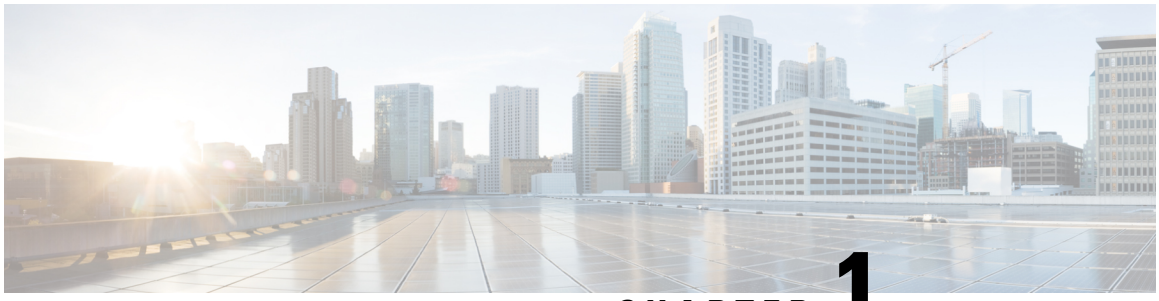
Cisco WAE 7.1.2 Installation Guide

First Published: 2018-10-30

Last Modified: 2018-10-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco WAE Overview

Cisco WAE Overview

The Cisco WAN Automation Engine (WAE) platform is an open, programmable framework that interconnects software modules, communicates with the network, and provides APIs to interface with external applications.

Cisco WAE provides the tools to create and maintain a model of the current network through the continual monitoring and analysis of the network and the traffic demands that is placed on it. At a given time, this network model contains all relevant information about a network, including topology, configuration, and traffic information. You can use this information as a basis for analyzing the impact on the network due to changes in traffic demands, paths, node and link failures, network optimizations, or other changes.

The Cisco WAE platform has numerous use cases, including:

- Traffic engineering and network optimization—Compute TE LSP configurations to improve the network performance, or perform local or global optimization.
- Demand engineering—Examine the impact on network traffic flow of adding, removing, or modifying traffic demands on the network.
- Topology and predictive analysis—Observe the impact to network performance of changes in the network topology, which is driven either by design or by network failures.
- TE tunnel programming—Examine the impact of modifying tunnel parameters, such as the tunnel path and reserved bandwidth.
- Class of service (CoS)-aware bandwidth on demand—Examine existing network traffic and demands, and admit a set of service-class-specific demands between routers.

Cisco WAE Applications

Cisco WAE applications work with the Cisco WAE platform software, providing greater insight into your network.

- Cisco WAE Design—The WAE Design GUI provides graphical layouts of the network, showing views of different regions and layers, as well as utilizations and routings. It lets you model, simulate, and analyze

failures, changes, and impact of traffic growth, as well as optimize your network for maximum efficiency. Simulation tools let you perform interactive what-if simulations by:

- Failing objects
- Modifying the network topology
- Creating and changing traffic demands (which simulate traffic flows)
- Modifying routing configurations

For installation instructions, see the Cisco WAE Design GUI Installation Guide.

- Cisco WAE Live—Cisco WAE Live provides immediate and easy access to both current and historical network data. Combined, the Explore, Analytics, and Map tools offer a flexible and interactive means of finding summarized aggregate views or quickly narrowing the search on network data to only relevant details.

  For installation instructions, see Install Cisco WAE Live, on page 21.

- Cisco WAE Coordinated Maintenance—Cisco WAE Coordinated Maintenance (CM) simplifies and automates the process of managing controlled network outages by guiding you on when to perform maintenance events at optimal times. This not only reduces uncertainty about the impact of network changes, but also minimizes the impact on the network during scheduled outages.

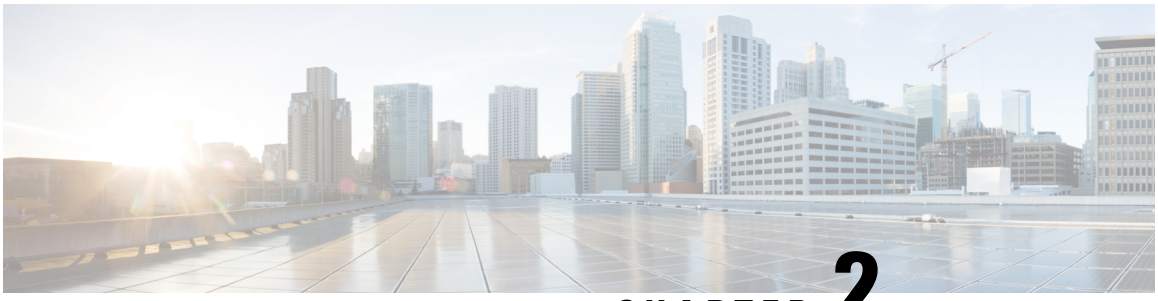
  For installation instructions, see Install Cisco WAE CM, on page 19.

- Bandwidth on Demand—The Bandwidth on Demand (BWoD) application utilizes the near real-time model of the network offered by WMD to compute and maintain paths for SR policies with bandwidth constraints delegated to WAE from XTC. In order to compute the shortest path available for a SR policy with a bandwidth constraint and ensure that path will be free of congestion, a Path Computation Element (PCE) must be aware of traffic loading on the network. The WAE BWoD application extends the existing topology-aware PCE capabilities of XTC by allowing delegation of bandwidth-aware path computation of SR policies to be sub-delegated to WAE through a new XTC REST API. Users may fine-tune the behavior of the BWoD application, affecting the path it computes, through selection of application options including network utilization threshold (definition of congestion) and path optimization criteria preferences.

  For information about enabling, configuring, and properly shutting down the BWoD application, see the "Automation Applications" chapter in the Cisco WAE User Guide.

- Bandwidth Optimization—The Bandwidth Optimization application is an approach to managing network traffic that focuses on deploying a small number of LSPs to achieve a specific outcome in the network. Examples of this type of tactical traffic engineering are deploying LSPs to shift traffic away from a congested link, establishing a low-latency LSP for priority voice or video traffic, or deploying LSPs to avoid certain nodes or links. WAE provides the Bandwidth Optimization application to react and manage traffic as the state of the network changes.

  For information about enabling, configuring, and properly shutting down the Bandwidth Optimization application, see the "Automation Applications" chapter in the Cisco WAE User Guide.



CHAPTER 2

Cisco WAE Installation Requirements

Cisco WAE requirements vary depending on which components are installed together. This section provides general guidelines and minimum requirements for individual components installed on a single server, unless otherwise specified.

This section contains the following topics:

Cisco WAE Server Requirements

You can install Cisco WAE on a server that meets the following requirements.

Operating System	Software	CPU	Memory	Hard Drive
Linux-x86_64	CentOS and RHEL 7.5 with latest patches	8+ cores	64 GB	50 GB

Important Notes

- Cisco WAE software is qualified on CentOS 7.5 and Red Hat Enterprise Linux 7.5.
- Only Linux distributions available in English are supported.
- Modify the `/etc/security/limits.conf` file by adding or updating the following lines to make sure your hardware supports sufficient number of threads for starting poller:

```
[user] soft stack 8192
[user] soft nproc 257805
[user] soft nofile 1000000
```

Where `[user]` is the userid which starts the WAE process.

Required Software Packages

Software	Version
JDK/JRE	Oracle or OpenJDK 1.8.0_102 **Note** Java environment variables must be configured correctly and JRE_HOME must point to a valid JRE/JDK 1.8 installation. Download the JRE package from the Oracle distribution site. For example: • Windows (64-bit): • Add a new system variable named JAVA_HOME and enter the variable value as the JDK installation path (C:\Program Files\Java\jre1.8.0_102). • Linux: • Enter the following command: `admin@system1 ~ # export JRE_HOME=<JDK/JRE_installation_path>` • Mac: • Add the following line in the startup shell (~/.bash_profile): `export JAVA_HOME=$(/usr/libexec/java_home -v 1.8)` If you are using MacOS X 10.12 or later with the WAE Design GUI and the Parse Configs tool (**File** > **Get Plan from** > **Configs**), add the following lines in ~/.bash_profile: `launchctl setenv JAVA_HOME `/usr/libexec/java_home -v 1.8` export JAVA_HOME=$(/usr/libexec/java_home -v 1.8)`
Perl	5.16.3
fontconfig	2.10.95
Python	2.7.5
python-paramiko.noarch	1.16.1
python-lxml	3.2.1
python-requests	2.18.4
redhat-lsb	4.0.7 This is required for the License Server. For more information, see the "WAE Design Floating License Server" chapter in the Cisco WAE Design GUI Installation Guide.

