



Cisco WAE 6.4 System Administration Guide

July 2016

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2016 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Overview 1-1

- New and Changed Information 1-1
- Bookmarks 1-2
 - Add Bookmarks 1-2
 - Manage Bookmarks 1-2
 - Add System-Wide Bookmarks 1-2

CHAPTER 2

Licenses 2-1

- Upload Licenses 2-1

CHAPTER 3

User Management 3-1

- User and Admin Roles 3-1
 - Default Roles and Passwords 3-2
- User Fields 3-2
 - Required Fields 3-2
 - Optional Fields 3-2
- Available Applications on the WAE UI 3-3
- User Profile Settings 3-3
 - Change Time Zone 3-3
 - Change Password 3-3

CHAPTER 4

LDAP Configuration 4-1

- Overview** 4-1
- Pre-Installation Steps 4-1
- Configuring LDAP** 4-3

CHAPTER 5

SMTP Server 5-1

- SMTP Fields 5-1
 - Required Fields 5-1
 - Optional Fields 5-2

CHAPTER 6**Log Settings 6-1**

Configuring Log Settings 6-1

Configuring an Application Server Access Log 6-1

CHAPTER 7**Services and Statistics 7-1**

Services 7-2

Service Types 7-2

Monitor Services 7-2

Service Location 7-3

Ports 7-3

Viewing Service Status Details 7-3

Managing and Configuring Services 7-4

Events 7-4

Viewing Event Log Details 7-4

Viewing Event Log Graphs 7-5

Platform Diagnostics 7-5

Using the Events and Diagnostic UIs 7-7

Time Filters and Refresh Intervals 7-7

Viewing Database Information 7-8

CHAPTER 8**Local Server Status 8-1**

System 8-1

Load 8-2

Status 8-2

Memory 8-2

Disk 8-3

CHAPTER 9**Applications 9-1**

Installing the Application 9-1

Application File Contents 9-2

CHAPTER 10**Core Security Concepts 10-1**

HTTPS 10-1

SSL Certificates 10-1

1-Way SSL Authentication 10-2

Installing an SSL Certificate 10-3

CHAPTER 11

Additional Administrative Tasks 11-1

Starting and Stopping Services Using the CLI 11-1

Changing Encrypted Passwords 11-1

Viewing Temporary Files 11-2

Limiting Application Server Access to Specific IP Addresses 11-2

CHAPTER 12

Troubleshooting 12-1



Overview

New and Changed Information

The following table describes changes to this document.

Date	Revision
2018-05-18	<ul style="list-style-type: none">Added Chapter 10, “Core Security Concepts.”
2017-04-17	<ul style="list-style-type: none">Added the Configuring an Application Server Access Log section which describes how to configure logging of when an application server is accessed.Added the Limiting Application Server Access to Specific IP Addresses section which describes how to limit access to the application server to approved IP addresses.
2016-07-08	Initial publication.

This guide describes both the System UI and the Statistics UI, as well as other system-related tasks.

- **Statistics UI**—Enables you to monitor processes (services), logged events, and diagnostics for either a single-system deployment or for a distributed (high-availability) one using multiple servers.
 - [Services and Statistics](#)—Describes the services, as well as how to start and stop them. Describes the Process Status, Event Logs, and Platform Diagnostics UIs and how to use them.
- **System UI**—Enables you to manage configurations that apply to accessing and using the web UI. These configurations (and thus, the corresponding documentation) are only for the local server.
 - [Licenses](#)—Describes how to install local licenses, and view relevant information, such as their licensed features and expiration dates.
 - [User Management](#)—Describes how to add, edit, activate/de-activate, and delete users and their roles from the local user database.
 - [LDAP Configuration](#)—Describes how to configure access to the LDAP server for user authentication, and configure mappings between LDAP groups and local system roles.
 - [SMTP Server](#)—Describes how to configure access to the local SMTP server used for emailing WAE Live reports.

- [Log Settings](#)—Describes how to configure aggregation of all syslog messages to a syslog server.
- [Local Server Status](#)—Describes the status information about the local device: system load, memory, and disk space.
- [Applications](#)—Describes how to install applications in the WAE UI.
- [Additional Administrative Tasks](#)—Describes additional administrative tasks that are not done using the WAE UI.
- [Troubleshooting](#)—Offers a few tips on troubleshooting WAE products.

Bookmarks

Add Bookmarks

You can set bookmarks for any page in the UI.



-
- Step 1** Go to the page you want to bookmark.
 - Step 2** Click the bookmark icon.
 - Step 3** Click **Bookmark This Page**.
-

Manage Bookmarks

-
- Step 1** Click the bookmark icon.
 - Step 2** Click **Bookmark Manager**.
 - To edit a bookmark, hover over the bookmark name and click it, or click the **Edit** (pencil) icon. Change the Caption or URL as needed, and click **Update**.
 - To delete a bookmark, click the associated **Delete** icon and then click **OK** to confirm.
 - Step 3** Click **Save**.
-

Add System-Wide Bookmarks

If you have an admin role, you can set bookmarks for all users of the local server.

-
- Step 1** Go to the page you want to bookmark.
 - Step 2** Click the bookmark icon.

- Step 3 Click **Bookmark This Page**.
 - Step 4 Select **System bookmark** and click **Save**.
-



Licenses

Access: **System > Licenses**

All web-based products use a dedicated license, and each license grants specific usage rights for software features.

This page gives immediate information on which licenses are installed, including the expiration date and the number of nodes for which it is valid. This page also lists the Cisco license version number, which is not the same as the product's release number.

- To view a list of the details about a license, click the **Features** button.
- To install a new license, click the **Upload License** button.

The lower left identifies on which host the license is installed, and where the license is located.

This chapter is specific to the web UI Licenses page. For more comprehensive information on license installation, see the *Cisco WAE Server Installation Guide*.



Note

The license installation and information accessed from this UI apply only to the local server.

Upload Licenses

-
- Step 1** Choose **System > Licenses**.
- Step 2** Click **Upload Licenses**.
- Step 3** Click **Select Licenses**.
- a. Browse to the location or enter the name of the license file (.lic extension), and click **Open**.
 - b. If there is already a license installed, the default is to replace the existing license. To merge the two licenses instead, select the merge option. If you are uncertain whether you have a complete set of desired features in the new license, we recommend that you merge the licenses.
 - c. Click **Upload License**.
- Step 4** Verify the license installed correctly by locating it on the **System > Licenses** page.
-



User Management

The **System > Users** and **System > User Access** pages enables administrators to manage users in a local database. Administrators can add, edit, delete users and their passwords, as well as activate and de-activate them. Users are assigned roles, which sets their permissions for using the web applications, WAE Collector UI, System UI, and Statistics UI. These roles cannot be set on a per product basis.

When the system verifies a user, it first checks this local database. If it cannot find the user, it checks the LDAP Server database.



Note

These configurations apply only to the local server.

User and Admin Roles

Each user can be assigned one or more roles: administrator or user.

