf/props/
```

b. Uncomment the "#admin=admin" line.

c. Restart each Identity Managementserver in this manner:

```
service im stop
service im start
```

10. If you installed a second policy server, set fix the CHS\TWS configuration as follows:

a. Edit the following file:

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

Change IM_WEBSERVICE_HOST to the host of the second Identity Management server.

b. Restart Tomcat on the second policy server as follows:

```
/opt/CA/AdvancedAuth/Tomcat/bin/shutdown.sh
/opt/CA/AdvancedAuth/Tomcat/bin/startup.sh
```

11. On each Identity Managementserver rnnning JBoss EAP, perform these steps:

a. Restart each Identity Managementserver in this manner:

```
service im stop
service im start
```

b. Restart Tomcat on each policy server:

```
/opt/CA/AdvancedAuth/Tomcat/bin/shutdown.sh
/opt/CA/AdvancedAuth/Tomcat/bin/startup.sh
```

Web Services Authentication

To ensure that users are challenged for credentials when downloading the tenant WSDL, reset the authentication.

Follow these steps:

1. Log in to the Management Console.
2. Navigate to Environment, *Tenant_Environment*, Advanced settings.
3. In Web Services, change the SiteMinder Authentication to Other, and click Save.
4. Restart the environment.
5. Select Basic Authentication again, and click Save.
6. Restart the environment again.

Post-Installation and Upgrade Steps: User Synchronization

Following installation or upgrade, you need to set common user synchronization parameters on the Provisioning Server. In a high-availability environment, these settings are required on one of the Provisioning Server nodes. These settings do not interrupt service or require a reboot.

Follow these steps:

1. SSH into the Provisioning Server system.
2. Log in (for example, as the root user).
3. Change the user and open the bash shell with su - imps.
4. Enable the following settings by running the following commands:

   Note: _impd_etaadmin_pwd refers to the password set in the properties.sh during the Provisioning Server kit installation.

   - Automatic Correlation (See the description following these instructions for more information on each attribute.)

     ```
     etautil -u etaadmin -p _impd_etaadmin_pwd update
     'eTConfigParamFolderName=Synchronization,eTConfigParamConta
     inerName=Parameters,eTConfigContainerName=Configuration,eTN
     amespaceName=CommonObjects' eTConfigParam
     eTConfigParamName="Automatic Correlation" to
     eTConfigParamValue=yes
     ```

   - Force single account across multiple containers

     ```
     etautil -u etaadmin -p _impd_etaadmin_pwd update
     'eTConfigParamFolderName=Synchronization,eTConfigParamConta
     inerName=Parameters,eTConfigContainerName=Configuration,eTN
     amespaceName=CommonObjects' eTConfigParam
     eTConfigParamName="Force single account across multiple
     containers" to eTConfigParamValue=ActiveDirectory
     ```

   - Use Existing Accounts

     ```
     etautil -u etaadmin -p _impd_etaadmin_pwd update
     'eTConfigParamFolderName=Synchronization,eTConfigParamConta
     inerName=Parameters,eTConfigContainerName=Configuration,eTN
     amespaceName=CommonObjects' eTConfigParam
     eTConfigParamName="Use Existing Accounts" to
     eTConfigParamValue=yes
     ```

Automatic Correlation

The automatic correlation attribute enables the alternative User Synchronization behavior whereby an attempt to update an existing, uncorrelated account triggers an automatic correlation of the account to the global user prior to the update of the account. If the parameter is No (default), the attempt to update the account will fail with a message indicating the account has not yet been correlated to this global user.

Note: This setting applies to all tenants and endpoints.

Run the following command to enable the attribute:

```
etautil -u etaadmin -p _impd_etaadmin_pwd update
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Automatic
Correlation" to eTConfigParamValue=yes
```

Run the following command to read the current value of the attribute:

```
etautil -u etaadmin -p _impd_etaadmin_pwd select
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Automatic
Correlation" list eTConfigParamValue
```

Run the following command to return the value to its original configuration:

```
etautil -u etaadmin -p _impd_etaadmin_pwd update
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Automatic
Correlation" to eTConfigParamValue=no
```

Force single account across multiple containers

On some hierarchical endpoints, creates one account for a certain endpoint instance when a global user's account templates specify the same account name in different account containers (on same endpoint). In this case only one account is created despite the account container differences.

This behavior can be useful if the assigned account templates nominate different account containers on the same endpoint where you only want to create one account in one of these account containers.

Note: This setting applies to all tenants and Active Directory.

Run the following command to enable the attribute:

