# HP Universal CMDB Configuration Manager

For the Windows and Linux operating systems

Software Version: 9.30

# Deployment Guide

Document Release Date: November 2011

Software Release Date: November 2011

# Legal Notices

## Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

## Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Copyright Notice

## Trademark Notices

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

# Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

**http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

**http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

# Support

Visit the HP Software Support Online web site at:

**http://www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

**http://h20229.www2.hp.com/passport-registration.html**

To find more information about access levels, go to:

**http://h20230.www2.hp.com/new_access_levels.jsp**

# Contents

# Installation and Configuration

# Chapter 1

## Overview

This chapter includes:

## Components

HP Universal CMDB Configuration Manager is a joint release of several components:

- **HP Universal CMDB foundation**

  HP Universal CMDB foundation (UCMDB foundation) is a configuration management database (CMDB) for enterprise IT organizations to document, store, and manage business service definitions and associated infrastructure relationships.

  UCMDB foundation implements a data model, data flow management, and data modeling capabilities, and also provides impact analysis, change tracking, and reporting capabilities in order to transform CMDB data into comprehensible, actionable information that helps answer critical questions and solve business problems.

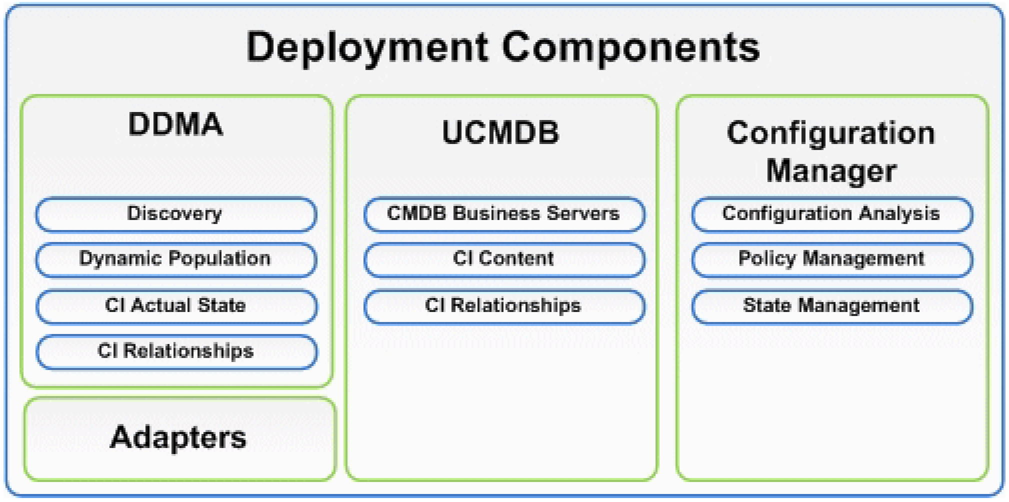
- **HP Universal CMDB Configuration Manager**

  HP Universal CMDB Configuration Manager (Configuration Manager) introduces new policy-based topology and inventory configuration governance. Created specifically for configuration managers and configuration owners, it allows these users to perform though analysis in addition to the CI data and topology content available in or through UCMDB. Configuration Manager provides configuration managers and owners the required tools for easily setting up both topology and inventory configuration policies, as well as automatically determining their level of compliance to organizational standards.

  Configuration Manager is deployed as an additional Tomcat-based server. It communicates with the UCMDB server using the extensive UCMDB SDK.

- **HP Discovery and Dependency Mapping Advanced Edition**

  HP Discovery and Dependency Mapping Advanced Edition (DDMA) software, with rich and constantly updated content, is UCMDB's preferred method for acquiring and maintaining the IT



## Identify Your Environment

This guide describes the process of deploying HP Universal CMDB Configuration Manager from different possible starting points:

### For Configuration Manager

- If Configuration Manager version 9.10 or 9.20 is installed

  For details about upgrading Configuration Manager to the current version, see "Upgrade Configuration Manager" (on page 34).

- If Configuration Manager is not installed

  For details, about installing Configuration Manager, see "Install HP Universal CMDB and Configuration Manager Using the Deployment Manager for Windows" (on page 14)

### For UCMDB

- If a version of UCMDB earlier than 9.03 with CUP 2 is installed

  Do the following:

  - Upgrade to UCMDB version 9.04. For details, see the *HP Universal CMDB Deployment Guide*. You can download the manual from www.hp.com/go/hpsoftwaresupport.
  - Install the latest Cumulative Update Pack. You can either obtain the CUP from the Configuration Manager installation media, or download it from www.hp.com/go/hpsoftwaresupport.

- If UCMDB version 9.04 is installed

  Install the latest Cumulative Update Pack. You can either obtain the CUP from the Configuration Manager installation media, or download it from www.hp.com/go/hpsoftwaresupport.

- If no version of UCMDB is installed

  Use the Deployment Manager to install UCMDB at the same time that you install Configuration Manager. For details, see "Install HP Universal CMDB and Configuration Manager Using the Deployment Manager for Windows" (on page 14).

### General Information

This guide also takes into account special UCMDB deployments you may have in your environment (for example, high availability deployment) and provides the necessary adjustments to the deployment procedure for those deployments.

> **Note:** Installing both UCMDB and Configuration Manager together on the same server is supported. For scaling purposes in a production environment, HP Software recommends that you install these components on separate servers.

Using Configuration Manager requires that UCMDB is configured with a consolidated schema mode and that a new UCMDB state created (Authorized state). These configurations are performed automatically by the deployment procedure in both installation cases (whether an installation of UCMDB already exists or if it is installed by the Deployment Manager).

> **Note:** If you reference an existing UCMDB installation and its schema is not already consolidated, the consolidation step may take a long time (20 to 60 minutes) for heavily populated databases (those that contain more than 5 million CIs).

Be aware that if you are deploying only Configuration Manager (that is, using an existing or upgraded installation of UCMDB), the UCMDB server must be running to complete the installation of Configuration Manager.

## Support Matrix

### Server System Requirements

| | |
|---|---|
| CPU | Minimum 4 core |
| Memory (RAM) | Minimum of 4 GB |
| Free Disk Space | Minimum of 4 GB |
| Platform | x64 |
| Operating System | Windows (64-bit)<br>• Windows Server 2003 EE SP2<br>• Windows Server 2003 5.2 EE SP2<br>• Windows Server 2008 EE R2<br>• Windows Server 2008 EE R2 SP1<br>Linux (64-bit)<br>• Red Hat Enterprise Linux 6.1 |

| | |
|---|---|
| Database | Microsoft<br>• Microsoft SQL Server 2005 SP4<br>• Microsoft SQL Server 2008 SP2 EE<br>• Microsoft SQL Server 2008 R2<br>• Microsoft SQL Server 2008 R2 SP1 EE<br>Oracle<br>• Oracle 10.2.0.1.0 EE<br>• Oracle 10.2.0.4.0 EE<br>• Oracle 11.1.0.7.0 EE<br>• Oracle 11.2.0.1.0 EE<br>• Oracle 11.2 RAC EE |
| Web Server | • Microsoft IIS 7<br>• Apache 2 |
| HP Universal CMDB | HP Universal CMDB version 9.03 with CUP 2, or any subsequent release with the latest CUP (typical CMDB installation)<br>• Minimum of 3 GB disk space<br>• Minimum of 3 GB of RAM<br>For a full list of system requirements, refer to the *HP Universal CMDB Deployment Guide.*<br>**Note:**<br>• When the HP Universal CMDB server is deployed in combination with Configuration Manager, the Enterprise Edition of Oracle and the Oracle Partitioning option are required.<br>• If you previously deployed the HP Universal CMDB server with the Standard Edition of Oracle, and you intend to add Configuration Manager to your installation, you must first convert your Standard Edition database to an Enterprise Edition database with the Partitioning option enabled. |
| LDAP (optional) | • Active Directory<br>• SunONE 6.x |
| Minimum Recommended Database Schema Size (optional) | 2 GB |

## Client Requirements

| | |
|---|---|
| Operating System | - Windows XP x86 (32-bit)Windows<br>- Vista x86 (32-bit and 64-bit)<br>- Windows 7 x86 (32-bit and 64-bit) |
| Browser | - Microsoft Internet Explorer 7.0, 8.0, 9.0<br>- Mozilla Firefox 3.x and later<br>- Google Chrome 15.0 |
| Flash Player Browser Plugin | Flash Player 9.x, 10.x, or 11<br>**Note:** Download Flash Player from: http://www.adobe.com/products/flashplayer/. |
| Screen Resolution | - Minimum 1024x768<br>- Recommended 1280x1024 |
| Color Quality | Minimum of 16 bit |

## HP Operations Orchestration (optional)

| | |
|---|---|
| HP Operations Orchestration | 9.0 |

## HP Service Manager (optional)

| | |
|---|---|
| HP Service Manager | 9.20 or 9.30 |

# Chapter 2

# Install HP Universal CMDB and Configuration Manager Using the Deployment Manager for Windows

**Note:** Be sure to see the release notes for the most updated installation instructions.

This chapter includes:

## Introduction

The Deployment Manager for Windows enables you to install and configure Configuration Manager, together with its associated components (UCMDB and DDMa) at the same time.

The Deployment Manager must be executed on a Windows machine, and can install the associated components on any other Windows machine or system.

For information about all of the components that can be installed, see "Components" (on page 9).

For details about installation of Configuration Manager on a Linux system, see "Install Configuration Manager Using the Standalone Installer on a Linux or Windows System" (on page 28).

## Pre-Installation Setup

### Manually Configure the Database or User Schema (optional)

**Note:** You can either use the Deployment Manager to create a database or user schema, or perform the task manually if you choose to do so.

To work with Configuration Manager, you must provide a database schema. Configuration Manager and UCMDB use different schemas. Configuration Manager supports Microsoft SQL Server and Oracle Database Server. This task describes how to create a schema for Configuration Manager. If you are installing UCMDB, you will need to set up a separate database or user schema for it as well. For details, see the *HP Universal CMDB Deployment Guide*.

Alternatively, if you install CM or UCMDB using the deployment manager, you can use the deployment manager to create a new database or user schema

**Note:** For Microsoft SQL Server and Oracle Server system requirements, see "Server System Requirements" (on page 11).

**To configure your database:**

1. Allocate a Microsoft SQL Server database or an Oracle Server user schema.

    - For **Microsoft SQL Server**: Activate snapshot isolation.

      Execute the following command once after creating the database:

      ```
      alter database <ccm_database_name> set read_committed_snapshot on
      ```

      For more information about the SQL Server snapshot isolation feature, see http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx.

    - For **Oracle**: Assign the Oracle schema user the **Connect** role, and the **Create Procedure**, **Create Sequence**, **Create Table**, **Create Trigger**, **Create View**, and **Unlimited Tablespace** system privileges. The database administrator must also provide the names of the **Default Tablespace** and **Temporary Tablespace** that can be used for the schema. (Granting the **Select any table** privilege causes the schema population procedure to fail).

2. Verify the following information, which you need during this configuration process:

| | Required Information |
|---|---|
| | DB host name and port |
| | **For MSSQL**: DB username and password<br>**For Oracle**: Schema name and password |
| | **For MS SQL**: Database name |
| | **For Oracle**: SID<br>If you are creating a new Oracle schema using the Deployment Manager, you also need the following information:<br>▪ DB Administrator username & password<br>▪ Default and temporary tablespace |

**Note:** HP Software recommends that you set up your database on the same subnetwork on which Configuration Manager is installed.

## Install Configuration Manager When an Existing UCMDB Installation is Configured for High Availability

To use Configuration Manager in a UCMDB High Availability environment, proceed with the following steps:

1. Shut down the backup (passive) server. Wait for two minutes after shutting down.

2. Install only the Configuration Manager version 9.30 component, as described in "Install Configuration Manager With or Without Other Components" (on page 16).

   Install Configuration Manager version 9.30 on a third server (not on either of the UCMDB servers). Use your load balancer host details when asked for the UCMDB connection details.

3. Start the backup (passive) UCMDB server to provide high availability only when you have ensured that UCMDB and Configuration Manager are working properly.

> **Note:** High Availability mode is not supported for HP Universal CMDB Configuration Manager version 9.30 itself.

## Install Configuration Manager With or Without Other Components

The Deployment Manager can install UCMDB, Configuration Manager, and DDMA in different configurations (chosen and configured in the Products Selection page of the installation wizard):

- Installing a new instance of UCMDB version 9.04 with CUP3
- Installing a new instance of Configuration Manager and connecting it to either a new or existing instance of UCMDB
- Integrating a new instance of Configuration Manager to an existing instance of OO
- Installing multiple instances of DDMA

> **Note:**
>
> - The Deployment Manager provides you with the ability to install products, components, and integrations on a remote or local target machine. Uninstalling products, modification of products, and patch installation on an installed product is not supported by the Deployment Manager, and must be performed manually.
> - Once the **Next** button is pressed in the Product Selection page, you cannot go back to that page and re-select the deployment configuration. If changes need to be made to the deployment configuration, restart the Deployment Manager.

**To install Configuration Manager on a Windows system:**

1. To start the installation, insert the Configuration Manager installation media into the machine.
2. Extract the contents of **HP_UCMDBCM_9.30.zip** to a temporary directory.
3. Locate the **setup.exe** file and do one of the following:
   - Double-click the **setup.exe** file.
   - Right-click the **setup.exe** file and select **Run as Administrator**.
4. Disable the Windows firewall on the remote or local target machine for the duration of the installation.
5. Accept the terms of the End User License Agreement and click **Next** to open the Product Selection page.

   > **Note:** The terms of license agreement apply to all of the products selected in the Product Selection page of the Deployment Manager.

6. Select the required products for deployment on the Product Selection page. When finished, click **Next** to continue to the Server Location page.

The Product Selection page enables you to select the products that you want to install, and specify the configuration options that are performed during deployment.

a. Select an HP Universal CMDB foundation installation option.

   There are two UCMDB foundation installation options available:

   - **Connect to an Existing Server** – When selected, this option connects and configures Configuration Manager or Discovery and Dependency Mapping to an existing instance of a UCMDB foundation server.

     > **Note:** The UCMDB version on an existing server must be version 9.03 with CUP 2, or any subsequent release with the latest CUP.

   - **Install New Server** – when selected, this option installs, configures, and connects a new instance of a UCMDB foundation server version 9.04 with CUP3, and configures and connects Configuration Manager or DDMA to the new instance of the UCMDB foundation server.

b. Select the **Configuration Manager** checkbox to install and configure a new instance of Configuration Manager.

   If desired, select **Connect to an Existing HP Operation Orchestration instance**. This option configures an integration between Configuration Manager and Operations Orchestration by populating Configuration Manager with the OO server connection details.

c. Discovery and Dependency Mapping Advanced Edition**.** When selected, this option installs and configures new instances of DDMA version 9.04.

   The **Number of DDMA instances** option enables you to install multiple DDMA instances. The number specified in the input field indicates the number of DDMA instances connected to a single UCMDB server instance.

   > **Note:** The Deployment Manager supports multiple deployments of DDMA instances in the same DMZ. Deployment Manager supports a maximum number of 10 instances of discovery probes in each deployment. If additional discovery probes are required, install them in multiple deployment phases in groups of ten.

7. Specify the remote Windows servers location and credentials of the target deployment machines for each of the products selected for deployment on the Server Location page. When finished, click **Next** to continue to the Connections page.

   **Deployment Options**

   Select a deployment option for the target location. There are two options available:

   - **Deploy on the local machine** – use this option when deploying a product on the same machine as the Deployment Manager. In this case, the fields for remote host details and credentials are disabled.

   - **Deploy on the following machine** – when selected, you must provide the remote host address and operating system details. The user credentials provided must have administrator privileges on the remote host.

> **Note:** When you provide the host name for the product deployment, make sure to use only letters (a-z), digits (0-9), a period (.), and the hyphen sign ('-').

The following information is relevant when specifying remote machine details:

- **WMI and SMB Protocols** – used to connect to the remote machine. The following prerequisites must exist for Deployment Manager to successfully connect to the remote machine.
  - **WMI Service** – the WMI service must be running on the remote machine.
  - **Server Service** – to enable the SMB protocol, the Server Service must be running on the remote machine.

**Test Connection**

Click **Test Connection** to verify that the connection credentials and details are correct and to analyze the local and remote system resources.

If the connection test fails, the Deployment Manager displays an error message detailing the failure. Pressing the **Next** button automatically forces the test connection verification.

The machine resources validation is performed on the following:

- **OS Platform** – verifies that the operating system is certified for the product deployment.
- **Disk space** – verifies that there is sufficient disk space.
- **Memory** – verifies that there is sufficient physical memory.
- **Ports** – verifies that the required ports are available.

  The resource validations performed by the test connection vary according to the supported product matrixes.

  > **Note:** If the test returns an **Unknown** error, verify that the following services are running on the deployment host machine:
  >
  > - Server
  > - Windows Management Instrumentation

- Ensure that User Account Control (UAC) is turned off before you click **Next**. For details about UAC, go to http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx.

8. Configure connections between the selected products on the Connections page. The connection options that appear in the Connections page reflect the components selected for deployment in the Product Selection page. When finished, click **Next** to continue to the Installation Configuration page.

   - UCMDB to Configuration Manager Integration

     This section appears when you choose to install Configuration Manager with the **Connect to an Existing Server** option, and enables you to configure the integration of Configuration Manager with UCMDB.

> **Note:** In order to connect to an existing instance of UCMDB, that installation must be UCMDB version 9.03 with CUP 2, or any subsequent release.

Provide the following UCMDB details:

| Field | Definition |
|---|---|
| **UCMDB Host Name/IP** | UCMDB deployment location address.<br>○ If UCMDB is configured in high availablity mode, follow the instructions in "Install Configuration Manager When an Existing UCMDB Installation is Configured for High Availability " (on page 15).<br>○ If UCMDB is installed on the local machine and Configuration Manager is installed on a remote machine, the name of the local UCMDB instance must be the fully qualified domain name and not **localhost**.<br>○ If UCMDB and Configuration Manager have different DNS domain names and LW-SSO integration is required, you must specify the fully qualified domain name in the existing UCMDB host input field. |
| **Protocol** | HTTP or HTTPS protocol. |
| **UCMDB HTTP(S) Port** | The HTTP or HTTPS port default values are **8080** for HTTP and **8443** for HTTPS. |
| **Server Certificate File** | This field appears when the HTTPS protocol is selected. You must manually place the UCMDB server certificate file on the Configuration Manager target host, and specify the full file path including the file name in the adjacent input field.<br>If UCMDB uses HTTPS, then using a key exchange is required. The key exchange is not validated during the connection test.<br>**Note:** The certificate file must be a *.cer file (other file formats are not supported). |
| **Customer Name** | The default UCMDB customer name is **Default Client**. The customer name value is used during the UCMDB and Configuration Manager integration configuration. This value is not validated by the connection test. If you provide an incorrect value, the deployment will fail. |
| **JMX Port** | The default value is **29601**. |
| **UCMDB System User (JMX)** | The UCMDB (JMX) system user is used for activating JMX functions such as creating a Configuration Manager integration user and deploying the Configuration Manager package. The out-of-the-box default value is **sysadmin**. |

| Field | Definition |
|---|---|
| **UCMDB System Password** | The UCMDB system user password. The default value is **sysadmin**.<br>**Note:** The password must not contain spaces, and can use only English letters (a-z), digits (0-9), the hyphen sign ('-'), and the underscore sign (_). |

**Note:** Configuration Manager is configured with an internal user repository. If you want to use an external LDAP as your user repository, you must configure Configuration Manager post-installation to use it, from the Configuration Manager Settings page. For details, see "System Settings" in the *HP Universal CMDB Configuration Manager User Guide*.