- Administrator—Can see and use all of the products and applications. With this role, you have these permissions.
 - Add and delete other users, edit their information (including password), temporarily enable or disable them, and assign them roles.
 - Upload templates to remote servers through the WAE Design GUI.
 - Configure the WAE Collector UI and augmented snapshots.
 - Configure application settings.
 - Configure licenses from the web UI.
 - Configure the SMTP and LDAP servers.
 - Enable/disable monitoring of services, as well as to start and stop services from the Statistics UI.
 - Change encrypted passwords used by configuration files. For more information, see [Chapter 11, “Additional Administrative Tasks.”](#)
 - Hide applications on the WAE UI from a user.
- User—Can use all of the application tasks that are available outside of the above scope.

Default Roles and Passwords

There are two default login and password combinations, one for each role.



Note

To increase security, we recommend that you immediately change both of these default passwords. See the [User Fields](#) section.

Default Username	Default Password	Default Role
admin	cariden	Administrator
user	cariden	User

User Fields

Required Fields

- **Add User**—Add new users and passwords, assign roles, activate and de-activate user access, and edit any of this information. Users cannot access the UI unless they are administratively added. The exception is they can use the default user login and password if those are available.
- **Username**—Login name for all the web UIs. Once the username is saved, neither the administrator, nor the user can change it.
- **Password**—When adding users, you must enter a password for them. Users can change their passwords once they log into the UI. They will be prompted to change their password when they first log in. The new password must contain at least one uppercase letter, lowercase letter, number, and a special character (excluding space). It must also be at least 8 characters. Once a password is added, it remains in effect until changed even though it is not visible on the page.



Note

LDAP users cannot manage passwords using the WAE UI.

- **Roles**—This option determines whether users can perform administrative functions. For more information, see the [User and Admin Roles](#) section.
- **Active**—Turn UI access on and off for existing users. This is a convenient way to temporarily disable users, for example, if they have to be away for an extended period.

Optional Fields

- **Edit (pencil icon)**—Edit all user information, and activate or de-activate user access.
- **Delete (trash can icon)**—Permanently delete users from accessing the UI. The exception is they can use the default user login and password if those are available. There is no undo.
- **Description**—Summary explanation to give more information about this user.
- **First Name**—First name of the user.
- **Last Name**—Last name of the user.

- **Advanced Config**—This is for advanced configuration editing only. Consult your support representative for assistance.

Available Applications on the WAE UI

As an administrator, you can configure which applications are visible on the WAE UI for all users.

-
- Step 1** From the WAE UI, select **WAE System > User Access**.
- Step 2** Under each application, toggle the On/Off button to show or hide the application from appearing on the WAE UI.
- Step 3** Click **Save**.



Note

- Home and Statistics cannot be hidden from the WAE UI.
 - Users with the User role do not see the System application and it cannot be hidden from administrators.
 - Users with the User role do not see the Collector application. However, an administrator can choose to hide the Collector application from the WAE UI for administrators.
-

User Profile Settings

Each user can change their password and customize the time zone displayed in WAE Live, Statistics > Database Info, and Coordinate Maintenance.

Change Time Zone

-
- Step 1** From the WAE UI, click the user icon located in the upper right corner.
- Step 2** Select **Profile**.
- Step 3** Select the **Display Time Zone** tab.
- Step 4** From the drop-down list, select the appropriate time zone that you want displayed.
- Step 5** Click **Save**. The selected time zone is now displayed.
-

Change Password

-
- Step 1** From the WAE UI, click the user icon located in the upper right corner.
- Step 2** Select **Profile**.
- Step 3** Select the **Change Password** tab and type in the appropriate passwords.

Step 4 Click **Change Passwords**.



LDAP Configuration

Overview

Cisco WAE supports authentication and authorization of foreign users using the LDAP protocol. The embedded directory service within the WAE system is based upon Java Enterprise Directory libraries that are linked with the Tomcat server instance. The objective of the LDAP module is to allow customers to map multiple LDAP user groups to privilege level roles in the WAE system.

Before You Begin

You should have the following:

- Cisco WAE Release 6.0 or above installed
- An external LDAP server
- An ldapsearch Linux library
- An LDAP user account with permissions to read the necessary LDAP schema

Pre-Installation Steps

Step 1 Install the ldapsearch binary.



Note

The ldapsearch binary is not required for the normal operation of LDAP with a WAE server. It is only necessary to discover the correct formatting of the LDAP schema required to configure the LDAP server settings. If necessary, the ldapsearch binary can be installed on an alternative machine. We recommend installing the binary on the WAE server as it can assist in troubleshooting LDAP protocol connection issues with the LDAP servers.

For Redhat or Centos systems:

```
sudo yum install openldap-clients
```

For Debian systems:

```
sudo apt-get install ldap-utils openssl libpam-ldap
```

Step 2 Gather LDAP server information. See [Table 4-1](#) for a list of information required and the variables that are used throughout this chapter to represent this information.

Step 3 Retrieve the LDAP schema from the LDAP server.

```
ldapsearch -x -v -W -LLL -a always -h <ldap-server> -b <ldap-base-ou> -D <admin-user-dn>
```

This command assumes that the LDAP server does not use certificates or SSL encryption.

Note If you are dealing with a large LDAP dataset we recommend you use command line filters and/or pipe the output to a file.

This example uses parameters from a fictitious company:

```
ldapsearch -x -v -W -LLL -a always -h ldap-server.company.com -b "dc=company, dc=com" -D
"cn=admin,dc=company,dc=com"
```

```
ldap_initialize( ldap://ldap-server.company.com )
```

```
Enter LDAP Password: <admin-password>
```

Step 4 Review the LDAP schema.

[Example 4-1](#) shows a trimmed down version of an LDAP schema. Bold text denotes information that is required later for LDAP authentication and authorization.

Example 4-1 *Trimmed Example of LDAP Schema*

```
filter: (objectclass=*)
requesting: All userApplication attributes
dn: dc=company,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: ipnec
dc: ipnec

dn: cn=admin,dc=company,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: *****
```

(These are Organization Units containing other LDAP objects)

```
dn: ou=People,dc=company,dc=com
objectClass: organizationalUnit
ou: People
```

```
dn: ou=Groups,dc=company,dc=com
objectClass: organizationalUnit
ou: Groups
```

(This is a User Object)

```
dn: uid=cisco-mate-user1,ou=People,dc=company,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
uid: cisco-mate-user1
sn: mate-user1
givenName: cisco
cn: cisco-mate-user1
displayName: cisco-mate-user1
uidNumber: 1001
gidNumber: 101
loginShell: /bin/bash
```

```
homeDirectory: /home/cisco-mate-user1
userPassword: : *****
```

(This is a Group Object)

```
dn: cn=cisco-mate-admin,ou=Groups,dc=company,dc=com
objectClass: groupOfUniqueNames
cn: cisco-mate-admin
uniqueMember: uid=cisco-mate-user1,ou=People,dc=company,dc=com
uniqueMember: uid=cisco-mate-user2,ou=People,dc=company,dc=com
```

Table 4-1 LDAP Server Information Needed for Configuration

Required Information	Notes / Variables Used
LDAP username and password	<p>This user account must have at least read permissions to all the LDAP server tree scope that you wish use.</p> <p>For the remainder of this document the LDAP user Distinguished Name (DN) will be denoted as <admin-user-dn></p> <p>For the remainder of this document the LDAP user password will be denoted as <admin-password></p> <p>For examples used in this document the DN for the LDAP user name will be "cn=admin,dc=company,dc=com"</p> <p>Please consult your LDAP systems administrator if you are unsure about the DN for the LDAP user name.</p>
LDAP search base Organizational Unit (OU) for all possible WAE users	<p>For the remainder of this document the base OU will be denoted as <ldap-base-ou></p> <p>The examples used in this document will use the base OU "dc=company, dc=com"</p> <p>There are performance benefits for the WAE/MATE login process if a more specific base OU is used</p>
LDAP server IP or DNS address	<p>LDAP servers can be clustered and use DNS load balancing, it is recommended that you use the DNS name.</p> <p>For the remainder of this document the LDAP server address will be denoted as <ldap-server></p> <p>The examples used in this document will use the LDAP dns server address "ldap-server.company.com"</p>

Configuring LDAP

You must have administrator privileges to configure LDAP.

