



Managing the WLSE System

This chapter contains the following major topics:

- [Ports Used by the WLSE, page 16-2](#)
- [Overview of the Admin Tab, page 16-3](#)
- [Managing the Appliance, page 16-4](#)
- [Managing Firmware Version Support, page 16-67](#)
- [Managing GUI Users, page 16-69](#)
- [Modifying Your Profile, page 16-77](#)
- [Creating Links, page 16-80](#)



Note

Some of the Admin subtabs may not be visible to some users; what you see under the Admin tab depends on the roles assigned to your login.

Ports Used by the WLSE

Table 16-1 and Table 16-2 list the ports used by WLSE services.



Note The NAT protocol is not used by the WLSE.

Table 16-1 Ports Used by WLSE

Destination Port Number	Protocol and WLSE Service	Port Hosted By
TCP 21	FTP—IOS AP configuration	FTP server
TCP 22	SSH—IOS AP configuration	Access point
TCP 23	TELNET—IOS AP configuration	Access point
TCP 25	SMTP—fault notification	SMTP server
UDP 53	DNS—IOS AP configuration	DNS server
TCP 80	HTTP—non-IOS (VxWorks) access point configuration	Access point
TCP 9851	WHISK—repository for upgrading WLSE software	Windows repository server
UDP 161	SNMP—discovery, inventory, configuration of APs	Access point, other devices
UDP 162	SNMPTRAP—fault notification	Trap server
UDP 514	SYSLOG—fault notification	Syslog server
UDP 1645 and 1646	RADIUS—AAA synthetic authentication (ACS versions prior to 3.2.3)	Cisco ACS server
UDP 1812 and 1813	RADIUS—AAA synthetic authentication (ACS 3.2.3 version)	Cisco ACS server
UDP 2887	WLCCP—Wireless Domain Service (WDS) radio management	Master WDS access point

Table 16-2 Ports Hosted by WLSE

Destination Port Number	Protocol and WLSE Service	Source
TCP 443	HTTPS—WLSE secure Web port	Client browser
TCP 1741	HTTP—WLSE Web port	Client browser
TCP 2004	Default port used by remote agent for built-in AAA server. Only used for Windows domain authentication on the WLSE Express.	Windows domain controller
UDP ephemeral	TFTP—firmware image transfer	Access point
UDP 69	TFTP—firmware image transfer	Access point

Overview of the Admin Tab

Table 16-3 on page 16-3 describes the subtabs and options that are displayed under the Admin tab.

Table 16-3 Functions of the Admin Tab

Subtab	Description	Reference
Appliance	Manage the WLSE system.	Managing the Appliance, page 16-4
System	View and manage information about supported access point firmware versions.	Managing Firmware Version Support, page 16-67
AAA Administration	Internal AAA server on the WLSE Express only.	Chapter 18, “Using the Internal AAA Server (WLSE Express Only)”
User Admin	Manage users and user roles.	Managing GUI Users, page 16-69
My Profile	Set the password, email address, and customize the Web interface for an individual user.	Modifying Your Profile, page 16-77
Links	Set up links to other systems (such as CiscoWorks servers) and run an ACS failed login report.	Creating Links, page 16-80

Managing the Appliance

Options under the Appliance subtab allow you to manage the WLSE system and use connectivity tools. When you select **Administration > Appliance**, the following options are displayed.


Note

Your login determines whether you can use these options.

Table 16-4 Appliance Subtab Options

Option	Description	References
Status	Use WLSE log files. Restart the WLSE.	Using WLSE Log Files, page 16-5 Restarting the WLSE, page 16-9
Software	Manage WLSE system software.	Managing WLSE System Software, page 16-10
Security	Manage WLSE security: <ul style="list-style-type: none"> • Use authentication modules for WLSE users. • Obtain a certificate for secure Web access. • Configure Telnet and SSH access. • View the last 10 users who have logged on. 	Managing Security, page 16-22
Backup and Restore	Back up and restore WLSE data.	Backing Up and Restoring Data, page 16-28
Master Configuration	Export WLSE configuration to a file. Used on the WLSE Express only.	Managing WLSE Master Configuration Files (WLSE Express Only), page 16-36
Redundancy	Manage redundant WLSEs. Two WLSEs are managed as a high-availability cluster.	Managing WLSE Redundancy, page 16-39

Table 16-4 Appliance Subtab Options (continued)

Option	Description	References
Diagnostics	Use WLSE status reports. Create and display self tests. Manage processes.	Using WLSE Diagnostics Options, page 16-53
Splash Screen	Add a message to users at login.	Specifying a Splash Screen Message, page 16-59
Time/NTP/Name/ Web Timeout	Set system time, use NTP, specify name servers, and reset the Web timeout period.	Setting Time, Time Servers, Name Servers, and Web Session Timeout, page 16-59
Configure Mailroute	Specify a mail server for email forwarding.	Configuring the Mail Route, page 16-62
TFTP Management	Manage files on the WLSE by using the internal TFTP server.	Managing Files for the WLSE TFTP Server (WLSE Express Only), page 16-63
Connectivity Tools	Test network connectivity.	Using Connectivity Tools, page 16-65

Using WLSE Log Files

This option allows you to view the contents of WLSE log files, download logs, search for data in logs, and email logs.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Administration > Appliance > Status > View Log File**. The following information is displayed:

Field	Description
Log file	Name of the log file.
Directory	Location of log file on WLSE.
File Size	Size of file in bytes.

Field	Description
View	Displays a log file in a separate window.
Download	Saves a log file to your desktop or other location.

Step 2 To see a log file's details, click **View**. For a description of each file:

- For AAA server log files, see [Using AAA Server Log Files, page 18-40](#).

**Note**

The AAA server is available only on the Wireless LAN Solution Engine Express (WLSE 1030 hardware).

- For other log files, see [About Log Files, page 16-7](#).

**Note**

Some files must first be downloaded before you can view them.

Step 3 To download a log file, click **Download**.

**Note**

If this method of saving does not work, right-click **Download** and use the browser menu to save the file.

Step 4 To search within log files, select one or more files and enter a keyword into the Keyword text box. Click **Case Sensitive** if you want your search to be case sensitive, then click **Search**. A separate window displays the results of the search.

Step 5 To email log files, select one or more files and enter one or more comma-separated email addresses in the E-Mail Addresses textbox. Click **Send**.

Related Topics

[Viewing System Information via CLI, page 17-22](#)

About Log Files

The WLSE maintains the following log files:

- Log files for the internal AAA server (WLSE Express only)—See [Using AAA Server Log Files, page 18-40](#). The internal AAA server is available only on the Wireless LAN Solution Express (WLSE 1030 hardware).
- Log files for other functions—See [General WLSE Log Files, page 16-7](#).