```
etautil -u etaadmin -p _impd_etaadmin_pwd update
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Force single account
across multiple containers" to eTConfigParamValue=ActiveDirectory
```

Run the following command to read the current value of the attribute:

```
etautil -u etaadmin -p _impd_etaadmin_pwd select
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Force single account
across multiple containers" list eTConfigParamValue
```

Run the following command to return the value to its original configuration:

```
etautil -u etaadmin -p _impd_etaadmin_pwd update
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Force single account
across multiple containers" to eTConfigParamValue=""
```

Use Existing Accounts

Enable the alternative User Synchronization behavior whereby a global user's set of assigned account templates (through assigned provisioning roles) will only attempt to prescribe one account that is correlated to the global user on any particular managed endpoint. This behavior can be useful if some accounts already correlated to the global user are named differently or are in different containers than what is prescribed by the account templates included in the global user's provisioning roles and only one account is needed or allowed. If the parameter is enabled and multiple account templates for one endpoint prescribe different names and/or different containers for the account, only one account will be created.

Note: This setting applies to all tenants and endpoints.

Run the command to enable the attribute:

```
etautil -u etaadmin -p _impd_etaadmin_pwd select
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Use Existing
Accounts" list eTConfigParamValue
```

Run the following command to read the current value of the attribute:

```
etautil -u etaadmin -p _impd_etaadmin_pwd update
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Use Existing
Accounts" to eTConfigParamValue=yes
```

Run the following command to return the value to its original configuration:

```
etautil -u etaadmin -p _impd_etaadmin_pwd update
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Use Existing
Accounts" to eTConfigParamValue=no
```

Load Balancing

To configure load balancing, make the following changes on each server.

Provisioning Servers

Create these VIPs/Pools on each server:

- CA IAM CS Requests over port 22001 – Used to talk to on-premise CA IAM CS
- CA IAM CS over port 20080 – Used for accessing the Connector Server Admin console
- CA IAM CS over port 20410 – Used for configuring connxp for acquiring the endpoint required for Directory Sync.
- CA IAM CS over port 20498 – Used for the Directory Sync from On-premise to Cloud.

SiteMinder Policy Server and Advanced Authentication

Make the following changes on each SiteMinder Policy Server.

Create these VIPs/Pools:

- SiteMinder Policy Server over port 44441 – This is for the agent to communicate with the Policy Server
- SiteMinder Policy Server over port 44442 - This is for the agent to communicate with the Policy Server
- SiteMinder Policy Server over port 44443 - This is for the agent to communicate with the Policy Server
- Authminder over port 9090 – Used for connecting to Arcot Admin Console
- Authminder over port 9745 – Used by Authminder Admin Service

- Authminder over port 9742 – Used by Authminder server for issuance
- Riskminder over port 7680 – Used by RiskMinder

Make the following file and configuration changes.

1. Log in to the Arcot Administration console as master admin.
   a. Navigate to Services and Server Configurations, Administration Console, UDS Connectivity
   b. Change the hostname from localhost to the internal host (SiteMinder Policy Server Load Balancer).
   c. Refresh the caches of AuthMinder and RiskMinder (WebFort and RiskFort).
2. Edit /opt/CA/siteminder/arcot/conf/adaptershim.ini
   a. For each authscheme entry, the following properties have the URL for end user browser redirects:

   AuthSchemeParam, ArcotAFMLandingURL, ErrorPageURL, InitialFCCURL, FinalFCCURL

   - Replace all Secure Proxy Server hostnames with your Secure Proxy Server load balancer VIP in the URL.
   - Change http to https.

   b. For each authscheme entry, the following properties have the URL for internal calls:

   ArcotSMBaseURL

   - Replace all localhost with your SiteMinder Policy Server load balancer VIP.
   - Do not change http.

3. Edit /opt/CA/AdvancedAuth/Tomcat/webapps/tenant-services/WEB-INF/classes/resources/config.properties
   - Replace the internal Identity Management base URL with the Identity Management load balancer, as follows:

     imBaseURL=http://<*Identity Management load balancer VIP*>:8080/iam/im
4. Copy the Secure Proxy Server load balancer SSL certificate and import it to the Java key store. Import it to the Java key store that is used by Tomcat.

Make these changes to the Advanced Authentication database:

1. In the table AOK_SYSTEM_DATA
   a. Change com.ca.cm.sso.ShimTokenServer to your SiteMinder Policy Server load balancer VIP
   b. Change com.ca.cm.uds to your SiteMinder Policy Server load balancer VIP
   c. Change webfort to your SiteMinder Policy Server load balancer VIP

2. In the table AOK_OVERLOADED_PROPS

   a. Change tws.base.url to http://<SMPS LB VIP>:9090/tenant-services/cm/tenantws

3. Restart the SiteMinder Policy Server, Tomcat, and the Secure Policy Server.

Secure Proxy Server

Make the following changes on each Secure Proxy Server.

Create these VIPs/Pools:

Secure Proxy Server over port 443 with offload to port 80 on Secure Proxy Server – used for all communication through Secure Proxy Server.

Make the following file and configuration changes.

1. Edit /opt/CA/secure-proxy/proxy-engine/conf/server.conf

   Add your Secure Proxy Server Load Balancer VIP with the domain to the hostnames under VirtualHost section

2. Edit /opt/CA/secure-proxy/proxy-engine/conf/proxyrules.xml

   a. Change the Identity Management Server hostname to your Identity Management Server Load Balancer VIP

   b. Change CA IAM CS hostname with port 20080 to your CA IAM CS Admin Load Balancer VIP

   c. Change CA IAM CS hostname with port 20001 to your CA IAM CS Request Load Balancer VIP