-
- Step 1** From the WAE UI, select **System > LDAP Server**.
- Step 2** Enter the information needed for all fields, except within the Groups To Roles Mapping area. Leave the Groups To Roles Mapping area blank. For field descriptions, see [Table 4-2](#).

Table 4-2 LDAP Server Field Descriptions

Field	Description
Enabled	Select to enable use of the LDAP server for user authentication. This must be selected to use the LDAP server for authentication.
Server <ldap-server>	LDAP server IP address or FQDN, which is the server's hostname with the DNS domain name appended to the end. FQDN format: <LDAP_hostname>.<domain>.com
Protocol	Protocol used to reach the LDAP server. <ul style="list-style-type: none"> LDAP—Transmits communication in clear text. LDAPS—Transmits communication that is encrypted and secure. Default value is LDAP.
Accept Any SSL Certificates	Applicable only if LDAPS is selected as the protocol. Use this option if you do not expect the LDAP server to have a valid SSL certificate for establishing encrypted communication with this system. If this option is not selected, the communication cannot be established unless the certificate used by the LDAP server to establish communication is valid.
Port	Port used to reach the LDAP server. For unencrypted authentication the default is TCP 389. For encrypted authentication the default is TCP 636. Default value is 389.
LDAP Client Username <admin-user>	The DN for the LDAP user login which requires minimum read only access to the necessary sections of the LDAP Tree schema. This should be in the DN format: "cn=admin,dc=company,dc=com" This information was collected in Pre-Installation Steps .
Password <admin-password>	The LDAP user password. This information was collected in Pre-Installation Steps .
Search Base <ldap-base-ou>	This is the Distinguished Name of the base search OU for all user accounts that should have permission to login to the WAE Server. This information was collected in Pre-Installation Steps .

Step 3 Click **Validate** to test the LDAP configuration you have entered. A window displaying test results appears.



Note If there are failures, you may have entered an incorrect server address or the LDAP user login is invalid. To resolve these issues, contact your LDAP system administrator.

Step 4 Configure LDAP group to roles mapping.

WAE mappings defaults to support Microsoft's Active Directory LDAP Schema. If you are using Active Directory you will not need to perform any advanced configurations.

The WAE LDAP system supports only one of the following mappings (cannot be mixed):

- LDAP Administrative Groups to Mate/WAE Groups in a Many : One relationship
- LDAP Specific Users to Mate/WAE Groups in a Many : One relationship



Note To configure LDAP specific users group mappings, contact your support representative.

- a. From the LDAP schema that you downloaded in [Pre-Installation Steps](#), identify the LDAP administrative groups (see [Example 4-1](#)). Locate the DN for the LDAP group objects that contain the LDAP attribute **objectClass: groupOfUniqueNames**.
- b. Click **+Add Mapping**.
- c. Enter the Distinguished Name. For example, `cn=cisco-mate-admin,ou=Groups,dc=company,dc=com`.
- d. Check either the User or Administrator Role check box.
- e. Repeat these steps to add more mappings.

[Figure 4-1](#) shows an example of an LDAP Server page with populated fields.

Figure 4-1 Example of LDAP Server Page With Populated Fields

LDAP Server

Enabled

Server

Protocol

Port

LDAP Client Username

Password

Search Base

Groups To Roles Mapping + Add Mapping

Distinguished Name	Role	
cn=cisco-mate-admin,ou=Groups,dc=comp...	Administrator	
cn=cisco-mate-user,ou=Groups,dc=compan...	User	

« < 1 > »

[Advanced Config](#)

- Step 5** Click the **Advanced Configuration** link located at the bottom left of the LDAP Server page. The Edit System Object window appears.
- Step 6** View [Table 4-3](#) and determine if lines 7 and 8 must be edited, then click **Save**.

Table 4-3 System Object Attributes

Attribute	Description
LDAP.Principal.Expr	<p>Default : "LDAP.Principal.Expr": "(userPrincipalName={0})",</p> <p>The {0} token will be replaced by the user's input for username at the login page.</p> <p>The userPrincipalName= must match a User Objects' LDAP attribute that identifies the user under the LDAP search base.</p> <p>From the LDAP schema (Example 4-1), use the User Unique Attribute uid.</p> <p>The WAE server will search all objects under the LDAP search base tree for:</p> <pre>uid=cisco-mate-user1</pre> <p>Common alternatives include userPrincipalName or userName etc.</p>
LDAP.Principal.Group.Attr	<p>Default : "LDAP.Principal.Group.Attr": "user.memberOf"</p> <p>There are 2 options available here:</p> <ul style="list-style-type: none"> • User searches (default): <p>The WAE server will look for user.memberOf attributes, located under the LDAP User object itself. User based searches requires the ability for the server to execute a reverse LDAP lookup. For example, looking at a user object to determine the user's primary group object using the memberOf user attribute.</p> • Group searches: <p>Group based searches locates the membership of each administrative group that a particular user is a member of. Administrative Groups are based on objectClass: groupOfUniqueNames LDAP objects types.</p> <p>From the LDAP schema, find the unique attribute that lists the user association to the Group of Unique Names.</p> <p>In Example 4-1, this is</p> <pre>uniqueMember: uid=cisco-mate-user1,ou=People,dc=company,dc=com</pre> <p>uniqueMember is the attribute that the software is looking for to determine if a particular user is a member of a particular group.</p>

[Table 4-4](#) lists configuration examples that were based on tested default installations of the LDAP servers with default LDAP schema that were provided by the software vendor.

- Step 7** From the LDAP Server page, click **Save**.
- Step 8** To validate configuration, log off and log on to the WAE UI with a valid LDAP user account.