Table 16-5 General WLSE Log Files

File	Contents
AAA log files	Logs for the internal AAA server. The internal AAA server is available only on the Wireless LAN Solution Engine Express (WLSE 1030 hardware). For information on these log files, see Using AAA Server Log Files, page 18-40 .
Repository.log	Actions performed by the repository web server.
access.log	Web server user access.
backup.log	Appears after you back up WLSE data, restore data, or test the reachability of the backup location. To clear this log, which can become very large, see Clearing the Backup/Restore Log, page 16-32 .
ciscoinstall.log	Information on upgrades of the WLSE software.
configbackup.log	The WLSE backs up the startup configuration once a day in order to detect any configuration changes. This log file contains information for that backup process. Information is kept for only the latest backup.
configexport.log	Information generated when a master configuration file is generated (WLSE Express only).
cwexport.log	Information about device exports to CiscoWorks RME.
daemons.log	Messages that dmgttd does not log.
dataUpdate.log	Appears after WLSE software is updated.
db2.log	Database startups due to installations or reboots.
db2runstat.last.log	Information on the latest run of the runstats facility, specifically size information on all the database tables and which tables were updated.
db2runstat.times.log	Summary of recent runs of the runstats facility, specifically which tables were updated and how long it took for the entire run to finish.

Table 16-5 General WLSE Log Files (continued)

File	Contents
db2uext2.log	Generated by the database user exit script, which is part of the redundancy code. This file is for troubleshooting by TAC only.
device_events.log	Logs for the following device events detected by the WLSE: <ul style="list-style-type: none"> • Device reboots • Address changes on APs caused by reboots and DHCP • Changes between pending and managed states on devices
dhcp.log	Processing that occurs when a WLSE boots up and gets its startup configuration tar file from a TFTP server via DHCP.
diagnostic-info.log	Output of the diagnostic-info CLI command.
dmgtd.log	Process management daemon log.
dumptcp.cap	Binary log file created by the dumptcp CLI command. To view this file, save it to the desktop. Then, use a utility such as tcpdump.
dumptechn.tgz	Output of the dumptechn CLI command. To view this file, save it to the desktop and unzip the file.
error.log	Web server errors.
faults.log	Device faults.
install.log	Software package installation.
jobvm.log	Errors and other information on scheduled jobs.
logs.tgz	Output of the tarlog CLI command (an archive of system logs). To view these logs, save this file to the desktop, then unzip the file.
mfgtest.log	Manufacturing tests.
mod_jk.log	Messages between Tomcat and Apache.
procps_last.log	Output from last running of the ps CLI command.
redundancy.log	Redundancy messages.
runstats.log	Output of utility that updates statistics on data in tables and indexes.
snmpd.log	SNMP agent log file.
ssl_request.log	Secure HTTPS socket layer web server events.
swan.log	Radio management log.

Table 16-5 General WLSE Log Files (continued)

File	Contents
tftp.log	Access points deployed by the Deployment Wizard (access points that have downloaded the wlsestartup.ini file).
tomcat.log	Java servlet messages, including review and error information for configuration templates.
updateWLSE-x.x.log	Results of upgrading WLSE software; for example, update WLSE-2.11.log.
var_logs.tgz	Output of the tarlog CLI command (an archive of system logs). To view these logs, save this file to the desktop, then unzip the file.

Restarting the WLSE

This option allows you to restart the WLSE. After restarting, discovery and inventory will resume at the next scheduled time.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Appliance > Status > Restart**.

Step 2 Click **OK** to restart the WLSE.



Note

To perform a manual soft restart (for example, when modifying a network interface) you can use the CLI commands. For information on CLI commands, see [Appendix A, “Command Line Interface \(CLI\) Commands.”](#)

Related Topics

- [Rebooting the WLSE via CLI, page 17-14](#)
- [Shutting Down and Powering Off the WLSE, page 17-15](#)

- [Administering Management Services via CLI, page 17-22](#)

Managing WLSE System Software



Caution

Before attempting to upgrade WLSE software, check the readme file associated with the upgrade image in the Software Center on Cisco.com for changes to the procedures and caveats. Some procedures in this section may not be applicable to certain software upgrades.



Caution

Upgrading a redundant cluster of WLSEs requires special procedures, see [Upgrading Software on Redundant WLSEs, page 16-50](#).



Caution

You cannot upgrade from a pre-release version of WLSE software to a released version.

For information on which previous versions of WLSE software can be upgraded to WLSE 2.11, see the *Software Upgrade Guide for the CiscoWorks Wireless LAN Solution Engine* on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm.

The options under **Admin > Appliance > Software** are:

- **Status**—View information on the installed software, such as software description, installation date, and installation status—See [Viewing Status of Installed Software, page 16-11](#).
- **Define Repository**—Specify the repository location. The repository provides software update services to the WLSE—See [Managing the Repository, page 16-13](#).
- **Upgrading Software**—Select and install a software image from the repository—See [Installing the Software Upgrade, page 16-17](#).
- **Browse Repository**—Browse the available complete images in the repository—See [Browsing the Repository, page 16-19](#).

- **Software Update History**—View information about current and previous versions of installed software, including version number, install date, and installation status—See [Viewing Software Update History, page 16-20](#).

The topics in this section are:

- [Viewing Status of Installed Software, page 16-11](#)
- [Downloading the Upgrade Image, page 16-13](#)
- [Creating the Repository, page 16-14](#)
- [Defining the Repository, page 16-16](#)
- [Installing the Software Upgrade, page 16-17](#)
- [Viewing Software Update Logs, page 16-21](#)
- [Data Preserved or Changed After Upgrade, page 16-22](#)

For information on other upgrade methods, see the *Software Upgrade Guide for the CiscoWorks Wireless LAN Solution Engine* on Cisco.com.

Viewing Status of Installed Software

You can view information about the software currently installed on the WLSE.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Software > Status**. The Installed Software table contains the following information about the software versions that have been installed on the WLSE:

Field	Description
Software Name	Brief description of the software.
Installation Date	Date and time (UTC) the software was installed.

Field	Description
Status	Status of the installation: Success—Installed with no errors. Warning—Installed successfully with minor errors. Error—Installation was unsuccessful.
Details	Detailed install log for this software.

Last Installation Information shows the following information about the most recent software installation:

Field	Description
Name	Brief description.
Installation Status	Status of the installation: Success—Installed with no errors. Warning—Installed successfully with minor errors. Error—Installation was unsuccessful.
Log File	Detailed install log.

Step 2 To view details about an installation, click **View Log** in the Details field.

Result: The install log for the selected installation opens, showing information about the most recent software installation.