- Configuration Manager to OO Integration

  This section appears when you select the **Connect to an Existing HP Operation Orchestration instance** option and allows you to configure a Configuration Manager integration with OO.

  Provide the following OO details:

| Field | Definition |
|---|---|
| **OO Version** | Valid OO version is 9.0. |
| **OO Host Name/IP** | The host or IP address of the OO server machine. |
| **OO Port Number** | The default port number is **8443**. |
| **OO Username** | The default OO username is **admin**. The user must be configured as external in OO. |
| **OO Password** | The default OO password is **admin**. |

- DDMA Configuration

  The following fields appear when you select the **Discovery and Dependency Mapping Advanced Edition instance** option and enables you to configure a DDMA connection to UCMDB.

  Provide the following DDMA details:

| Field | Definition |
|---|---|
| **Data Flow Probe Identifier** | The default value is the DDMA machine host name, and this field is automatically populated. You can change this value. |
| **Use Default Domain** | This option is selected by default, and affects the domain name value. If you deselect this checkbox, you can change the default name to a different value. |

| Field | Definition |
|---|---|
| **Domain Name** | The default value is set to **DefaultDomain**. **Deselect the Use Default Domain** checkbox to enable this field. |
| **Initial Heap Size in MB** | The initial memory size assigned to the JVM of the DDMA. The default value is 256 MB. |
| **Maximum Heap Size in MB** | The maximum memory size assigned to the JVM. The default value is 512 MB. |

9. Set the deployment target directory details for the product deployments that you selected on the Installation Configuration page. When finished, click **Next** to continue to the Database Configuration page.

   A default directory path is provided for each selected product. If you are deploying on a local machine, a Browse option is available for you to select a different directory path. If you are installing on a remote machine, this option is disabled.

   > **Note:** The installation directory must not contain spaces in its name, and can use only English letters (a-z), digits (0-9) and the hyphen sign ('-').

10. Configure each product's database connection and database schema on the Database Configuration page. If a schema does not already exist, it will be created automatically. When finished, click **Next** to continue to the Ports Configuration page.

    You can configure the following databases (schemas):

    - UCMDB-CM schema
    - UCMDB schema
    - UCMDB History schema

| Field | Definition |
|---|---|
| **Database Host Name/IP** | The database server location address. |
| **Port** | MSSQL and Oracle use different default ports. The default Oracle database port is 1521 and the default MSSQL database port is 1433. |
| **SID (Oracle)** | The Oracle database instance name. |
| **Admin Username (Oracle)** | Enter the Oracle administrator username according to the Oracle server. |
| **Admin Password (Oracle)** | Enter the Oracle administrator password according to the Oracle server. |
| **Test Connection** | Test the connection to the target DB host, using the provided credentials. |

| Field | Definition |
|---|---|
| **Schema Name (Oracle)** | Enter the schema name. |
| **Schema Password (Oracle)** | Enter the schema password. This field appears when you create a new schema |
| **Default Tablespace (Oracle)** | Enter the default tablespace name. |
| **Temporary Tablespace (Oracle)** | Enter the temporary tablespace name. |
| **Database Name (MSSQL)** | Enter database schema name to use/create in the MSSQL server. |
| **Database Username (MSSQL)** | Enter the MSSQL administrator username according to the MSSQL server. |
| **Database Password (MSSQL)** | Enter the MSSQL administrator password according to the Oracle server. |

**Note:**

- The Oracle administrator account must have Create User and Drop User priveleges.
- In the event that the UCMDB tablespace is full, the product deployment will succeed but the products and components will not work properly.
- Creating a new UCMDB schema and connecting to an existing UCMDB History schema is not supported.
- Using NTLM authentication when configuring UCMDB schemas with an MSSQL database when UCMDB is installed remotely is not supported, for security reasons. If NTLM authentication is required, deploy UCMDB locally.
- The Oracle Real Application Cluster (RAC) and SQL Server NTLM connections are not supported as part of this installation. If these connections are required, first install Configuration Manager with a simple database connection and when the installation process is complete, change the connection from the specific product configuration. To do this, modify the **database.properties** file according to your database specifications. For details, see "Advanced Database Configuration (for Configuration Manager)" (on page 23).

### UCMDB Schema Mode

Configuration Manager requires that UCMDB be configured with a consolidated schema mode and that a new UCMDB state be created.

If you reference an existing UCMDB installation and its schema is not already consolidated, the automatic consolidation step may take a long time (20 to 60 minutes) for heavily populated databases (those that contain more than 5 million CIs).

**Database Configuration Mode**

Configuration Manager and UCMDB must use different schemas.

The Deployment Manager enables the user to configure each schema on either an Oracle or MSSQL database server.

**Configuration Types**

You can either connect to an existing schema or create a new schema. Connecting to an existing schema overrides its contents.

**Database Configuration**

This step is performed automatically by the Deployment Manager. To perform this step manually, see "Manually Configure the Database or User Schema (optional)" (on page 14).

**Advanced Database Configuration (for Configuration Manager)**

A database connection must be configured and associated with a standard URL connection. If advanced features are required, such as an Oracle Real Application Cluster, set up a standard connection and then manually edit the **database.properties** file to configure the advanced features. The **database.properties** file is stored in the **<Configuration Manager installation directory>\conf\** folder.

Configuration Manager uses native drivers for both the Oracle and Microsoft SQL Server databases. All native driver features are supported, provided that these features can be configured using the database URL. The URL is located in the **database.properties** file.

When the Deployment Manager wizard is finished, additional database and schema configurations can be performed.

**Database Configuration Fields**

Two types of databases available – Oracle and MSSQL. The input fields change according to the database type selected.

11. Specify the Configuration Manager connection ports on the Port Configuration page. When finished, click **Next** to continue to the Users Configuration page.

    Configuration Manager provides out-of-the-box default port settings which appear in the input fields on the Port Configuration wizard page.

    If a port number conflicts with an existing installation, consult with an IT manager before changing the port number.

| Field | Definition |
|---|---|
| **Application HTTP Port** | 8180 |

| Field | Definition |
|---|---|
| **JMX HTTP Port** | 39900 |
| **Tomcat Port** | 8005 |
| **AJP Port** | 8009 (Apache Java Protocol) |
| **Application HTTPS Port** | 8143 |
| **JMX Remote Port** | 39600 |

Click the **Revert to Default Values** button to reset the ports to the default values provided by the Deployment Manager.

12. Create the following users on the User Configuration page:

    - UCMDB-CM default administrator user.
    - Integration user in UCMDB - An integration user is created in UCMDB on demand by Configuration Manager to support the integration between these two products.

    > **Note:** When you provide the initial user login, make sure to use only letters (a-z), digits (0-9), the hyphen sign ('-'), and the underscore (_).

    When finished, click **Next** to continue to the Security Configuration page.

13. Activate Global LW-SSO on a new instance of UCMDB and Configuration Manager on the Security Configuration page. LW-SSO is configured only on new instances of Configuration Manager or UCMBD, according to the selection made in the Product Selection page. When finished, click **Next** to continue to the Summary page.

    LW-SSO is modular framework used to validate different types of authentication and security tokens (such as LW-SSO and SAML2). LW-SSO is used to bridge and leverage authenticated information from different environments into application security contexts within an application or security framework.

    LW-SSO configuration differs according to the product components selected.

    When connecting Configuration Manager to an existing UCMDB or OO instance, LW-SSO is configured on Configuration Manager only. You must extract the LW-SSO init string (shared-secret string) from UCMDB or OO, and enter that string into the LW-SSO String input field. When connecting to both UCMDB and OO, verify that the LW-SSO strings defined in UCMDB and OO instances match.

    When connecting a new instance of Configuration Manager to an existing instance of UCMDB, use the FQDN as the UCMDB host name.

    **To extract the LW-SSO string from UCMDB:**

    a. Open UCMDB and select **Administration > Infrastructure Settings Manager**.

    b. In the **Name** column, select and double click the LW-SSO init string field.

    c. Copy the string from the Current value input field.

d. Paste the value into the LW-SSO string input field in the Security Configuration page.

When connecting Configuration Manager to a new UCMDB instance, LW-SSO is automatically configured on UCMDB as well as Configuration Manager.

14. Review your installation and configuration settings on the Summary page. When finished, click **Next** to continue to the Validation page.

The Summary page centralizes all of the configuration details and user input. You can revise the content of the summary, if necessary, by clicking the Back button on the pages until you reach the desired page, and adjust the deployment settings. Return to the Summary page by clicking **Next** as required.

15. The Deployment Manager now executes a series of actions that verify that the system resources of the remote machines are sufficient, that check that the user input is correct, and that validates the database configuration settings. These validations indicate whether the user definitions settings conform to known environmental limitations. The validation process begins automatically, or if you have returned to a previous page in the Deployment Manager and made changes to the configuration, click **Run Validation** to begin the validation process. When finished, click **Deploy** to continue to the Deployment page.

16. The Deployment page reflects the status of the deployment process as it progresses. The deployment process includes product installations, the start procedures, and their integrations and connections with other products.

The deployment process is completed once all of the products are successfully started.

Click **Details** to view the deployment progress details, including the steps undertaken by the Deployment Manager for each selected product's deployment.

Click **Cancel** to cancel the deployment gracefully, allowing the current deployment action to complete before stopping deployment.

Click **Abort** (available only after clicking **Cancel**) to forcefully terminate the current action and the deployment. Aborting the deployment may cause the products to be in an undetermined state.

## Validations

The following table provides a list of validations that are performed by the Deployment Manager.

| Validation | Error Message | Description |
|---|---|---|
| Verify login credentials | Credentials verification failed | The provided user credentials are incorrect. |
| | | Connection could not be established. |
| Verify operating system compatibility | Target operating system platform is <Platform><br>Product <Product Name> supports the following platforms <Platform> | The actual target operating system does not correspond to the list of certified operating systems for the product. |

| Validation | Error Message | Description |
|---|---|---|
| Verify memory | The assigned memory (<Memory> MB) exceeds the available memory (<Memory> MB) on <Target> | There is insufficient memory on the target machine for all of the assigned products |
| | <Memory> MB of memory are verified to be available on <Target Machine> | The validation was successful. |
| Verify disk space | assigned disk space for (<Memory> MB) exceeds available disk space (<Memory> MB) on drive <Target> | There is insufficient disk space on the target machine for all of the assigned products. |
| | <Memory> MB of disk space are verified to be available on drive <Target> | The validation was successful. |
| Verify that all mandatory properties were provided | Missing the target storage device for the product: <Target> | The installation directory of the product is not set. |
| Verify that a deployment machine is defined | No deployment machine is defined for <Product Name> | The product is not configured to be deployed on any machine. |
| Verify login credentials | Credentials verification failed | Incorrect login credentials. |
| Verify that UAC is disabled | The UAC is enabled | The UAC is enabled on the target machine. |
| Verify free ports | The required port number <Port> is already in use on <Target> | The required port on the target machine is already in use. |
| Verify that the target storage device exists | The target storage device <Device> does not exist on <Target> | The selected target storage device does not exist on the target machine. |
| Validate Schema existence | Schema <Name> does not exist/ already exist | The schema on the target machine exists/does not exist. |
| Validate Schema permission existence | Validate <Permissions> schema tables user permissions existence | DB User does not have enough permissions |
| Validate Schema Tables existence | Schema Tables <Tables> on the database: <Tables> already exist | The schema tables on the database already exist. |
| Validate Schema Tables user permissions existence | The database user does not have the correct permissions | The database user does not have the correct permissions. |

| Validation | Error Message | Description |
|---|---|---|
| Verify the UCMDB connection | Connection failed. Connection to UCMDB failed, host: <Host>, username: <User name>, port: <Port>, protocol: <Protocol> due to <Error> | Test connection to UCMDB with the given connection settings failed. |
| Verify the DB connection | The host name/IP address validation failed | The database host name/IP address specified is not reachable |
|  | The username or password validation failed | The user credentials specified are not valid. |
|  | The port validation failed | The database port specified is not reachable. |
|  | The SID validation failed | The database SID specified doesn't exist in DB. |
| Installation verification | The product is already installed | The product is already installed on the target host |

# Chapter 3

# Install Configuration Manager Using the Standalone Installer on a Linux or Windows System

**Note:** Be sure to see the release notes for the most updated installation instructions.

This chapter includes:

## Pre-Installation Setup

### Prerequisites

Install HP Universal CMDB version 9.03 with Content Pack 9 and the latest CUP release, or 9.04 with Content Pack 9 or 10 and the latest CUP release.

Download the Content Pack from the HP Live Network Web site (**https://h20090.www2.hp.com/**). Follow the **DDM Content Packs** link. You need an HP Passport user name and password to log in.

### Manually Configure the Database or User Schema

When installing Configuration Manager using the standalone installation, you must first create a database or user schema.

Configuration Manager and UCMDB use different schemas. Configuration Manager supports Microsoft SQL Server and Oracle Database Server. This task describes how to create a schema for Configuration Manager.

**Note:** For Microsoft SQL Server and Oracle Server system requirements, see "Server System Requirements" (on page 1).

**To configure your database:**

1. Allocate a Microsoft SQL Server database or an Oracle Server user schema.

   - For **Microsoft SQL Server**: Activate snapshot isolation.

     Execute the following command once after creating the database:

     ```
     alter database <ccm_database_name> set read_committed_snapshot on
     ```

     For more information about the SQL Server snapshot isolation feature, see http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx.

- For **Oracle**: Assign the Oracle schema user the **Connect** role, and the **Create Procedure**, **Create Sequence**, **Create Table**, **Create Trigger**, **Create View**, and **Unlimited Tablespace** system privileges. The database administrator must also provide the names of the **Default Tablespace** and **Temporary Tablespace** that can be used for the schema. (Granting the **Select any table** privilege causes the schema population procedure to fail).

2. Verify the following information, which you need during this configuration process:

| | Required Information |
|---|---|
| | DB host name and port |
| | **For MSSQL**: DB username and password<br>**For Oracle**: Schema name and password |
| | **For MS SQL**: Database name |
| | **For Oracle**: SID<br>If you are creating a new Oracle schema using the Deployment Manager, you also need the following information:<br>▪ DB Administrator username & password<br>▪ Default and temporary tablespace |

**Note:** HP Software recommends that you set up your database on the same subnetwork on which Configuration Manager is installed.

## Install Configuration Manager When an Existing UCMDB Installation is Configured for High Availability

To use Configuration Manager in a UCMDB High Availability environment, proceed with the following steps:

1. Shut down the backup (passive) server. Wait for two minutes after shutting down.
2. Install only the Configuration Manager version 9.30 component, as described in "Install Configuration Manager" (on page 29).

   Install Configuration Manager version 9.30 on a third server (not on either of the UCMDB servers). Use your load balancer host details when asked for the UCMDB connection details.
3. Start the backup (passive) UCMDB server to provide high availability only when you have ensured that UCMDB and Configuration Manager are working properly.

**Note:** High Availability mode is not supported for HP Universal CMDB Configuration Manager version 9.30 itself.

## Install Configuration Manager

**Note:** The standalone installer can install Configuration Manager on either a Windows or a

> Linux system. If you are installing on a Linux system, you can either run the installer in GUI mode (using X11 protocol), or run a silent installation. For details, see "Silent Installation" (on page 38).

**To install Configuration Manager:**

1. To start the installation, insert the Configuration Manager installation media into the machine. Do one of the following:
   - On a Windows system, extract the contents of **HP_UCMDBCM_9.30.zip** to a temporary directory. Locate the **CM-install.exe** file in the **\Windows** folder and double-click it to run the Configuration Manager Installation wizard.
   - On a Linux system, locate the **CM-install.bin** file and run it. You can either run the installer in GUI mode (using X11 protocol), or run a silent installation.
2. Accept the terms of the End User License Agreement and click **Next** to open the Installation Configuration page.
3. Select the location for the installation:
   - On Windows systems:

     Click **Choose** to select the directory where Configuration Manager will be installed. The default location is **C:\HP\CM_9.30.0.0**. Click **Next** to open the UCMDB Foundation Connection page.

     > **Note:** The installation directory must not contain spaces, and can use only English letters (a-z), digits (0-9), the hyphen sign ('-'), and the underscore sign (_).

     > **Note:** If a previous version of Configuration Manager is detected, you are given the option to perform a new installation or to upgrade the previously existing installation. Select one of the radio buttons and click **Next** to open the UCMDB Foundation Connection page. For details about the upgrade procedure, see "Upgrade Configuration Manager" (on page 34).
   - On Linux systems, do one of the following:
     - If you are performing a new installation, specify the folder where you want to install Configuration Manager.
     - If you are reconfiguring an existing installation of Configuration Manager version 9.30, specify the folder that contains the current installation.
     - If you are upgrading from a version of Configuration Manager earlier than 9.30, specify the new (target) installation folder, the folder that contains the previous installation folder, and the version number of the previous installation.

4. Provide the following details for connecting to the UCMDB Foundation installation:

| Field | Definition |
|---|---|
| **Host Name** | UCMDB deployment location address.<br>▪ If UCMDB is configured in high availability mode, follow the instructions in "Install Configuration Manager When an Existing UCMDB Installation is Configured for High Availability " (on page 15).<br>▪ If UCMDB is installed on the local machine and Configuration Manager is installed on a remote machine, the name of the local UCMDB instance must be the fully qualified domain name and not **localhost**.<br>▪ If UCMDB and Configuration Manager have different DNS domain names and LW-SSO integration is required, you must specify the FQDN in the existing UCMDB host input field. |
| **Protocol** | HTTP or HTTPS protocol. |
| **UCMDB Port** | The HTTP or HTTPS port default values are **8080** for HTTP and **8443** for HTTPS. |
| **Customer Name** | The default UCMDB customer name is **Default Client**. The customer name value is used during the UCMDB and Configuration Manager integration configuration. This value is not validated by the connection test. If you provides an incorrect value, the deployment will fail. |
| **Server Certificate File** | This field appears when the HTTPS protocol is selected. You must manually place the UCMDB server certificate file on the Configuration Manager target host, and specify the full file path including the file name in the adjacent input field.<br>If UCMDB uses HTTPS, then using a key exchange is required. The key exchange is not validated during the connection test.<br>**Note:** The certificate file must be a *.cer file (other file formats are not supported). |
| **JMX Port** | The default value is **29601**. |
| **System User (JMX)** | The UCMDB (JMX) system user is used for activating JMX functions such as creating a Configuration Manager integration user and deploying the Configuration Manager package. The out-of-the-box default value is **sysadmin**. |
| **System Password** | The UCMDB system user password. The default value is **sysadmin**.<br>**Note:** The password must not contain spaces, and can use only English letters (a-z), digits (0-9), the hyphen sign ('-'), and the underscore sign (_). |

5. Click **Test** to test the connection settings and then click **Next** to continue to the Database Configuration page.

   A database connection must be configured and associated with a standard URL connection. If advanced features are required, such as an Oracle Real Application Cluster, set up a standard connection and then manually edit the **database.properties** file to configure the advanced features.

   Configuration Manager uses native drivers for both the Oracle and Microsoft SQL Server databases. All native driver features are supported, provided that these features can be configured using the database URL. The URL is located in the **database.properties** file.

   Two types of databases available – Oracle and MSSQL. The input fields change according to the database type selected.

   > **Note:** The installer does not support the creation of a new Oracle or MSSQL database, only connection to an existing database or schema.