NetFlow Requirements

NetFlow Collection - (Exclusive) Memory size and CPU per server

Centralized NetFlow (WAE YANG runtime server)		
	Memory	CPU
Collector Server	32 GB	
flow_get	4 GB	
TOTAL	**36 GB**	**8+ Cores**

Distributed NetFlow (Server where the agent resides)		
	Memory	CPU
Collector Server	32 GB	
flow_cluster_agent	4 GB	
TOTAL	**36 GB**	**8+ Cores**

Distributed NetFlow (WAE YANG runtime server)		
	Memory	**CPU**
flow_cluster_broker	2 GB	
flow_cluster_master	2 GB	
flow_cluster_ias flow_cluster_dmd	4 GB	
TOTAL	**8 GB**	**8+ Cores**

Note

- One flow collection server is required per 100 Mbps of flow export bandwidth.
- Only English Linux is supported.
- Qualified on CentOS 7.4 and Red Hat Enterprise Linux 7.4.
- Flow collection requires Linux Kernel 2.6.32 or greater.
- The memory requirement listed above per collection server instance is based on the assumption of an approximate figure of 100 Mbit/s of NetFlow traffic.

Optical Collection Agents

Vendor	Supported Node Version	Software
Cisco	Cisco Network Convergence System (NCS) 2000 Series Routers, Release 10.9	Cisco Evolved Programmable Network Manager

Note The Cisco Transport Controller (CTC) optical plug-in is used for collecting topology for Cisco NCS 2000 releases 10.7 and 10.8 devices. The CTC optical plug-in is packaged with Cisco WAE.

Collection from Network Service Orchestrator

Software/Driver	Version
IOS NED	6.0.13
IOS-XR NED	7.0.10
Junos NED	3.2.20
Network Service Orchestrator	4.4.6
Traffic Engineering	Contact your Cisco WAE representative.

Scale Support

Parameters	Scale
Total number of Network Devices	4000
Total number of Interfaces	100000

Parameters	Scale
Total number of Demands	100000
Total number of Policies (SR or RSVP or Both)	5000

Cisco WAE Design Requirements

WAE Design is a 64-bit installation on all supported operating systems.

Operating System	Software	CPU	Memory
Linux-x86_64	CentOS and RHEL 7.5 with latest patches	Intel or AMD 2+ GHz	Minimum: 8 GB Recommended: 16 GB
Windows (64-bit)	Windows 2008 Windows 10.0	Intel or AMD 2+ GHz	Minimum: 8 GB Recommended: 16 GB
macOS x86_64	10.8.5 to 10.13.4	Intel or AMD 2+ GHz	Minimum: 8 GB Recommended: 16 GB

Software	Version

JDK/JRE	Configuration parsing inside WAE Design requires JRE Version 1.8.0_102 (64-bits) downloaded from the Oracle distributed site. No other JRE version, variant, or source is supported.
	• Windows (64-bit):
	• Set JRE_HOME (**Control Panel** > **System** > **Advanced** > **Environment Variables**) to point to the JRE installation path. Typically, the path is C:\Program Files\Java\jre1.8.0_102.
	• Linux:
	• The session that launches WAE Design should include in its environment:
	`JRE_HOME=<JRE_installation_path>`
	• Mac:
	• Add the following line into ~/.bash_profile:
	`export JRE_HOME=$(/usr/libexec/jre_home -v 1.8)`
	For MacOS X 10.12 or later, also add following line in ~/.bash_profile:
	`launchctl setenv JRE_HOME` `` `/usr/libexec/jre_home -v 1.8` ``

Perl	A Perl (5.10+) installation is required for certain WAE Design features.
Python	A Python installation is required for certain WAE Design features. See Required Software Packages, on page 4.

Important Notes

- A standalone WAE Design system does not require the use of WAE Collector.
- Only Linux distributions available in English are supported.

WAE Live Requirements

Note WAE Live must be installed on a separate server than the WAE server.

Requirement	~1000 Node Network	~2000 Node Network
Supported operating system	CentOS 7.5	CentOS 7.5
CPU	8 cores, 16 threads	16 cores, 32 threads
Memory	24 GB	48 GB
Disk speed	200 MBs	320 MBs
Disk size	3 TB	10 TB
Number of network objects	100,000	500,000

Note

- Only Linux distributions available in English are supported.
- Other CentOS Red Hat Enterprise Linux versions should work, but has not been tested.

Kernel Parameters

Kernel Parameters	Value
SHMALL	4294967296
SHMMAX	4398046511104
SHMMNI	4096
SEMMNS	32000
SEMMSL	250
SEMOPM	32
Maximum number of file descriptors	65535

Modify the `/etc/security/limit.conf` file by adding or updating the following lines to make sure your hardware supports sufficient number of threads for starting poller:

```
[user] soft stack 8192
[user] soft nproc 257805
```

Where `[user]` is the userid which starts the WAE process.

Supported Web Browsers

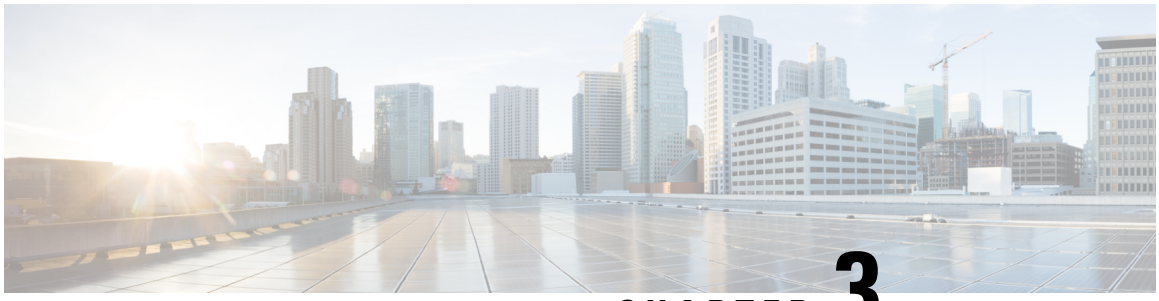
Browser	Version
Google Chrome	62 or later

Browser	Version
Firefox	56 or later
Internet Explorer **Note** Not supported on WAE Live or WAE Coordinated Maintenance.	11 or later

Cisco WAE Ports

Port	Protocol	Type	Description
*:4000	UDP	Listening	Cisco WAE Server
*:8080	TCP	Listening	Cisco WAE Server
*:8443	TCP	Listening	Cisco WAE Server, Live Server
2022 - 2023	TCP	Listening and outgoing	Cisco WAE Server
*:2024	TCP	Listening	Cisco WAE Server
4569	TCP	Listening and outgoing	Cisco WAE Server
4570	TCP	Listening	Cisco WAE Server HA
8080	TCP	Outgoing	XTC collection
127.0.0.1:9901 - 9902	TCP	Listening	SNMP polling
164	UDP	Outgoing	SNMP-based NIMOs
22	TCP	Outgoing	Collection via Telnet
23	TCP	Outgoing	Collection via SSH
*:2181	TCP	Listening	Message broker
*:9092 - 9094	TCP	Listening	Message broker
*:9000	TCP	Listening	Optical plug-in
8161	TCP	Listening	NetFlow JMS OOB
61616	TCP	Listening	NetFlow JMS IB
9090	TCP	Listening	NetFlow HTTP
2100	UDP	Listening	NetFlow
179	TCP	Listening	NetFlow BGP

Port	Protocol	Type	Description
*:8843	TCP	Listening	Cisco WAE Coordinated Maintenance (standalone or as part of WAE Server)
See "Configuring License Server Ports" in the Cisco WAE Design GUI Installation Guide.	TCP	Listening	License Server



CHAPTER 3

Install Cisco WAE

This section contains the following topics:

Install Cisco WAE

Before you begin

Note If upgrading from Cisco WAE 7.1.1, see Upgrade from Cisco WAE 7.1.1.x, on page 14.

- Confirm that you have met all requirements described in Cisco WAE Server Requirements, on page 3.
- If one does not yet exist, create a UNIX user (assigned to a group). You must be this UNIX user to run installation.

Step 1 Navigate to and download the Cisco WAE package from the Cisco Download Software site.

Step 2 Log in to the server, copy the Cisco WAE package (<*wae_linux-xxxxx_bin*> or <*wae-darwin-xxxx.bin*>) to a local directory, and start a bash shell.

Step 3 Install the Cisco WAE package.

```
# chmod 755 <wae_linux-xxxxx_bin> ; ./<wae_linux-xxxxx_bin>
 <wae_installation_directory>
```

The installation program creates a bash script file named `waerc` that sets the environment variables.

Step 4 Source this file to get the settings.

```
# source <wae_installation_directory>/waerc
```

Note If, later, you get a "`wae: command not found`" error, reenter the command to source the settings.