Note If you are experience issues, we recommend the following:

- Use an unencrypted LDAP first
- Review the log files listed in
 - \$CARIDEN_HOME/lib/web/apache-tomcat-6.0.37/logs/catalina.
 - \$CARIDEN_HOME/lib/web/apache-tomcat-6.0.37/logs/catalina.out
 - \$CARIDEN_HOME/lib/web/apache-tomcat-6.0.37/logs/mate_live.log
 - \$CARIDEN_HOME/lib/web/apache-tomcat-6.0.37/logs/user_manager.log

Table 4-4 *Advanced Configurations Tested on Default LDAP Server Installations With Default LDAP Schema*

LDAP Server / Vendor	Search Type	Default Advanced Configuration Settings
Sun One Directory Server	Group	"LDAP.Principal.Expr": "(uid={0})"
Sun Enterprise Directory Server		"LDAP.Principal.Group.Attr": "group.uniquemember"
Oracle Directory Server Enterprise Edition		
OpenLDAP	Group	"LDAP.Principal.Expr": "(uid={0})" "LDAP.Principal.Group.Attr": "group.uniqueMember"
Microsoft Active Directory (default)	User	"LDAP.Principal.Expr": "(userPrincipalName={0})" "LDAP.Principal.Group.Attr": "user.memberOf"
Novell Directory Services	Group	"LDAP.Principal.Expr": "(Uif={0})"
Novell eDirectory		"LDAP.Principal.Group.Attr": "group.uniquemember"
NetWare Directory Services		
NetIQ eDirectory		



SMTP Server

Access: System > SMTP Server

This page enables you to configure the SMTP server used for emailing WAE Live reports. If the SMTP server is not configured, the email feature for scheduled WAE Live reports will not work.



Note

These configurations apply only to the local server.

SMTP Fields

Using the SMTP server is not mandatory. If you do not wish to use it, set the Encryption field to None, and then no other fields are required. The following sections identify required and optional fields based on the assumption are you are configuring the SMTP server to use it.

Required Fields

- **Server**—SMTP server IP address or FQDN, which is the server’s hostname with the DNS domain name appended to the end.
FQDN format: `<SMTP_hostname>.<domain>.com`
- **Username**—Username of the SMTP server.
- **Password**—Authentication password for the SMTP server.
- **From Address**—The address from which the emailed report is sent. For example, this could be a support address so that recipients could respond for assistance.
- **Encryption**—The type of encryption to use when mailing WAE Live reports. For more information on WAE Live, see the *Cisco WAE Live Administration Guide* and the *Cisco WAE Live User Guide*.
 - **SSL**—Encrypt the communication between the SMTP server and the device to which the emailed report is going.
 - **STARTTLS**—Convert an insecure connection to use either TLS or SSL.
 - **None**—Do not use encryption. This is not recommended since the SMTP server is emailing reports containing your network data.
- **Port**—Port that the SMTP server uses when sending emails.

Optional Fields

- **Advanced Config**—This is for advanced configuration editing only. Consult your support representative for assistance.



Log Settings

Access: System > Log Settings

This page enables you to aggregate all syslog messages to a local syslog server or remote syslog server.

Configuring Log Settings

To configure syslog messages to go to a local or remote syslog server, do the following:

-
- Step 1** Go to the WAE UI and select **WAE System > Log Settings**.
 - Step 2** Check the **Enable** check box.
 - Step 3** Do one of the following:
 - **Local**—Select this option if you want messages to go to a local syslog server.
 - **Remote**—Select this option if you want messages to go to a remote syslog server and enter the IP address of the remote server.
 - Step 4** From the drop-down list, select a facility (Local 0 - 7). The local use facilities are not reserved. Processes and applications that do not have pre-assigned facility values can use any of the eight local use facilities.
 - Step 5** Enter the port number to be used on the server.
 - Step 6** Click **Save**.
-

Configuring an Application Server Access Log

The following procedure describes how to generate logs for application server access. The application server log contains the following information:

- Access timestamp
- Source (IP address)
- Account (if known)
- URL
- HTTP status code of application server response

-
- Step 1** Stop the Tomcat application server.
- Step 2** Edit the `$CARIDEN_HOME/lib/web/apache-tomcat/conf/server.xml` file by uncommenting the following line:
- ```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log." suffix=".txt" pattern="common" resolveHosts="false"/>
```
- Step 3** Start the Tomcat application server.
- Step 4** Retrieve the Tomcat access log at  
`$CARIDEN_HOME/lib/web/apache-tomcat/logs/localhost_access_log.<timestamp>.log`
-



## Services and Statistics

---

### Access: Home > WAE Statistics

The Statistics pages enable you to configure, monitor and troubleshoot all services and servers.



Note

The WAE Statistics page does not appear in some web browsers if you do not have the correct SSL certificates. To work around this, install the correct SSL certificates (see the [“” section on page 11-2](#)) or do the following:

1. Click the WAE Statistics link. The URL format is `https:// <server_IP> :8443`. For example, `https://192.0.2.14:8443`
2. Copy the URL of this page to another browser window.
3. In the new browser, change the URL port from 8443 to 8843. For example, `https://192.0.2.14::8843 Ex`
4. Follow the browser messages to accept the connection and add it as an exception.

The following terms are used on these UI pages and in this documentation.

- **Service**—An instance of a program that is being executed. Depending on the process, it may have multiple threads of concurrent execution.

Note that the terms *service*, *process*, and *function* are used interchangeably. For example, the Processes page lists services. The Platform Diagnostics page, Functions tab shows services per component.

- **Component**—A server or host that is running services. It can be either a device or a virtual machine. A component can reside as a stand-alone system or it can be one of the servers in a distributed (high-availability) environment.

Note that the terms *component*, *server*, and *host* are used interchangeably.



Note

If you do not see the Statistics UI, make sure the System services are running. If they are not, turn on the System services through the CLI. For information, see [Events](#).

# Services

## Service Types

| Service                                                   | Description                                                                                                                                        |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Automation Services</b>                                |                                                                                                                                                    |
| wae-appenginecore                                         | Service API that manages and routes requests to load the network model to the appropriate wae-designapiserver.                                     |
| wae-core                                                  | Service that enables the WAE Core server to use WAE Core REST and Thrift APIs.                                                                     |
| wae-db                                                    | Service for the WAE Core database server.                                                                                                          |
| wae-designapiserver                                       | Service that enables wae-appenginecore to use the Design APIs. This wraps the Design APIs and controls Design API instances.                       |
| wae-messaging                                             | WAE messaging service that uses JMS (Java Message Service).                                                                                        |
| wae-osc                                                   | Service that enables the OSC (Open SDN Controller) server.                                                                                         |
| <b>WAE Services</b>                                       |                                                                                                                                                    |
| All of the above Automation services, plus the following. |                                                                                                                                                    |
| wae-mls                                                   | Service that enables the WAE Live datastore server.                                                                                                |
| wae-ni                                                    | Service that enables the northbound WAE Network Interface (NI) APIs. WAE NI is used for continuous polling and for continuous PCEP LSP collection. |
| wae-web-server                                            | Service that enables the web server used by the Collector server, all web applications, web System UI, and web Statistics UI.                      |
| <b>System Services</b>                                    |                                                                                                                                                    |
| wae-svcs-dashui                                           | Service that controls the UI dashboard used for displaying logs and diagnostics in the Statistics UI.                                              |
| wae-svcs-db                                               | Service that enables the datastore that stores statistic information.                                                                              |
| wae-svcs-logagent                                         | Service that forwards log entries from client applications to wae-svcs-db.                                                                         |
| wae-svcs-metricsbkr                                       | Service that receives the collected diagnostic entries from client applications to wae-svcs-db.                                                    |
| wae-svcs-metricsd                                         | Service that collects diagnostic entries from client applications.                                                                                 |
| wae-svcs-mon                                              | Service that monitors all services and automatically restarts them in the event of ungraceful terminations (such as with a kill command).          |
| wae-svcs-ui                                               | Service used to enable the Statistics UI.                                                                                                          |
| wae-svcs-log                                              | Service that forwards client application log entries to syslog.                                                                                    |

## Monitor Services

The `wae-svcs-mon` service automatically monitors all `wae-svcs*`, `wae-ni`, and `wae-web-server` upon installation completing. It also monitors the Automation services once they are started. If the system is rebooted or if you “ungracefully” stop a process, such as with a `kill` command, `wae-svcs-mon` automatically restarts the service. Therefore, the only way to shut down a service is as follows:

```
service <service_name> stop
```



**Note** The `wae-mld` service is not monitored.

## Service Location

The scripts for starting and stopping Automation and WAE services are located in `/etc/init.d` and `/usr/local/bin`. Whether these scripts are executed on startup is handled by symbolic links created in `/etc/rc#.d` directories, where # is a number 0 through 6.