Related Topics

- [Viewing Software Update History, page 16-20](#)
- [Installing the Software Upgrade, page 16-17](#)
- [Managing WLSE System Software, page 16-10](#)

Managing the Repository

The software repository stores the available software updates for the WLSE. The repository can be either local (on the WLSE) or remote (on a Windows NT, Windows 2000, or Windows XP server). The tasks for managing the repository are:

Task	Reference
1. Download software from Cisco.com.	Downloading the Upgrade Image, page 16-13
2. Create repository.	Creating the Repository, page 16-14
3. Define repository.	Defining the Repository, page 16-16

Downloading the Upgrade Image

To locate the upgrade files, navigate to the Software Center for WLSE on Cisco.com or use the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/wlan-sol-eng>



Note

WLSE update images are subject to import/export regulations on strong encryption. You may be directed to edit your Cisco.com profile to confirm that you are allowed to download such images before you can complete the download.

Download the relevant upgrade files:

- If you are using a local repository on the WLSE, download the zip file, the info file, and the readme to an FTP server. The upgrade zip file and the info file must be in the same directory on the FTP server. *Do not extract the zip file.*
- If you are using a Windows server as a repository, download the zip file and the readme file to the Windows server. *Do not extract the zip file.*

Creating the Repository

Adding files to the repository and deleting files from the repository require the use of CLI commands. For more information on CLI commands, see [Appendix A, “Command Line Interface \(CLI\) Commands.”](#)

The topics in this section are:

- [Creating a Local Repository, page 16-14](#)
- [Creating a Repository on a Windows Server, page 16-15](#)

Creating a Local Repository

To create a local repository on the WLSE:



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Open a [CLI](#) window to the WLSE, using Telnet or [SSH](#).
- Step 2** Specify the FTP site that will be the source of the software updates. Enter the following CLI command:
- ```
repository source ftp://hostname/path
```
- where *hostname* is the name of the remote FTP server and *path* is the directory path on the remote FTP where you placed the zip file and info file.
- Step 3** Find the software you want on the FTP site by entering the following command. This command requires a valid username and password on the remote FTP server.
- ```
repository list remote
```
- Step 4** Download the software to the local repository using the following command. This command requires a valid username and password on the remote FTP server.
- ```
repository add package
```

For example, if the name of the zip file is WLSE-2.7-K9.zip, the *package* is WLSE-2.7-K9.

---

## Creating a Repository on a Windows Server

A remote repository can serve as the repository for numerous WLSEs. You can create a repository on a Windows NT, Windows 2000, or Windows XP server.



### Note

A remote repository created on a Windows server is temporary; it will not exist after the server reboots.

---

Use the following procedure to set up a Windows NT, Windows 2000, or Windows XP server as a remote repository.

### Procedure

---

- Step 1** If you are using a Windows XP or Windows 2000 server as a repository and you are using the Internet Explorer 6.0 browser on the client, configure the browser *on the repository* as follows to make sure the update process works properly. Otherwise, the display during the update process does not work properly.
- Install Java Plugin 1.3.1\_08 or later.
  - In the browser, select **Tools > Internet Options > Privacy** and lower the slider all the way down to achieve the **Accept all Cookies** setting.



**Note** For information on supported browsers, see [Supported Browsers, page 1-6](#).

---

- Step 2** Extract the zip file to any empty directory; for example, D:\WLSE\_repository.
- Step 3** Open a command window, create a virtual drive, and map the virtual drive to the drive containing the update file; for example:
- ```
subst f: d:\WLSE_repository
```



Note The virtual drive (f: in this example) will be removed after you reboot the Windows 2000, Windows NT, or Windows XP server.

Step 4 Double-click the virtual drive icon. Then, double-click the autorun.bat file if it does not automatically run.

The Appliance Update screen appears in a browser.

Defining the Repository

By defining the repository, you are telling the WLSE where to look for available software updates.



Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Admin > Appliance > Software > Define Repository**.

Step 2 To define or redefine the repository, complete the following:

Text Box	Description
Host Name	Hostname or IP address of the repository. For a local repository, enter <code>localhost</code> . For a remote repository, enter the hostname or IP address of the repository.
Port Number	Port number used by the software on the repository. The default port number for a repository is 9851.
Description	(Optional) Description of the repository.

Step 3 Click **Connect to Repository** to verify that the hostname and port number you entered are correct. If the data is incorrect, an error message appears.

- Step 4** Select **Admin > Appliance > Software > Browse Repository** to check the update image.
-

Related Topics

- [Installing the Software Upgrade, page 16-17](#)
- [Browsing the Repository, page 16-19](#)
- [Managing WLSE System Software, page 16-10](#)

Installing the Software Upgrade



Caution

Before upgrading WLSE software, back up the configuration. The upgrade attempts to preserve the WLSE database, but a backup is needed in case of errors during the upgrade. For information on backing up the WLSE's configuration, see [Backing Up and Restoring Data, page 16-28](#).

Before upgrading WLSE software, check the readme file that accompanies the image in the Software Center on Cisco.com for possible changes to the procedure, caveats, and new features.

Upgrading on a redundant cluster requires special procedures. Before upgrading software on a redundant cluster of WLSEs, see [Upgrading Software on Redundant WLSEs, page 16-50](#).

When you update or reinstall software, the WLSE stops and restarts. Therefore, you cannot access the WLSE during a software update, and you must log in again after updating software.



Note

Your login determines whether you can use this option.

Procedure

-
- Step 1** If you are using Internet Explorer 6.0 on a Windows XP client to update WLSE software, make sure Java Plugin 1.3.1_08 is installed on the browser. Otherwise, certain displays during the upgrade process do not work properly.
- Step 2** Select **Admin > Appliance > Software > Install Software Updates**. The Install Software Updates window opens and displays information about the WLSE, the currently defined repository, and the compatible software available for updating.
- Step 3** Select a software version from the Compatible Updates table, Compatible Reinstallations table, or Complete Images table.

These tables display the following information about the software you can install.

Field	Description
Name	Software identifier.
Version	Version number.
Summary	Brief description.
Release Date	Release date.
Details	Detailed description.

- Step 4** To view details on an image in the table, click **README** in the Details field.
- Step 5** To begin the installation, make a selection from the Compatible Updates table, Compatible Reinstallations table, or Complete Images table.
- Step 6** To install the selected software, click **Install**. The Install Software Updates window opens.
- Step 7** Click **Confirm** to continue the installation. Click **Cancel** to cancel the installation.
- Step 8** When the installation is complete, the WLSE will be unavailable for a few minutes while it restarts.
- If the Appliance Update window reappears, click the **Cancel** button to remove it.
- Step 9** To view details of the installation after the installation is complete, select **Admin > Appliance > Software > Status > View Log**.
-

Related Topics

- [Managing the Repository, page 16-13](#)
- [Viewing Status of Installed Software, page 16-11](#)
- [Viewing Software Update History, page 16-20](#)
- [Browsing the Repository, page 16-19](#)
- [Managing WLSE System Software, page 16-10](#)

Browsing the Repository

You can browse the available complete images and software upgrades on the repository using this option.