Step 5 Create a run-time directory.

```
# wae-setup <wae_run_time_directory>
```

Step 6 (Optional) Edit the ~/.bash_profile to source waerc settings automatically at login.

```
# echo "source ~/<wae_installation_directory>/waerc" >> ~/.bash_profile
```

Step 7 Run Cisco WAE.

```
# cd <wae_run_time_directory>
# wae
```

Example

For example:

```
# bash wae-linux-v7.0a3-2153-ga539952.bin wae_install
# source wae_install/waerc
# wae-setup wae_run
# echo "source ~/wae_install/waerc" >> ~/.bash_profile
# cd wae_run
# wae
```

What to do next

Start and log in to Cisco WAE. For more information, see Next Steps, on page 41.

Upgrade from Cisco WAE 7.1.1.x

This procedure outlines the steps necessary to upgrade from Cisco WAE 7.1.1.x.

Before you begin

Download the upgrade script package (upgrade_scripts.zip) from the same location where the Cisco WAE 7.1.2 software package resides in the Cisco Download Software site.

Step 1 Start Cisco WAE 7.1.1.

Step 2 Unzip the upgrade_scripts.zip file and run the wae_upgrade script.

```
# wae_upgrade.sh -export -install-dir <WAE_7.1.1_install_directory> -run-dir <WAE_7.1.1_run_directory>
 -conf-dir <store_config_data_directory>
```

Step 3 Stop Cisco WAE 7.1.1.

```
# wae --stop
```

Step 4 Install and run Cisco WAE 7.1.2.

Step 5 Run the script to import all the configurations from Cisco WAE 7.1.1.

```
# wae_upgrade.sh -import -install-dir <WAE_7.1.2_install_directory> -run-dir <WAE_7.1.2_run_directory>
 -conf-dir <import_data_config_directory>
```

Step 6 Run collections in Cisco WAE 7.1.2 to update the network models.

Install Cisco WAE License

A license determines which Cisco WAE features are available for use. To obtain a license, contact your Cisco account representative.

Advanced OPM simulation, optimization, and predictive analysis functionality require a license. To install the license, complete the following steps:

Step 1 Run the license_install tool, passing it the name of the license file (.lic extension). By default, the tool merges the features that are granted by the new license with those features in an existing license.

```
license_install -file <path>/<license_name>.lic
```

Step 2 When prompted, enter the number that is associated with the directory in which you want to install the license.

Start and Stop Cisco WAE

From the Cisco WAE run-time directory, enter the relevant Cisco WAE CLI command to start or stop Cisco WAE services:

- **wae --start**—Starts or restarts Cisco WAE services.
- **wae --stop**—Stops Cisco WAE services.

Update Packages or Templates

If any packages or templates are updated or added in the *<wae_run_time_directory>*/packages directory, you must do one of the following:

- Restart Cisco WAE by running a package reload command.

  ```
  # wae --with-package-reload
  ```

- Request a package reload using the Cisco WAE CLI.

  ```
  # request packages reload
  ```

For example, you must perform a package reload when edit the wae.conf file.

Troubleshoot a Cisco WAE Installation

To check the status of Cisco WAE, enter `wae --status`.

Cisco WAE comes with standard logging features in the YANG run time. Cisco WAE logs to multiple log files in the *<wae-run-time>*`/logs` directory.

The LDAP authentication logs are logged in *[wae-run-time]/logs/wae-ldap-auth.log* file. The tool located in *[wae-install-dir]lib/exec/test-java-ssl-conn* is useful to test SSL connectivity for java applications like LDAP Authentication and EPNM notifications which provide useful information to debug certification issues.

The most useful log is *<wae-run-time>*`/logs/ncs-java-vm.log`. Most Cisco WAE packages log to this file. Some Cisco WAE packages also log to *<wae-run-time>*`/logs/ncs-python-vm-`*<package-name>*`.log`. The following example shows Python-VM based logs:

```
[wae@wae logs]$ pwd
/home/wae/wae-run/logs
[wae@host logs]$ ls -ltr ncs-python-vm*
-rw-rw-r-- 1 wae wae    0 Feb 26 07:50 ncs-python-vm-cisco-wae-opm-tte.log
-rw-rw-r-- 1 wae wae    0 Feb 26 07:50 ncs-python-vm-cisco-wae-get-plan.log
-rw-rw-r-- 1 wae wae    0 Feb 26 07:50 ncs-python-vm-cisco-wae-dmdmesh-creator-nimo.log
-rw-rw-r-- 1 wae wae    0 Feb 26 07:50 ncs-python-vm-cisco-wae-layout-nimo.log
-rw-rw-r-- 1 wae wae    0 Feb 26 07:50 ncs-python-vm-cisco-wae-opm-load-plan.log
-rw-rw-r-- 1 wae wae    0 Feb 26 07:50 ncs-python-vm-cisco-wae-dmddeduct-nimo.log
-rw-rw-r-- 1 wae wae    0 Feb 26 07:50 ncs-python-vm-cisco-wae-archive.log
-rw-rw-r-- 1 wae wae 2238 Feb 26 07:50 ncs-python-vm.log
-rw-rw-r-- 1 wae wae  270 Feb 26 08:20 ncs-python-vm-nso_wae_nodes_insert.log
```

By default, the log level is set to INFO. You can configure logging in the following ways:

- Define the log level of various logs in the run-time directory `wae.conf` file. For information about the `wae.conf` file, see the *Cisco WAE User Guide*.
- Use the Expert Mode to set logging capabilities for some network interface modules (NIMOs). For example, you can set logging capabilities such as topology NIMOs and the lsp-snmp-nimo module. For information about the Expert Mode, see the Cisco WAE User Guide.
- Use the Cisco WAE CLI to define the log level for various NIMO components. To define the log level, enter the following command at the command line:

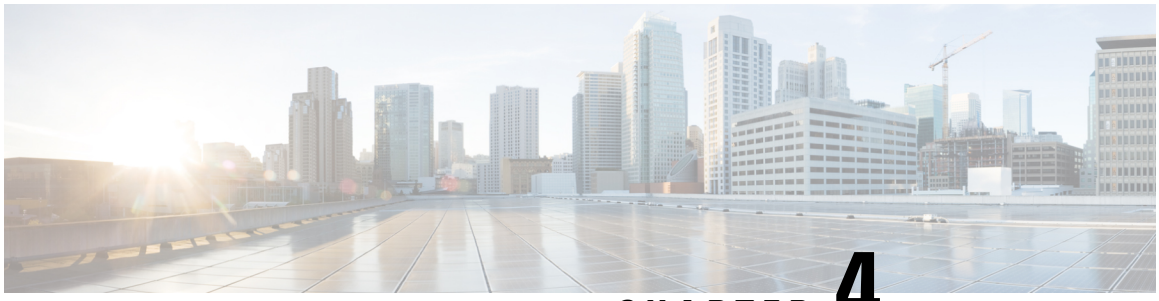
  ```
  admin@wae% set java-vm java-logging logger <nimo-component> level <level-x>
  ```

  Level types are `level-info`, `level-debug`, and `level-all`. The logs are saved to `ncs-java-vm.log` and can be used for troubleshooting.

  The following table lists basic NIMO components.

NIMO Component	Description
com.cisco.wae	General debugging
com.cisco.wae.nimo.topo	Topology-based NIMO debugging
com.cisco.wae.nimo.lspconfig	LSP configuration through NED debugging

NIMO Component	Description
com.cisco.wae.nimo.lsp	LSP debugging
com.cisco.wae.nimo.snmptrafficpoller	SNMP traffic poller debugging
com.cisco.cisco.wae.aggr	Aggregation debugging
com.cisco.wae.nimo.optical	Optical NIMO debugging



CHAPTER 4

Install Cisco WAE CM

Install Cisco WAE Coordinated Maintenance

Cisco WAE CM can be installed as standalone, in the same server where the Cisco WAE server software is installed, or with Cisco WAE Live. Do not install WAE CM as a root user.

Step 1 Navigate to and download the Cisco WAE Coordinated Maintenance zip file from the Cisco Download Software site.

Step 2 Log in to the server, copy the Cisco WAE Coordinated Maintenance zip file (<*CoordMaint.zip*> to a local directory, and unzip the file.

Example:

```
# unzip CoordMaint.zip
Archive: CoordMaiint.zip
    creating:  CoordMaint/
   inflating:  CoordMaint/install.sh
   inflating:  CoordMaint/maintenance.tar.gz
  extracting:  CoordMaint/ccordmaint.war
# ls
CoordMaint    Coordmaint.zip
```

Step 3 Navigate to the CoordMaint directory and install Cisco WAE Coordinated Maintenance.

```
# . ./install.sh
```

Step 4 When prompted, enter the directory for CM_HOME (location to install the database, the plan file, and the CM configuration file).

Step 5 Follow the installation prompts.

Step 6 If installed as standalone or on the same server as the Cisco WAE server software, from the *<CM_installation_directory>*/maintenance enter the following command to start WAE Coordinated Maintenance:

:

```
# ./start.sh
```

If installed on the same server as Cisco WAE Live, then restart the web server.

Note If not installed on the same server as Cisco WAE Live, you can also stop Cisco WAE Coordinated Maintenance at anytime using the `stop.sh` command.