3. Edit /opt/CA/secure-proxy/Tomcat/webapps//chs/WEB-INF/classes/config/chsConfig.properties

   Change tenantwebservicebaseurl=http://SiteMinder Policy Server LB VIP:9090/tenant-services/cm/tenantws

4. Edit /opt/CA/secure-proxy/proxy-engine/conf/defaultagent/SmHost.conf

   Change policyserver="SiteMinder Policy Server Load Balancer VIP,44441,44441,44441"

5. Copy the Secure Proxy Server Load Balancer VIP SSL certificate and import it to the Java key store. Import it to the Java key store that is used by Tomcat.

   Use the command: keytool -import -alias <*any name*> -keystore cacerts -file <*certificate file*>

6. Edit /opt/CA/secure-proxy/Tomcat/properties/instance.properties

   The value of the property service.host should be the internal host (SiteMinder Policy Server Load Balancer)

7. Restart the Secure Proxy Server.

Identity Management Server

Make these changes on each Identity Management Server.

Create these VIPs/Pools on each server:

Identity Management Server over port 8080 - used for communicating with the Identity Management Server

Make the following file and configuration changes.

1. Edit /opt/jboss-5.1.0.GA/server/all/deploy/iam_im.ear/policyserver.rar/META-INF/ra.xml

   Change <config-property-value>*Secure Proxy Server Load Balancing VIP*,44441,44441,44441</config-property-value>

2. Restart the Identity Management server by running the following commands:

   ```
   /etc/init.d im stop
   /etc/init.d/im start
   ```

3. If you have deployed any tenants, modify the Advanced Authentication Connection for the tenant:

   a. Log in to the User Console.

   b. Go to Advanced Authenication, Configure AuthMinder Connection

c. Change the AuthMinder Host Name to the VIP for the SiteMinder Policy Server

http://*<SiteMinder Policy Server Load Balancer VIP>*

CSP console

Be sure to make the following changes before creating any tenant:

1. In the CSP console navigate to Infrastructure, Hosts, Host Configuration Objects
2. Click DefaultHostSettings, then click Modify.
   a. Under Configuration Values, delete all individual hosts.
   b. Add your SiteMinder Policy Server Load Balancer VIP. Enter port 44441 for all port values.
   c. Uncheck Enable Failover.
   d. Click Submit.
3. Navigate to Tenants, Manage Hosting Containers.
4. From the drop-down menu, select Modify Hosting Container for your host.
   a. Change Environment Base URL to *https://<Secure Policy Server Load Balancer VIP>*/iam/im
   b. Change Internal Base URL to http://*<Identity Management Load Balancer VIP>*:8080/iam/im

c. Change AuthMinder Host to http://<*SiteMinder Policy Server Load Balancer VIP*>

5. Configure Siteminder to use the load balancer IP address.
   a. Click Infrastructure, Agent, Agent Configuration Objects.
   b. Modify the AgentConfigurationObject being configured for the Secure Proxy Server.
   c. Set the CustomIpHeader to HTTP_ORIGINAL_IP.
   d. Click Save.

Configure SSL from Secure Proxy Server to Identity Management Load Balancer

Network traffic coming from Secure Proxy Server to the load balancer must use SSL. Traffic coming from the load balancer to Identity Management is non-SSL. Perform the following steps to configure this transform from SSL to non-SSL through the load balancer.

1. Create a new virtual server for SSL traffic, port 8443, and assign it to the same pool that was being used for port 8080 to Identity Management.
2. Create a certificate for the Identity Management VIP.
3. Create SSL profile (client). Use the certificate created in the load balancer for the Identity Management VIP.
4. Export the certificate from the Identity Management load balancer to all Secure Proxy Servers:

   /opt/CA/secure-proxy/SSL/certs
5. Run the following command from the above location, on all Secure Proxy Servers:

   openssl x509 -in IM_LB1-<*Your VIP*>.crt -text >> ca-bundle.cert
6. Edit the following file on all Secure Proxy Servers:

   /opt/CA/secure-proxy/proxy-engine/conf/proxyrules.xml

   Update the file to use port 8443 (rather than port 8080), and to use https (rather than http), as follows:

   <nete:case value="/iam/im/">

   <nete:forward>https://<Identity_Management_fully_qualified_domain_name>:8443$0</nete:forward>