   Provide the following details for connecting to the Configuration Manager database:

| Field | Definition |
|---|---|
| **Host Name/IP** | The database server location address. |
| **Port** | MSSQL and Oracle use different default ports. The default Oracle database port is 1521 and the default MSSQL database port is 1433. |
| **Schema ID** | The SID (Oracle) or database name (MSSQL) . |
| **Schema Username** | The schema username (Oracle) or database username (MSSQL). |
| **Schema Password** | The schema password (Oracle) or database password (MSSQL). |

6. Click **Test** to test the connection settings and then click **Next** to continue to the Ports Configuration screen.

7. Specify the Configuration Manager connection ports on the Port Configuration page. When finished, click **Next** to continue to the Users Configuration page.

   Configuration Manager provides out-of-the-box default port settings which appear in the input fields on the Port Configuration wizard page.

   If a port number conflicts with an existing installation, consult with an IT manager before changing the port number.

| Field | Definition |
|---|---|
| **Application HTTP Port** | 8180 |
| **JMX HTTP Port** | 39900 |
| **Tomcat Port** | 8005 |

| Field | Definition |
|---|---|
| **AJP Port** | 8009 (Apache Java Protocol) |
| **Application HTTPS Port** | 8143 |
| **JMX Remote Port** | 39600 |

8. Enter details for the following users on the User Configuration page:

   - UCMDB-CM default administrator user.
   - Integration user in UCMDB - An integration user is created in UCMDB on demand by Configuration Manager to support the integration between these two products.

   When finished, click **Next**.

9. If you choose to enable integration with HP Operations Orchestration during the installation, you must supply the following information:

   Provide the following OO details:

| Field | Definition |
|---|---|
| **OO Version** | Valid OO version is 9.0. |
| **OO Host Name/IP** | The host or IP address of the OO server machine. |
| **OO Port Number** | The default port number is **8443**. |
| **OO Username** | The default OO username is **admin**. The user must be configured as external in OO. |
| **OO Password** | The default OO password is **admin**. |
| **OO Cyclic Interval** | (optional) The default value is 60 seconds. |

10. Review your installation and configuration settings on the Pre-Installation Summary page. When finished, click **Install** to continue to the Installing page.

    The Summary page centralizes all of the configuration details and user input. You can revise the content of the summary, if necessary, by clicking **Previous** on the pages until you reach the desired page, and adjust the deployment settings. Return to the Summary page by clicking **Next** as required.

11. The Installing page shows the progress of your installation. During the installation, the progress bar displays the progress of the installation. When the process finishes, the configuration settings are applied to Configuration Manager. This phase may take several minutes. You can press **Cancel** during the installation to stop the process and roll back the installation. During the configuration phase, the **Cancel** button is disabled.

    When the installation process finishes, a message appears indicating that Configuration Manager was successfully installed in the selected folder. In addition, error messages or warnings are displayed, as well as the path of the log file. To finish, press **Done**.

# Upgrade Configuration Manager

The upgrade procedure assumes the following before beginning:

- that there is a working connection to the UCMDB server.
- that the necessary CUP patch has been installed for UCMDB.

If any of these items have not been installed or configured properly, you will see an error message informing you of this. You can fix the indicated problem and then perform the upgrade.

- If the upgrade fails because you cannot connect to UCMDB, check that the UCMDB server is up and running.
- If the upgrade fails due to the patch not being installed, install the necessary CUP patch according to the instructions found at the HP Software support site: http://support.openview.hp.com/selfsolve/patches

To upgrade, perform the following steps:

> **Note:** Before you begin the upgrade procedure, make sure that:
>
> - the UCMDB server is up and running
> - the Configuration Manager server is stopped

1. Back up your Configuration Manager and UCMDB schemas.
2. To start the installation, insert the Configuration Manager installation media into the machine. Do one of the following:
   - On a Windows system, extract the contents of **HP_UCMDBCM_9.30.zip** to a temporary directory. Locate the **CM-install.exe** file in the **\Windows** folder and double-click it to run the Configuration Manager Installation wizard.
   - On a Linux system, locate the **CM-install.bin** file and run it. You can either run the installer in GUI mode (using X11 protocol), or run a silent installation.
3. Click **Next** to open the End User License Agreement page.
4. Accept the terms of the license and click **Next**.
5. Select the folder where Configuration Manager will be installed. Make sure that you select a different location than the one that was used for the previous version.

   By default, Configuration Manager is installed in the following directory: **c:\hp\CM-9.3.0.0**. Click **Next** to accept the default location, or click **Browse** to select a different location and then click **Next**.

   > **Note:** The installation directory must not contain spaces in its name.

6. Click **Next** until you are asked whether to perform a new installation of Configuration Manager or to upgrade.

> **Note:** If you are upgrading on a Linux system, specify the new (target) installation folder, the folder that contains the previous installation folder, and the version number of the previous installation. For the version number, enter either **9.10** or **9.20** for the version number, as required.

7. Select **Upgrade** and click **Next** to confirm and begin the installation.
8. When the installation finishes, check the installation log file (located in the **<Configuration Manager installation directory/_installation/logs** folder) to ensure that the installation completed with no errors.

   If an error occurs during the upgrade process, a message is displayed. If this occurs, contact HP support.
9. The Configuration Manager service starts automatically. Wait several minutes for the service to restart.

> **Note:** After upgrading, you must perform the SSL configuration again. For details, see "Hardening" (on page 57).

# Chapter 4

## Reconfigure Configuration Manager

To reconfigure an existing installation of Configuration Manager, do the following:

1. In the **<Configuration Manager installation directory>/_installation** folder, run the **CM_Install.exe** file. The End User License Agreement is displayed. Select the radio button and click **Next** to continue.

2. The installation process checks if there is a previous installation of Configuration Manager, and displays the following message:

   ```
   A previous installation of the product has been detected.
   This installation will not reinstall the product, but will
   allow you to reconfigure the product parameters.
   ```

   Click **Next** to continue.

3. Continue with the reconfiguration process as described in "Install Configuration Manager" (on page 29). You can update the following information:

   - UCMDB Foundation connection information
   - Database configuration information
   - Tomcat ports
   - User configurations
   - LW-SSO configuration
   - Integration with HP Operations Orchestration

# Chapter 5

## Start or Stop the Configuration Manager Application Server

You can start or stop Configuration Manager on a Linux system from the command line.

**To start the Configuration Manager server:**

```
$ cd /<Configuration Manager installation directory>
$ ./start-server-0.sh
```

You can create a script in the **/etc/init.d** directory to automatically start Configuration Manager on machine startup.

**To stop the Configuration Manager server:**

```
$ cd /<Configuration Manager installation directory>
$ ./stop-server-0.sh
```

# Chapter 6

## Silent Installation

To perform a silent installation of Configuration Manager, run the following command:

```
>CM-install.exe -i silent -f installvariables.properties
```

An example of the **installvariables.properties** file is displayed below:

```
# Enter 1 for a new installation or 0 to upgrade
CM_NEW_INSTALLATION=1
VALIDATE_PING_TO_UCMDB=true

# Logging file
INSTALL_LOG_NAME=HP_Universal_CMDB_Configuration_Manager.log

# User installation directory
# Enter the full absolute path to be used for the installation
# Make sure to use double backslashes; for example, c:\\hp\\cm_9.30
USER_INSTALL_DIR=

# UCMDB connection config:
UCMDB_HOST_NAME=
UCMDB_HOST_IP=
UCMDB_DOMAIN=
UCMDB_PROTOCOL=
UCMDB_PORT=
# Enter the full path for the UCMDB Foundation certificate file (.cer
file only)
UCMDB_CLIENT_CERT_FILE=
UCMDB_CUSTOMER_NAME=
UCMDB_JMX_PORT=
UCMDB_SYSTEM_USER=
UCMDB_SYSTEM_PASSWORD=

# CM host
CM_DOMAIN=
CM_HOSTNAME=

# Database config:
# Enter 1 to create a new schema; otherwise, enter 0
DB_CREATE_NEW_SCHEMA=
# Enter 1 to use an existing schema; otherwise, enter 0
DB_USE_EXISTING_SCHEMA=
# Enter 1 for an Oracle database; otherwise, enter 0
DB_VENDOR_ORACLE=
# Enter 1 for an MSSQL database; otherwise, enter 0
DB_VENDOR_MSSQL=
DB_HOST_NAME=
DB_PORT=
# For an Oracle database, enter the SID name; for an MSSQL database,
enter the database name
ORACLE_SID_OR_MSSQL_DB_NAME=
ORACLE_SCHEMANAME_OR_MSSQL_DB_USERNAME=
ORACLE_SCHEMA_PASSWORD_OR_MSSQL_DB_USER_PASSWORD=

# Oracle only:
# These four values are required only for the creation of a new Oracle
schema
ORACLE_ADMIN_USERNAME=
ORACLE_ADMIN_PASSWORD=
DB_DEFAULT_TABLE_SPACE=
DB_TEMP_TABLE_SPACE=

# Tomcat Ports:
HTTP_PORT=
HTTPS_PORT=
TOMCAT_PORT=
AJP_PORT=
JMX_HTTP_PORT=
JMX_REMOTE_PORT=

# User config:
ADMIN_USERNAME=
ADMIN_PASSWORD=
UCMDB_ADMIN_USERNAME=
UCMDB_ADMIN_PASSWORD=

# LWSSO:
# Enter 1 to configure LWSSO; otherwise, enter 0
LWSSO_CONFIGURE=
LWSSO_INIT_STRING=

# OO:
# Enter 1 to configure a connection to an existing HP Operations
Orchestration installation
OO_CONFIGURE=
OO_HOST_NAME=
OO_VERSION=
OO_PORT=
OO_USERNAME=
OO_PASSWORD=
```

For additional details about the various parameters that can be set, see "Install Configuration Manager" (on page 29).

# Chapter 7

## Uninstall Configuration Manager

To uninstall Configuration Manager, do one of the following:

| | |
|---|---|
| On Windows systems | From the Start menu:<br>- Click **Start > Programs > HP Universal CMDBConfiguration Manager 9.30 > Uninstall HP Universal CMDBConfiguration Manager 9.30**.<br>From the Control Panel:<br>- In Windows Server 2003:<br>Click **Control Panel > Add or Remove Programs > HP Universal CMDB Configuration Manager 9.30**, and then click **Change/Remove**.<br>- In Windows Server 2008:<br>Click **Control Panel > Programs and Features > HP Universal CMDB Configuration Manager 9.30**, and then click **Uninstall**.<br>A notification is displayed that you are about to uninstall. Click **Uninstall** to continue or click **Cancel** to exit. |
| On Linux systems | In the **<Configuration Manager installation directory>/_installation/** folder, execute **CM-uninstall**. |

# Chapter 8

## Logging In to Configuration Manager

This chapter includes:

## Accessing Configuration Manager

You access Configuration Manager using a supported Web browser, from any computer with a network connection (intranet or Internet) to the Configuration Manager server. The level of access granted a user depends on the user's permissions. For details on granting user permissions, see User Management in the *HP Universal CMDBConfiguration Manager User Guide*.

For details on Web browser requirements, as well as minimum requirements for successfully viewing Configuration Manager, see "Support Matrix" (on page 11).

For details on accessing Configuration Manager securely, see "Hardening" (on page 57).

For troubleshooting information about accessing Configuration Manager, see "Appendix B: Troubleshooting" (on page 80).

### Log In to Configuration Manager

1. In the Web browser, enter the URL of the Configuration Manager Server, for example, `http://<server name>.<domain name>:<port>/cnc`**,** where **<server name>.<domain name>** represents the fully qualified domain name (FAQ) of the Configuration Manager server and **<port>** represents the port selected during installation.

   **Note:** If you want to log in to Configuration Manager with the IP address instead of the server name, do the following:

   a. Open the **client-config.properties** file, located in the **conf** directory of the Configuration Manager installation directory.

   b. Locate the following properties:

   ```
   bsf.server.services.url=http\://localhost\:8180/bsf
   bsf.server.url=http\://vmcncdev63.devlab.ad\:8180/bsf
   ```

   c. Replace all the server names (or the localhost strings) with the IP addresses, for example:

   ```
   bsf.server.services.url=http\://16.59.62.235\:8180/bsf
   applicationId=cnc
   bsf.server.url=http\://16.59.62.235\:8180/bsf
   ```

   d. Restart Configuration Manager.

2. Enter the username and password you defined in the Configuration Manager Post Install wizard.
3. Click **Log In**. After logging in, the user name appears at the top right of the screen.
4. (Recommended) Connect to the organizational LDAP server and assign administrative roles to LDAP users to enable Configuration Manager administrators to access the system. For details on assigning roles to users in the Configuration Manager system, see User Management in the *HP Universal CMDB Configuration Manager User Guide*.

### Log Out

When you have completed your session, it is recommended that you log out of the Web site to prevent unauthorized entry.

To log out, click **Logout** at the top of the page.

> **Note:** There is a default session expiration time of 30 minutes.

## Accessing the JMX Console for Configuration Manager

For troubleshooting purposes or to modify certain configurations, you may need to access the JMX console.

**To access the JMX console:**

1. Open the JMX console at `http://<server name or IP address>:<port>/cnc/jmx-console`. The port is the port configured during installation of Configuration Manager.
2. Enter the default user credentials. They are the same as the user credentials for logging in to Configuration Manager.

# Chapter 9

## Additional Use Cases

This chapter includes:

## Assign Permission to Access the JMX Console

This procedure describes how to enable a user to access the JMX console, whose role would not normally have permission to do so. This task is usually performed by an administrator.

1. In Configuration Manager, select **System > User Management** and click the **Role Management** tab.

2. Click the **Create Role** button. Enter a name and description for the new role.

3. Click the **Attach Permission** button in the **Role Details** pane.

4. Select **Execute JMX Operations** and click **Next**.

   All permissions, except for global permissions, must have an Environment assignment.

5. Click **Finish**, or click **Commit** and **Add Another Permission** to assign additional permissions to the role.

   For user interface details, see the section on setting up Configuration Manager users and permissions in the *HP Universal CMDB Configuration Manager User Guide*.

6. To access the JMX console, launch your Web browser and enter the following address: **http://<server_name>:<port_number>/cnc/jmx-console,** where **<server_name>** is the name of the machine on which Configuration Manager is installed.

7. Enter the JMX console administrator authentication credentials that were chosen during the installation process.

## Port a Configuration Manager Installation Between Machines

This procedure should be used when you want to transfer an installation of Configuration Manager from one machine to another while keeping the database schema intact and connecting to the same UCMDB server.

1. In the **<Configuration Manager installation directory>\bin** folder, execute the following command: `edit-server-0.bat`.

2. Log all the parameters that you find, including ports (for example, JMX port).
3. Stop the Configuration Manager server on the source machine. (If the source machine is installed on a Windows system, do this by stopping the Configuration Manager service).
4. Install Configuration Manager on the target machine.
5. Cancel the Post-Installation Wizard when it begins.
6. Copy all files from the previous installation directory on the source machine into the location of the new installation on the target machine.
7. On the target machine, change the hostname to the target machine name in the **client-config.properties** and **resources.properties** (located in the **\conf** folder).

   > **Note:** If the target machine is in a different domain from the source machine, modify the old domain reference in the **lwssofmconf.xml** file as well.

8. On the target machine, run the **bin/create-windows-service.bat** file to create the Windows service. Set the **-h** flag to see the available options and use the logged parameters from the source machine's service (that you recorded in step 2) as required. For the domain name parameter, use `server-0`. Using default values, the command will look like this:

   ```
   c:\HP\CM_9.3.0.0\bin>create-windows-service.bat -j 39900 -n server-0 -r 39600
   ```

9. Start the Configuration Manager server on the target machine.

## Change Port Numbers After Installation

1. Stop the Configuration Manager server.
2. Back up the contents of the **<**Configuration Manager **installation directory>\servers\server-0** folder.
3. Delete the **<Configuration Manager installation directory>\servers\server-0** folder.
4. Run the **create-node.bat** script with the **-h** flag to see the available options. Pass all required port numbers to the utility.
5. On the target machine, change the port to your new HTTP port number in the **client-config.properties** and **resources.properties** (located in the **\conf** folder).
6. Run the **edit-server-0.bat** script, located in the **<**Configuration Manager **installation directory>\bin** folder.
7. (For Windows systems) In the HP Universal CMDB Configuration Manager Properties window that opens, click the Java tab and change the **jmx.http.port** and **com.sun.management.jmxremote.port** settings to your new port numbers.
8. Start the Configuration Manager service on the target machine.

## Copy System Settings Between Systems

1. On the source machine, open Configuration Manager. Go to **System > Settings** and click the **Export configuration set to a zip file** button.

Before exporting, you can exclude specific parts of the configuration by unchecking the checkbox next to the relevant configuration items.

2. Copy the exported configuration to the target machine.

3. On the target machine, open Configuration Manager. Go to **System > Settings** and click the **Import configuration set** button.

## Back Up and Restore

You can back up an installation of Configuration Manager in order to be able to recover from any type of failure that would otherwise require a complete new installation.

### Back up

Back up the following information:

- the **conf** and **security** subfolders in the Configuration Manager installation directory. This can be done while the system is up and running, without interrupting operation.

- the database schema

### Restore

This procedure should be performed on a new system with that has no Configuration Manager installation on it.

1. Install Configuration Manager on the target machine by running the **cm-install.exe** file (on Windows systems) or **cm-install.bin** file (on Linux systems).

2. Stop the Configuration Manager server.

3. Restore the **conf** and **security** directories. Use the matching method to restore that you used to back up. Overwrite the directories created by the installation that you performed in step 1.

4. Restore the database schema. If you restore to a different database server, you must modify the **url** property in the **database.properties** file (located in the **conf** directory) to match the new database server name.

5. Start the Configuration Manager server.

# Chapter 10

## Advanced Configuration

This chapter includes:

## Advanced Database Connection Options

If you require more advanced database connection properties to support your database deployment, you can do this after the Post Installation wizard has finished running. Configuration Manager supports all database connection options that are supported by the vendor's JDBC driver and can be configured with the database connection URL. To configure more advanced connections, edit the **jdbc.url** property in the **<Configuration Manager installation directory>\conf\database.properties** file.

> **Note:** Do the following when performing advanced configuration on a Linux system:
>
> - Change the direction of the slashes in the instructions to forward (/) slashes.
> - Replace **.bat** with **.sh** in script executions.

The following are examples of more advanced options for Microsoft SQL Server:

- **Windows (NTLM) authentication.** To apply Windows authentication, add the domain property to your JTDS connection URL in the **database.properties** file. Specify the Windows domain to authenticate.

  For example: `jdbc:jtds:sqlserver://myServer:1433/myDatabase; sendStringParametersAsUnicode=false;domain=myDomain`

  In addition, update the **db.user** and **db.password** parameters in the **database.properties** file with the Windows authentication credentials for the database server.

- **SSL.** For details on securing the MS SQL server connection using SSL, see http://jtds.sourceforge.net/faq.html.

The following are examples of more advanced options for Oracle Database Server:

- **Oracle URL.** Specify the connection URL of the Oracle native driver. Include a valid Oracle server name and SID. Alternatively, if you are using **Oracle RAC**, specify the Oracle RAC configuration details.

  To use an Oracle RAC database with Configuration Manager, do the following:

  - First install Configuration Manager on a regular Oracle database.
  - Create another schema on the Oracle RAC.
  - In the **database.properties** file, change **db.username** to the new schema name.
  - Change **jdbc.url** in the **database.properties** file to:

    ```
    (DESCRIPTION=(LOAD_BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=host1)
    (PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host2)(PORT=1521))
    (CONNECT_DATA=(SERVICE_NAME=service name)))
    ```

    where the bolded strings should be edited to include the appropriate hosts and service names. Additional hosts may be added.