Step 7 To start Cisco WAE Coordinated Maintenance, open one of the supported browsers, and enter **http://*server-ip*:*port_number*/coordmaint/**, where *server-ip* is the IP address of the server on which you have Cisco WAE Coordinated Maintenance installed and *port_number* is one of the following:

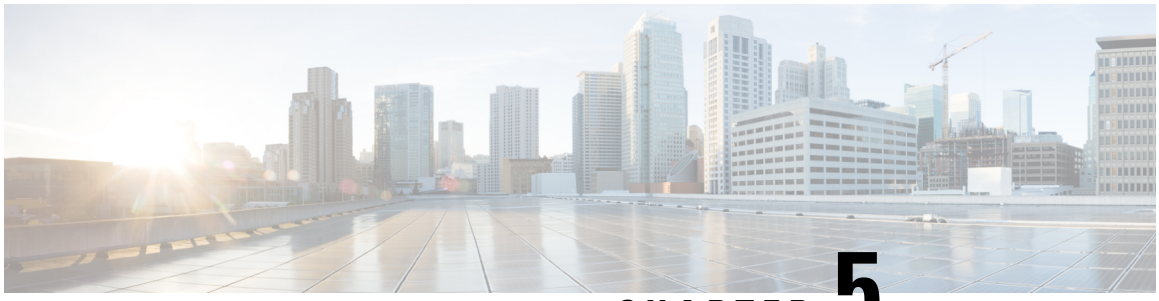
- **8843**—If installed as standalone or on the same server where the Cisco WAE server software is installed.
- **8443**—If installed on the same server where Cisco WAE Live is installed.

Note For WAE Coordinated Maintenance to work with Cisco WAE 7.1.2, remove `redirect` from the *wae.conf* file and restart Cisco WAE.

Step 8 Click the **Maintenance** link.

Step 9 Set the topology template (prompted only during initial setup). Navigate to **Settings** > **Data Source** tab. Enter the Cisco WAE 7.1 server and network information in the Topology Template fields.

For information about using Cisco WAE Coordinated Maintenance, see the Cisco WAE Coordinated Maintenance User and Administration Guide.



CHAPTER 5

Install Cisco WAE Live

This section contains the following topics:

Install Cisco WAE Live

Before you begin

- Cisco WAE Live cannot be installed on the same machine where the Cisco WAE 7.1 server software is installed.
- Confirm that the Cisco WAE Live server requirements are met (see WAE Live Requirements, on page 8).
- Do not install Cisco WAE Live as a root user.
- Confirm that you have a Cisco WAE 7.1 Live license on the server.
- WAE Live is installed in `$CARIDEN_ROOT/software/live`. For example: `/opt/wae/software/live` or `/opt/cariden/software/live`.
- If you plan to migrate Cisco WAE Live 6.4.9 or older data, first upgrade to Cisco WAE Live 6.4.10. Then, enter the same installation directory that was used in Cisco WAE Live 6.4.x when prompted to install Cisco WAE Live 7.1. For example, if `$CARIDEN_ROOT` is defined as `/opt/cariden` in Cisco WAE Live 6.4.x, then confirm that `$CARIDEN_ROOT` in Cisco WAE 7.1 is also defined as `/opt/cariden`.

Note Install Cisco WAE Live 7.1.1 before upgrading to Cisco WAE Live 7.1.2.

Step 1 Navigate to and download the Cisco WAE Live package from the Cisco Download Software site.

Step 2 Log in to the server, copy the Cisco WAE Live package <*WAE-Live-7x-xxxxxLinux-x86_64.bin*> to a local directory, and start a bash shell.

Step 3 Install the Cisco WAE Live package.

```
# bash <WAE-Live-7x-xxxxxLinux-x86_64.bin>
```

Step 4 If prompted, install the required software packages using the yum command.

Step 5 Follow the installation prompts.

Step 6 After installation, set environment variables and source ~/.profile to get the necessary settings.

```
# source ~/.profile
```

Step 7 Install Cisco WAE Live data store. For more information, see Install WAE Live Data Store, on page 27.

Step 8 Start Cisco WAE Live services.

```
# wae-live-start
```

Note The data store must be configured before starting Cisco WAE Live.

Step 9 Start one of the supported browsers and enter **`https://`***server-ip*`:8443`, where *server-ip* is the IP address of the server on which you have WAE Live installed. The default password for the **`admin`** user is "admin". The default password for the **`user`** user is "user". You will be prompted to change the default login credentials upon first login.

Upgrade from Cisco WAE Live 7.1.x to Cisco WAE Live 7.1.2 or Later

Before you begin

You must have Cisco WAE 7.1 or later installed to perform this upgrade. For Cisco WAE 6.4.x installations, see Migrate WAE 6.4.10+ Live Data to WAE Live 7.1.x, on page 23.

Step 1 Stop the web server and mld.

```
# wae-live-stop
```

Step 2 Install Cisco WAE Live 7.1.2 or later. For more information, see Install Cisco WAE Live, on page 21.

Step 3 Stop mld if it is running.

```
# mld -action stop
```

Step 4 Execute the upgrade.

```
# mld -action upgrade
```

Step 5 Start the web server and mld.

```
# wae-live-start
```

Migrate WAE 6.4.10+ Live Data to WAE Live 7.1.x

Before you begin

- ***You can only migrate data from WAE 6.4.10 or later to WAE 7.1.x.*** If you have an earlier WAE 6.x release installed, you must upgrade to at least WAE 6.4.10 before proceeding with the WAE 7.1.x upgrade.
- WAE Live 7.1.x and data store must be installed on a different machine than WAE 6.4.x. For installation steps, see Install Cisco WAE Live, on page 21. In addition, the WAE Live 7.1.x installation directory and data store (mld) options must use the same directory path and mld options that was used for the WAE 6.4.x installation. For example, if WAE 6.4.10 was installed on `/opt/cariden`, then you must also install WAE Live 7.1.x in `/opt/cariden` in another server. mld parameters, such as CPUs, memory, storage, and so forth, must also have the same values. To view existing mld parameters, you can look in the config.xml file.

  Note Install WAE Live 7.1.1 before upgrading to WAE Live 7.1.2.

- The WAE Live 7.1.x data store must be installed before doing this procedure. For data store installation instructions, see Install WAE Live Data Store, on page 27.
- You must continue to use the same WAE 6.4.x user ID (UID) and group ID (GID) after upgrading to WAE 7.1.x.

Step 1 From the WAE Live 7.1.x server, stop the web server.

```
embedded_web_server -action stop
```

Step 2 From the WAE Live 6.4.x Live server, do the following:

a) Stop the web server.

```
service wae-web-server stop
```

b) Back up the WAE Live data store. For example:

```
ml_backup -L 0
```

Step 3 From the WAE Live 7.1.x server:

a) Back up the WAE Live data store. For example:

```
ml_backup -L 0
```

b) Edit parameters in `$CARIDEN_ROOT/software/mld/current/scripts/sqlhosts.ml`.

Example:

On the WAE Live 6.4.x server, sqlhosts.ml has the following:

```
ml_remote onsoctcp 172.131.130.112 9089
mltcp     onsoctcp 127.0.0.1    9088
ml        onipcshm 127.0.0.1    dummy
```

On the WAE Live 7.1 server, change the sqlhosts.ml file to the following:

```
ml_remote onsoctcp <Live71_mld_IP_address> <Live71_port>
mltcp     onsoctcp 127.0.0.1    9088
ml        onipcshm 127.0.0.1    dummy
```

Step 4 Confirm that the data store directory (attribute in config.xml) is the same. If there are missing files on the WAE 7.1.x server, then create zero size files with the same name using the touch command.