7. Restart the Secure Proxy Server using startssl.

High-Availability: Network Peers for Connector Servers

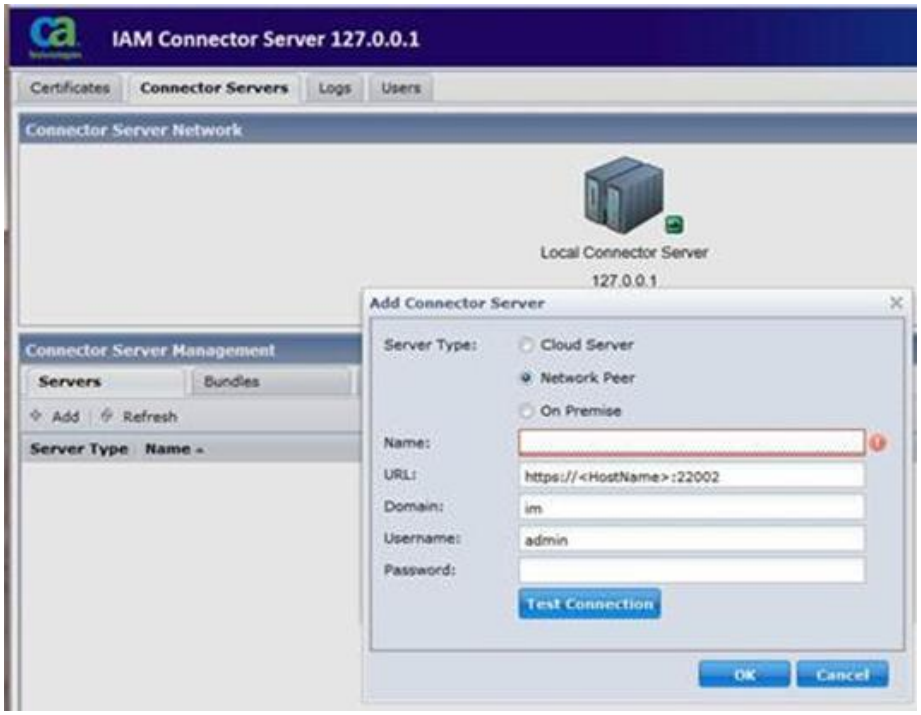
In a high-availability deployment, CA IAM CS systems are load balanced. The load balanced CA IAM CS systems need to be configured as network peers so that they can share configuration and requests. For this procedure, you use the management console of each connector server. Do not access the management console through the Apache server.

Follow these steps:

Log in to the CA IAM CS console using the admin/eTrust01 account.

1. Select the Servers tab.
2. Select the Add button to add a new server.
3. When the Add Connector Server dialog appears, select the Network Peer radio button.

Equation 2: Connector Server UI



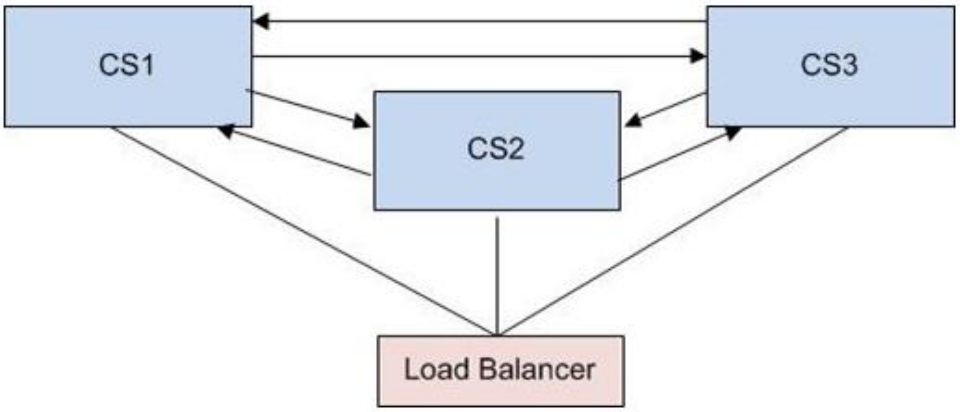
4. Enter the details.

   The domain can usually be left unchanged.

5. Select Test Connection to make sure a connection can be established between the connector servers
6. Select OK

Each of the other peers must be added. If a connection cannot be established, check that the clocks on the peers are synchronized. Use the following diagram as an example:

Equation 3: Synchronize Connector Servers

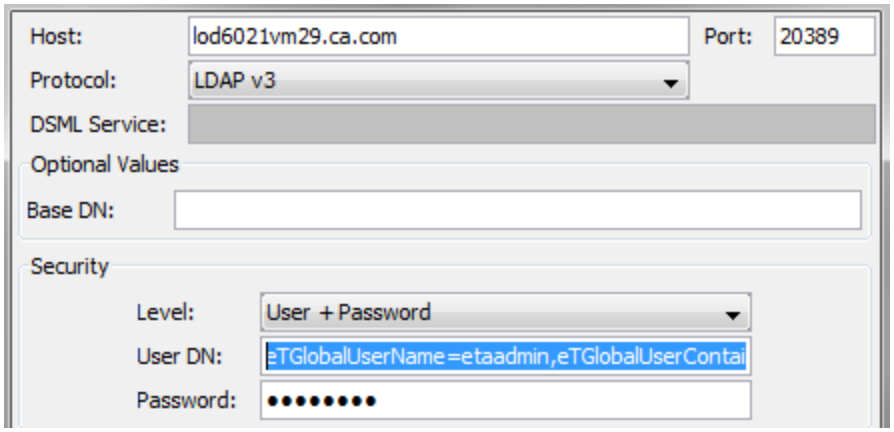


- A peer configuration for CS2 and CS3 must be added to CS1
- A peer configuration for CS1 and CS3 must be added to CS2
- A peer configuration for CS1 and CS2 must be added to CS3
- The three connector servers should be configured as a load balanced cluster in the apache HTTP server

Password Synchronization

To implement password synchronization, you may need to modify the agent response threshold. The default value is 600 seconds, or 10 minutes. You can modify this threshold by connecting to the Provisioning Server from an LDAP browser such as JXplorer.

Log into the LDAP browser using the following fields on the login screen:



Host

The host name of the Provisioning Server.

Port

20389

Level

Username + password

User DN

eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=im,dc=eta

Password

The password used for the _impd_etaadmin_pwd in the Provisioning Server installation.

The agent response threshold is the maximum expected duration of each password change that the Provisioning Server sends to a managed endpoint on which a password synchronization agent is installed. This parameter allows the Provisioning Server to recognize when a Password Synchronization agent is processing a password change that is sent to it by the Provisioning Server as distinct from a password change originating on that managed endpoint.

If, during the Agent Response Threshold, a password other than the password just sent to the managed endpoint is provided in a password validation or password change notification, this password is rejected. Two concurrent password changes to the same account are not allowed.

In the LDAP browser, navigate to the following location to set this parameter:
`eta, im, Commonobjects, Configuration, Parameters, Password Synchronization, Agent Response Time`

Enable Explore and Correlate Tasks

If you decide tenant administrators should be allowed to run Explore And Correlate Definition tasks, log in to the User Console as the CSP admin. Modify the Tenant Provisioning Manager admin role and add the following tasks:

- Create Explore And Correlate Definition
- Modify Explore And Correlate Definition
- Delete Explore And Correlate Definition

Identity Management Sensitive Tasks

Follow these steps:

1. Enable ODBC Session Store Policy Servers as follows:
   a. Set the X11 DISPLAY variable.
   b. Issue the command: /opt/CA/siteminder/bin/smconsole
2. Login to CSP console and use the Modify Agent Configuration task.
   Select CAM-AgentObj and make sure that the FCCCompatMode is set to no.
3. Create a response *Response* in domain *tenant*Domain and create the following attribute:
   - Attribute: WebAgent-OnReject-Redirect
   - Attribute Kind: Static
   - Variable Value: /siteminderagent/forms/reauthenticate.fcc:validate
4. Create a policy *Policy* in the domain *tenant*Domain.
5. Select Add All for User Directories.

6. Add two rules in tenant_ims_realm:

```
<Rule1>:
Resource:        *task.tag=ChangeMyPassword
   Regular Expression: checked
   Action:                   Web Agent Actions, GET and POST
<Rule2>:
Resource:        *task.tag=ChangeMyPassword
   Regular Expression: checked
   Action:                   Authorization events,
OnAccessValidateIdentity
```

7. Add the response *Response* to *Rule2.*
8. Commit the creation.
9. In the Policy Server, run the command tool xpsexplorer and make the following change:
   a. Modify policy *Policy*, set ValidateIdentity to true.
   b. Restart each policy server configured for high availability.
   c. Restart policy engine in each Secure Proxy Server configured for high availability.

Maximum Number of Tenants

CA CloudMinder limits the number of tenants to 10. However, you can increase that limit.

Follow these steps:

1. Edit the following file:

```
/opt/CA/siteminder/adminui/server/default/deploy/iam_siteminder
.ear/management_console.war/WEB-INF/web.xml
```

2. Set AccessFilter to enabled:

```
<filter>
  <filter-name>AccessFilter</filter-name>

<filter-class>com.netegrity.ims.manage.filter.AccessFilter</fil
ter-class>
  <init-param>
    <param-name>Enable</param-name>
    <param-value>true</param-value>
  </init-param>
</filter>
```

3. Save the web.xml.
4. Stop the application server:

   ```
   /opt/CA/siteminder/adminui/bin/shutdown.sh –S
   ```

5. Start the application server:

   ```
   nohup /opt/CA/siteminder/adminui/bin/run.sh &
   ```

6. Export the role definitions for the CSP console:
   a. Access the Management Console.
   b. Select Environments, SiteMinder, Role and Task Settings, Export.
   c. Save SiteMinder-RoleDefinitions.xml
   d. Edit SiteMinder-RoleDefinitions.xml
   e. Edit the screen field for Maximum Tenants on Create Hosting Container Profile Screen to have options for all possible values of max tenants:

```
     <ScreenField name="Maximum Tenants" permission="RWM"
attribute="maxTenants">
        <PropertyDict name="Config">
          <Property name="allowNonOptions">1</Property>
          <Property name="CSSStyle"></Property>
          <Property name="DefaultValue"></Property>
          <Property
name="DefaultValueJavaScript"><![CDATA[]]></Property>
          <Property name="FieldSpan">1</Property>
          <Property
name="InitJavaScript"><![CDATA[]]></Property>
          <Property name="LabelRight"></Property>
          <Property name="LabelSpan">1</Property>
          <Property name="Options"><![CDATA[1
220]]></Property>
          <Property name="optionsMethod">Options</Property>
          <Property name="SCREENLOGICAL">true</Property>
          <Property name="Style">Dropdown</Property>
          <Property
name="StyleClass">im-autoFormField</Property>
          <Property name="ValidateOnChange">0</Property>
          <Property
name="ValidationExpression"><![CDATA[]]></Property>
          <Property name="ValidationJava"></Property>
          <Property
name="ValidationJavaScript"><![CDATA[]]></Property>
        </PropertyDict>
      </ScreenField>
```

7. Edit the screen field for Maximum Tenants on Default Hosting Container Profile Screen to have script for generating all possible values of max tenants:

```
      <ScreenField name="Maximum Tenants" permission="RWM"
attribute="maxTenants">
        <PropertyDict name="Config">
          <Property name="allowNonOptions">1</Property>
          <Property name="CSSStyle"></Property>
          <Property name="DefaultValue"></Property>
          <Property
name="DefaultValueJavaScript"><![CDATA[]]></Property>
          <Property name="FieldSpan">1</Property>
          <Property
name="InitJavaScript"><![CDATA[]]></Property>
          <Property name="LabelRight"></Property>
          <Property name="LabelSpan">1</Property>
          <Property name="optionsMethod">jsOptions</Property>
          <Property name="jsOptions"><![CDATA[function
getOptions(ctx) {
  var state = ctx.getProfileObject().getAttribute("state");
  var maxTenants = 1;
  if (!"INACTIVE".equals(state) && !"FAILED".equals(state)) {
    maxTenants = java.lang.Integer.parseInt(
ctx.getProfileObject().getLastCommittedAttribute("maxTenants")
);
  }
  var options = maxTenants;
  for (i=maxTenants+1 ; i<=20 ; i++) {
    options += "|";
  options += i;
  }
  return options;
}
]]></Property>
          <Property name="SCREENLOGICAL">true</Property>
          <Property name="Style">Dropdown</Property>
          <Property
name="StyleClass">im-autoFormField</Property>
          <Property name="ValidateOnChange">0</Property>
          <Property
name="ValidationExpression"><![CDATA[]]></Property>
          <Property name="ValidationJava"></Property>
          <Property
name="ValidationJavaScript"><![CDATA[]]></Property>
        </PropertyDict>
      </ScreenField>
```

8. Save SiteMinder-RoleDefinitions.xml
9. Import the role definitions for the CSP console.
   a. Access the Management Console.

b. Select Environments, SiteMinder, Role and Task Settings, Import.

c. Select SiteMinder-RoleDefinitions.xml and click Finish.

d. Restart the environment in the Management Console.

2-Way SSL for Adeptra Voice Service

Follow these steps:

1. Get the external IP of the system (the IP as seen by Adeptra, not the internal IP) whitelisted by Adeptra.
2. Obtain the keystore and certificate for the test environment from CA Support.
3. Connect to the AA DB using SQLDeveloper.

   SQLPlus will not work since blob uploads are involved.
4. Obtain the certificate from Adeptra and generate the key.

   Pass the corresponding certificate to Adeptra through the person managing the partnership account.
5. Update the keystore for 2 way SSL as follows:
   a. Open the table AOK_SYSTEM_DATA.
   b. Find the row with (NAME='ws.client.keystore'), and upload the wskey.keystore file to the column VALUEBLOB.

      The keystore should be in JKS format.The key alias and password should match the value in the row with name='ws.client.keystore.pwd'
6. Update certificate for 2 way SSL
   a. Open the table AOK_SYSTEM_DATA.
   b. Change directory to the row with (NAME='adeptra.cert') and upload the Adeptra.der certificate file to the VALUEBLOB column.

      The certificate should be in binary der format.

Chapter 4: Logs

This section contains the following topics:

Provisioning Server Logs

The Provisioning Server generates logs in the following locations:

- On the Provisioning Server:
  - **Location:**

    /opt/CA/IdentityManager/ProvisioningServer/logs

    Logs:

    Etanotify*date-time*.log

    Etatrans*date-time*.log

    im_ps.log
- On the Directory Server:
  - Location:

    /opt/CA/Directory/dxserver/logs

    Logs

    ProvisioningServerHostName-imps-router_*date*.log

    ProvisioningServerHostName-imps-router_alarm.log

    ProvisioningServerHostName-imps-router_diag_*date*.log

    ProvisioningServerHostName-imps-router_stats_*date*.log

    ProvisioningServerHostName-imps-router_time_*date*.log