    > **Note:** 1521 is the default port for Oracle databases. If you use a different port, enter that port number instead of 1521.

  - Then, run the following batch file: **populate.bat i**.

  > **Note:** For details about configuring the native Oracle JDBC URL format, see http://www.orafaq.com/wiki/JDBC#Thin_driver. For details about configuring the URL for Oracle RAC, see http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm.

- **SSL.** For details on securing the Oracle connection using SSL, see the following explanations:

  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6

## Database Configuration - MLU (Multi-Lingual Unit) Support

This section describes the database settings required to support localization.

### Oracle Server Settings

The following table lists the required settings for Oracle Server:

| Option | Supported | Recommended | Remarks |
|---|---|---|---|
| Character set | WE8ISO8859P1; UTF8,AL32UTF8 | AL32UTF8 | |

### Microsoft SQL Server Settings

The following table lists the required settings for Microsoft SQL Server:

| Option | Supported | Recommended | Remarks |
|---|---|---|---|
| Collation | Case-Insensitive. HP Universal CMDB It does not support binary sort order and case sensitivity. Only case-insensitive order with a combination of accent, kana, or width settings is supported. | Use the Collation Settings dialog box to select the collation. Do not select the binary check box. Accent, kana, and width sensitivity should be selected according to the relevant data language requirements. The selected language must be the same as the OS Windows regional settings language. | Limited to the Collation locale and the default English definitions. |
| Collation Database Property | Server default | | |

**Note:**
For all languages: **<Language>_CI_AS** is the minimum required option.
For example, in Japanese, if you want to select the Kana-sensitive and Width-sensitive options, the recommended option is: **Japanese_CI_AS_KS_WS** or **Japanese_90_CI_AS_KS_WS**. This recommendation indicates that the Japanese characters are Accent-sensitive, Kana-sensitive, and Width-sensitive.

- **Accent-sensitive (_AS).** Distinguishes between accented and unaccented characters. For example, **a** is not equal to . If this option is not selected, Microsoft SQL Server considers the accented and unaccented versions of letters to be identical for sorting purposes.
- **Kana-sensitive (_KS).** Distinguishes between the two types of Japanese kana characters: Hiragana and Katakana. If this option is not selected, Microsoft SQL Server considers Hiragana and Katakana characters to be equal for sorting purposes.
- **Width-sensitive (_WS).** Distinguishes between a single-byte character and the same character when represented as a double-byte character. If this option is not selected, Microsoft SQL Server considers the single-byte and double-byte representation of the same character to be identical for sorting purposes.

## Single Sign-On (SSO)

Single sign-on between Configuration Manager and UCMDB is performed using HP's LWSSO technology. For details, see "Appendix A: Lightweight Single Sign-On Authentication (LW-SSO) – General Reference" (on page 78).

This section includes:

- "Enable LW-SSO between Configuration Manager and UCMDB" (on page 48)
- "Configure LW-SSO in Operations Orchestration" (on page 50)
- "Perform Identity Manager Authentication" (on page 52)

### Enable LW-SSO between Configuration Manager and UCMDB

Some Configuration Manager users also have permission to log in to UCMDB. For convenience, Configuration Manager provides a direct link to the UCMDB user interface (select **Administration > UCMDB Foundation**). To use single sign-on (which precludes the need to log in to UCMDB after logging in to Configuration Manager), you must enable LW-SSO for both Configuration Manager and UCMDB and ensure that they are both working with the same initString. This task should be performed manually unless it was already performed as part of the Deployment Manager installation.

**To enable LW-SSO:**

1. In the **<Configuration Manager installation directory>\conf** folder, edit the **lwssofmconf.xml** file.
2. Locate the following section:

   ```
   enableLWSSO enableLWSSOFramework="true"
   ```

   and verify that the value is **true**.
3. Locate the following section:

   ```
   lwssoValidation id="ID000001">
   <domain> </domain>
   ```

   and enter the Configuration Manager server domain after **<domain>**.
4. Locate the following section:

   ```
   <initString="This string should be replaced"></crypto>
   ```

   and replace `"This string should be replaced"` with a shared string that is used by all trusted applications integrating with LW-SSO.
5. Locate the following section:

   ```
   <!--multiDomain>
   <trustedHosts>
   <DNSDomain>This value should be replaced by your application
   domain</DNSDomain>
   <DNSDomain>This value should be replaced by domain of other
   application</DNSDomain>
   </trustedHosts>
   </multiDomain-->
   ```

   The second DNSDomain should be included only if Configuration Manager and another application are located in different domains.
   Remove the comment character at the beginning and enter all server domains (if necessary) in the DNSDomain elements (in place of `This value should be replaced by your application domain` or `This value should be replaced by domain of other application`. The list should include the server domain entered in step 3.
6. Save the file with your changes and restart the server.
7. Launch a Web browser and enter the following address:

   `http://<UCMDB server address>.<domain_name>:8080/jmx-console.`

   Enter the JMX console authentication credentials, which by default are:

   - Login name = **sysadmin**
   - Password = **sysadmin**

8. Under **UCMDB-UI**, select **LW-SSO Configuration** to open the JMX MBEAN View page.
9. Select the **setEnabledForUI** method, set the value to **true** and click **Invoke**.
10. Select the **setDomain** method. Enter the domain name of the UCMDB server and click **Invoke**.
11. Select the **setInitString** method. Enter the same initString that you entered for Configuration Manager in step 4 and click **Invoke**.
12. If Configuration Manager and UCMDB are located in separate domains, select the **addTrustedDomains** method and enter the domain names of the UCMDB and Configuration Manager servers. Click **Invoke**.
13. To view the LW-SSO configuration as it is saved in the settings mechanism, select the **retrieveConfigurationFromSettings** method and click **Invoke**.
14. To view the actual loaded LW-SSO configuration, select the **retrieveConfiguration** method and click **Invoke**.

## Configure LW-SSO in Operations Orchestration

If LW-SSO is enabled in both Configuration Manager and Operations Orchestration (OO), users who have logged on to Configuration Manager are allowed to sign on to Operations Orchestration through the web tier without providing a user name and password (for system administrators).

**Note:**

- In the following procedure, <OO_HOME> represents the Operations Orchestration home directory.
- LW-SSO requires that the accounts used to log on to Operations Orchestration and Configuration Manager have the same account name (but can have different passwords).
- LW-SSO requires that the account in Operations Orchestration not be internal.

**To configure LW-SSO in Operations Orchestration:**

1. Stop the RSCentral service.
2. In **<OO_HOME>\Central\WEB-INF\applicationContext.xml**, enable the import between LWSSO_SECTION_BEGIN and LWSSO_SECTION_END as shown below:

   ```
   <!--  LWSSO_SECTION_BEGIN-->
            <import resource="CentralLWSSOBeans.xml"/>
   <!--  LWSSO_SECTION_END -->
   ```

3. In **<OO_HOME>\Central\WEB-INF\web.xml**, enable all the filters and mappings between LWSSO_SECTION_BEGIN and LWSSO_SECTION_END as shown below:

   ```
   <!-- LWSSO_SECTION_BEGIN  -->

   <filter>
             <filter-name>LWSSO</filter-name>
             <filter-name>LWSSO</filter-name>
             <filter-
   class>com.ic-
   onclude.dharma.commons.util.http.DharmaFilterToBeanProxy
   ```

```
            </filter-class>
            <init-param>
                  <param-name>targetBean</param-name>
                  <param-value>dharma.LWSSOFilter</param-value>
            </init-param>
    ......
    </filter>
<!-- LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
    <filter-mapping>
        <filter-name>LWSSO</filter-name><url-pattern>/*</url-
pattern>
    </filter-mapping>
<!--LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
     <filter-mapping>
<filter-name>LWSSO2Acegi</filter-name><url-pattern>/*</url-pattern>
     </filter-mapping>
     <filter-mapping>
            <filter-name>dharmaLWSSOGroupsFilter</filter-name><url-
pattern>/*</url-pattern>
            </filter-mapping>
<!--LWSSO_SECTION_END -->
```

4. In **<OO_HOME>\Central\conf\lwssofmconf.xml**, edit the following two parameters:

   - domain: Domain name of the OO server.
   - initString: Must be same as the initString value in the OO LW-SSO configuration (minimum length: 12 characters). For example, `smintegrationlwsso`.

   For example:

```
<webui>
<validation>
        <in-ui-lwsso>
         <lwssoValidation id="ID000001">
                <domain>asia.hpqc.net</domain>
                <crypto cipherType="symmetricBlockCipher"
                                 engineName="AES"
paddingModeName="CBC" keySize="256"  encodingMode="Base64Url"
                                 initString=" smintlwsso
"></crypto>
         </lwssoValidation>
        </in-ui-lwsso>
</validation>
<creation>
         <lwssoCreationRef id="ID000002">
                <lwssoValidationRef refid="ID000001"/>
                <expirationPeriod>600000</expirationPeriod>
```

```
            </lwssoCreationRef>
    </creation>
    </webui>
```

5. Restart the RSCentral service for the configuration to take effect.

## Perform Identity Manager Authentication

This task describes how to configure HP Universal CMDB Configuration Manager to accept Identity Manager authentication.

If you use an Identity Manager and intend to add HP Universal CMDB Configuration Manager, you must perform this task.

This task includes the following steps:

- "Prerequisites" (on page 52)
- "Configure HP Universal CMDB Configuration Manager to Accept Identity Manager" (on page 52)

### Prerequisites

The Configuration Manager Tomcat server should be connected to your Web Server, which is protected by your Identity Manager via a Tomcat Java (AJP13) connector.

For instructions on using a Tomcat Java (AJP13) connector, see Tomcat Java (AJP13) documentation.

### Configure HP Universal CMDB Configuration Manager to Accept Identity Manager

**To configure Tomcat Java (AJP13) with IIS6:**

1. Configure Identity Manager to send a personalization header/callback that contains the user name, and request the name of the header.
2. Open the **<Configuration Manager installation directory>\conf\lwssofmconf.xml** file and locate the section that begins with **in-ui-identity-management**.

   For example:

   ```
   <in-ui-identity-management enabled="false">
      <identity-management>
          <userNameHeaderName>sm-user</userNameHeaderName>
      </identity-management>
   </in-ui-identity-management>
   ```

   a. Activate the functionality by removing the comment character.

   b. Replace **enabled="false"** with **enabled="true"**.

   c. Replace **sm-user** with the header name that you have requested in step 1.
3. Open the **<Configuration Manager installation directory>\conf\client-config.properties** file and edit the following properties:
4. Change **bsf.server.url** to the Identity Manager URL and change the port to the Identity Manager port:

```
bsf.server.url=http://< Identity Manager URL>:< Identity Manager
port >/bsf
```

5. Change **bsf.server.services.url** to the HTTP protocol and change the port to the original Configuration Manager port:

   ```
   bsf.server.services.url=http://<Configuration Manager
   URL>:<Configuration Manager Port>/bsf
   ```

### Example of Using Java Connector to Configure Identity Management for Configuration Manager with IIS6 on a Windows 2003 Operating System

This example task describes how to install and configure Java Connector to be used to configure identify management for use with Configuration Manager with IIS6 running on a Windows 2003 operating system.

**To install Java Connector and configure it for IIS6 on a Windows 2003:**

1. Download the latest version of Java Connector (for example, **djk-1.2.21**) from the Apache web site.

   a. Click `http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/`.

   b. Select the latest version.

   c. Download the **isapi_redirect.dll** file from the **amd64** directory.

2. Store this file under **<Configuration Manager installation directory>\tomcat\bin\win32**.

3. Create a new text file named **isapi_redirect.properties** in the same directory with **isapi_redirect.dll**.

   The content of this file is:

   ```
   # Configuration file for the Jakarta ISAPI Redirector
   # The path to the ISAPI Redirector Extension, relative to the
   website
   # This must be in a virtual directory with execute privileges
   extension_uri=/jakarta/isapi_redirect.dll
   # Full path to the log file for the ISAPI Redirector
   log_file=<Configuration Manager installation directory>\servers
   \server-0\logs\isapi.log
   # Log level (debug, info, warn, error or trace)
   log_level=info
   # Full path to the workers.properties file
   worker_file==<Configuration Manager installation directory>\tomcat
   \conf\workers.properties.minimal
   # Full path to the uriworkermap.properties file
   worker_mount_file==<Configuration Manager installation
   directory>\tomcat
   \conf\uriworkermap.properties
   ```

4. Create a new text file named **workers.properties.minimal** in **<Configuration Manager installation directory>\tomcat\conf**.

The content of this file is:

```
# workers.properties.minimal -
#
# This file provides minimal jk configuration
# properties needed to
# connect to Tomcat.
#
# Defining a worker named ajp13w and of type ajp13
# Note that the name and the type do not have to
# match.
    worker.list=ajp13w
    worker.ajp13w.type=ajp13
    worker.ajp13w.host=localhost
    worker.ajp13w.port=8009
#END
```

5. Create a new text file named **uriworkermap.properties** in **<Configuration Manager installation directory>\tomcat\conf**.