Example:

On the WAE Live 6.4.10 server:

```
[cariden@wodl114 archives]$ cd $CARIDEN_ROOT/software/mld/current/data/

[cariden@wodl114 data]$ ls -la

total 63591328

drwxr-xr-x  2 cariden caridenstaff       4096 Dec  5 12:55 .

drwxr-xr-x 10 cariden caridenstaff       4096 Dec  5 12:35 ..

-rw-------  1 cariden caridenstaff 2147483648 Dec  5 13:01 catdbs001

. . . . . .

-rw-------  1 cariden caridenstaff 4294967296 Dec  5 14:31 sbspace000

-rw-------  1 cariden caridenstaff 2147483648 Dec  5 14:54 tempdbs000

-rw-------  1 cariden caridenstaff 2147483648 Dec  5 14:54 tempdbs001

-rw-------  1 cariden caridenstaff 4294967296 Dec  5 14:54 tsdbs000

-rw-------  1 cariden caridenstaff 4294967296 Dec  5 14:54 tsdbs001

-rw-------  1 cariden caridenstaff 4294967296 Dec  5 14:31 tsdbs002000

-rw-------  1 cariden caridenstaff 4294967296 Dec  5 14:31 tsdbs002001
```

Example:

On the WAE Live 7.1.x server, the missing files are `tsdbs002000` and `tsdbs002001`:

```
$CARIDEN_ROOT/software/mld/current/data

[cariden@wodl113 data]$ ls -la

total 46814024

drwxr-xr-x  2 cariden caridenstaff       4096 Dec  5 01:56 .

drwxr-x--- 10 cariden caridenstaff        143 Dec  5 01:44 ..

-rw-------  1 cariden caridenstaff 2147483648 Dec  5 22:52 catdbs001
```

```
. . . . . .

-rw-------  1 cariden caridenstaff 4294967296 Dec  5 22:50 sbspace000

-rw-------  1 cariden caridenstaff 2147483648 Dec  5 22:52 tempdbs000

-rw-------  1 cariden caridenstaff 2147483648 Dec  5 22:52 tempdbs001

-rw-------  1 cariden caridenstaff 4294967296 Dec  5 22:52 tsdbs000

-rw-------  1 cariden caridenstaff 4294967296 Dec  5 22:52 tsdbs001
```

You would then create zero size files so that WAE Live 7.1.x has the same contents as WAE Live 6.4.10.

```
touch tsdbs002000
touch tsdbs002001
chmod go-r tsdbs002000
chmod go-r tsdbs002001
```

Step 5 Copy the Live 6.4.x data store backup file to the Live 7.1 server.

Example:

```
scp $CARIDEN_ROOT/software/mld/current/backups/fullbackups/hostABC_1_L0
user@live71:$CARIDEN_ROOT/software/mld/current/backups/fullbackups/
```

Step 6 Rename the copied WAE 6.4.x data store backup file to the WAE 7.1 backup file.

Example:

If WAE Live 7.1.x backup file is named `host456_1_L0`, then

```
mv $CARIDEN_ROOT/software/mld/current/backups/fullbackups/hostABC_1_L0
$CARIDEN_ROOT/software/mld/current/backups/fullbackups/host456_71_L0
```

Step 7 Stop WAE 7.1.x mld and restore the data store backup.

```
mld -action stop
ml_restore -directory $CARIDEN_ROOT/software/mld/current/backups/fullbackups
```

Step 8 Run a sanity check. This process may take awhile.

```
mld -sanity all
```

Step 9 Restart mld.

```
mld -action restart
```

Step 10 From the WAE Live 6.4.x server, do the following:

a) Check the config.xml file to see if the following attributes are set to specific directories. If not, it is specified under the `MLData` attribute and the default path is `$CARIDEN_ROOT/data/mldata/`:

- `AppData`
- `Backup`
- `Map.ArchivePath`
- `ReportData`

If these attributes are set, copy the data from the respective directory to the same directory in the WAE Live 7.1.x server.

b) If the preceding attributes are not set, then use the tar command to pack all the respective directories and copy `mldata.tar` to the same directory on the WAE Live 7.1.x server.

Example:

```
tar -cvf mldata.tar appdata/ archives/ customdata/ jobs/ plans/ reports/
```

Copy `mldata.tar` to the WAE Live 7.1 server:

```
scp mldata.tar <WAE_71_host>:$CARIDEN_ROOT/data/mldata/.
```

On the WAE Live 7.1.x server, navigate to where the MLdata property values are located. For example:

```
cd $CARIDEN_ROOT/data/mldata/
tar -xvf mldata.tar
```

Step 11 From the WAE Live 6.4.x server, copy the following contents from `$CARIDEN_ROOT/etc` to the same path in WAE Live 7.1.x:

a) `$CARIDEN_ROOT/etc/config/config.xml`

b) `$CARIDEN_ROOT/etc/matelive`

c) `$CARIDEN_ROOT/etc/user_manager`

Example:

```
# tar -cvf etc.tar config/ matelive/ user_manager/
config/
config/config.xml
config/config.xml.bak
matelive/
user_manager/
user_manager/auth.db.properties
user_manager/auth.db.script

# scp etc.tar <WAE_64x_host>:$CARIDEN_ROOT/etc/.
```

From WAE Live 7.1.x server, copy the $CARIDEN_ROOT/etc directory.

```
# cd $CARIDEN_ROOT/etc
# tar -xvf etc.tar
```

Step 12 Start the WAE Live 7.1.x web server and data store:

```
wae-live-start
```

Cisco WAE Live Data Store

This section describes how to install, upgrade, back up, and restore a Cisco WAE Live data store. It also describes how to purge data using the `ml_purge` tool.

If the defaults were used during installation, `$CARIDEN_HOME` is the same as `/opt/cariden/software/live/current`.

Install WAE Live Data Store

The following procedure describes how to install the Cisco WAE Live Data Store using mld_tool. The `mld` tool installs both the mld server and an empty data store directory.

Before you begin

- For better performance, create a separate ext2 partition for the directory that is specified with the `-datastore` option.
- Understand what type of production environment you want to create.

Note

- After the data store is created, it is difficult to modify any of the installation options (including the user name).
- A 'demo' data store is just for pilot purpose. If you start with 'demo', then you must recreate the data store when it is time to move to production and the data in 'demo' data store will be lost.

- The `-demo` or `-storage`, `-cpu` and `-memory` options are required. For more information on the mld command and options, see mld Options, on page 27.

Step 1 If WAE Live is running, stop the web server:

```
# wae-live-stop
```

Step 2 Enter appropriate mld command to install the data store. For mld commands and options see mld Options, on page 27.

Example 1: To be prompted through installation and obtain sizing recommendations:

```
# mld -installchk
```

Example 2: To install mld with a demo data store size:

```
# mld -action install -demo true
```

Example 3: To install a small mld server into $CARIDEN_ROOT/data/matelive, reserve 2 CPUs, reserve 542 GB of disk storage and allocate 2.2 GB (2200 MB) of memory:

```
# mld -action install -mldata $CARIDEN_ROOT/data/matelive -cpus 2 -storage 1:1:540 -memory 200:55:2000
```

Step 3 Start mld and the web server:

```
# wae-live-start
```

mld Options

Option	Description	Default
`-version`	Displays the data store version.	

Option	Description	Default
`-action`	`install` —Installs a new mld server and data store, and start the mld server. `upgrade` —Updates an existing mld server and start the mld server. `start` —Alternative way to start the mld server. `stop` —Alternative way to stop the mld server. `status` —Alternative way to show the status of the mld server. `restart` —Alternative way to stop and then restart the mld server.	Default installation directory `$CARIDEN_ROOT/software/mld/current`
`-installchk`	Prompts you through installation and gives sizing recommendations.	
Use only with -action install (If an option is not given, the installation performs the same tasks as `-installchk` .)		
`-demo true`	Installs a demo data store. **Note** If both `-demo` and `-storage` options are used, `-demo` takes precedence.	
`-storage <n:n:n>`	Allocates the disk and memory based on the anticipated data store size, where <n:n:n> is data:indices:timeseries in GB. For details and recommended values, use `-installchk` and `-verbose` options. **Note** If the data store is larger than the demo size, this option is required when using `-action install`.	
`-memory <n:n:n>`	Allocates the requested memory of the data store, where <n:n:n> is data:indices:timeseries in MB. For details and recommended values, use `-installchk` and `-verbose` options.	
`-mldata <directory>`	Specifies directory where all application data is stored. This directory includes the data store, report output, and other application data.	`$CARIDEN_ROOT/data/mldata`
`-datastore <directory>`	Specifies directory where the data store is initialized. Once set, this directory cannot be changed. You can, however, use symbolic links.	`$CARIDEN_ROOT/data/mldata/datastore`

Option	Description	Default
`-cpus <#>`	Reserves the number of CPUs for the data store and the mld server.	Half of the total CPUs
Use only with -action install or -action upgrade		
`-mld <directory>`	Specifies directory where the mld server is installed. Once set, this directory cannot be changed. You can, however, use symbolic links.	`$CARIDEN_ROOT/software/mld/current`
`-backup <directory>`	Specifies directory for saving data store backups.	`$CARIDEN_ROOT/data/mldata/backup`

Back Up the Data Store

Cisco WAE Live backs up the time-series derived data from plan files. It does not back up transaction logs or other WAE Live data, such as application data and report data.

The required amount of space for backups depend on the installation size and how long a system has been running.

Best Practices

- Perform the backup to a different disk drive, or copy the backup to a different physical device after you finish the backup.
- Perform backups outside of peak traffic hours.
- Set up a backup directory that is on a different physical disk when you first install the mld server and data store. Doing so sets the default backup directory for all backups.

```
mld -action install -backup <backup_directory>
```

- The backup process makes a copy of the data store, but it does not back up other Cisco WAE Live data, such as application data and report data. Therefore, with some regularity, copy this other data to a safe location, such as to a different physical disk.
- Perform a full backup at least weekly or monthly, with numerous incremental backups in between them.
- Rather than running manual backups, call `ml_backup` from a cron job.
- Perform only 1 backup at a time so that their schedules do not overlap. Running simultaneous backups are not supported. Ensure that there is at least 1 hour between each backup. After it completes, verify that the backup was completed within the hour.