Note

A [repository](#) must be defined before you can browse software. To create and define a repository, see [Managing the Repository, page 16-13](#).



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Software > Browse Repository**.
- Step 2** To view detailed information about a complete image or update, click **README** in the Complete Images table or Updates table. These tables display the following about all the software available on the repository:

Field	Description
Name	Software identifier.
Version	Version number.
Appliance Type	The appliance type that the software is designed for.
Release Date	Release date.
Summary	Brief description.
Details	Detailed description. Click README to display details.

Related Topics

- [Installing the Software Upgrade, page 16-17](#)
- [Managing WLSE System Software, page 16-10](#)

Viewing Software Update History

This window shows only the update history, not a history of installed images. When you install a complete new image, the previous update history is erased.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Software > Software Update History**. The following information is displayed:

Table 16-6 Software Update History Window

Field	Description
Name	Software identifier.
Version	Software version.

Table 16-6 Software Update History Window (continued)

Field	Description
Summary	Summary of the installed software.
Install Date	Date and time (UTC) the software was installed.
Status	Status of the installed software.
Status	The status of the installation: Success—Software was installed with no errors. Warning—Software installed successfully with minor errors. Error—Software installation was unsuccessful.
Details	The detailed install log for this installation, including warning and error messages.

Step 2 Click **View Log** in the Details field to view the detailed installation log.

Related Topics

- [Viewing Status of Installed Software, page 16-11](#)
- [Browsing the Repository, page 16-19](#)
- [Managing WLSE System Software, page 16-10](#)

Viewing Software Update Logs

The WLSE maintains the following software update logs:

- dataUpdate.log
- updateWLSE-x.x.x.log

To view these logs, select **Admin > Appliance > Status > View Log File**. These logs are not listed until you have performed an update of WLSE software.

Data Preserved or Changed After Upgrade

For information on data that is not preserved or data that is changed after upgrading to WLSE 2.11, see the *Software Upgrade Guide for the CiscoWorks Wireless LAN Solution Engine* on Cisco.com.

Managing Security

You can manage the WLSE's by using the options under **Admin > Appliance > Security**:

- **Authentication Modules**—Set up the authentication module to be used (see [Using an Authentication Module, page 16-24](#)).
- **SSL (HTTPS)**—Obtain a permanent, signed Certificate Signed Request for secure Web access (see [Managing SSL \(HTTPS\), page 16-26](#)).
- **Telnet and SSH**—Configure Telnet and **SSH** settings (see [Enabling Telnet and Selecting SSH Type, page 16-27](#)).
- **Last 10 Logins**—View information about the last 10 users who have logged on to the WLSE (see [Viewing the Last 10 Logged-On Users, page 16-27](#)).

Related Topics

[Overview: Security, page 16-22](#)

Overview: Security

The WLSE provides the following security features:

- Optional secure connection through the Web browser—See [Managing SSL \(HTTPS\), page 16-26](#).
- Connection through the **CLI** via Telnet or SSH—See [Enabling Telnet and Selecting SSH Type, page 16-27](#).
- Authentication through the local database or alternative authentication services—See [Using an Authentication Module, page 16-24](#) and [Managing User Accounts, page 16-71](#).
- Flexible user access to managed devices and WLSE services through configurable roles—See [Managing Roles, page 16-69](#).

Overview: Authentication Modules

The WLSE provides a mechanism for authenticating users through the local authentication module and a local database of user IDs and passwords. Many network managers, however, already have an authentication service. To use your own authentication service instead of the local module, you can select one of the alternative modules:

- TACACS+
- Radius
- MS NT Domain

After you select and configure a module, all authentication transactions are performed by the authentication service associated with that module. Users log in with the user ID and password associated with the current authentication module.

The WLSE determines user roles; therefore, all users must be in the local database of user IDs and passwords. A user's role determines the services and devices that the user can access. Users must have the same user ID locally as they have in the alternative authentication source, but the local password and authentication service password do not have to be same.

Users who are authenticated by an alternative service and who are not in the local database have no roles assigned to them. Users who have no roles see only the splash screen after logging in and cannot view screens or perform tasks.

If the alternative authentication service fails, the WLSE defaults to the Local authentication module. Even if the local user database fails, you can always log in as the admin user.

Related Topics

- [Using an Authentication Module, page 16-24](#)
- [Managing GUI Users, page 16-69](#)

Using an Authentication Module

You can use your existing authentication method to authenticate WLSE users by selecting and configuring one of the WLSE's login modules.

To configure an authentication module for users logging in to the CLI via Telnet or SSH, use the **auth** CLI command.

After you change the authentication module, you do not have to restart the WLSE. Changing the module does not affect users who are currently logged on. Users who log on after the change use the new module.



Note

Even if you are using your own authentication service, all users must still be in the local database of users. That is, for each user of the WLSE, there must be a local user account matching the name of the user on the external authentication server. While authentication is performed by the authentication service, authorization is done on the WLSE by using local user accounts. For information on adding users to the local database, see [Managing GUI Users, page 16-69](#).



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Security > Authentication Modules**.
- Step 2** Select an authentication module from the Select Module drop down list, then click **Submit**.
- Step 3** Depending on the authentication module you selected, enter the following data, then click **Submit**:
- Step 4** Select the module you want to use and enter the following data accordingly.

Table 16-7 Authentication Modules

Module	Parameters and Notes
Local	Use local authentication only. This is the default setting. No configuration required.

Table 16-7 Authentication Modules

Module	Parameters and Notes
RADIUS	<p>Primary Server and Secondary Server—IP addresses or device names of the primary and secondary authentication servers. A secondary server is optional.</p> <p>Shared Secret—Secret key.</p>
TACACS+	<p>Primary Server and Secondary Server—IP addresses or device names of the primary and secondary authentication servers. A secondary server is optional.</p> <p>Shared Secret—Secret key.</p> <p>Note If you select this module, only the users configured on the TACACS+ server and the admin user can log into the WLSE.</p>
MS NT Domain	<p>Domain—Name of the Windows domain.</p> <p>Primary Domain Controller and Backup Domain Controller—Names of the primary and backup Windows domain controllers. A backup domain controller is optional.</p> <p>When entering the primary domain controller:</p> <ul style="list-style-type: none"> • Use the WINS name (simple hostname); for example, myhost. • <i>Do not</i> specify the primary domain controller as a fully-qualified domain name (for example, myhost.mycompany.com) or as an IP address.

Step 5 Click **Submit** to save your changes.

Related Topics

- [Overview: Authentication Modules, page 16-23](#)
- [Setting Up TACACS+ or RADIUS Authentication for CLI Login, page 17-6](#)

Managing SSL (HTTPS)

SSL (secure socket layer) protocol provides a secure connection between Web clients and the WLSE. When you initially set up the WLSE, normally, an unsigned certificate and a CSR (Certificate Signed Request) are automatically generated and SSL is enabled. The unsigned certificate expires in one year. To obtain a permanent, signed certificate, use the following procedure.