You can use `chkconfig` to disable, enable, and view startup settings. Note that you must have root permission to execute `chkconfig` commands.

For more information on `service` and `chkconfig` utilities, use their `man` pages.

```
man service
man chkconfig
```

The System services are located in `/etc/init.d`.

## Ports

The ports that servers are listening to are listed in the *System Requirements* document posted on [cisco.com](http://cisco.com). Following is an example of how to verify that the WAE Core service started and is listening to the correct port, which by default is 7777.

```
netstat -anp | grep 7777
```

## Viewing Service Status Details

**Access:** WAE Statistics > Processes.

The Process Status page shows the status of all services except `wae-mld`. The column headings list the hostname and IP address for each server (host). For each service that is running on a host, an icon appears on the service row under the appropriate host column. The icon color indicates the status of the service under the related host.

- Green—The service is operational and running.
- Red—The service is not reachable.
- Gray—The service is either initializing or is not being monitored. To enable monitoring, see

If a service is not available, a dash appears in the cell for that host.

Click the circular icon to view service status details, such as the service uptime, data collection timestamp, and the memory and CPU usage on that server.

There are two types of services monitored: WAE services and System services.

- WAE services—These services operate WAE. Monitoring these services enables you to determine if the products are properly communicating. For instance, if `wae-ni` displays red, then you know the WAE Network Interface (NI) server might have stopped running. You could also determine network issues, such as if a port were blocked by a firewall or if a WAE server could not communicate with the network.

- System services—These services enable you to gather and view the statistics. Checking these services is a good way to stay informed of whether you are properly gathering the data needed to monitor and troubleshoot WAE.

The status is updated every 15 seconds. You can also refresh the status by clicking the upper right Refresh icon.

## Managing and Configuring Services

If you have an admin role, you can perform the following tasks using the WAE UI:

- Start, stop, and restart a service.
- Enable or disable monitoring of a service.
- Enable or disable a service from automatically starting at system boot.




---

**Note** System services and `wae-web-server` cannot be disabled at boot. You can only start, end, and restart `wae-web-server` using the CLI. For more information, see [Starting and Stopping Services Using the CLI](#).

---

- 
- Step 1** From the WAE UI, select **WAE Statistics > Processes**. The Process Status lists all running services.
- Step 2** Click the circular icon that belongs to the WAE service that you want to configure.
- Step 3** Click the appropriate button to perform the desired action. If there are no buttons available, then that service cannot be configured.
- 

## Events

**Access:** WAE Statistics > Events.

### Viewing Event Log Details

The Log Events Detail section shows detailed log information for each service except `wae-mls` and thus, can be used for troubleshooting the system or simply better understanding it. You could use this information for investigating a wide range of issues. For example, you could find logs that identify why a collection failed or find warnings applicable to PCEP LSP deployments.

The most recent 100 logs appear, and log data is kept up to 30 days.

All columns are sortable.

- Time—Time the message was logged.
- ServiceType—Service on which the message is logged.
- ClientId—IP address of the host (component) running the service.
- LogLevel—Type of Log4j log message from Failure to Trace. Each row is color-coded to show its log level. For example, Debug is light green and Info is light blue.



- **Logger**—Method within the service that generated the message.
- **Thread**—Process thread that generated the message.
- **Bundle**—Karaf software component (not the same as a WAE component).
- **Message**—Log message.

You can search for any word in the Log Events Detail section. This search feature uses the query string syntax produced by Elasticsearch. For information on these capabilities, see the Query String Syntax information in the Elasticsearch documentation.

<https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html#query-string-syntax>

## Filter Log Events by Severity

To filter what type of log events are displayed, do the following:

- 
- Step 1** From the WAE UI, select **WAE Statistics > Events**.
  - Step 2** From the Select Log Level drop-down list, select the minimum log level severity.

The Log Events Detail immediately displays events with the minimum severity level you selected. For example, if you select WARN, all severity levels set to WARN or higher will be displayed. The log level severities are listed in the following order (from highest to lowest): FATAL, ERROR, WARN, INFO, and DEBUG.

---

## Viewing Event Log Graphs

| Graph               | Description                                                                                                                                                                                                                    |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Events Source   | Shows the percentage of total logs by service. Each color represents a different service. This enables you to see which of the services is returning the most log messages.                                                    |
| Log Level Counts    | Shows the number (count) of messages for the most frequently appearing message type. This enables you to compare the number of log levels that are appearing most frequently.                                                  |
| Log Events Timeline | Shows how events are coming in over time in a stacked graph manner. Each color represents a different log level. A sudden spike in the more serious logs, such as errors, would be indicative of problems that need attention. |

## Platform Diagnostics

**Access:** WAE Statistics > Diagnostics.

The Platform Diagnostics page is particularly useful for analyzing trends over time and for being alerted to sudden changes in those trends, which could indicate either problems with one of the servers or a problem in the network. Diagnostics data is kept up to 7 days.

**Note**

You can switch between the system status or utilization graphs by clicking the toggle icon underneath the Refresh icon. For more information on system status, see [Chapter 8, “Local Server Status.”](#)

The default view is Summary of Components in distributed deployments or Components in single-system deployments.

- **Summary of Components and Components**—Summary of Components shows trends of diagnostics for all components. The Components tab show trends for the component in a single-system deployment, or for a selected component in a distributed deployment.

These trends enable you to clearly see changes and potentially correlate these changes with events. If a component is sluggish or not performing as expected based on the past, you would see this as a trend change. For example, if a CPU is running generally at 25% usage and suddenly jumps to 90%, that spike would appear in the graph, and you could then check the Event Logs for errors or warnings that indicate why the CPU percentage drastically increased. If the memory usage trend changed from 5 GB to 25 GB, this change would appear in the graph, and you could check the network to see if a problem had occurred to cause such an increase.

Component diagnostics include CPU percentage usage, memory usage, network usage, and free disk space. For distributed deployments, this is also selectable as “Summary of all Components” from the top, right selection menu. The following options are also available in the top left.

- **Functions**—Shows diagnostics per service running on the selected component. Diagnostics include heap size, thread count, and CPU percentage used. This option is useful when you need more information than available in the Components view.
- **WAE-NI**—Shows interface and LSP diagnostics from WAE NI.