Backup Steps

Caution If you delete the previous mld installation directory, you may delete all the data. To check the current location, enter the following command: `mld -diag -c | egrep ROOTPATH`

The `ml_backup` tool enables you to perform multiple levels of backups to save disk space. An OS file system backup cannot be used to restore the data store. Use the `ml_backup` tool to perform a complete backup to use for data store restoration.

You can execute `ml_backup` to run a manual backup at any time. However, the first time you use backup levels, you must perform backups in this sequence.

Note Keep both the data store and the web server running.

Sequence	Enter	Description

1	`ml_backup`
	or
	`ml_backup -L 0`
		Level 0—Back up everything.

2	`ml_backup -L 1`	Level 1—Back up everything since the most recent Level 0 backup was performed.
3	`ml_backup -L 2`	Level 2—Back up everything since the most recent Level 1 backup was performed.

Note For larger systems that frequently run plan file processes, less incremental Level 1 and Level 2 backups are available in between Level 0 backups. The following error appears when a Level 1 or Level 2 backup is not available:

```
Archive failed - The existing level-0 backup for DBspace rootdbs is too old to allow any
      incremental backup.
```

When this error appears, run a Level 0 backup.

To run a backup using all defaults, enter `ml_backup`. The tool uses the default backup directory, and creates a full backup.

- To override the default backup directory, use the `-directory` option. The default backup directory is `$CARIDEN_ROOT/data/mldata/backup`.
- To set a different backup level, use the `-L` option.

The following example sets the backup directory to `$CARIDEN_ROOT/data/waelive/backups` and backs up only data that is new since the last level 0 backup was run. This assumes that you ran `ml_backup` one time using the default level of 0.

```
ml_backup -directory /data/waelive/backups -L 1
```

Restore the Data Store

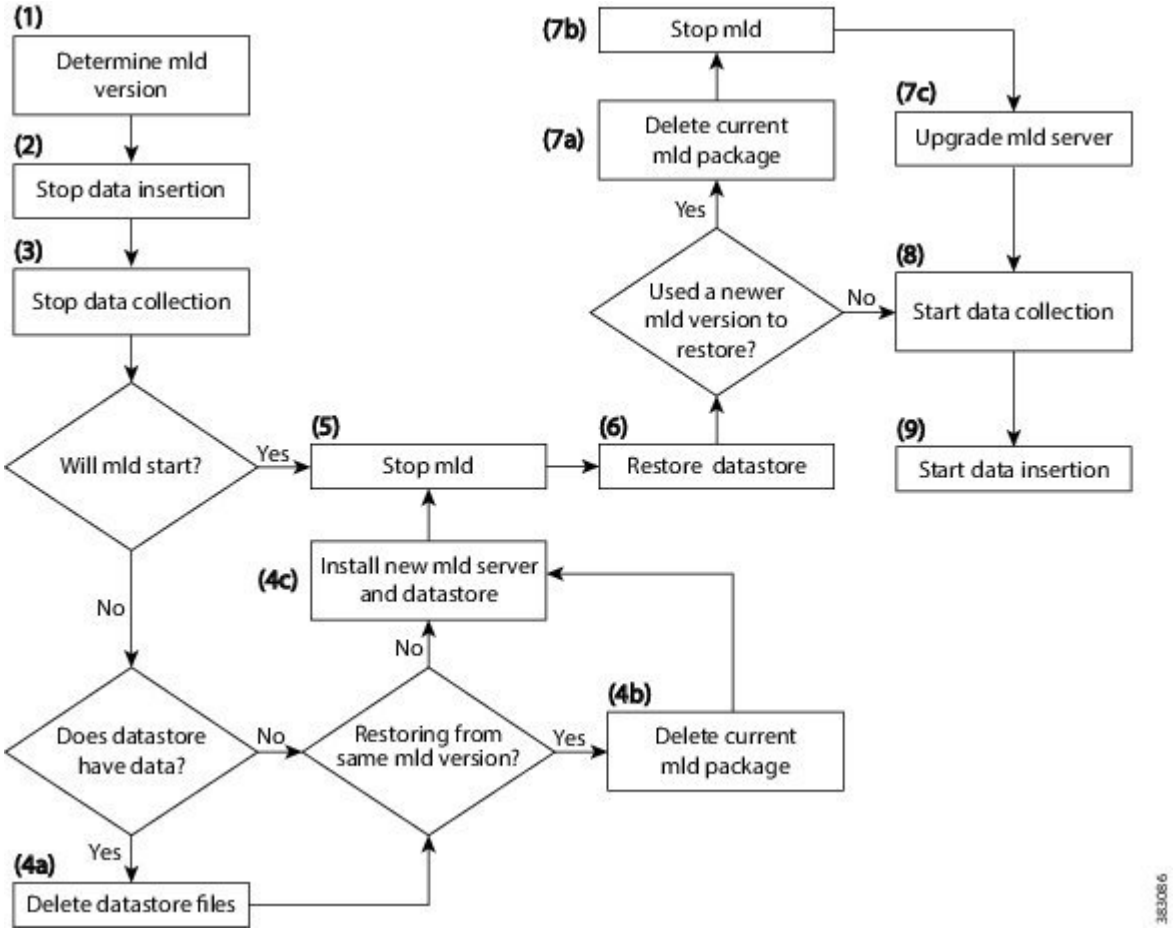
Note the following before attempting to restore the data store:

- To restore a data store, you must have a backup of it. For information about backing up the data store, see the Backing Up the Data Store section.

- Ensure you have a proper disk and disk space. For example, if your data was corrupted, you would need a new disk. If the restoration is due to a space issue, then add more space to the existing disk.
- If you have a single device configuration, the collection of data will be interrupted during the restoration of a WAE Live data store.
- If the backup data store resides on a different device, confirm that the following prerequisites are met:
  - The username and user ID (uid) of both devices must be the same.
  - The backup data store name uses a hostname as a portion of its name. This hostname portion of the backup data store name must be changed to be the same as the hostname on the device to which it is being restored.

    Example: The backup data store name is akdobi.acme.com_1_L0. The hostname on the device on which the data store is being restored is akgudei.acme.com. In this case, change the backup data store name to akgudei.acme.com_1_L0.

Figure 1: Data Store Restoration Workflow



Delete Data from the Data Store

The `ml_purge` tool removes all data prior to the specified timestamp.

Before you begin

Before running `ml_purge`, confirm that there are no insertions running (`ml_insert_ctl -status`). Insertions might fail due to locks created by `ml_purge` while it is in operation. You might need to pause the scheduler to prevent scheduled insertions (`ml_insert_ctl -disable-scheduler`).

To run `ml_purge`:

```
# ml_purge <timestamp>
```

where <*timestamp*> is in the following UTC format: *year-month-day* `T` *hour:minutes*. For example:

```
# ml_purge 2017-01-31T00:00
```

Install the Cisco WAE Live License

Before you begin

Confirm you have the Cisco WAE Live license on your server.

Step 1 If Cisco WAE Live is not running, start it.

```
# embedded_web_server -action start
```

Step 2 Start the Cisco WAE Live UI in a supported browser: `https://<server_IP>:8443`. The default username is "admin" and the password is "admin".

Step 3 Choose **System** > **Licenses**.

Step 4 Click **Upload Traditional License**.

Step 5 Click **Select Licenses**.

Step 6 Browse to the location or enter the name of the license file (.lic extension), and click **Open**.

Step 7 Click **Upload License**.

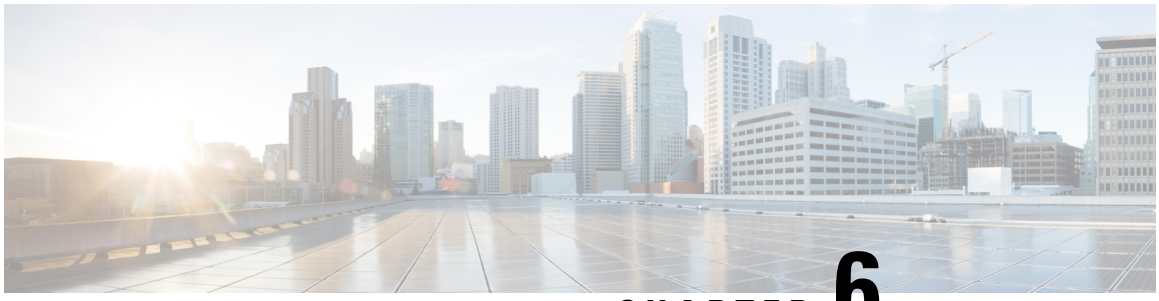
Step 8 Restart Cisco WAE Live.

```
# embedded_web_server -action restart
```

What to do next

You can begin using Cisco WAE Live and collect plan files. To collect plan files from Cisco WAE 7.1.x, go to **Settings** > **Data Source** and click the 7.1 Remote Archive option. Enter the appropriate Cisco WAE 7.1.x

network and server details. For information about using Cisco WAE Live, see the Cisco WAE Live User Guide.