Note

If you did not generate an unsigned certificate during initial installation and setup of the WLSE, You must log in to the CLI and use the **mkcert** command to generate an unsigned certificate, then log back in to the Web interface to complete the procedure for enabling SSL.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Security > SSL (HTTPS)**.
- Step 2** Click **View CSR**. The encrypted CSR is displayed.
- Step 3** Copy the encrypted CSR (between the *begin* and *end* lines). Send the CSR to a certificate authority (such as Verisign), following the authority's procedure.
- Step 4** When you receive the signed certificate:
 - a. Copy it into an ASCII file on a client system.
 - b. On the same client, select **Admin > Security**.
 - c. Under SSL (HTTPS), type the path to the signed certificate or click **Browse** to locate the file, then click **Submit Certificate**.
 - d. To use the new certificate, you need to restart the WLSE by logging on through the **CLI**, running the **services stop** command to stop the system, then running the **services start** command to restart the system.
- Step 5** You should block logins on the regular HTTP port (1741):
 - a. Log in to the WLSE by using the console or by using Telnet or SSH.
 - b. Enter the following CLI command:

```
# firewall eth0 1741
```

- Step 6** To establish a connection to the WLSE by using SSL, use the prefix https instead of http when entering the URL into the browser and do not append a port number to the URL.
-

Enabling Telnet and Selecting SSH Type

Telnet can be used for connecting to the WLSE through the [CLI](#). By default, Telnet is disabled, which prevents unsecure connections through the CLI.

SSH is enabled by default. SSH provides a secure Telnet connection, encrypting all traffic, including passwords. By default, both SSH1 and SSH2 are used.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Appliance > Security > SSH and Telnet**.
- Step 2** To change the type of SSH used, select the desired SSH version from Select Protocol, then click **Change Protocol**.
- Step 3** To enable or disable Telnet, make a selection from Telnet, then click **Configure**. Changes occur immediately.
-

Viewing the Last 10 Logged-On Users

To view information about the last 10 users who have logged on to the WLSE:

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Admin > Appliance > Security > Last 10 Logins**.

The Last 10 Logins table shows the following information for the last 10 logins:

Field	Description
Login Name	User's login name.
Logged In Since	Date and time the user logged in (UTC).
IP Address	IP address of the system from which the user logged in.
Associated role	Role assigned to the user.

Backing Up and Restoring Data

Backup and restore allows you to backup the WLSE's configuration and restore it if necessary.

**Caution**

You cannot restore a backup from a WLSE running pre-release (beta) software to a WLSE running released software.

The following options are provided for backup and restore:

- **Configure**—You must set the backup location before you can run backups (see [Specifying the Backup Location, page 16-29](#)).
- **Backup**—Schedule a backup of WLSE data or run an immediate backup (see [Scheduling and Running Backups, page 16-32](#)).
- **Restore**—Restore an available backup image (see [Restoring Data, page 16-34](#)).
- **Backup log**—The backup log appears after you back up WLSE data, restore data, or test the reachability of the backup location (see [Using WLSE Log Files, page 16-5](#)). To clear the backup/restore log, see [Clearing the Backup/Restore Log, page 16-32](#).

Related Topics

- [About Backup and Restore, page 16-29](#)
- [Backing Up and Restoring via CLI, page 17-6](#)

About Backup and Restore

Backing up the WLSE saves its configuration data in case you need to restore the data. The backup operation backs up the entire WLSE database and configuration, which includes appliance setup, fault and performance data, device credentials, WLSE users, configuration templates, user-created groups, and jobs.

Backups are typically done on a regular basis (for example, weekly). However, you may choose to back up infrequently and use one or more of the data export mechanisms to gather interesting data from the WLSE.

The backup operation may take some time depending on the size of the database: the larger the database, the more the backup time will be required.

The restore operation includes all the information in the backup, including the information entered during initial configuration of the WLSE (setup program).

The restore process disrupts normal WLSE operation because the process shuts down the WLSE internal database and then restarts it.

You can restore data backed up on one WLSE to another WLSE. For information on restoring from one WLSE to another, see [Copying Configuration Data from One WLSE to Another, page 16-35](#).

Specifying the Backup Location

You must set the backup location before you can run backups. The backup location must be an FTP server because the WLSE uses FTP to transfer the data.

Please observe the following cautions about the backup location:

- Backup has only been tested on the standard Windows 2000, Windows XP, and Unix FTP servers. Therefore, only these servers are explicitly supported for WLSE backups. However, any server that uses standard FTP commands and protocol should work.
- Make sure the target FTP directory has enough free space, especially if you are running frequent backups. If there is not enough space, the backup may fail or the backup data may be corrupted.

- If you are using a Windows 2000 or Windows XP server as the backup location, you must configure the server for UNIX directory mode. See [Configuring a Windows System as a Backup Location, page 16-31](#).

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Admin > Appliance > Backup and Restore > Configure**.

Step 2 Enter the following data:

Field	Description
Hostname/IP	Hostname or IP address for the backup location.
Username	Valid username on the backup location.
Password	Valid password on the backup location.
Verify Password	
Path (Optional)	<p>Path to the backup location. When specifying the path on a Windows 2000 or Windows XP server:</p> <ul style="list-style-type: none"> • Use either forward slashes (/) or backslashes (\) as directory separators. • Do not include the drive specifier; for example, c:\. • Path is relative to the ftp root. • Backup mechanism can create multiple directory levels for you.
Use Secure Transfer	<p>Select this to use secure copy (SCP) to move the backup files to the remote host. SCP is based on SSH.</p> <p>SCP uses keys to identify the remote host and stores these keys on the WLSE. If the key on the remote host changes, the backup cannot be transferred. If you know that a key was legitimately changed on the remote host, you can use the clearbackuphosts CLI command to clear the stored keys. After that, the new keys can be stored.</p>

- Step 3** Click **Save**, or click **Erase** to clear your entries or remove the previously configured backup location.
- Step 4** Click **Test** to verify that the backup location is reachable and is configured as an FTP server.
- The message “Test OK” should be displayed. Any other response indicates a problem with the backup.
- Step 5** Click **Clear Log** to delete from the View Log File window the backup.log file that was created after the previous backup or restore operation.
-

Related Topics

- [Scheduling and Running Backups, page 16-32](#)
- [Restoring Data, page 16-34](#)
- [Configuring a Windows System as a Backup Location, page 16-31](#)
- [About Backup and Restore, page 16-29](#)
- [Backing Up and Restoring via CLI, page 17-6](#)

Configuring a Windows System as a Backup Location

You can use a Windows 2000 Server, Advanced Server, or Windows XP Professional system as a backup location. Before use, the system be configured as follows.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** On the server, select **Start > Programs > Administrative Tools > Internet Services Manager**.
- If this option is not available on the server, first enable it as follows:
- a. Select **Start > Settings > Control Panel > Add/Remove Programs**.
 - b. On the left side of the Add/Remove window, click **Add/Remove Windows Components**. The Windows Components wizard starts.