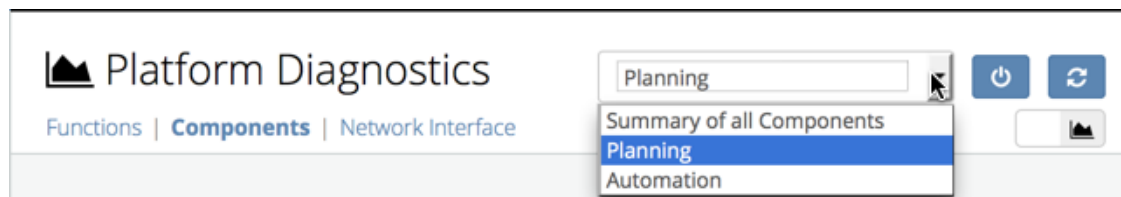
Note that whether the page displays services and whether the page displays information for a distributed deployment differs depending on the option selected.

| Option                | Shows Single-System Deployment?                 | Shows Distributed Deployment?                   |
|-----------------------|-------------------------------------------------|-------------------------------------------------|
| Summary of Components | NA (does not appear as an option)               | Yes, all components                             |
| Component             | Yes                                             | Yes, selected component                         |
| Functions             | Yes, shows status of component-related services | Yes, shows status of component-related services |

**Note**

The `wae-mltd` service is not available from the Platform Diagnostics page.

**Figure 7-1** Platform Diagnostics Selections



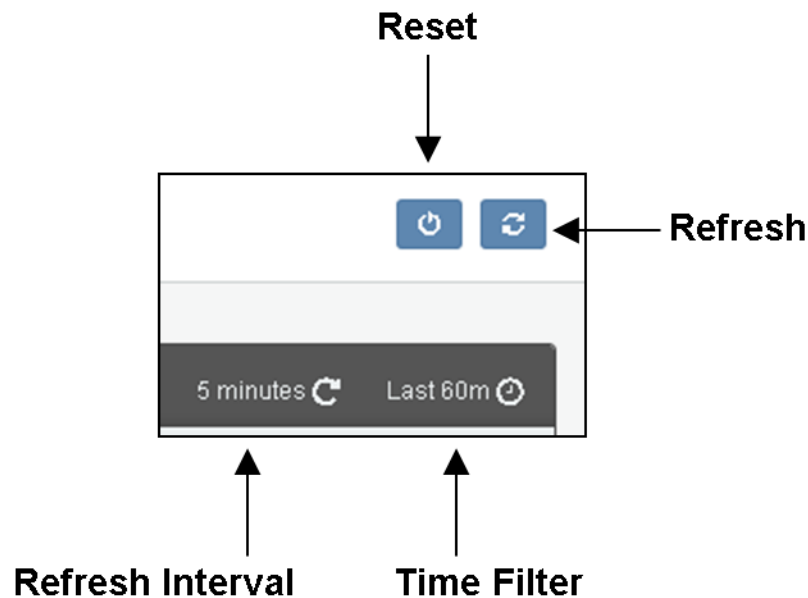
# Using the Events and Diagnostic UIs

## Time Filters and Refresh Intervals

The time filter and refresh interval in the top right are toggles for showing and hiding the selections to change them (Figure 7-2). The two act in conjunction with each other. The time filter is the amount of time for which the events or diagnostics are displayed. The refresh interval is how often the data is refreshed. For example, on the Platform Diagnostics page, if the time filter is the last 30 minutes and the refresh interval is 5 minutes, this means that every 5 minutes the diagnostics are updated to show the last 30 minutes from that point in time.

The default time filter is 60 minutes, and by default, the information on the pages is not automatically refreshed.

Figure 7-2 Event and Diagnostic Time Features



404575

## Change Time Filter

To change the time filter, click it. A set of choices appear. Once you set the time filter, click **Go**.

- **Quick**—Enables you to select from a set of preset time filters, ranging from the last 15 minutes up to the last 5 years.
- **Relative**—Enables you to specify a time that is relative to the current time. For instance, you could set it to show the data for 2 hours ago. The time extends down to the milliseconds. To round this number, select “round to the <increment>” button, where increment changes, depending on your selection.
- **Absolute**—Enables you to a specific date range. Selecting a future time is not applicable.

## Change Refresh Interval

To change the time interval, click the time filter or the refresh interval, select Refresh Interval, and then make your selection. You can also turn off the viewing of this interval.



Note

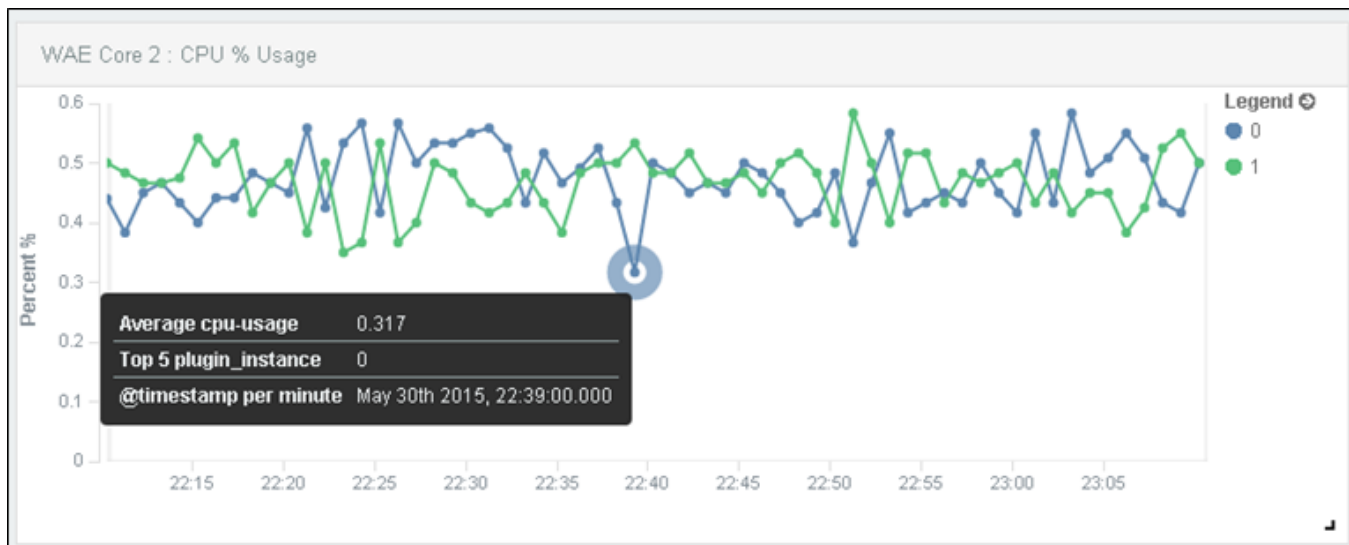
If you leave the page, the refresh setting reverts to the default of not refreshing (off).

## UI Tips

- Click the arrow to expand or close the legend that defines what each color represents.
- To highlight information represented by any color, move the cursor over it in the legend or in the graph.
- To reset the time filter, refresh interval, and graph positions to their defaults, click the **Reset** button.
- To move a graph, drag it to the desired location.
- To get more detail about a datapoint in the graph, hover over it.
- To expand or shrink a graph, click and drag the bottom, right corner.