   The content of this file is:

```
# uriworkermap.properties - IIS
#
# This file provides sample mappings for example:
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]
/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

> **Note:** Notice that Configuration Manager must have two rules. The new syntax allows them to unite into one rule, such as:
>
> **/cnc|/*=ajp13w**

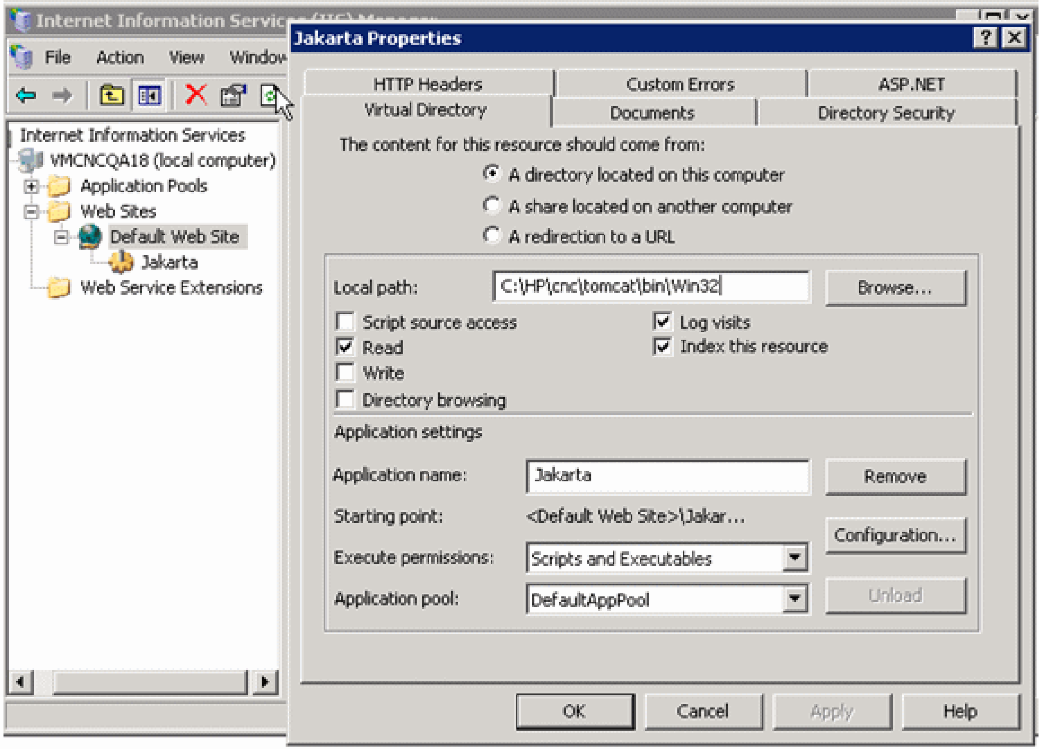
6. Create the virtual directory in the corresponding Web Site object in the IIS configuration.

   a. In the Windows Start menu, open **Settings > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.

   b. In the right pane, right click **<Local Computer name>\Web Sites\<Your Web Site name>** and select **New\Virtual Directory**.

   c. Name the directory the alias name **Jakarta**, and set the local path to the directory containing **isapi_redirect.dll**.

The Manager's window looks similar to the following:



The content for this resource should come from:

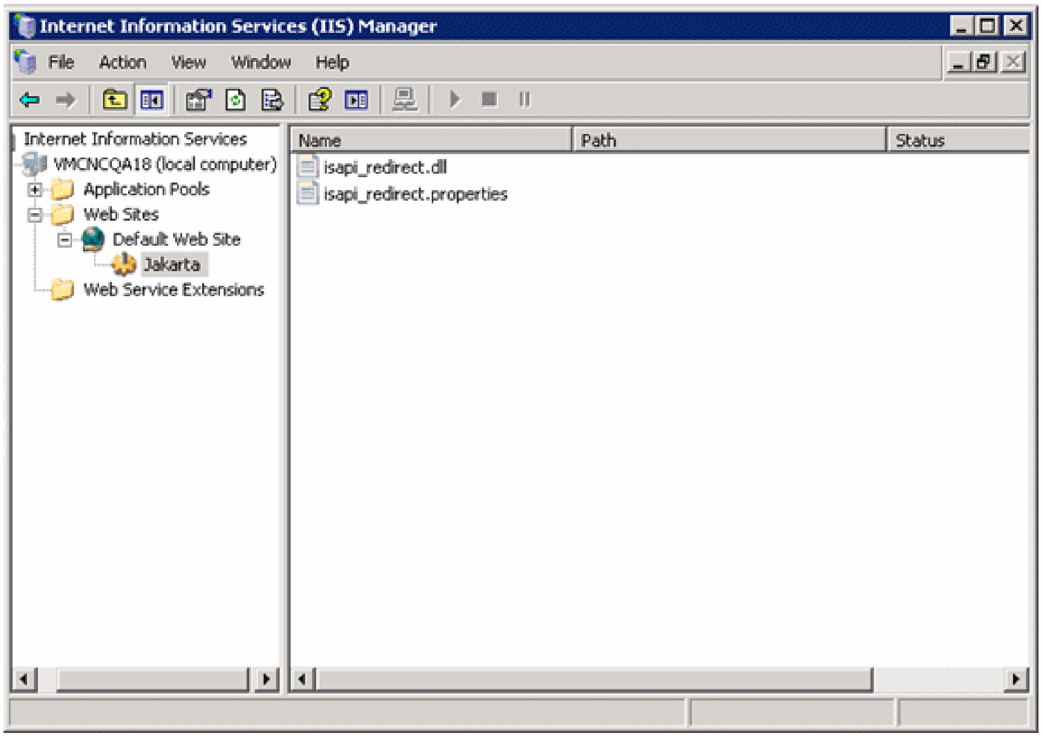
● A directory located on this computer
○ A share located on another computer
○ A redirection to a URL

Local path: C:\HP\cnc\tomcat\bin\Win32

□ Script source access
☑ Read
□ Write
□ Directory browsing
☑ Log visits
☑ Index this resource

Application settings

Application name: Jakarta
Starting point: <Default Web Site>\Jakar...
Execute permissions: Scripts and Executables
Application pool: DefaultAppPool


Internet Information Services (IIS) Manager
File
Action
View
Window
Help
Internet Information Services
VMCNCQA18 (local computer)
Application Pools
Web Sites
Default Web Site
Jakarta
Web Service Extensions

| Name | Path | Status |
|---|---|---|
| isapi_redirect.dll | | |
| isapi_redirect.properties | | |

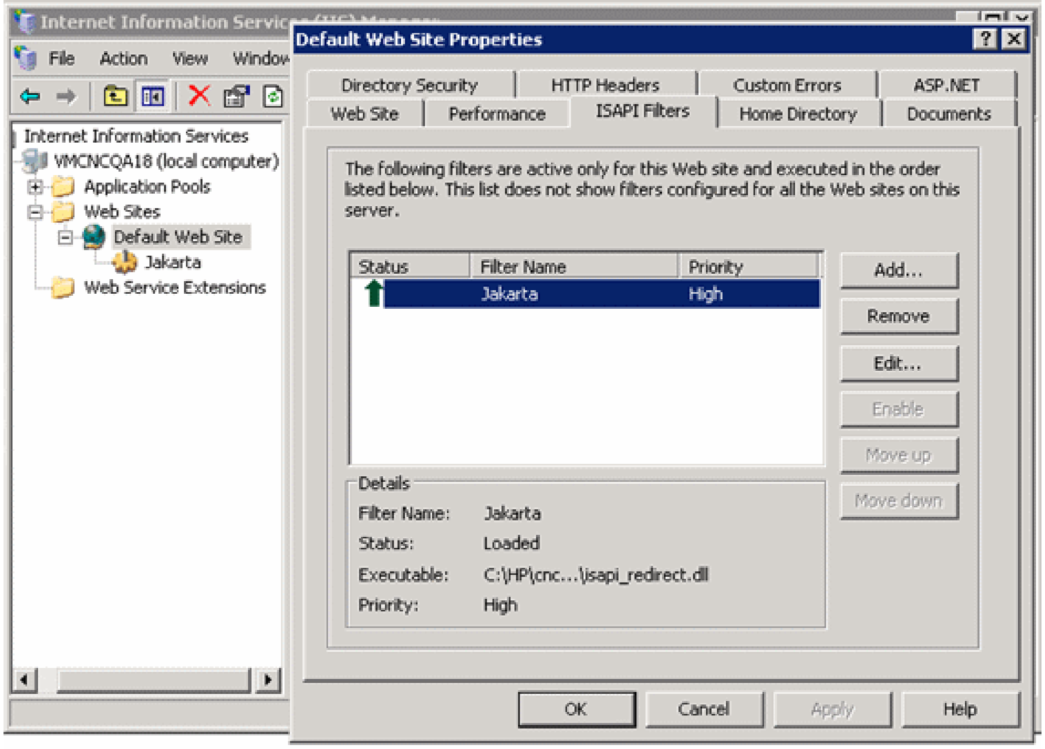
7. Add **isapi_redirect.dll** as an ISAPI filter.

a. Right click **<Your Web Site name>** and select **Properties**.

b. Select the **ISAPI Filters** tab, and click the **Add...** button.

c. Select the Filter Name **Jakarta**, and browse to **isapi_redirect.dll**. The filter is added, but it is still inactive.

The configuration window looks similar to the following:



The following filters are active only for this Web site and executed in the order listed below. This list does not show filters configured for all the Web sites on this server.

| Status | Filter Name | Priority |
|---|---|---|
| ⬆ | Jakarta | High |

Details

Filter Name: Jakarta
Status: Loaded
Executable: C:\HP\cnc...\isapi_redirect.dll
Priority: High

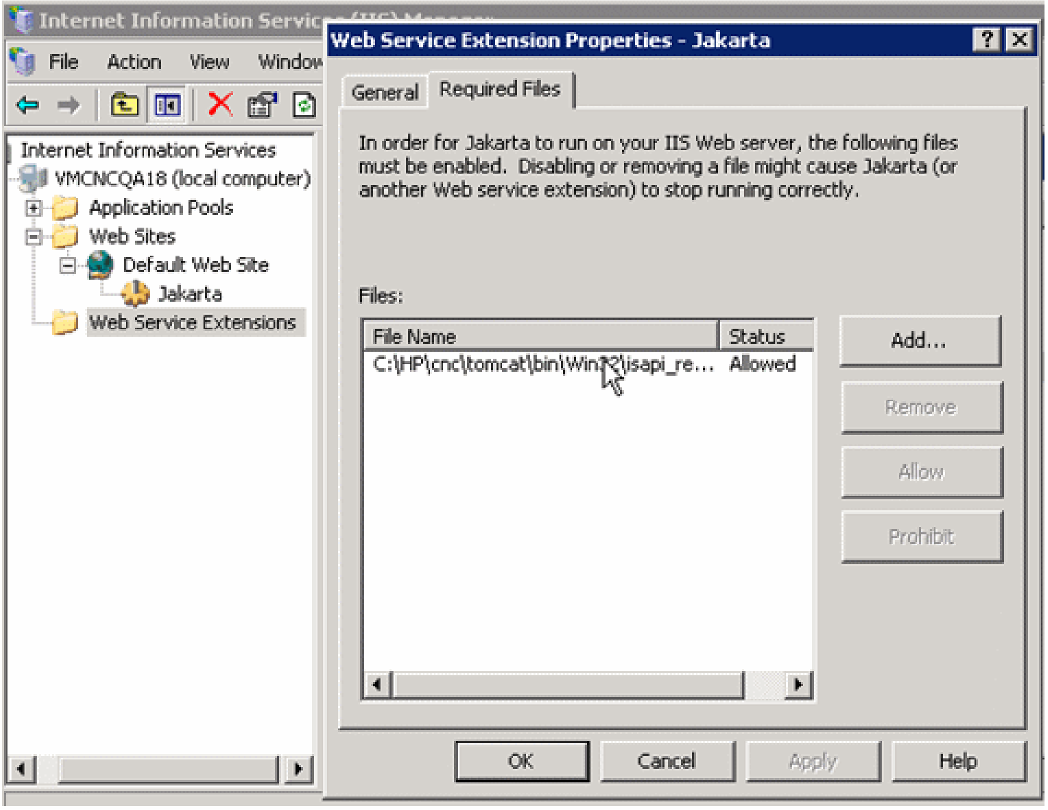
d. Click the **Apply** button.

8. Define and allow the new Web Service extension.

a. Right click the **<Local Machine name>\Web Service extensions** entry and select the **Add new Web Service Extension...** menu item.

b. Name the new Web Service extension **Jakarta**, and browse to the **isapi_redirect.dll** file.

> **Note:** Before clicking the **OK** button, select the **Set Extension Status to allowed** check box.



In order for Jakarta to run on your IIS Web server, the following files must be enabled. Disabling or removing a file might cause Jakarta (or another Web service extension) to stop running correctly.

Files:

| File Name | Status |
|---|---|
| C:\HP\cnc\tomcat\bin\Win32\isapi_re... | Allowed |

9. Restart the IIS Web Server, and access the application through the Web Service.

## IPv6 Support

Configuration Manager supports IPv6 for customer-facing URLs only. To work with Configuration Manager using an IPv6 address ensure that your operating system supports both IPv6 and IPv4. Consult the relevant operating system documentation for details. For additional details, see "IPv6 Support - Troubleshooting and Limitations" (on page 91).

## LDAP

LDAP can be configured within Configuration Manager. For details, see System Settings in the *HP Universal CMDB Configuration Manager User Guide*.

## Hardening

This section includes:

- "Hardening" (on page 57)
- "Encrypt the Database Password" (on page 59)
- "Enable SSL on the Server Machine with a Self-Signed Certificate" (on page 61)

- "Enable SSL on the Server Machine with a Certificate from a Certification Authority" (on page 62)
- "Enable SSL with a Client Certificate" (on page 63)
- "Enable SSL for Authentication Only" (on page 64)
- "Enable Client Certificate Authentication " (on page 64)
- "Client Certificates" (on page 65)
- "Configure Configuration Manager to work with UCMDB Using SSL" (on page 73)

**Note:** After upgrading, you must perform the SSL configuration again. For details, see "Upgrade Configuration Manager" (on page 34).

## Hardening Configuration Manager

This section introduces the concept of a secure Configuration Manager application and discusses the planning and architecture required to implement security. It is highly recommended that you read this section before proceeding to the hardening discussion in the following sections.

Configuration Manager is designed so that it can be part of a secure architecture, and can therefore meet the challenge of dealing with the security threats to which it might be exposed.

The hardening guidelines deal with the configuration required to implement a more secure (hardened) Configuration Manager.

The hardening information provided is intended primarily for Configuration Manager administrators who should familiarize themselves with the hardening settings and recommendations prior to beginning the hardening procedures.

The following are the recommended preparations for hardening your system:

- Evaluate the security risk/security state for your general network, and use the conclusions when deciding how to best integrate Configuration Manager into your network.
- Develop a good understanding of the Configuration Manager technical framework and Configuration Manager security capabilities.
- Review all the hardening guidelines.
- Verify that Configuration Manager is fully functioning before starting the hardening procedures.
- Follow the hardening procedure steps chronologically in each section.

**Note:**

- The hardening procedures are based on the assumption that you are implementing only the instructions provided in these sections, and that you are not performing other hardening steps documented elsewhere.
- Where the hardening procedures focus on a particular distributed architecture, this does not imply that this is the best architecture to fit your organization's needs.
- It is assumed that the procedures included in the following sections are to be performed on machines dedicated to Configuration Manager. Using the machines for other purposes in

addition to Configuration Manager may yield problematic results.

- The hardening information provided in this section is not intended as a guide to making a security risk assessment for your computerized systems.

## Encrypt the Database Password

The database password is stored in the **<Configuration Manager installation directory>\conf\database.properties** file. If you want to encrypt the password, our default encryption algorithm complies with the standards of FIPS 140-2.

The encryption is accomplished by means of a key, through which the password is encrypted. The key itself is then encrypted using another key, known as a master key. Both keys are encrypted using the same algorithm. For details on the parameters used in the encryption process, see "Encryption Parameters" (on page 59)

**Caution:** If you change the encryption algorithm, all previously encrypted passwords are no longer usable.

**To change the encryption of your database password:**

1. Open the file **<Configuration Manager installation directory>\conf \encryption.properties** and edit the following fields:
   - **engineName.** Enter the name of the encryption algorithm.
   - **keySize.** Enter the size of the master key for the selected algorithm.
2. Run the **generate-keys.bat** script, which creates the following directory: **CM_ 9.3.0.0\security\encrypt_repository** and generates the encryption key.
3. Run the **bin\encrypt-password** utility to encrypt the password. Set the **-h** flag to see the available options.
4. Copy the result of the password encryption utility and paste the resulting encryption into the **conf\database.properties** file.

## Encryption Parameters

The following table lists the parameters included in the **encryption.properties** file used for the database password encryption. For details on encrypting the database password, see "Encrypt the Database Password" (on page 59).

| Parameter | Description |
|---|---|
| cryptoSource | Indicates the infrastructure implementing the encryption algorithm. The available options are:<br>• **lw.** Uses Bouncy Castle lightweight implementation (Default option)<br>• **jce.** Java Cryptography Enhancement (standard Java cryptography infrastructure) |
| storageType | Indicates the type of the key storage. |

| Parameter | Description |
|---|---|
| | Currently, only **binary file** is supported. |
| binaryFileStorageName | Indicates the place in the file where the master key is stored. |
| cipherType | The type of the cipher. Currently, only **symmetricBlockCipher** is supported. |
| engineName | The name of the encryption algorithm.<br>The following options are available:<br>• **AES.** American Encryption Standard. This encryption is FIPS 140-2 compliant. (Default option)<br>• **Blowfish**<br>• **DES**<br>• **3DES.** (FIPS 140-2 compliant)<br>• **Null**. No encryption |
| keySize | The size of the master key. The size is determined by the algorithm:<br>• **AES.** 128, 192, or 256 (Default option is 256)<br>• **Blowfish.** 0-400<br>• **DES.** 56<br>• **3DES.** 156 |
| encodingMode | The ASCII encoding of the binary encryption results.<br>The following options are available:<br>• **Base64** (Default option)<br>• **Base64Url**<br>• **Hex** |
| algorithmModeName | The mode of the algorithm. Currently, only **CBC** is supported. |
| algorithmPaddingName | The padding algorithm used.<br>The following options are available:<br>• **PKCS7Padding** (Default option)<br>• **PKCS5Padding** |
| jceProviderName | The name of the JCE encryption algorithm.<br>**Note:** Only relevant when crytpSource is jce. For lw, engineName is used. |

## Enable SSL on the Server Machine with a Self-Signed Certificate

These sections explain how to configure Configuration Manager to support authentication and encryption using the Secure Sockets Layer (SSL) channel.

Configuration Manager uses Tomcat 7.0.19 as the application server.

> **Note:** All directory and file locations depend on your specific platform, OS and installation preferences.

1. ### Prerequisites

   Before starting the following procedure, remove the old **tomcat.keystore** file located in **<Configuration Manager installation directory>\java\lib\security\tomcat.keystore**.

2. ### Generate a Server Keystore

   Create a keystore (JKS type) with a self-signed certificate and matching private key:

   - From the bin directory of the Java installation in the Configuration Manager installation directory, run the following command:

     ```
     keytool -genkey -alias tomcat -keyalg RSA -keystore ..\lib\
     security\tomcat.keystore
     ```

     The console dialog box opens.

   - Enter the keystore password. If the password has changed, change it manually in the file.

   - Answer the question, **What is your first and last name?** Enter the Configuration Manager Web server name. Enter the other parameters according to your organization.

   - Enter a key password. The key password MUST be the same as the keystore password.

     A JKS keystore is created named **tomcat.keystore** with a server certificate named **hpcert**.

3. ### Place the Certificate in the Client's Trusted Store

   Add the certificate to the client's trusted stores in Internet Explorer on your computer (**Tools > Internet Options > Content > Certificates**). If not, you will be prompted to do so the first time you attempt to use Configuration Manager.

   For details about using client certificates, see "Client Certificates" (on page 65).

   > **Limitation**: There can be one server certificate only in **tomcat.keystore**.

4. ### Verify the Client Configuration Settings

   Open the **client-config.properties** file, located in the **conf** directory of the Configuration Manager installation directory. Set the protocol of **bsf.server.url** to **https** and the port to **8143**.

5. ### Modify the server.xml File

   Open the **server.xml** file, located in **<Configuration Manager installation directory>\servers\server-0\conf**. Locate the section beginning with

   ```
   Connector port="8143"
   ```

which appears in comments. Activate the script by removing the comment character and add the following attributes to the HTTPS connector:

`keystoreFile="<tomcat.keystore file location>"` (see step 2)
`keystorePass="<password>"`

Comment out the following line:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />
```

> **Note:** You must not block the HTTP connection port. If you want to block HTTP communication, you can use a firewall for this purpose.

6. **Restart the Server**

   Restart the Configuration Manager server.

7. **Verify the Server Security**

   To verify that the Configuration Manager Server is secure, enter the following URL in the Web browser: **https://<**Configuration Manager **Server name or IP address>:8143/cnc**.

> **Tip:** If you fail to establish a connection, try using a different browser or upgrade to a newer version of the browser.

### Enable SSL on the Server Machine with a Certificate from a Certification Authority

To use a certificate issued by a Certification Authority (CA), the keystore must be in Java format. The following example explains how to format the keystore for a Windows machine.

1. **Prerequisites**

   Before starting the following procedure, remove the old **tomcat.keystore** located in **<Configuration Manager installation directory>\java\lib\security\tomcat.keystore**.

2. **Generate a Server Keystore**

   a. Generate a CA signed certificate and install it on Windows.

   b. Export the certificate into a ***.pfx** file (including private keys) using Microsoft Management Console (**mmc.exe**).

   Enter any string as the password for the **pfx** file. (You are asked for this password when converting the keystore type to a JAVA keystore.)
   The **.pfx** file now contains a public certificate and a private key and is password protected.

   Copy the **.pfx** file you created to the following folder: **<Configuration Manager installation directory>\java\lib\security**.

   c. Open the command prompt and change the directory to **<Configuration Manager installation directory>\java\bin**.

   Change the keystore type from **PKCS12** to a **JAVA** keystore by running the following command:

```
keytool -importkeystore -srckeystore <Configuration Manager
installation directory>\conf\security\<pfx file name> -
srcstoretype PKCS12 -destkeystore tomcat.keystore
```

You are asked for the source (**.pfx**) keystore password. This is the password you supplied when creating the pfx file in step b.

3. ### Verify the Client Configuration Settings

   Open the following file: **<Configuration Manager installation directory>\conf\client-config.properties** and verify that the **bsf.server.url** property is set to **https** and the port is **8143**.

4. ### Modify the server.xml File

   Open the **server.xml** file, located in **<Configuration Manager installation directory>\servers\server-0\conf**. Locate the section beginning with

   ```
   Connector port="8143"
   ```

   which appears in comments. Activate the script by removing the comment character and add the following two lines:

   ```
   keystoreFile="../../java/lib/security/tomcat.keystore"
   keystorePass="password" />
   ```

   Comment out the following line:

   ```
   <Listener className="org.apache.catalina.core.AprLifecycleListener"
   SSLEngine="on" />
   ```

   > **Note:** You must not block the HTTP connection port. If you want to block HTTP communication, you can use a firewall for this purpose.

5. ### Restart the Server

   Restart the Configuration Manager server.

6. ### Verify the Server Security

   To verify that the Configuration Manager server is secure, enter the following URL in the Web browser: **https://<Configuration Manager Server name or IP address>:8143/cnc**.

   > **Limitation**: There can be one server certificate only in **tomcat.keystore**.

   > **Note:** All directory and file locations depend on your specific platform, operating system, and installation preferences.
   >
   > For example: `java/{os name}/lib`.

## Enable SSL with a Client Certificate

If the certificate used by the Configuration Manager Web server is issued by a well-known Certificate Authority (CA), it is most likely that your Web browser can validate the certificate without any further action.

If the CA is not trusted by the server trust store, import the CA certificate into the server trust store.

The following example demonstrates how to import the self-signed **hpcert** certificate into the server trust store (cacerts).

**To import a certificate into the Server trust store:**

1. On the client machine, locate and rename the **hpcert** certificate to **hpcert.cer**.
2. Copy **hpcert.cer** to the server machine in the **<Configuration Manager installation directory>\java\bin** folder.
3. On the server machine, import the CA certificate into the trust store (cacerts) using the keytool utility with the following command:

   ```
   <Configuration Manager installation directory>\java\bin\keytool.exe
   -import
   -alias hp -file hpcert.cer -keystore ..\lib\security\cacerts
   ```

4. Modify the **server.xml** file (located in the **<Configuration Manager installation directory>\servers\server-0\conf** folder) as follows:

   a. Make the changes described in "Modify the server.xml File" (on page 63).

   b. Right after those changes, add the following attributes to the HTTPS connector:

   ```
   truststoreFile="../../java/lib/security/cacerts"
   truststorePass="changeit" />
   ```

   c. Set `clientAuth="true"`.

5. Verify the server security as described in "Verify the Server Security" (on page 63).

## Enable SSL for Authentication Only

This task describes how to configure Configuration Manager to support authentication only. This is the minimum level of security required for working with Configuration Manager.

1. Follow one of the following procedures for enabling SSL on the server machine:

   - "Enable SSL on the Server Machine with a Self-Signed Certificate" (on page 61) up to step 6.

   - "Enable SSL on the Server Machine with a Certificate from a Certification Authority" (on page 62)up to step 5.

2. Enter the following URL in the Web browser: `http://<Configuration Manager Server name or IP address>:8180/cnc`.

## Enable Client Certificate Authentication

This task describes how to set up Configuration Manager to accept client-side certificate authentication.