CHAPTER 6

Security

Core Security Concepts

If you are an administrator and are looking to optimize the security of your product, you should have a good understanding of the following security concepts.

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) uses Secure Sockets Layer (SSL) or its subsequent standardization, Transport Layer Security (TLS), to encrypt the data transmitted over a channel. Several vulnerabilities have been found in SSL, so now supports TLS only.

Note TLS is loosely referred to as SSL often, so we will also follow this convention.

SSL employs a mix of privacy, authentication, and data integrity to secure the transmission of data between a client and a server. To enable these security mechanisms, SSL relies upon certificates, private-public key exchange pairs, and Diffie-Hellman key agreement parameters.

SSL Certificates

SSL certificates and private-public key pairs are a form of digital identification for user authentication and the verification of a communication partner’s identity. Certificate Authorities (CAs), such as VeriSign and Thawte, issue certificates to identify an entity (either a server or a client). A client or server certificate includes the name of the issuing authority and digital signature, the serial number, the name of the client or server that the certificate was issued for, the public key, and the certificate's expiration date. A CA uses one or more signing certificates to create SSL certificates. Each signing certificate has a matching private key that is used to create the CA signature. The CA makes signed certificates (with the public key embedded) readily available, enabling anyone to use them to verify that an SSL certificate was actually signed by a specific CA.

In general, setting up certificates involve the following steps:

1. Generating an identity certificate for a server.

2. Installing the identity certificate on the server.
3. Installing the corresponding root certificate on your client or browser.

The specific tasks you need to complete will vary, depending on your environment.

1-Way SSL Authentication

This authentication method is used when a client needs assurance that it is connecting to the right server (and not an intermediary server), making it suitable for public resources like online banking websites. Authentication begins when a client requests access to a resource on a server. The server on which the resource resides then sends its server certificate (also known as an SSL certificate) to the client in order to verify its identity. The client then verifies the server certificate against another trusted object: a server root certificate, which must be installed on the client or browser. After the server has been verified, an encrypted (and therefore secure) communication channel is established. At this point, the server prompts for the entry of a valid username and password in an HTML form. Entering user credentials after an SSL connection is established protects them from being intercepted by an unauthorized party. Finally, after the username and password have been accepted, access is granted to the resource residing on the server.

Note A client might need to store multiple server certificates to enable interaction with multiple servers.

To determine whether you need to install a root certificate on your client, look for a lock icon in your browser's URL field. If you see this icon, this generally indicates that the necessary root certificate has already been installed. This is usually the case for server certificates signed by one of the bigger Certifying Authorities (CAs), because root certificates from these CAs are included with popular browsers.

If your client does not recognize the CA that signed a server certificate, it will indicate that the connection is not secure. This is not necessarily a bad thing. It just indicates that the identity of the server you want to connect has not been verified. At this point, you can do one of two things: First, you can install the necessary root certificate on your client or browser. A lock icon in your browser's URL field will indicate the certificate was installed successfully. And second, you can install a self-signed certificate on your client. Unlike a root certificate, which is signed by a trusted CA, a self-signed certificate is signed by the person or entity that created it. While you can use a self-signed certificate to create an encrypted channel, understand that it carries an inherent amount of risk because the identity of the server you are connected with has not been verified.

Install Certificates

This section contains information about installing security certificates on the Cisco WAE server, Cisco WAE Coordinated Maintenance, and Cisco WAE Live.

Install a Certificate for the Cisco WAE Server

Cisco WAE comes with a default certificate. Because this certificate is not from a “trusted CA", the browser shows an unsecured connection warning. This is the expected behavior. The warning can be removed by applying an appropriate Certificate Authority (CA) issued certificate.

Step 1 Create a private server key and store it in a secure location. For example:

```
# openssl genrsa -out server.key 2048
```

Step 2 Create the Certificate Signing Request (CSR). The CSR is used by CA to create a certificate that identifies your website as secure. For example:

```
# openssl req -sha256 -new -key server.key -out server.csr
```

Step 3 Submit the CSR to the Certificate Authority to obtain your Certificate (for example, server.crt).

Step 4 Modify the *<WAE_installation_directory>*`/wae.conf` by changing `<key-file/>` and `<cert-file/>` elements to point to the location of the server.key and server.crt files.

Step 5 Restart the Cisco WAE server.

```
# wae --stop
# wae --start
```

Install a Certificate for Cisco WAE CM

Cisco WAE CM includes a default certificate that causes the browser to indicate that the certificate is not trusted. This is the expected behavior. The warning can be removed by installing an appropriate CA issued certificate. This procedure is not applicable if Cisco WAE CM is installed under Cisco WAE Live 7.1.1.

Before you begin

Note This procedure is only applicable if Cisco WAE CM is installed in standalone mode or under Cisco WAE 7.1.1 and later.

- You must be an administrator with Cisco WAE user privileges to perform this task.
- Add the following environment variable:

```
# export CM_INSTALLATION_DIR=<CM_installation_directory>
# export
JETTY_BASE=$CM_INSTALLATION_DIR/maintenance/jetty-distribution-9.2.10.v20150310/cm2
```

Confirm that JRE is installed as part of the Cisco WAE CM requirement. You can verify that JRE is installed by using the **keytool** command to list the current certificate.

```
# keytool -list -keystore $JETTY_BASE/etc/keystore
```

Step 1 In order to obtain a certificate from the Certificate Authority (CA) of your choice, you have to create a Certificate Signing Request (CSR). To create a CSR follow these steps:

a) Delete the default certificate.

```
# keytool -delete -alias jetty -keystore $JETTY_BASE/etc/keystore
```

b) Create a local self-signed certificate.

```
# keytool -genkey -alias jetty -keyalg RSA  -keystore $JETTY_BASE/etc/keystore
```

c) Create the CSR.

```
# keytool -certreq -keyalg RSA -alias jetty -file jetty.csr -keystore $JETTY_BASE/etc/keystore
```

d) Submit the CSR to a Certificate Authority to obtain your certificate.

e) Restart Cisco WAE CM.

```
# cd $CM_INSTALLATION_DIR/maintenance
# ./stop.sh
# ./start.sh
```

Step 2 Install the certificate.

a) Download a Chain Certificate (also called a Root Certificate) from the CA you obtained the certificate from.

b) Import the Chain Certificate into the keystore.

```
# keytool -import -alias root -keystore $JETTY_BASE/etc/keystore -trustcacerts -file
<filename_of_the_chain_certificate>
```

c) Import the new certificate.

```
# keytool -import -alias jetty -keystore $JETTY_BASE/etc/keystore -file <your_certificate_filename>
```

d) Restart Cisco WAE CM.

```
# cd $CM_INSTALLATION_DIR/maintenance
# ./stop.sh
# ./start.sh
```

Install a Certificate for Cisco WAE Live

Cisco WAE Live includes a default certificate that causes the browser to indicate that the certificate is not trusted. This is the expected behavior. The warning can be removed by applying an appropriate CA issued certificate.

To install a CA certificate for Cisco WAE Live, do the following:

Before you begin

Note This procedure is only applicable for Cisco WAE Live 7.1.1 and later.

- You must be an administrator with Cisco WAE user privileges to perform this task.
- Modify the path to add access to the Java keytool by adding the following line to the user .profile or .bash_profile file. For example:

```
# export PATH=$PATH:$CARIDEN_HOME/lib/ext/jre/1.8.0/bin/
```

Note The previous example is applicable if your shell is sh, ksh, or bash. Use equivalent commands for other shells.

- Log out and in again, or enter the following command using the appropriate profile filename.

```
# source ~/.profile
```

Step 1 In order to obtain a certificate from the Certificate Authority (CA) of your choice, you have to create a Certificate Signing Request (CSR). To create a CSR follow these steps:

a) Delete the default certificate. For example:

```
# keytool -delete -alias tomcat -keystore $CARIDEN_HOME/lib/web/apache-tomcat-8.5.15/conf/keystore
```

b) Create a local self-signed Certificate. For example:

```
# keytool -genkey -alias tomcat -keyalg RSA -keystore
$CARIDEN_HOME/lib/web/apache-tomcat-8.5.15/conf/keystore
```

c) Create the CSR. For example:

```
# keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr -keystore
$CARIDEN_HOME/lib/web/apache-tomcat-8.5.15/conf/keystore
```

d) Submit the CSR to a Certificate Authority to obtain your certificate.

e) (Optional) Restart Cisco WAE Live to use the new certificate immediately.

```
# embedded_web_server -action stop
# embedded_web_server -action start
```

Step 2 Install the certificate.

a) Download a Chain Certificate (also called a Root Certificate) from the CA you obtained the certificate from.

b) Import the Chain Certificate into the keystore.

```
# keytool -import -alias root -keystore $CARIDEN_HOME/lib/web/apache-tomcat-8.5.15/conf/keystore
 -trustcacerts -file <filename_of_the_chain_certificate>
```

c) Import the new certificate.

```
# keytool -import -alias tomcat -keystore $CARIDEN_HOME/lib/web/apache-tomcat-8.5.15/conf/keystore
 -file <your_certificate_filename>
```

d) Restart Cisco WAE Live.

```
# embedded_web_server -action stop
# embedded_web_server -action start
```

Install a Certificate for the LDAP Server

Cisco WAE supports authentication and authorization of foreign users using Lightweight Directory Access Protocol (LDAP).