- c. Select Internet Information Services, then click **Next**.
- Step 2** Right-click the FTP site for which you want to set the directory output style, then select **Properties**.
- Step 3** Select FTP Service from the Master Properties list and click **Edit**.
- Step 4** Select the Home Directory property sheet:
- Select **Write** under FTP Site Directory.
 - Select **UNIX** under Directory Listing Style.
 - Click **OK**.
-

Clearing the Backup/Restore Log

To remove the backup.log file from the View Log File window, select **Admin > Appliance > Backup and Restore > Configure**. Then, click **Clear Log**. This removes from the View Log File window the file created by the last backup or restore operation. This log file is called backup.log.

Scheduling and Running Backups

Data backed up includes role and user information, discovery configuration information, and other configuration information. The following procedure includes a verification step; it is recommended that you always verify that the backup succeeded. You can run an immediate backup or schedule regular backups.

Before scheduling backups, verify that the system time is set correctly. To set the system time, see [Set the Current Local and UTC Time, page 16-59](#).



Note Normal operations continue during backup.



Note You should perform a backup whenever you add users.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Make sure the backup location has been specified (see [Specifying the Backup Location, page 16-29](#)).
- Step 2** Select **Admin > Appliance > Backup and Restore > Backup**.
- Step 3** To run an immediate backup, click **Backup Now**.
- Step 4** To schedule automatic backups:
- a. Enter the start date and time:
 - Select Every Month or a specific month.
 - Select Every Day, a day of the week, or a day of the month.
 - Select the time as hours (24-hour clock) and minutes (5-minute increments).
 - b. Click **Schedule Backup**.
- Step 5** To cancel a scheduled backup, click **Remove Scheduled Backup**.
- Step 6** There are several ways to verify that the backup succeeded:
- Check the log file under backup.log file under **Admin > Appliance > Status > View Log File**.
 - Select **Admin > Appliance > Backup and Restore > Restore**. The backup image should be listed in the Available Images list. Click **Cancel**.
 - Log in to the backup location system and verify that there is a backup directory containing *WLSE hostname_date_time.inf* and *WLSE hostname_date_time.tar* files.
-

Related Topics

- [Restoring Data, page 16-34](#)
- [About Backup and Restore, page 16-29](#)
- [Backing Up and Restoring via CLI, page 17-6](#)

Restoring Data



Caution

If you are restoring a backup on a WLSE that is configured for redundancy, see the special instructions in [Backing Up and Restoring on Redundant WLSEs](#), page 16-51.

After you click **Restore** and **OK** in the following procedure, the following occur in sequence:

1. The WLSE shuts down automatically.
2. The data is restored.
3. The WLSE reboots.



Note

Your login determines whether you can use this option.

Procedure

To restore the WLSE's configuration data from a backup:

- Step 1** Select **Admin > Appliance > Backup and Restore > Restore**.
- Step 2** From the Available Images list, select a backup image. Images are listed by WLSE hostname and date and time of backup.
- Step 3** Click **Restore Appliance Network Information** if you want to restore the following information that is stored in flash memory:
 - Network information—WLSE hostname, IP address, domain name, name servers, NTP server, and firewall settings.
 - Users' CLI privileges.



Caution

Deselect **Restore Appliance Network Information** if you are restoring a backup created on another WLSE. For more information on restoring from one WLSE to another, see [Copying Configuration Data from One WLSE to Another](#), page 16-35.

- Step 4** Click **Restore**. The Restore Backup window opens.

Step 5 Click **OK**.

Result: The WLSE shuts down, the data is restored, then the WLSE restarts.

Related Topics

- [Scheduling and Running Backups, page 16-32](#)
- [Specifying the Backup Location, page 16-29](#)
- [About Backup and Restore, page 16-29](#)
- [Backing Up and Restoring via CLI, page 17-6](#)

Copying Configuration Data from One WLSE to Another

You can back up data from one WLSE and copy it to another by using the backup and restore features. If you are replacing one WLSE with another, see the instructions in [Installing a Replacement WLSE, page 17-11](#).

Step 1 Back up the data on the source WLSE. For more information, see [Backing Up and Restoring Data, page 16-28](#).

Step 2 If you have installed a new WLSE and have not configured it yet, complete the initial configuration.

For information on the setup program and initial configuration, see relevant installation guide for your WLSE hardware.

Step 3 Restore configuration data to the destination WLSE, using the backup you made in Step 1.



Caution

Be sure to deselect **Restore Appliance Network Information**. Otherwise, the network information in flash memory will be overwritten and you will have to erase the WLSE's configuration and run the setup program.

For more information on restoring backups, see [Restoring Data, page 16-34](#).

Related Topics

[Copying Configuration Data to another WLSE via CLI, page 17-13](#)

Managing WLSE Master Configuration Files (WLSE Express Only)

Using this option, you can create master configuration files that contain the current basic configuration data of a WLSE Express and use these files to configure other WLSEs.

For details on the content of the master configuration files, see [About the Master Configuration Files, page 16-38](#).

Use the following procedure to create WLSE configuration files and download them from the WLSE to a TFTP server.

For details on the contents of the configuration files, editing the .xml file, parameters that can be saved, and procedures for using the master configuration to configure other WLSEs, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine Express, Release 2.11*.

**Note**

Your login determines whether you can use this option. This option is available on the WLSE Express only.

Procedure**Step 1**

To create configuration files:

- a. Configure the current (reference) WLSE with the data you want to save.
- b. Select **Admin > Appliance > Master Configuration**.
- c. Enter a filename in the Filename field.
- d. Click **Create New Config**.

Result: The types of data you can include in the configuration files are displayed.

- e. Select the data that you want to save. See [Table 16-8 on page 16-37](#) for more information about the data that is saved.

f. Click **Create Config**.

Results: The .xml, .info, and .dat files are created and combined into a tar archive and stored on the WLSE. The name of the archive and the date it was created are added to the Saved Configurations list.

Table 16-8 Data Saved in the Master Configuration Files ¹

Type	Parameters	In .xml File	In .dat File
Faults	Default fault profile settings		X
	Notification settings	X	
Discover	Discovery schedule, including seed devices and CDP distance setting	X	
	Device credentials	X	
	Advanced options (auto-manage, DNS lookup, and name format)	X	
	Inventory polling parameters	X	
	AAA server monitoring	X	
	Client tracking enable	X	
Rule Based Groups	User-defined rule-based groups		X
Configure	Templates ²	X	X
	Startup configuration assignments	X	
	Auto-managed template assignments	X	
Administration	Appliance Settings (redundancy, splash screen)	X	
	User role definitions		X
	Users	X	
Radio Management	AP locations	X	
	Radio management configuration	X	

1. For parameters that cannot be saved from the UI, you can add CLI commands to the .xml file. For example, settings for the internal AAA server are not saved from the UI.
2. Any custom commands in templates are saved to the .xml file. Template settings made from the UI are saved in the .dat file.