1. Follow the procedure for enabling SSL on the server machine as described in "Enable SSL on the Server Machine with a Self-Signed Certificate" (on page 61).
2. Open the following file: **<Configuration Manager installation directory>\conf\lwssofmconf.xml**. Locate the section that begins with `in-client certificate`.

For example:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart"
userIdentifierRetrieveFieldPart="e" />
```

Activate the client certificate functionality by removing the comment character.

3. Extract the username from the certificate according to the following procedure:

   a. The parameter **userIdentifierRetrieveField** indicates which certificate field contains the username. The options are:
      - **SubjectDN**
      - **SubjectAlternativeName**

   b. The parameter **userIdentifierRetrieveMode** indicates whether the username consists of the entire content of the relevant field or only part of it. The options are:
      - **EntireField**
      - **FieldPart**

   c. If the value of **userIdentifierRetrieveMode** is **FieldPart**, the parameter **userIdentifierRetrieveFieldPart** indicates which part of the relevant field constitutes the username. The value is a code letter based on a legend defined in the certificate itself.

4. Open the **<Configuration Manager installation directory>\conf\client-config.properties** file and edit the following properties:

   - Change **bsf.server.url** to use the HTTPS protocol and change the HTTPS port to the port described in "Enable SSL on the Server Machine with a Self-Signed Certificate" (on page 61).
   - Change **bsf.server.services.url** to use the HTTP protocol and change the port to the original HTTP port.

### Client Certificates

This section includes:

- "Client Certificate Information" (on page 65)
- "Configuration" (on page 68)
- "Examples" (on page 69)

## Client Certificate Information

This section describes client certificate information and how to take a user identifier from a client certificate.

- **User Identifier**

  The user identifier is the unique part of information from the client certificate that used to identify the identity of the user.

- **Basic Client Certificate Information**

  Basic client certificate information includes the following:

| Certificate Field | Description |
|---|---|
| Version | The version of the encoded certificate.<br>Example: `1 (0x1)` |
| Serial Number | A positive integer assigned by the certificate authority to each certificate.<br>Example: `0 (0x0)` |
| Signature Algorithm | The algorithm identifier for the algorithm used by the certificate authority to sign the certificate.<br>Example: `md5WithRSAEncryption` |
| Issuer | The entity that has signed and issued the certificate.<br>Example: `CN=Issuer, C=US, ST=NY, L=New York, O=Work Organization, O=example.com` |
| Validity | The time interval during which the certificate authority warrants that it will maintain information about the status of the certificate:<br>▪ **Not Before**. Specifies the date on which the certificate validity period begins.<br>Example: `Nov 25 04:34:49 2009 GMT`<br>▪ **Not After**. Specifies the date on which the certificate validity period ends.<br>Example: `Nov 25 04:34:49 2010 GMT` |
| Subject | The entity associated with the public key stored in the subject public key field. |
| Subject Public Key Info | Used to carry the public key and identify the algorithm with which the key is used (for example, RSA, DSA, or Diffie-Hellman). |

For further information, see the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile:

http://tools.ietf.org/html/rfc5280

- **Subject Field**

  The Subject field (also called Subject Distinguish Name or SubjectDN) identifies the entity associated with the public key.

  The Subject field contains the following relevant attributes (it can also contain other attributes):

| Subject Attribute | Subject Attribute Description | Example |
|---|---|---|
| CN | Common Name | CN=Bob BobFamily |

| Subject Attribute | Subject Attribute Description | Example |
|---|---|---|
| emailAddress | Email Address | *emailAddress=bob@example.com* |
| C | Country Name | C=US |
| ST | State or Province Name | ST=NY |
| L | Locality Name | L=New York |
| O | Organization Name | O=Work Organization |
| OU | Organizational Unit Name | OU=Managers |

To retrieve the user identifier from the subject, you can use the entire SubjectDN field or the SubjectDN attribute.

- **Client Certificate Information Extension**

  The extensions defined for X.509 v3 certificates provide methods for associating additional attributes with users or public keys and for managing relationships between certificate authorities. The Subject Alternative Name Field can contain the user identifier.

- **Subject Alternative Name Field**

  The subject alternative name extension allows identities to be bound to the subject of the certificate. These identities may be included in addition to or in place of the identity in the subject field of the certificate.

  The Subject Alternative Name field can contain the following identities:

| Identity | Example |
|---|---|
| otherName | Other Name: Principal Name= *bobOtherAltName@example.com* |
| rfc822Name | RFC822 Name =*bobRFC822AltName@example.com* |
| dNSName | DNS Name=example1.com |
| x400Address | |
| directoryName | Directory Address:<br>E=*bobDirAltName@example.com*, CN=bob,<br>OU=Gold Ballads, O=Gold Music, C=US |
| ediPartyName | |
| uniformResourceIdentifier | URL=http://example.com/ |
| iPAddress | IP Address=192.168.7.1 |
| registeredID | Registered ID=1.2.3.4 |

To retrieve the user identifier from the subject alternative name, you can use one of the identities.

## Configuration

Configuration Manager uses LW-SSO to leverage the user identifier from a client certificate. The following attributes are used by the client certificate handler to configure LW-SSO to leverage the user identifier:

To leverage information from a client certificate, Configuration Manager should be configured how to retrieve the user identifier.

The following items should be decided:

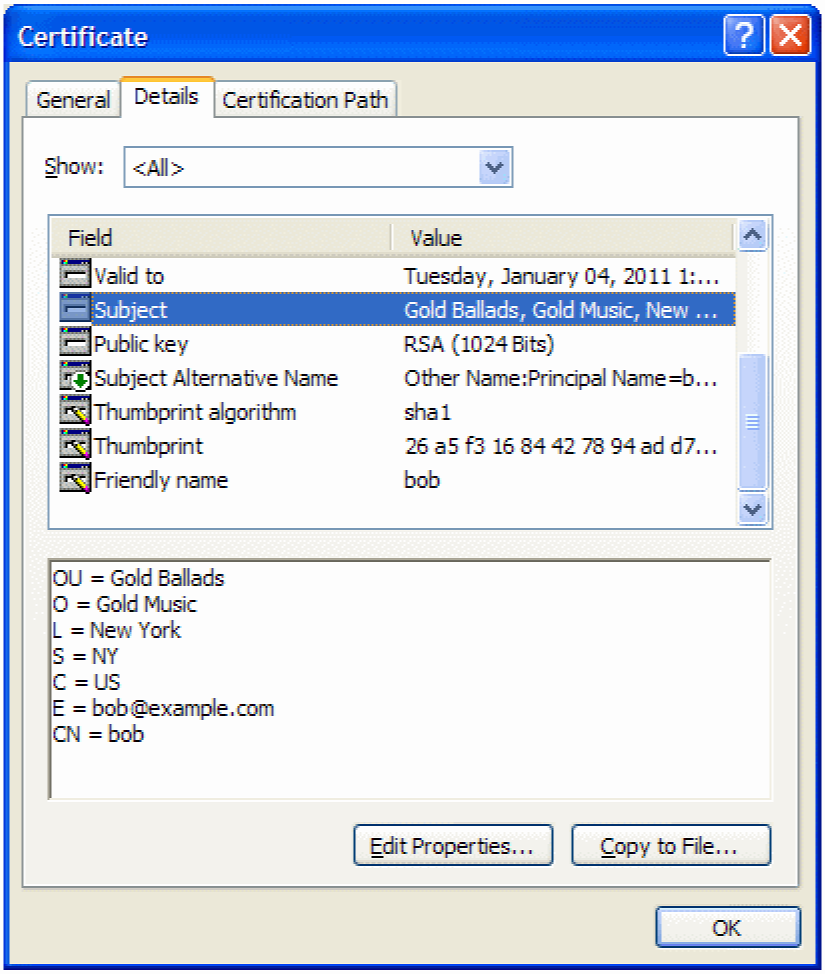
- Which field should be used: SubjectDN or Subject Alternative Name?
- Should the entire field or only part of the field be used?
- If a part of the input field is used, then provide it with a value: provide the subject attribute for the SubjectDN or provide the identity for the Subject Alternative Name.

The following attributes are used by the client certificate handler to configure LW-SSO:

| Attribute name | Description |
|---|---|
| enabled | Specifies whether the handler is enabled or disabled.<br>**Note**: It is strongly recommended to explicitly set the value to false and enable the handler only when the client certificate validation is required. |
| userIdentifierRetrieveField | The parameter indicates which certificate field contains the User Identifier. Options are: **SubjectDN** or **SubjectAlternativeName**. |
| userIdentifierRetrieveMode | The parameter userIdentifierRetrieveMode indicates whether the User Identifier consists of the entire content of the relevant field or only part of it. Options are: **EntireField** or **FieldPart**. |
| userIdentifierRetrieveFieldPart | If the value of **userIdentifierRetrieveMode** is **FieldPart**, this parameter indicates which part of the relevant field constitutes the username. The value is a code letter based on a legend defined in the certificate itself<br>**Note**: This attribute cannot be empty when **userIdentifierRetrieveMode** is set to **FieldPart**. In addition, it cannot be empty when **userIdentifierRetrievField** is set to **SubjectAlternativeName**. |

## Examples

- **Subject is used to hold the User Identifier**



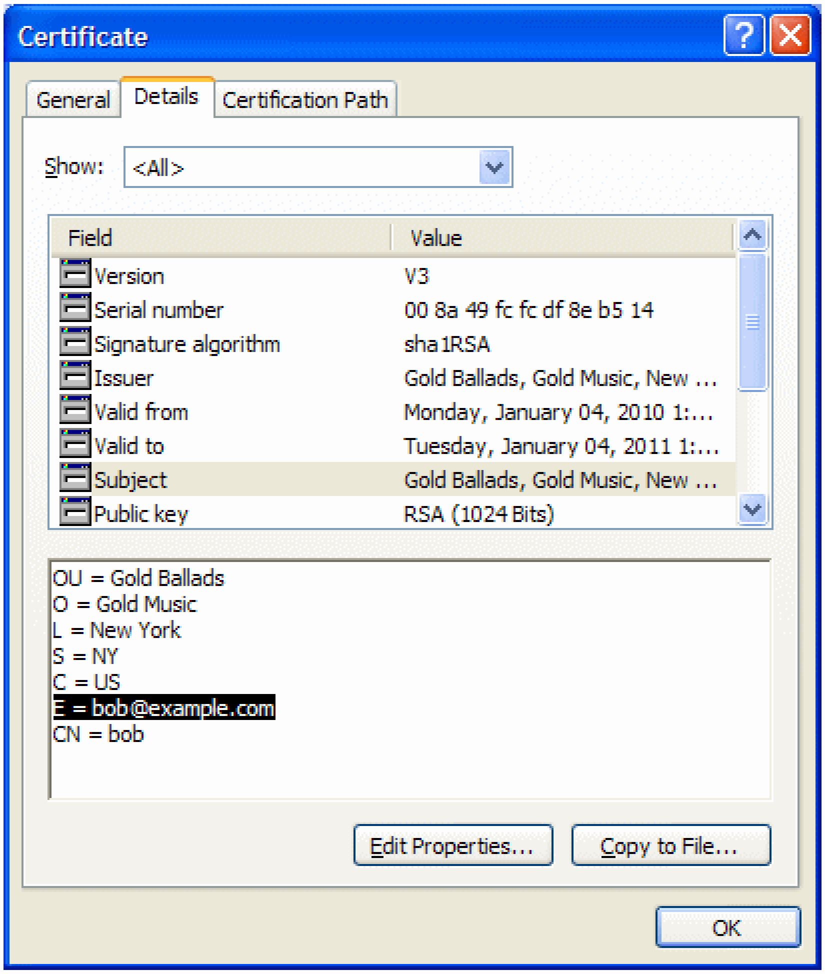
| Field | Value |
|---|---|
| Valid to | Tuesday, January 04, 2011 1:... |
| Subject | Gold Ballads, Gold Music, New ... |
| Public key | RSA (1024 Bits) |
| Subject Alternative Name | Other Name:Principal Name=b... |
| Thumbprint algorithm | sha1 |
| Thumbprint | 26 a5 f3 16 84 42 78 94 ad d7... |
| Friendly name | bob |

OU = Gold Ballads
O = Gold Music
L = New York
S = NY
C = US
E = bob@example.com
CN = bob

The following example shows how to configure the handler to take the User Identifier from the whole SubjectDN:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="EntireField" />
```

- **Email field of Subject is used to hold the User Identifier**



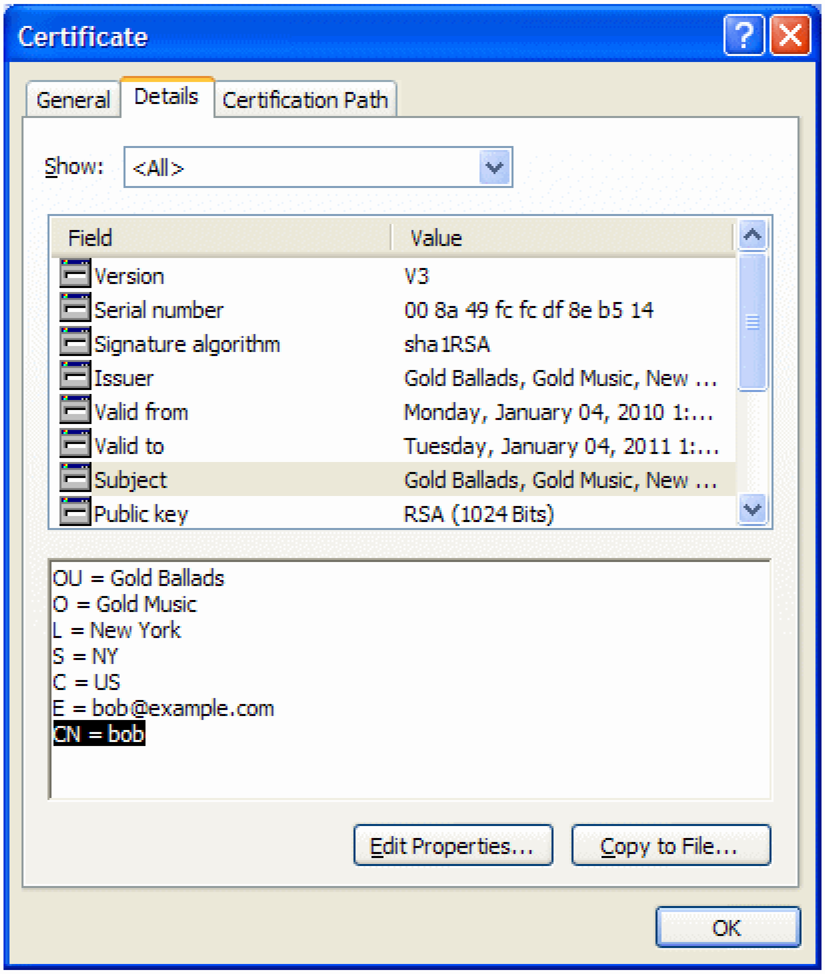
| Field | Value |
|---|---|
| Version | V3 |
| Serial number | 00 8a 49 fc fc df 8e b5 14 |
| Signature algorithm | sha1RSA |
| Issuer | Gold Ballads, Gold Music, New ... |
| Valid from | Monday, January 04, 2010 1:... |
| Valid to | Tuesday, January 04, 2011 1:... |
| Subject | Gold Ballads, Gold Music, New ... |
| Public key | RSA (1024 Bits) |

OU = Gold Ballads
O = Gold Music
L = New York
S = NY
C = US
E = bob@example.com
CN = bob

Use the names of fields that you see in the client certificate legend. The following example shows how to configure the handler to take the User Identifier from the email field of Subject:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart"
userIdentifierRetrieveFieldPart="E" />
```

- **Command Name field of Subject is used to hold the User Identifier**



Show: <All>

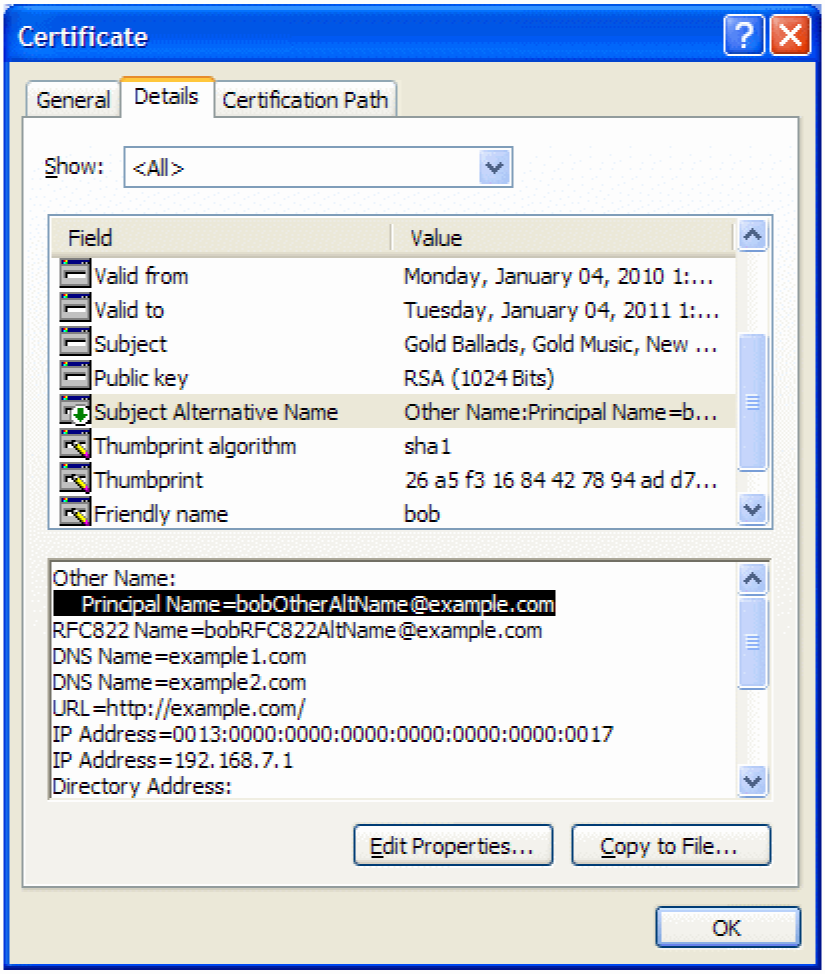
| Field | Value |
|---|---|
| Version | V3 |
| Serial number | 00 8a 49 fc fc df 8e b5 14 |
| Signature algorithm | sha1RSA |
| Issuer | Gold Ballads, Gold Music, New ... |
| Valid from | Monday, January 04, 2010 1:... |
| Valid to | Tuesday, January 04, 2011 1:... |
| Subject | Gold Ballads, Gold Music, New ... |
| Public key | RSA (1024 Bits) |

```
OU = Gold Ballads
O = Gold Music
L = New York
S = NY
C = US
E = bob@example.com
CN = bob
```

Use the names of fields that you see in the client certificate legend. The following example shows how to configure the handler to take the User Identifier from the Custom Name field of Subject:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart"
userIdentifierRetrieveFieldPart="CN" />
```

- **otherName Identity of Subject Alternative Name is used to hold the User Identifier**