    ProvisioningServerHostName-imps-router_trace.log

    ProvisioningServerHostName-imps-router_warn_*date*.log

CA IAM CS Logs

The CA IAM CS generates logs in the following locations:

- On the Connector Server:
  - **Location:**

    /opt/CA/IdentityManager/ConnectorServer/jcs/logs

    Logs:

    jcs_daily.log

    jcs_stderr.log

    jcs_stdout.log

    servicemix.log
- On the Directory Server:
  - **Location:**

    /opt/CA/Directory/dxserver/logs

    Logs:

    ProvisioningServerHostName-imps-router_*date*.log

    ProvisioningServerHostName-imps-router_alarm.log

    ProvisioningServerHostName-imps-router_diag_*date*.log

    ProvisioningServerHostName-imps-router_stats_*date*.log

    ProvisioningServerHostName-imps-router_time_*date*.log

    ProvisioningServerHostName-imps-router_trace.log

    ProvisioningServerHostName-imps-router_warn_*date*.log

CA Directory Logs

CA Directory generates logs in the following location on the Directory server machine:

- **Location:**

  /opt/CA/Directory/dxserver/logs

  Logs:

  tenant-*tenantName*-*DirHostName*_diag_*date*.log

  tenant-*tenantName*-*DirHostName*_stats_*date*.log

  tenant-*tenantName*-*DirHostName*_summary_*date*.log

  tenant-*tenantName*-*DirHostName*_trace.log

  tenant-*tenantName*-*DirHostName*_warn_*date*.log

  DirHostName-cam-tenant-*tenantName*_summary_*date*.log

  DirHostName-cam-tenant-*tenantName*_warn_*date*.log

  DirHostName-cam-tenant-*tenantName*_stats_*date*.log

  DirHostName-cam-tenant-*tenantName*_diag_*date*.log

  DirHostName-cam-tenant-*tenantName*_trace.log

  DirHostName-cam-tenant-*tenantName*_alarm.log

DirHostName-impd-main_warn_*date*.log

DirHostName-impd-main_trace.log

DirHostName-impd-main_time_*date*.log

DirHostName-impd-main_diag_*date*.log

DirHostName-impd-main_*date*.log

DirHostName-impd-main_stats_*date*.log

DirHostName-impd-inc_stats_*date*.log

DirHostName-impd-inc_diag_*date*.log

DirHostName-impd-inc_warn_*date*.log

DirHostName-impd-inc_trace.log

DirHostName-impd-inc_time_*date*.log

DirHostName-impd-co_warn_*date*.log

DirHostName-impd-co_trace.log

DirHostName-impd-co_diag_*date*.log

DirHostName-impd-co_time_*date*.log

DirHostName-impd-co_*date*.log

DirHostName-impd-co_stats_*date*.log

DirHostName-impd-notify_diag_*date*.log

DirHostName-impd-notify_*date*.log

DirHostName-impd-notify_warn_*date*.log

DirHostName-impd-notify_trace.log

DirHostName-impd-notify_time_*date*.log

DirHostName-impd-notify_stats_*date*.log

CA SiteMinder Logs

CA SiteMinder generates logs in the following locations:

- On the Policy Server:
  - **Location:**

    /opt/CA/siteminder/log

    Logs:

    smps.log

    smaccess.log

    smexec.log
  - **Location:**

    /opt/CA/siteminder/adminui/server/default/log

    Log:

    server.log
  - **Location:**

    /opt/CA/AdvancedAuth/logs/

    Logs:

    arcotriskfortcasemgmtserver.log

    arcotriskfortcasemgmtserverstartup.log

    arcotriskfort.log

    arcotriskfortstartup.log

    arcotwatchdog.log

    arcotwebfort.log

    arcotwebfortstartup.log

- **Location:**

  /opt/CA/AdvancedAuth/Tomcat/logs

  Logs:

  catalina.*date*.log

  catalina.out

  host-manager.*date*.log

  localhost.*date*.log

  localhost_access_log.*date*.txt

  manager.*date*.log

  cm-aads.log

- **Location:**

  /opt/CA/

  Log:

  Twslogging.log

- On the Directory Server:
  - **Location:**

    /opt/CA/Directory/dxserver/logs

    Logs:

    SMPSHostName-cam-tenant-router_trace.log

    SMPSHostName-cam-tenant-router_alarm.log

    SMPSHostName-cam-tenant-router_diag_*date*.log

    SMPSHostName-cam-tenant-router_warn_*date*.log

    SMPSHostName-cam-tenant-router_summary_*date*.log

    SMPSHostName-cam-tenant-router_stats_*date*.log