- Step 2** To download the archive to your desktop:
- Select a configuration from the Saved Configurations list.
 - Click **Download**.
 - Specify the location, then download the file.
- Step 3** To delete a saved configuration file from the WLSE, select the file from the Saved Configurations list and click **Delete**.
-

Related Topics

[About the Master Configuration Files, page 16-38](#)

About the Master Configuration Files

When you use the Master Configuration option, 3 files are created and combined into a tar archive. For example, if you specify the filename “config,” a tar archive called myconfig.tar is created. The archive contains the following files:

- config.xml—This file contains most of the WLSE configuration parameters in XML format, as shown in [Table 16-8 on page 16-37](#). You can edit this file.

The following parameters must be manually added to the .xml file as CLI commands:

- AAA Administration parameters (internal AAA server)
- Most of the settings in the Appliance subtab

You can also add other WLSE CLI commands to the .xml file.

For information on editing the .xml file, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine Express, Release 2.11*.

- config.dat—This file contains parameters that are saved as binary data, as shown in [Table 16-8 on page 16-37](#). This file cannot be edited.
- config.info—This file contains information about the other two files and identifies the tar file as a valid WLSE configuration.

Configuration files can be automatically downloaded to WLSEs by storing the file on a TFTP server and using DHCP to download the file. For more information on this method of configuring WLSEs, see the *Installation and Configuration Guide*

for the CiscoWorks Wireless LAN Solution Engine Express, Release 2.11. For help in locating this guide on Cisco.com, see [Finding WLSE Documentation on Cisco.com, page 1-21](#).

Managing WLSE Redundancy

The redundancy feature allows you to enable high availability through a two-node cluster of WLSEs. If the WLSE designated as the primary node fails, fail-over occurs automatically to the secondary node. If, subsequently, the primary node is back in service and the secondary node fails, failback occurs to the primary node.

Configurable periodic synchronizations between primary and secondary nodes ensure that any data or configuration loss is minimal. During failover, all users are logged out and must log back in.



Tip

To force fail over from the active node to the standby node, see [Performing Manual Failover to the Standby Node, page 16-50](#).

Before enabling redundancy, see [Redundancy Prerequisites, page 16-40](#) for hardware and configuration prerequisites.

For details on how redundancy works, see [About Redundancy, page 16-41](#).

You can use the redundancy options to:

- Enable redundancy—See [Configuring Redundancy, page 16-44](#).
- Check redundancy settings—See [Checking Redundancy Settings, page 16-48](#).
- View the log of redundancy events—See [Viewing the Redundancy Log, page 16-49](#).

Related Topics

- [About Redundancy, page 16-41](#)
- [Redundancy Prerequisites, page 16-40](#)
- [Redundancy Email Messages, page 16-43](#)
- [Performing Manual Failover to the Standby Node, page 16-50](#)
- [Upgrading Software on Redundant WLSEs, page 16-50](#)

- [Replacing a Node](#), page 16-50
- [Backing Up and Restoring on Redundant WLSEs](#), page 16-51
- [Changing the Web Timeout Period on Redundant Nodes](#), page 16-52
- [Controlling Access via HTTP/HTTPS on Redundant Nodes](#), page 16-53

Redundancy Prerequisites

Following are the requirements for WLSE redundancy:

- You must have two operating WLSEs, which are installed and operating on the network.
- Both WLSEs must be running the same software version (2.7 or later).
- You can use either the WLSE 1130 or WLSE 1130-19. One node in the redundant pair can be a WLSE 1130, and the other a WLSE 1130-19.
- Both systems must be in the same IP subnet and connected to the same router.
- Both systems must have static IP addresses. In addition, one free IP address on the same subnet, which will be used as the virtual IP address, is required. Two free IP addresses are required if the virtual IP address is configured on both interfaces. The virtual IP address(es) will be automatically bound to the active WLSE, and users can use this address to always connect to the active node.
- Ethernet interface 0 on both WLSEs must be in the same subnet. If ethernet interface 1 is in use on both WLSEs, ethernet interface 1 on both WLSEs must be in the same subnet. You can use either ethernet interface for redundancy.
- Both WLSEs must be using the same HTTP port. The default port is 1741. You can set this port to 1741 or 80 by using the **http-server port** CLI command.
- The password for the admin user must be the same on both WLSEs.
- The mail route must be configured if you want to receive email notification of redundancy events. You can set the mail route by using the **mailroute** CLI command or by setting the mail route in Web interface (see [Configuring the Mail Route](#), page 16-62).

About Redundancy

Redundancy is achieved by configuring a cluster of two WLSEs. One WLSE is in active mode, performing all normal WLSE functions. The other WLSE is in warm standby; that is, the system is up but no WLSE applications are running and only certain diagnostic operations are allowed.

The user interface on the standby node is restricted. The only features displayed are the Admin tab and the Appliance subtab. This prevents users from accidentally using the standby node for other operations.

For more information, see the following topics:

- [Redundancy Configuration, page 16-41](#)
- [Status Checking, page 16-41](#)
- [Failover, page 16-42](#)
- [Messages, page 16-42](#)
- [Changes in Certain Functions under Redundancy, page 16-42](#)

Redundancy Configuration

Redundancy can only be configured in the Web interface. However, after you have configured it, you can turn it on or off by using the redundancy CLI command.

All redundancy configuration is performed on the primary node, which becomes the active WLSE after you set up redundancy. This configuration, plus all other data, is copied to the secondary node (the standby WLSE) automatically.

Periodically, incremental changes are applied to the standby to keep it synchronized with the active node. To make sure the active node is running normally, the standby node periodically checks the active node; and the active node periodically checks the standby node.

Status Checking

Under redundancy, the nodes synchronize with each other, the standby node checks the active node, and the active node checks itself.

Synchronization and checking intervals are configurable by the administrator. The minimum amount of time between data synchronizations is 20 minutes, and the maximum amount of time is 5 hours. The frequency of checks made by the standby node can be set to between 15 seconds and 5 minutes.

A second type of check is done by the active node, which periodically makes the following system checks on itself:

- Checks whether the database is up and running.
- Checks the file system by creating files.
- Checks the state of the process daemon manager.

If any of these system checks fail repeatedly on the active node, data will be synchronized with the standby node. Then the standby will become active and the original active node will reboot. This failover will not occur if the active node cannot reach the standby node. In that case, the active node will remain up and running until the standby comes back online.