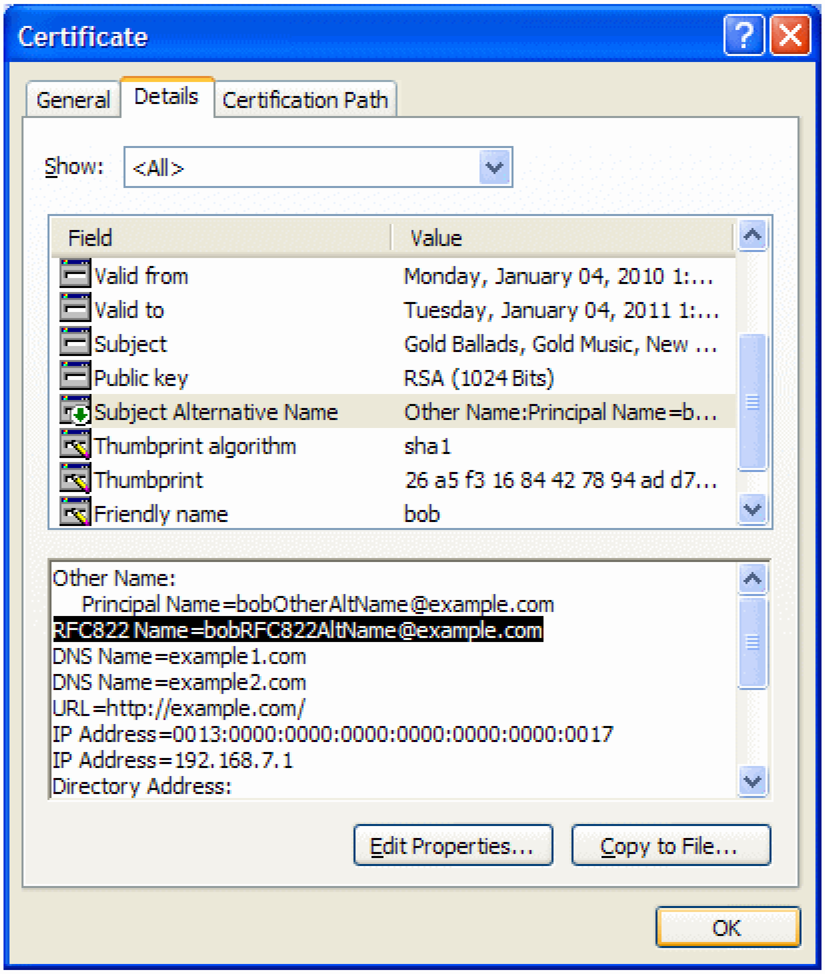
| Field | Value |
|---|---|
| Valid from | Monday, January 04, 2010 1:... |
| Valid to | Tuesday, January 04, 2011 1:... |
| Subject | Gold Ballads, Gold Music, New ... |
| Public key | RSA (1024 Bits) |
| Subject Alternative Name | Other Name:Principal Name=b... |
| Thumbprint algorithm | sha1 |
| Thumbprint | 26 a5 f3 16 84 42 78 94 ad d7... |
| Friendly name | bob |

```
Other Name:
     Principal Name=bobOtherAltName@example.com
RFC822 Name=bobRFC822AltName@example.com
DNS Name=example1.com
DNS Name=example2.com
URL=http://example.com/
IP Address=0013:0000:0000:0000:0000:0000:0000:0017
IP Address=192.168.7.1
Directory Address:
```

Use the name of Identity that you see in the client certificate legend. The following example shows how to configure the handler to take the User Identifier from the otherName Identity of Subject Alternative Name:

```
<in-clientCertificate
userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart"
userIdentifierRetrieveFieldPart="Principal Name" />
```

- **rfc822Name Identity of Subject Alternative Name is used to hold the User Identifier**



| Field | Value |
|---|---|
| Valid from | Monday, January 04, 2010 1:... |
| Valid to | Tuesday, January 04, 2011 1:... |
| Subject | Gold Ballads, Gold Music, New ... |
| Public key | RSA (1024 Bits) |
| Subject Alternative Name | Other Name:Principal Name=b... |
| Thumbprint algorithm | sha1 |
| Thumbprint | 26 a5 f3 16 84 42 78 94 ad d7... |
| Friendly name | bob |

```
Other Name:
     Principal Name=bobOtherAltName@example.com
RFC822 Name=bobRFC822AltName@example.com
DNS Name=example1.com
DNS Name=example2.com
URL=http://example.com/
IP Address=0013:0000:0000:0000:0000:0000:0000:0017
IP Address=192.168.7.1
Directory Address:
```

Use the name of Identity that you see in the client certificate legend. The following example shows how to configure the handler to take the User Identifier from the rfc822Name Identity of Subject Alternative Name:

```
<in-clientCertificate
userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart"
userIdentifierRetrieveFieldPart="Principal Name" />
```

## Configure Configuration Manager to work with UCMDB Using SSL

You can configure Configuration Manager to work with UCMDB using Secure Sockets Layer (SSL). The SSL connector on port 8143 is enabled by default in UCMDB.

### To export the server certificate and import it to the client truststore

1. Go to **<UCMDB installation directory>\bin\jre\bin** and run the following command:

   ```
   keytool -export -alias hpcert -keystore <UCMDB server dir>
   \conf\security\server.keystore -storepass hppass -file
   <certificatefile>
   ```

2. Import the certificate to the Configuration Manager truststore (the default jre truststore):

```
<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias hpcert -
keystore <CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -
file <certificatefile>
```

3. Set the UCMDB connection properties in Configuration Manager:

   Go to **System > Settings > Integrations > UCMDB Foundation > UCMDB Foundation**. Set the Connection strategy to **HTTPS**, the UCMDB server port to the UCMDB HTTPS port, and set the UCMDB access URL to https://<HostName>:8143.

4. Save the configuration set and activate it. Restart Configuration Manager.

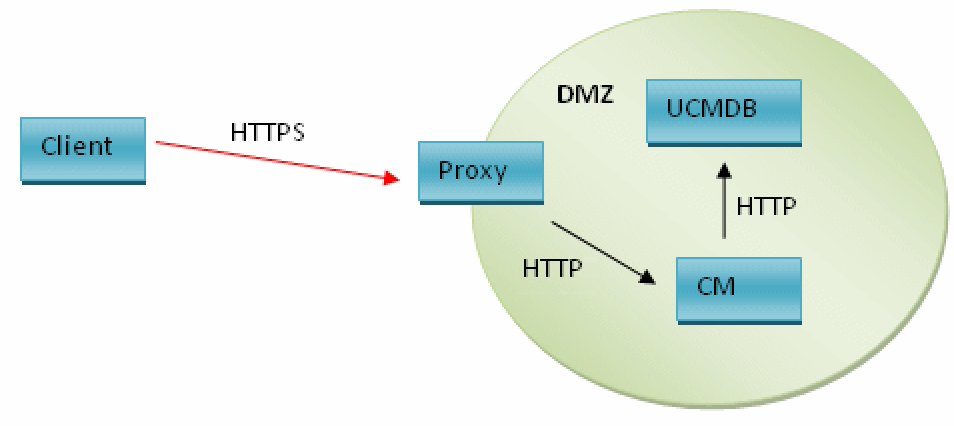
   To configure Configuration Manager to work with other products (such as load balancers) using Secure Sockets Layer (SSL), import the security certificate of the product to the Configuration Manager truststore (default jre truststore) by running the following command:

   ```
   <CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias <alias> -
   keystore <CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -
   file <certificatefile>
   ```

## Reverse Proxy

When Configuration Manager and UCMDB are located in a DMZ, it is recommended to configure the system to work with a reverse proxy server. The configuration steps are the same as for configuring UCMDB to work with a reverse proxy. To enable access to Configuration Manager you need to map the paths **/cnc** and **/bsf** to the URLs of the remote server where Configuration Manager is installed.

The following picture displays the configuration process for a reverse proxy for Configuration Manager:



For example, if the reverse proxy is Apache server, add the following lines to the **Apache2.2\conf\httpd.conf** file and then restart the Apache server:

```
ProxyPass /cnc http://<CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPassReverse /cnc http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPass /bsf http://< CM_HOSTNAME >:<CM_HTTP_PORT>/bsf
ProxyPassReverse /bsf http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/bsf
ProxyPass /docs http://< CM_HOSTNAME >:<CM_HTTP_PORT>/docs
ProxyPassReverse /docs http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/docs
```

Make sure that the following lines are uncommented:

```
* LoadModule proxy_module modules/mod_proxy.so
* LoadModule proxy_connect_module modules/mod_proxy_connect.so
* LoadModule proxy_http_module modules/mod_proxy_http.so
```

Different types of reverse proxy may require different configuration steps. Refer to your proxy server documentation for more information.

**To configure a reverse proxy for Configuration Manager:**

Update the **client-config.properties** file in the **<Configuration Manager installation directory>\conf** folder as follows:

```
bsf.server.url=https://<proxy-server-name>:443/bsf
```

The default HTTPS port of the Apache proxy is 443.

> **Note:** In a situation where the client is sitting outside of the DMZ (as displayed above), you cannot access UCMDB from within Configuration Manager using **Administration > UCMDB Foundation**.
>
> To enable UCMDB access from the **Administration > UCMDB Foundation** menu, do the following:
>
> 1. Select **System** > **Settings** > **Integrations** > **UCMDB Foundation** > **UCMDB Foundation**.
> 2. In the **UCMDB access URL** box, enter the URL that points to the proxy server. For example, **https://<PROXY_HOSTNAME>:<PROXY_PORT>/ucmdb-ui**.
> 3. Save and apply configuration changes. For details, see "Save and Apply Configuration Changes" in the *HP Universal CMDB Configuration Manager User Guide*.

## Enabling Large Views

Configuration Manager supports working with up to 20,000 composite CIs in a single managed view. To enable this functionality, do the following:

> **Note:**
>
> - If you want to enable this functionality, it is recommended to install Configuration Manager on a server that has a minimum of 8 GB of memory (RAM).
> - Managed views that are based on dynamic TQL queries and result in more than 20,000 composite CIs are not supported.

1. To access the JMX console, launch your Web browser and enter the following address: **http://<server_name>:<port_number>/cnc/jmx-console,** where **<server_name>** is the name of the machine on which Configuration Manager is installed.
2. Enter the JMX console authentication credentials, which by default are:

- Login name = **admin**
- Password = **admin**

3. Click **Amber > View Service**. Select **supportLargeViews** and click **Invoke**.
4. In UCMDB, change the value of the TQL Group View Result Size setting to 500,000 (**Administration > Infrastructure Settings Manager > TQL Settings**).
5. Do one of the following:
    - If you use the HP Universal CMDB Configuration Manager 9.30 Windows service to start Configuration Manager, navigate to the **<Configuration Manager installation directory>/bin/** directory and double-click the **edit-server-0.bat** file. In the Java tab, increase the value of the Maximum memory pool parameter to 4096 or greater.
    - If you use the **start-server-0.bat** file to start Configuration Manager, edit the **start-server-0.bat** file and raise the value of the –Xmx parameter to 4096m or greater.

# Appendixes

# Appendix A: Lightweight Single Sign-On Authentication (LW-SSO) – General Reference

This appendix includes:

## LW-SSO Authentication Overview

LW-SSO is a method of access control that enables a user to log on once and gain access to the resources of multiple software systems without being prompted to log on again. The applications inside the configured group of software systems trust the authentication, and there is no need for further authentication when moving from one application to another.

The information in this section applies to LW-SSO version 2.2 and 2.3.

For troubleshooting information about LW-SSO, see "LW-SSO - Troubleshooting and Limitations" (on page 88).

- **LW-SSO Token Expiration**

  The LW-SSO Token's expiration value determines the application's session validity. Therefore, its expiration value should be at least the same value as that of the application session expiration value.

- **Recommended Configuration of the LW-SSO Token Expiration**

  Each application using LW-SSO should configure token expiration. The recommended value is 60 minutes. For an application that does not require a high level of security, it is possible to configure a value of 300 minutes.

- **GMT Time**

  All applications participating in an LW-SSO integration must use the same GMT time with a maximum difference of 15 minutes.

- **Multi-domain Functionality**

  Multi-domain functionality requires that all applications participating in LW-SSO integration configure the **trustedHosts** settings (or the **protectedDomains** settings), if they are required to integrate with applications in different DNS domains. In addition, they must also add the correct domain in the **lwsso** element of the configuration.

- **Get SecurityToken for URL Functionality**

  To receive information sent as a **SecurityToken for URL** from other applications, the host application should configure the correct domain in the **lwsso** element of the configuration.

## LW-SSO Security Warnings

This section describes security warnings that are relevant to the LW-SSO configuration:

- **Confidential InitString parameter in LW-SSO.** LW-SSO uses Symmetric Encryption to validate and create a LW-SSO token. The **initString** parameter within the configuration is used for initialization of the secret key. An application creates a token, and each application using the same initString parameter validates the token.

  **Caution:**
  - It is not possible to use LW-SSO without setting the **initString** parameter.
  - The **initString** parameter is confidential information and should be treated as such in terms of publishing, transporting, and persistency.
  - The **initString** parameter should be shared only between applications integrating with each other using LW-SSO.
  - The **initString** parameter should have a minimum length of 12 characters.

- **Enable LW-SSO only if required.** LW-SSO should be disabled unless it is specifically required.

- **Level of authentication security.** The application that uses the weakest authentication framework and issues a LW-SSO token that is trusted by other integrated applications determines the level of authentication security for all the applications.

  It is recommended that only applications using strong and secure authentication frameworks issue an LW-SSO token.

- **Symmetric encryption implications.** LW-SSO uses symmetric cryptography for issuing and validating LW-SSO tokens. Therefore, any application using LW-SSO can issue a token to be trusted by all other applications sharing the same **initString** parameter. This potential risk is relevant when an application sharing an initString either resides on, or is accessible from, an untrusted location.

- **User mapping (Synchronization).** The LW-SSO framework does not ensure user mapping between the integrated applications. Therefore, the integrated application must monitor user mapping. We recommend that you share the same user registry (as LDAP/AD) among all integrated applications.

  Failure to map users may cause security breaches and negative application behavior. For example, the same user name may be assigned to different real users in the various applications.

  In addition, in cases where a user logs onto an application (AppA) and then accesses a second application (AppB) that uses container or application authentication, the failure to map the user will force the user to manually log on to AppB and enter a user name. If the user enters a different user name than was used to log on to AppA, the following behavior can arise: If the user subsequently accesses a third application (AppC) from AppA or AppB, then they will access it using the user names that were used to log on to AppA or AppB respectively.

- **Identity Manager**. Used for authentication purposes, all unprotected resources in the Identity Manager must be configured with the **nonsecureURLs** setting in the LW-SSO configuration file.

# Appendix B: Troubleshooting

This chapter includes:

## General Troubleshooting and Limitations

### Limitations

- The time settings on the UCMDB and Configuration Manager servers must be synchronized, down to the seconds.
- The time zone and time format on the UCMDB and Service Manager servers must be synchronized.
- You will not see a new CI type that you created in UCMDB until you log out of Configuration Manager and then log on again.

### Troubleshooting

**Problem**. The **name** attribute of the Node CI type is not qualified as change monitored, and is not copied to the authorized state during CI authorization. This occurs if Configuration Manager version 9.20 is installed without Content Pack 9 for UCMDB.

**Solution**. Do one of the following:

- Manually set the **name** attribute to be qualified as change monitored in the UCMDB CI Type Manager.
- Install Content Pack 9.

**Problem**. When you start the Configuration Manager service, you receive the following error message:

Windows could not start the HP Universal CMDB Configuration Manager on Local Computer. For more information, review the System Manager Event log. If this is a non-Microsoft service, contact the service vendor, and refer to service-specific error code 0.

**Solution**. Do the following:

1. Go to the **<Configuration Manager installation directory>\cnc\bin** folder and execute the following command:

```
edit-server-0.bat
```

2. Select the Startup tab. In the Mode dropdown list (at the bottom), select **jvm** instead of **exe**.
3. Select the Shutdown tab. In the Class field, change the last name from **Boostrap** to **Bootstrap**.
4. Click **OK**.
5. Run your service.

**Problem**. When installing, the Add Matching Rules step of the installation fails.

**Solution**. Disable the Windows firewall on the target machine for the duration of the installation.

# Deployment Manager - Troubleshooting and Limitations

To troubleshoot Deployment Manager, open the session log from the previous session, located in the following directory:

**%temp%\HP\ucmdb-dm\Workspace\Sessions**

## General Redeployment Guidelines

During installation, note the warnings and errors that appear on the Validation page of the Deployment Manager by clicking the details button located next to each deployed component.

Once a problem has been located during deployment and a solution has been found, perform the following steps:

1. Uninstall the deployed products and restart the machine.
2. Restart the Deployment Manager and reenter all of the configurations.

## Deployment Failure Issues

**Problem.** Permission error during deployment.

The session log indicates that there is a problem with the database user permissions when creating a new schema.

**Solution.** To create a new database, you must have the relevant permissions. Make sure that the user credentials used in the deployment are sufficient for tablespace and schema creation.

**Problem.** Schema/database configuration failure in UCMDB.

The session log indicates that the Deployment Manager failed to create a schema or database.

Solution:

> **Note:** Note that you cannot create a new UCMDB schema and connect to an existing UCMDB History schema (regardless of database server type).

Verify that the UCMDB schema and the UCMDB History schema do not use the following type of connection:

- UCMDB schema - Create New Schema
- UCMDB History Schema - Connect to Existing Schema

**Problem.** Schema/database configuration failure in UCMDB.

The session log indicates that the schema could not be created.

**Solution.** Open the session.log and locate the following message:

```
SQL error executing statement CREATE USER <schema name>
```

When naming the Oracle schema in the Database Configuration page of the Deployment Manager, make sure to use only letters (a-z), digits (0-9) and the hyphen sign ('-').

**Problem.** Cannot create the schema because there is not enough space.

**Solution.** Increase the amount of free space on the schema or database. Use the standard management interfaces provided by Oracle and Microsoft.

**Problem.** Database configuration failed with the following error:

```
NT AUTHORITY\ANONYMOUS LOGON - Could not connect to database.
```

When selecting an MSSQL server with NTLM authentication for UCMDB database configuration, the database configuration fails, causing a deployment failure.

**Solution.** Deploy UCMDB on a localhost machine (the only place that NTLM authentication is supported).

**Problem.**Configuration Manager database configuration failure when creating a new database.

The following errors may appear in the Deployment Manager details panel:

```
Failed to create Oracle schema due to error: ORA-01031: insufficient
privileges
```

or

```
Failed to create a schema to the database: machineName. Reason: ORA-
01919: role 'RESOURCE' does not exist
```

**Solution.** Verify that the database user has the following role privileges:

- Connect
- Resource

**Problem.** Failed to run the deployment because of insufficient disk space on the target host machine.

**Solution.** Log in to the target host machine and ensure that there is enough disk space for the deployment to succeed:

- UCMDB requires 1GB free space
- Configuration Manager requires 1GB free space
- DDMA requires 1GB free space

> **Note:** In addition to the specific product requirements, a further 1GB of free space required for temporary file handling.

**Problem.** Ping UCMDB utility fails.

This utility is executed from the Configuration Manager machine and verifies that the connection to the existing UCMDB instance is available. Open the session.log and locate the following message:

```
Failed to test connection due to error: java.net.ConnectException:
Connection refused: connect.
```

**Solution:**

- Verify that the port 8080 on the target UCMDB is not blocked by the Windows firewall.
- Verify that the UCMDB server is accessible from the Configuration Manager machine, and that the UCMDB deployment is successfully completed and up and running.

## Host Machine Connection Unavailable

**Problem**. RPC Unavailable or unknown error.

Pressing the Test Connection button results in an RPC Unavailable error.