Figure 7-3 shows an example of the CPU% Usage for the WAE Core 2 component. The expanded legend defines the trend lines for CPU cores 0 (blue) and 1 (green). Hovering over the lowest CPU utilization shows more details for it. Notice the icon in the bottom right for expanding and contracting the graph.

Figure 7-3 Example Expanded View with Legend and Tooltip



404676

## Viewing Database Information

Access: WAE Statistics > Database Info.

From this page, you can view and monitor database information such as space usage (MB), and read/write cache rate percentage and disk input/output performance.

## Change Date/Time Range

The graphs, by default, display information for the past day. To change the date or time range, do the following:

- 
- Step 1** From the WAE UI, select **WAE Statistics > Database Info**.
  - Step 2** Click the **Date/Time Range** link.
  - Step 3** Click the applicable radial button to enter the past number of days or to give a date and time range.
  - Step 4** Click the **Redraw Graphs** button to view the updated graphs.
- 

## Generate and Download Database Information

To generate and download a report of the information shown in the graphs, do the following:

- 
- Step 1** From the WAE UI, select **WAE Statistics > Database Info**.
  - Step 2** Click the **Generate Diagnostics Report** button. It may take some time for the report to generate.
  - Step 3** Click the **Download Report** button. This button is only enabled when the report is ready.
-





## Local Server Status

---

**Access:** Home > Statistics > Diagnostics > Components



**Note**

---

You can switch between the system status or utilization graphs by clicking the toggle icon underneath the Refresh icon. For more information on utilization graphs, see [Platform Diagnostics](#).

---

The Local Server Status page shows the status of the system load, free memory, and free disk space for the local device.

Each section is a “parent” section that reflects the status of its worst-performing unit being measured.

- **System** status shows the worst system load average for 1-, 5-, and 15-minute intervals.
- **Memory** status shows the amount of memory that is available on the device.
- **Disk** status shows the lowest available disk space for any of its partition types.

If you are on the Local Server Status page or if you are on the home page, then this information is updated every two minutes. To refresh the status sooner, click the Refresh icon in the top right of the page.

Click anywhere in the parent section to see more details.



**Note**

---

These configurations apply only to the local server. For information on monitoring services in a distributed environment, see [Chapter 7, “Services and Statistics.”](#)

---

## System

The System section shows the status of the average system load on the local device for three intervals: 1 minute, 5 minutes, and 15 minutes. If the system status of any one of these intervals is worse than the other, that is the status that shows in the parent system section.

Clicking the parent section shows the individual status of each of these intervals, as well as their load, and the top five processes contributing to the system load.

## Load

The Load column identifies the system load (for the given time interval) on the local device. The load is relative to the number of processor cores available. On a device with only one core, 1.0 means it is exactly at capacity (100% utilization), and any number over 1 means there are backup of processes waiting to run. This full-capacity number doubles to 2 on a dual-core system, to 4 on a quad-core, and this trend continues as the number of cores increases.

The number that is most likely indicative of your average load is the 5- or 15-minute interval, depending on how you are using the device. The closer the number moves to its full-capacity mark, the more likely it is you need to find a way to handle more processes.

## Status

The load average is based on the load divided by the number of cores on the local device. For example, if the load is 1 and there are 4 cores, the system load average is 25%. Following are the percentages that affect the status.

| Interval   | Green                   | Yellow         | Red       |
|------------|-------------------------|----------------|-----------|
|            | <b>x = Load Average</b> |                |           |
| 1 minute   | x < 250%                | 250% <=x< 300% | x >= 300% |
| 5 minutes  | x < 200%                | 200% <=x< 250% | x >= 250% |
| 15 minutes | x < 100%                | 100% <=x< 200% | x >= 200% |

## Memory

The Memory section shows the status on total memory that is available for the local device.

Clicking the Memory section provides total memory, free memory, and the status of the system-wide available memory. It also lists the amount of buffer and swap memory that is available.

Buffer memory is the portion of the hard drive's memory that is set aside as a temporary holding place for data that is to be sent to or received from an external device. Swap memory is the reserved amount of memory on the hard drive.

Following are the percentages that affect the status.

| Green                                       | Yellow       | Red      |
|---------------------------------------------|--------------|----------|
| <b>x = Total Amount of Available Memory</b> |              |          |
| x > 25%                                     | 25% <=x< 10% | x <= 10% |



# Disk

The Disk section shows the status of disk space that is available for the local device. Each partition type is measured, and if any one of these partition types is worse than the other, that is the status that shows in the parent Disk section. For instance, if disk partition type ext4 in /net/akd1 is red (low disk space available) and the rest of the types are green (sufficient disk space available), the color showing in the parent Disk section is red.

Clicking the parent section shows the individual status of each of these partition types, as well as their paths. For each type-path combination, the amount free space and total space are also listed.

Following are the percentages that affect the status.

| Green                                           | Yellow              | Red          |
|-------------------------------------------------|---------------------|--------------|
| <b>x = Total Amount of Available Disk Space</b> |                     |              |
| $x > 15\%$                                      | $15\% \leq x < 5\%$ | $x \leq 5\%$ |





## Applications


---

### Access: Home > Applications

Only WAE administrators have the ability to add and manage WAE applications or custom client menus to the WAE UI. These applications can then be launched directly from the Home > Applications window or the Applications page.

## Installing the Application

---

- Step 1** If a WAE application is available as an <application-name>.zip file, download the file to your server. You can search **WAN Automation Engine (WAE)** from the [Cisco download site](#), and navigate to the WAE application.
- Step 2** From the WAE UI, select **Home > Applications**.
- Step 3** Click **Apps Management** or the gear (Settings) icon located on the upper-right corner of the window. The Apps Management window appears.
- Step 4** Click the upload icon and upload the <application-name>.zip file that you downloaded. After the upload is complete, the following options for each application are available:
- **Enable**—Adds the application to the Applications window or page so that it can be easily launched. A user will only see the Applications window if a WAE administrator has enabled the application.
-  **Note** The application cannot be enabled if the application is not compatible with your license type or your WAE software version.
- **Delete**—Uninstalls the application software and no longer appears in the Apps Management window. This option appears only during initial upload or after disabling the application.
- Step 5** Click **Enable** to add the application to the Applications window. Once enabled, only the Disable option is available. The Disable option removes the application without uninstalling it from WAE. To uninstall the application, click **Disable**, then click **Delete**.
- Step 6** Close the window and confirm that the application is listed in the Applications window.
-

# Application File Contents

This section provides a high-level description of what WAE requires in order to add an application to the WAE UI. For more information, contact your support representative.