To use LDAPS protocol, get the SSL certificate and add it to a keystore.

Step 1 Save the self signed certificate to cert.pem file using the following command:

```
# openssl s_client -connect <ldap-host>:<ldap-ssl-port> </dev/null 2>/dev/null | sed -n
'/^-----BEGIN/,/^-----END/ { p }' > cert.pem
```

Step 2 Get the default key-store path by running the following command from `WAE_RUN` directory.

```
# $WAE_ROOT/lib/exec/test-java-ssl-conn <ldap-host> <ldap-ssl-port> 2>1 | grep "trustStore is:"
```

Running the above command helps you find the directory from where certs are picked up. It may be a directory similar to:

```
trustStore is: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86_64/jre/lib/security/cacerts
```

Step 3 Import cert into default key-store using following command:

```
# sudo keytool -import -keystore <default-key-store-path> -storepass changeit -noprompt -file cert.pem
```

Install a Certificate for the EPN-M Server

Install the certificate when using the Cisco Evolved Programmable Network Manager (Cisco EPN Manager) agent for L1 collection.

Step 1 Save the self signed certificate to cert.pem file using the following command:

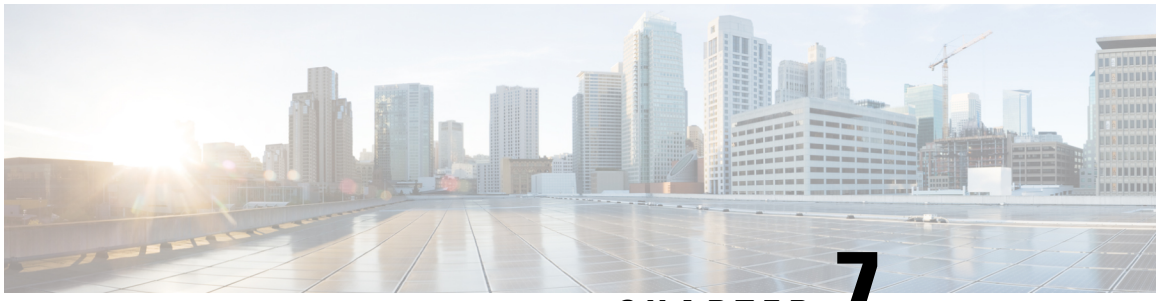
```
# openssl s_client -connect <epnm-host>:<epnm-port> </dev/null 2>/dev/null | sed -n
'/^-----BEGIN/,/^-----END/ { p }' > cert.pem
```

Step 2 Get the default key-store path using the following command. Typically the default key-store path is /etc/pki/java/cacerts for CentOS 7 with open-jdk

```
# $WAE_ROOT/lib/exec/test-java-ssl-conn <epnm-host> <epnm-port> 2>1 | grep "trustStore is:"
```

Step 3 Import cert into default key-store using following command:

```
# sudo keytool -import -keystore <default-key-store-path> -storepass changeit -noprompt -file cert.pem
```



CHAPTER 7

Next Steps

The following topics describe the next steps you perform to get started with Cisco WAE. You access the WAE UI, WAE Expert Mode, or WAE CLI to perform operations. For detailed information, see the *Cisco WAE User Guide*.

Log In to Cisco WAE

This section describes how to log in to the available Cisco WAE interfaces: Cisco WAE UI, Expert Mode, and the Cisco WAE CLI. For more information about these interfaces, see the Cisco WAE User Guide.

Log In to the Cisco WAE UI

Follow these steps to log in to the Cisco WAE web UI.

Before you begin

Confirm that all the appropriate services are running. All services automatically start after installation. For information about how to start or stop Cisco WAE, see Start and Stop Cisco WAE, on page 15.

Step 1 Start one of the supported browsers. See Cisco WAE Installation Requirements, on page 3.

Step 2 In the browser's address bar, enter `https://`*server-ip*`:8443`, where *server-ip* is the IP address of the server where Cisco WAE installed.

The Cisco WAE user interface displays the **Login** window.

Step 3 Enter the web UI username and password. The default credentials are:

- Username: admin
- Password: Admin@123

Step 4 Click **Login**.

The home page appears and you can now use the web UI.

What to do next

After you log in to Cisco WAE, you can start a network topology collection to create a network model. For information about creating a network model, see the Cisco WAE User Guide.

Log In to the Expert Mode

You must log in to the WAE UI before accessing the Expert Mode.

Before you begin

Confirm that all the appropriate services are running. All services automatically start after installation. For information about how to start or stop Cisco WAE, see Start and Stop Cisco WAE, on page 15.

Step 1 Start one of the supported browsers. See Cisco WAE Installation Requirements, on page 3.

Step 2 In the browser's address bar, enter **`https://`***server-ip*`:8443`**, where *server-ip* is the IP address of the server where Cisco WAE is installed.

The Cisco WAE UI displays the **Login** window.

Step 3 Enter the Cisco WAE UI username and password. The default credentials are:

- Username: admin
- Password: Admin@123

Step 4 Click **Login**.

The home page appears and you can now use the web UI.

Step 5 In the top-right corner of the Cisco WAE UI, click the tool icon to access the Expert Mode.

What to do next

After you log in to Cisco WAE, you can start a network topology collection to create a network model. See the Cisco WAE User Guide.

Log In to the WAE CLI

To log in to the WAE CLI:

Step 1 Navigate to the WAE run-time directory and enter `wae_cli`.

```
# wae_cli -u admin
admin@wae#
```

Note You can enter `wae_cli --help` to view all the WAE CLI options.

Step 2 (Optional) To enable configuration operations, switch to the configuration mode.

```
admin@wae# config
admin@wae%#
```

Example

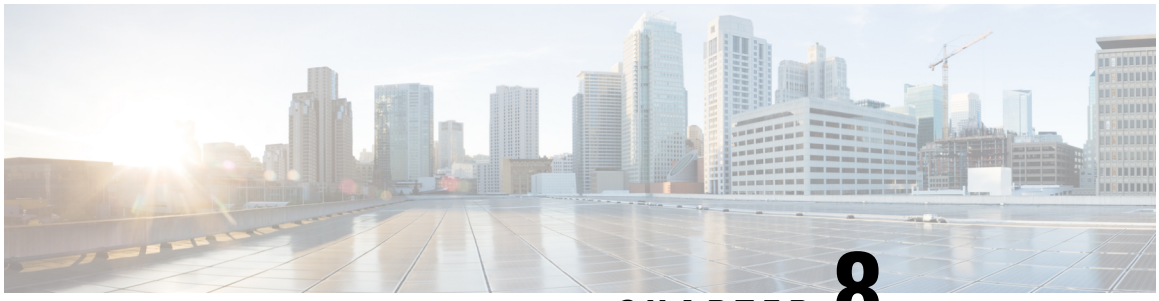
For example:

```
waerun# wae_cli -u admin
admin@wae# config
admin@wae%#
```

Build a Network Model

This topic gives a high-level description of tasks that are necessary to build a network model. For more detailed information, see the Cisco WAE User Guide.

1. Configure device authgroups, SNMP groups, and network profile access.
2. (Optional) Configure agents. This step is required only for collecting XTC, LAG and port interface, or multilayer information.
3. Configure an aggregated network and sources with a topology NIMO.
4. Configure additional collections such as demands, traffic, layout, inventory, and so on.
5. Schedule when to run collections.
6. Configure the archive file system location and interval at which plan files are periodically stored.
7. (Optional) View plan files in Cisco WAE applications.



CHAPTER 8

Uninstall Cisco WAE

Uninstall Cisco WAE

This procedure describes how to remove a Cisco WAE installation.

Note You can have more than one instance of Cisco WAE installed. When going through the uninstallation procedure, make sure you are removing the correct Cisco WAE installation and run-time directories.

Step 1 From the Cisco WAE run-time directory, stop Cisco WAE services.

```
# wae --stop
```

Step 2 Navigate to the parent directory and remove the Cisco WAE installation and run-time directories.

```
# rm -rf <wae_installation_directory>
# rm -rf <wae_run_time_directory>
```

Example

For example:

```
# wae --stop
# cd
# rm -rf waeinstall
# rm -rf waerun
```

Uninstall Cisco WAE