**Solution.** Correct the hostname if incorrect, and ensure that the WMI service and the Server services are running and that the Windows firewall is not blocking access to the WMI interface.

Disable the Windows firewall or add a firewall exception enabling to the remote administration access.

To do this, open the **Firewall** control panel and select **Inbound Rules.** Enable all File and Printers, WMI rules, and port 8080.

## Test Connection Failed

**Problem.** Access denied.

Access is denied because of an incorrect username and or password, invalid DNS settings, or because the username used in the deployment does not have administrative credentials on the target host machine.

**Solution.** Make sure that the user credentials specified are correct and that the user has administrative credentials on the target host machine.

## Failed to Access Application

**Problem.** After successful deployment – failed to access the application (UCMDB or Configuration Manager).

**Solution.** Verify that the following UCMDB and Configuration Manager services exist and are running.

- **UCMDB_Server** service
- **HPUCMDBCMoasisSNAPSHOTserver0** service

Review the deployment logs located in the sessions directory for errors.

## LW-SSO is Disabled

**Problem.** Successful Deployment - LW-SSO functionality is disabled.

**Solution.** Make sure that the LW-SSO init string and domain are identical on both UCMDB and Configuration Manager (and OO, if applicable).

Review the LW-SSO configuration settings in the products via the following methods:

- Configuration Manager – Open the **lwssofmconf.xml** file and check the domain and init string definitions. The file is located in the **<Configuration Manager installation directory>\conf** folder.
- UCMDB – Open UCMDB and select **Managers > Administration > Infrastructure Settings Manager**.

If both Configuration Manager and UCMDB reside on host machines that have different DNS domains, ensure that the **Trusted Domains** settings includes both of the DNS domains and are enabled in both products.

To receive additional information regarding the deployment, the Deployment Manager can be enabled in debug mode. Debug mode provides additional information about the deployment.

**To enable debug mode:**

1. After running the Deployment Manager, open a browser window and enter `%temp%` in the address bar.
2. Navigate to the **hp\ucmdb-dm** folder.
3. Open the **ini** file in a text editor and add the following property to the last line of the file:

   ```
   -Ddebug.mode=true
   ```

4. Use **%temp%\HP\ucmdb-dm\ucmdb-dm.exe** to run the Deployment Manager.

# Accessing Configuration Manager - Troubleshooting and Limitations

## Limitations

- Whenever the time is changed on the Configuration Manager Tomcat server, the server must be restarted to update the time on the server.

## Troubleshooting

**Problem**. After changing the configuration set in **System > Settings**, the server does not start.

**Solution**. Revert to the previous configuration set. Proceed as follows:

1. Run the following command to locate the ID of the last activated configuration set:

   ```
   <Configuration Manager installation directory>\bin\export-cs.bat
   <database properties> --history
   ```

   where **<database properties>** can be specified by pointing to the location of the **<Configuration Manager installation directory>\conf\database.properties** file or by specifying each database property. For example:

   ```
   cd <Configuration Manager installation directory>\bin export-cs.bat
   -p ..\conf\database.properties --history
   ```

2. Run the following command to export the last configuration set:

   ```
   <Configuration Manager installation directory>\bin\export-cs.bat
   <database properties> <configuration set ID> <dump file name>
   ```

where **<configuration set ID>** is the configuration set ID from the previous step and **<dump file>** is the name of a temporary file used to store the configuration set. For example, to export a configuration set with an ID of **491520** to the file **mydump.zip**, enter the following:

```
cd <Configuration Manager installation directory>\bin export-cs.bat
-p ..\conf\database.properties -i 491520 -f mydump.zip
```

3. Stop the Configuration Manager service.
4. Run the following command to import and activate the previous configuration set:

   ```
   <Configuration Manager installation directory>\bin\import-cs.bat
   <database properties> -i <dump file name> --activate
   ```

**Problem**. There is an error in the UCMDB connection.

**Solution**. One of the following may be the cause:

- The UCMDB server is down. Restart Configuration Manager after UCMDB is fully up (verify that the UCMDB server status is **Up**).
- The UCMDB server is up but the Configuration Manager connection credentials or URL is wrong. Start Configuration Manager. Go to **System > Settings > Integrations > UCMDB Foundation > UCMDB Foundation**, change the settings, and save the new configuration set. Activate the configuration set and restart the server.

**Problem**. The LDAP connection settings are wrong.

**Solution**. Revert to the previous configuration set. Set the correct LDAP connection settings and activate the new configuration set.

**Problem**. Changes to the UCMDB class model are not detected in Configuration Manager.

**Solution**. Restart the Configuration Manager server.

**Problem**. The Configuration Manager log contains a **UCMDBExecution timeout expired** error.

**Solution**. This occurs when the UCMDB database is overloaded. To correct this, increase the connection timeout as follows:

1. Create a **jdbc.properties** file in the **UCMDBServer\conf** folder.
2. Enter the following text: `QueryTimeout=<number in seconds>`.
3. Restart the UCMDB server.

**Problem**. Configuration Manager does not allow you to add a view to be managed.

**Solution**. When a view is added to be managed, a new TQL is created in UCMDB. If the maximum limit of active TQLs is reached, the view cannot be added. Increase the limit of active TQLs in UCMDB by changing the following settings in the Infrastructure Settings Manager:

- Max Number Of Active TQLs In Server
- Max Number Of Customer Active TQLs

**Problem**. The HTTPS Server certificate is not valid.

**Solution**. One of the following may be the cause:

- The validation date of the certificate has passed. You need to get a new certificate.
- The certification authority on the certificate is not a trusted authority. Add the certification authority to your Trusted Root Certification Authority list.

**Problem**. When logging in from the Configuration Manager login page, you get a login error or access denied page.

**Solution**. One of the following may be the cause:

- The username may not be defined in the authentication provider (external/shared LDAP). Add the user in the Authentication provider system.
- The user is defined but does not have login permission for Configuration Manager. Grant the user login permission. As a best practice, assign login permission to the root group of all Configuration Manager users.
- These solutions also apply in cases where login fails when coming from an IDM system login.

**Problem**. The Configuration Manager server does not start due to entering incorrect database credentials.

**Solution**. If you made a change to the database credentials and the server fails to start, the credentials may be wrong. (**Note**: the Post install wizard does not automatically test the entered credentials. You must click the **Test** button in the wizard.) You need to re-encrypt the database password and enter new credentials in the configuration file. Proceed as follows:

1. From a command line, run the following command to encrypt the updated database password:

   ```
   <Configuration Manager installation directory>\bin\encrypt-
   password.bat -p <password>
   ```

   which returns an encrypted password.

2. Copy the encrypted password (including the `{ENCRYPTED}` prefix), into the **db.password** parameter in **<Configuration Manager installation directory>\conf\database.properties**.

**Problem**. If the DNS is not configured correctly, you may need to log in using the server IP address. When entering the IP address, a second DNS error occurs.

**Solution**. Replace the machine name with the IP address again. For example:

If you login using the following IP address: `http://16.55.245.240:8180/cnc/`

and you get an address with the machine name showing a DNS error, such as:
`http://my.example.com:8180/bsf/secure/authenicationPointURL.jsp...`

replace it with:
`http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...`

and launch the application again in the browser.

**Problem**. The Configuration Manager tomcat server does not start.

**Solution**. Try one of the following:

- Run the Post install wizard and replace the Configuration Manager server ports.
- Abort the other process that occupies the Configuration Manager ports.

- Manually change the ports in Configuration Manager configuration files by editing the following file: **<Configuration Manager installation directory>\servers\server-0\conf\server.xml** and updating the relevant ports:
  - HTTP (8180): line 69
  - HTTPS (8143): lines 71, 90

**Problem**. You receive an "out of memory" message.

**Solution**. Do the following to change the server startup parameters:

1. Run the following batch file:

   **<Configuration Manager installation directory>/bin/edit-server-0.bat**

2. Change the following settings:

   **-Dapplication.ms=<inital memory pool size>**
   **-Dapplication.mx=<maximum memory pool size>**

**Problem**. The Post install wizard takes a long time after clicking **Finish**.

**Solution**. For a UCMDB system that was not pre-configured to consolidated mode, the operation of consolidating the schema might take a long time (depending on the amount of data). Wait 15 minutes. If no progress is detected, abort the Post install wizard and restart the process.

**Problem**. Changes in CIs in UCMDB are not reflected in Configuration Manager.

**Solution**. Configuration Manager runs an offline asynchronous analysis process. The process may not yet have processed the latest changes in UCMDB. To resolve this, try one of the following:

- Wait a few minutes. The default interval between analysis process executions is 10 minutes. It is configurable in **System > Settings**.
- Execute a JMX call to run the offline analysis calculation on the relevant view.
- Go to **Administration > Policies > Configuration Policies**. Click the **Recalculate Policy Analysis** button. This invokes the offline analysis process for all views (which may take some time). You may also need to make an artificial change to one policy and save it.

**Problem**. When you click **Administration > UCMDB Foundation**, the UCMDB login page appears.

**Solution**. In order to access UCMDB without logging in again, you need to enable single sign-on. For details, see "Single Sign-On (SSO)" (on page 48). Additionally, ensure that the Configuration Manager user logged on is defined in the UCMDB user management system.

**Problem**. When configuring a UCMDB connection in the Post install wizard to an IPv6 address, the menu item **Administration > UCMDB Foundation** does not work.

**Solution**. Proceed as follows:

1. Go to **System > Settings > Integrations > UCMDB Foundation > UCMDB Foundation.**
2. Add square brackets to the IP address in the UCMDB access URL. The URL should look like this: `http://[x:x:x:x:x:x:x:x]:8080/`.

3. Save the configuration set and activate it.
4. Restart Configuration Manager.

# LW-SSO - Troubleshooting and Limitations

## Known Issues

This section describes known issues for LW-SSO authentication.

- **Security context.** The LW-SSO security context supports only one attribute value per attribute name.

  Therefore, when the SAML2 token sends more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

  Similarly, if the IdM token is configured to send more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

- **Multi-domain logout functionality when using Internet Explorer 7**. Multi-domain logout functionality may fail under the following conditions:

  - The browser used is Internet Explorer 7 and the application is invoking more than three consecutive HTTP 302 redirect verbs in the logout procedure.

  In this case, Internet Explorer 7 may mishandle the HTTP 302 redirect response and display an **Internet Explorer cannot display the webpage** error page instead.

  As a workaround, it is recommended to reduce, if possible, the number of application redirect commands in the logout sequence.

## Limitations

Note the following limitations when working with LW-SSO authentication:

- **Client access to the application**.

  **If a domain is defined in the LW-SSO configuration**:

  - The application clients must access the application with a Fully Qualified Domain Name (FQDN) in the login URL, for example, http://myserver.**companydomain**.com/WebApp.
  - LW-SSO cannot support URLs with an IP address, for example, http://192.168.12.13/WebApp.
  - LW-SSO cannot support URLs without a domain, for example, http://myserver/WebApp.

  **If a domain is not defined in the LW-SSO configuration**: The client can access the application without a FQDN in the login URL. In this case, a LW-SSO session cookie is created specifically for a single machine without any domain information. Therefore, the cookie is not delegated by the browser to another, and does not pass to other computers located in the same DNS domain. This means that LW-SSO does not work in the same domain.

- **LW-SSO framework integration.** Applications can leverage and use LW-SSO capabilities only if integrated within the LW-SSO framework in advance.

- **Multi-Domain Support**.

    - Multi-domain functionality is based on the HTTP referrer. Therefore, LW-SSO supports links from one application to another and does not support typing a URL into a browser window, except when both applications are in the same domain.
    - The first cross domain link using **HTTP POST** is not supported.

      Multi domain functionality does not support the first **HTTP POST** request to a second application (only the **HTTP GET** request is supported). For example, if your application has an HTTP link to a second application, an **HTTP GET** request is supported, but an **HTTP FORM** request is not supported. All requests after the first can be either **HTTP POST** or **HTTP GET**.
    - LW-SSO Token size:

      The size of information that LW-SSO can transfer from one application in one domain to another application in another domain is limited to 15 Groups/Roles/Attributes (note that each item may be an average of 15 characters long).
    - Linking from Protected (HTTPS) to non-protected (HTTP) in a multi-domain scenario:

      Multi domain functionality does not work when linking from a protected (HTTPS) to a non-protected (HTTP) page. This is a browser limitation where the referrer header is not sent when linking from a protected to a non-protected resource. For an example, see: http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP
- **SAML2 token.**
    - Logout functionality is not supported when the SAML2 token is used.

      Therefore, if the SAML2 token is used to access a second application, a user who logs out of the first application is not logged out of the second application.
    - The SAML2 token's expiration is not reflected in the application's session management.

      Therefore, if the SAML2 token is used to access a second application, each application's session management is handled independently.
- **JAAS Realm.** The JAAS Realm in Tomcat is not supported.
- **Using spaces in Tomcat directories.** Using spaces in Tomcat directories is not supported.

  It is not possible to use LW-SSO when a Tomcat installation path (folders) includes spaces (for example, Program Files) and the LW-SSO configuration file is located in the **common\classes** Tomcat folder.
- **Load balancer configuration.** A load balancer deployed with LW-SSO must be configured to use sticky sessions.

## Troubleshooting

**Problem:** An LW-SSO cookie is not created after logging in.

- **Possible cause:** A non-empty domain is improperly defined in the LW-SSO element of the configuration.
- **Possible solution**: Make sure that the domain defined in the LW-SSO element of the configuration is equal to the application's domain.
- **Possible cause:** A non-empty domain that is passed as a parameter to the enableSSO function

is incorrect.

- **Possible solution**: Make sure that the domain that is passed as a parameter to the enableSSO function is equal to the application's domain.
- **Possible cause:** You did not access the application with the Fully Qualified Domain Name (FQDN) in the login URL when a domain is defined in the LW-SSO configuration (for example: http://192.168.12.13/WebApp).
- **Possible solution**: Make sure that you access the application with the Fully Qualified Domain Name (FQDN) in the login URL (for example: http://myserver.companydomain.com/WebApp).

**Problem:** LW-SSO fails to create a cookie for AutoCookieCreation functionality.

- **Possible cause:** A domain is not defined properly in the LW-SSO element of the configuration.
- **Possible solution**: Make sure that the domain defined in the LW-SSO element of the configuration is equal to the application's domain.

**Problem:** The LW-SSO token is not validated.

- **Possible cause:** The two applications have different initString parameters in the crypto element of the configuration (or other crypto parameters).
- **Possible solution**: Use the same initString in both applications (in addition to all other crypto parameters in the LW-SSO creation element).
- **Possible cause:** The GMT time difference between the two applications is greater than 15 minutes.
- **Possible solution**: Make sure that all applications participating in a LW-SSO integration are set to the same GMT time, with a maximum difference of 15 minutes.
- **Possible cause:** A domain is empty in the LW-SSO element of the configuration and you access a second application on other computer with same DNS domain.
- **Possible solution**: Make sure that the domain defined in the LW-SSO element of the configuration is equal to the application's domain.
- **Possible cause:** A domain is not defined in the LW-SSO element of the configuration and you access a second application on another computer with the same DNS domain.
- **Possible solution**: Add a domain to the LW-SSO element and make sure that the domain is defined as being equal to the application's domain.

**Problem:** LW-SSO fails to validate the LW-SSO token in a multi-domain environment

- **Possible cause:** In the configuration of one of the applications, a domain is improperly defined in the LW-SSO element.
- **Possible solution**: The domain defined in the LW-SSO element of the application's configuration must be the same as the application's domain according to actual domains in use.
- **Possible cause:** In the configuration of one of the applications, a domain is incorrectly defined in the trustedHosts settings (or protectedDomains settings).
- **Possible solution**: Make sure that the domains in the trustedHosts settings (or protectedDomains settings) of all of the applications' configurations are correctly defined.

- **Possible cause:** The LW-SSO session cookie is blocked or denied when using Internet Explorer 6.x, 7.x, or 8.x.
- **Possible solution**: Add all LW-SSO servers to the "Intranet"/"Trusted" zone in the Internet Explorer security zones on your computer (Tools > Internet Options > Security > Local Intranet > Sites > Advanced). This will allow all cookies to be accepted.
- **Possible cause:** Some applications have different initString parameters in the crypto element of the configuration (or other crypto parameters).
- **Possible solution**: Use the same initString in all applications (in addition to all other crypto parameters in the LW-SSO creation element).
- **Possible cause:** Some applications have a GMT time difference greater than 15 minutes.
- **Possible solution**: Make sure that all applications participating in a LW-SSO integration are set to the same GMT time, with a maximum difference of 15 minutes.
- **Possible cause:** A multi-domain link goes from the protected (HTTPS) to the non-protected (HTTP) resource.
- **Possible solution**: When linking or crossing from one domain to another, make sure that the first link/cross request goes from one protected resource (HTTPS) to another protected resource (HTTPS).

## IPv6 Support - Troubleshooting and Limitations

### Limitations

- The URL cannot contain an IP address.
- The operating system must support both IPv6 and IPv4. You will not be able to log on to the Configuration Manager server if the IPv4 address is not closed or is not supported.
- Whenever the time is changed on the Configuration Manager Tomcat server, the server must be restarted to update the time on the server.

### Troubleshooting

**Problem.** After configuring a UCMDB connection to an IPv6 address during installation, the **Administration > UCMDB Foundation** menu option does not work.

**Solution.** Do the following:

1. Go to **System > Settings > Integrations > UCMDB Foundation > UCMDB Foundation**.
2. Add square brackets to the IP address in the UCMDB access URL field. The URL should look like this: http://[x:x:x:x:x:x:x:x]:8080/ucmdb-ui/.
3. Save the configuration set and activate it.
4. Restart Configuration Manager.

## Authentication - Troubleshooting and Limitations

This section describes known authentication issues.

**Problem:** During authentication to an application after redirection to an authentication point, you receive error 500.

- **Possible cause:** The Configuration Manager WAR and BSF WAR have different initString parameters in the crypto element of the configuration (or other crypto parameters).
- **Possible solution:** Use the same initString in both applications (in addition to all other crypto parameters in the LW-SSO creation element).

**Problem:** During authentication to an application after redirection to an authentication point, you cannot see the login form.

**Solution:** The Configuration Manager authentication session cookie is blocked or denied when using Internet Explorer version 6.0, 7.0 or 8.0 browsers. Add the Configuration Manager server to the **Intranet/Trusted** zone in the Internet Explorer security zones on your computer (**Tools > Internet Options > Security > Local Intranet > Sites > Advanced**). This allows all cookies to be accepted.

**Problem:** After authentication, you receive error 403.

- **Possible cause:** A domain is improperly defined in the LW-SSO element of the application configuration.
- **Possible solution:** Make sure that the domain defined in the LW-SSO element of the application configuration is equal to the application's domain.
- **Possible cause:** You did not access the application with the Fully Qualified Domain Name (FQDN) in the login URL when a domain is defined in the LW-SSO configuration (for example: http://192.168.12.13/WebApp).
- **Possible solution:** Make sure that you access the application with the Fully Qualified Domain Name (FQDN) in the login URL (for example: http://myserver.companydomain.com/WebApp).

**Problem:** After authentication, the **Get Acegi User Details** page appears.

**Solution:** The Configuration Manager authentication session cookie is blocked or denied when using Internet Explorer version 6.0, 7.0 or 8.0 browsers. Add the Configuration Manager server to the **Intranet/Trusted** zone in the Internet Explorer security zones on your computer (**Tools > Internet Options > Security > Local Intranet > Sites > Advanced**). This allows all cookies to be accepted.