The .zip file must contain the following:

- application.json—Application configuration file
- application.war—Entire backend package of the application
- ROOT/services/<application.json>/<UI\_files>—All UI files required by the application contained in this directory structure

Contents of an application.json file:

```
{
 "name": "<app-name>",
 "caption": "<app-caption>",
 "description": "<app-description>",
 "icon": "fa fa-fw fa-wrench",
 "redirectPage": "<app-redirect>",
 "version": "<app-version>"
 "dependencies": {
 "wae-version": "<wae-version>",
 "wae-exclude-versions": ["<wae-exclude-versions>"],
 "licenses": ["license-type"]
 }
}
```

| Variable               | Description                                                                                                                |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <app-name>             | The name of the application. This has to match the ROOT/services/<app-name>                                                |
| <app-caption>          | The caption for the application that will be displayed in the UI.                                                          |
| <app-description>      | Description of the application.                                                                                            |
| <icon>                 | Icon to be used for the application. WAE supports font-awesome 4.3.0 icons.                                                |
| <app-redirect>         | The URL of the redirect page.                                                                                              |
| <app-version>          | Application version.                                                                                                       |
| <wae-version>          | Minimum WAE software version supported. All versions above will work except any versions listed in <wae-exclude-versions>. |
| <wae-exclude-versions> | All WAE software versions that are not supported.                                                                          |
| <license-type>         | License feature.                                                                                                           |

Example:

```
{
 "name": "MyNewApp",
 "caption": "My New Application",
 "description": "Sends statistics reports to a specified e-mail address",
 "icon": "fa fa-fw fa-wrench",
 "redirectPage": "rd_mynewapp",
 "version": "1.0"
```

```
"dependencies": {
 "wae-version": "6.1",
 "wae-exclude-versions": [
 "6.3",
 "6.2.1"
],
 "licenses": [
 "ML_Map",
 "MC_VPN",
 "MD_Sim"]
}
```

---





## Core Security Concepts

---

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

- [HTTPS](#)
- [SSL Certificates](#)
- [1-Way SSL Authentication](#)
- [Installing an SSL Certificate](#)

### 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 Cisco WAE 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 involves 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.
4. 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 Cisco WAE 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.



**Note**

Cisco WAE includes a default certificate that will cause 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.

## Installing an SSL Certificate

As an administrator with root privileges, you can use the `install_web_certificate` script to install certificates for WAE UI and WAE application use. The script is located in the WAE Planning server under the `/usr/local/bin` directory.

### Before You Begin

Obtain the proper SSL certificate from certificate authority (CA) and have your private key file.

**Step 1** Confirm that the WAE web service is running:

```
service wae-web-server status
```

**Step 2** Enter the following command:

```
wae_install_web_certificate -k <private_key_file> -c <signed_certificate_file> -a
<ca_authority_file>
```

For example:

```
wae_install_web_certificate -k /path/to/172.28.101.204.web.key -c
/path/to/172.28.101.204.web.crt -a /path/to/172.28.101.204.ca.crt
```

**Note**

- You must include `-key` and `-cert` options when running this tool. To view help information, enter `wae_install_web_certificate` command with no options.
- Backup certificate files are created in `$WAE_ROOT/etc/cert`. To view tasks being performed and what files are affected run the command with the `-verbose` option.

**Step 3** When prompted to restart services, enter `y`.

**Step 4** Launch WAE UI.





## Additional Administrative Tasks

---

This section describes administrative tasks that are not done through the WAE UI.

### Starting and Stopping Services Using the CLI



Note

To manage (start, stop, enable monitoring, or run services at system boot) WAE services using the WAE UI, see [Managing and Configuring Services](#).

---

To determine which services are running, enter the following command:

```
service --status-all | grep -i wae
```

The installation process automatically starts the `wae-web-server`, `wae-ni`, and all System services (`wae-svcs-*`).



Note

To change the behavior of the `wae-web-server` service upon restarting it, you can edit the `/opt/cariden/etc/sysconfig/wae-web-server.cfg` file. For information, see the *Cisco WAE Server Installation Guide*.

---

You can start, restart, and obtain the status of all Automation and WAE services using the following formats, respectively.

```
service <service_name> start
service <service_name> restart
service <service_name> status
```

You can start, stop, and restart Automation and WAE services from the Statistics > Processes page, as well as enable or disable the monitoring of them. The one exception is `wae-web-server`, which can only be stopped or restarted from the CLI.

You cannot shut down a System service since these are required for the Statistics UI to properly function.

---

### Changing Encrypted Passwords

You can update the associated configuration files for the following encrypted passwords:

- Northbound RESTful API user password
- Cisco Network Service Orchestrator (NSO) Network Configuration (NetConf) API access
- Internal system password
- SSH password for the upload of plan files to the target host

---

**Step 1** Enter the following command:

```
wae-automation-deploy -update passwords
```

**Step 2** When prompted, enter the following information:

- WAE user name—This should be the same username that was designated during software installation on the primary (local) server.
- Planning host—IP address of the primary (local) server.
- Automation host—IP address of the secondary server.
- Root user (cariden is the default root user) password for the primary server

**Step 3** When prompted for each encrypted password, do one of the following:

- To change the password, enter a new password and press the **Return** key.
  - To make no changes and keep the existing password, leave prompt blank and press the **Return** key.
- 

## Viewing Temporary Files

Temporary files can be found in the following directories:

- If \$WAE\_ROOT is set as a directory:  
\$WAE\_ROOT/data/<product\_component>/tmp/  
For example, /opt/cariden/data/wae-ni/tmp
- If \$WAE\_ROOT is not set, and \$TMPDIR is set:  
\$TMPDIR/<product\_component>/tmp/  
For example, /opt/tmpdir/wae-ni/tmp/
- If \$WAE\_ROOT and \$TMPDIR are not set:  
/tmp/<product\_component>/tmp/  
For example, /tmp/wae-ni/tmp/

## Limiting Application Server Access to Specific IP Addresses

---

**Step 1** Stop the Tomcat application server.

**Step 2** Edit the \$CARIDEN\_HOME/lib/web/apache-tomcat/conf/server.xml file by adding the following line:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve" allow="127.0.0.1,
[tomcat_IP], [approved_IP_addresses]" />
```

where *approved\_IP\_addresses* is the list of IP addresses that can access the application server and *tomcat\_IP* is the Tomcat IP address of the listening interface.

- Step 3** Start the Tomcat application server. Only the clients from the approved IP address list can access the application.





## Troubleshooting

---

To ease troubleshooting of the WAE Live application, Collector server, WAE Network Interface (NI) server, and WAE Core server, use the `mate_tech_support` CLI tool. This tool creates a tar file of support information and puts it into the `/tmp/MATE_TS` directory by default. If needed, you can then send this .tgz file to your support representative. To change the directory in which the results are stored, use the `-tar-path` option.

Example: This creates a tar file of support information and puts the output into the `/troubleshooting` directory.

```
mate_tech_support -tar-path /troubleshooting
```

Following are a few more areas to look for available troubleshooting information.

- To monitor diagnostics, view logs, and monitor processes for either a single-system deployment or a distributed deployment, use the WAE Statistics UI. For more information, see the [Services and Statistics](#) chapter.
- To monitor only the local server, use the [Local Server Status](#) tool on the home page and available through the System UI.
- From the WAE Collector UI, there are numerous tools available for troubleshooting the collection process, including a Node List table that identifies the status of every node in the collection, Status and Log pages for viewing errors and warnings for the local Collector server, and a Download Diagnostics tool for creating a file containing the state of the local Collector server during the last collection.
- From the WAE Live UI you can view the status of the most recently collected data that WAE Live received.
- To allocate or clean disk space, you may want to remove temporary files (see [Viewing Temporary Files](#)).