Failover

If the active node goes down or experiences a transient failure, all users are logged out and must log back in. No matter which node is active, users always log in to the same IP address, called the virtual IP.

When the formerly active node comes back into service, it automatically becomes the standby node. If both WLSEs go down, the current active node may become the standby node if the standby node restarts first.

In case of failover, a small amount of data that has not been committed to the standby will be lost. The amount of potential data loss is limited to the data accumulated during the interval between synchronization of the two nodes. It will take a few minutes for the standby node to become active after it detects that the other node has failed.

Messages

Redundancy troubleshooting messages are logged to the tomcat.log file. To troubleshoot a node, log in using the real IP address, not the virtual IP address.

Changes in Certain Functions under Redundancy

Certain WLSE functions require special treatment on a redundant cluster. See the following:

- [Upgrading Software on Redundant WLSEs, page 16-50](#)
- [Replacing a Node, page 16-50](#)
- [Backing Up and Restoring on Redundant WLSEs, page 16-51](#)

- [Changing the Web Timeout Period on Redundant Nodes](#), page 16-52
- [Controlling Access via HTTP/HTTPS on Redundant Nodes](#), page 16-53

Related Topics

- [Redundancy Prerequisites](#), page 16-40
- [Redundancy Email Messages](#), page 16-43
- [Performing Manual Failover to the Standby Node](#), page 16-50

Redundancy Email Messages

The messages sent by the redundancy module are described in [Table 16-9 on page 16-43](#). The sender of all messages is `WLSE@ip_address`, where `ip_address` is the IP address of the WLSE that is sending the message.

These messages are logged in the `redundancy.log` file. For information on viewing this and other WLSE logs, see [Using WLSE Log Files](#), page 16-5.

Table 16-9 Redundancy Email Messages

Email Subject	Meaning
Lost connectivity with standby on <code>ip_address</code> .	Standby node indicated by IP address is down.
Regained connectivity with standby on <code>ip_address</code> .	Standby node is up.
Lost connectivity with <code>ip_address</code> .	Node indicated by IP address is down.
Redundancy active mode.	WLSE that sent this message is now active; that is, the WLSE is providing WLSE services.
Redundancy standby mode.	WLSE that sent this message is now in standby mode.
Lost connectivity with router.	WLSE that sent this message was unable to ping the default router.
Regained connectivity with router.	WLSE that sent this message is now able to ping the default router.
Data may not have been successfully restored from active.	Standby WLSE detected failure of active WLSE and is becoming active before it successfully synchronized with the active node.
Redundancy turned off.	Redundancy has been disabled.

Table 16-9 Redundancy Email Messages (continued)

Email Subject	Meaning
Failed to ship database file.	Active WLSE failed to synchronize database data with the standby (probably caused by standby node failure).
Failed to ship config file.	Active WLSE failed to synchronize configuration data with the standby (probably caused by standby node failure).
Failed to ship transaction log file.	Active WLSE failed to synchronize database data with the standby (probably caused by standby node failure).
DB restore failed. Will reinitialize the DB on <i>ip_address</i> .	Standby node failed to apply data received from active and will attempt to reinitialize and reboot and try the data synchronization again.
DB rollforward failed. Will reinitialize the DB on <i>ip_address</i> .	Standby node failed to apply data received from active and will attempt to reinitialize and reboot and try the data synchronization again.
System check failed on <i>ip_address</i> for reason: <i>reason</i> .	System check failure.

Related Topics

- [About Redundancy, page 16-41](#)
- [Redundancy Prerequisites, page 16-40](#)
- [Performing Manual Failover to the Standby Node, page 16-50](#)
- [Upgrading Software on Redundant WLSEs, page 16-50](#)
- [TReplacing a Node, page 16-50](#)
- [Backing Up and Restoring on Redundant WLSEs, page 16-51](#)

Configuring Redundancy

Initial redundancy configuration is performed on the currently active WLSE. Initial configuration is done on whichever WLSE is to be designated as primary.

Subsequent configuration changes can be done on whichever WLSE is in active mode, but the node IP addresses should remain the same as when they were initially configured. If you need to change the node IP addresses, first turn redundancy off, then configure the node IP addresses.

**Caution**

When you enable and configure redundancy, all data on the standby system will be lost. Immediately after you complete the configuration and indicate that you wish to apply your changes, the active system is synchronized with the standby system. Thus, any existing data on the standby system is replaced by data from the active system.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Make sure that all prerequisites are met. See [Redundancy Prerequisites](#), page 16-40.
- Step 2** Log in to the primary node, which is the WLSE that will be active and providing management services.
- Step 3** Select **Admin > Appliance > Redundancy > Manage Redundancy**.
- Step 4** To enable redundancy, select **Redundancy Enabled**.
After redundancy is turned on, a backup and restore begins.
- Step 5** Enter data in the following fields.

Table 16-10 Redundancy Parameters

Field	Description
Redundancy Enabled	Select to enable redundancy. Deselect to disable redundancy. When this is selected, the other fields in the screen become active.
Admin Password	The admin password on both the active and standby systems. The password must be identical on both systems.

Table 16-10 Redundancy Parameters (continued)

Field	Description
Notification Email	Email address for notification of redundancy events. For information on these notifications, see Redundancy Email Messages, page 16-43 . For information on configuring email in general, see Configuring the Mail Route, page 16-62
HTTP Port	Port to use for client connections via HTTP. The default is 1741. The port must be the same on both systems. For information on setting the port, see the http-server port CLI command in Appendix A, “Command Line Interface (CLI) Commands.”
VIP IP eth0	<p>Unique IP addresses for the WLSE’s Ethernet interfaces. The virtual IP is the address for all accesses to the redundant pair, including logins to the WLSE.</p> <ul style="list-style-type: none"> You must always define VIP eth0. If the WLSE has two Ethernet interfaces, defining VIP eth1 is optional if redundancy functions will not be used on the eth1 interface. <p>The VIP is a static (non-DHCP) address that must be officially allocated by the site’s network administrator. The VIP must be in the same subnet as the interface. That is, VIP eth0 must be in the same subnet as eth0 and VIP eth1 must be in the same subnet as eth1.</p> <p>The VIP address is always assigned to the active WLSE. All accesses to the redundant pair are done by using the VIP address. Thus, if a failover occurs, the active WLSE always responds when addressed by the VIP.</p>
VIP IP eth1	
This Node IP ¹	Static IP address of the current (active) node. If both Ethernet interfaces are configured, you can select the address/interface for redundancy communication.
Other Node IP ¹	Static IP address of the system that will become the standby node.
Minutes between sync	How often the active and standby WLSEs are synchronized. Synchronization consists of incrementally backing up the database on the active WLSE and restoring on the standby WLSE. Default is 60 minutes. Can be set between 15 minutes and 5 hours. On networks with more than 500 devices, it is not recommended that you set this to less than 30 minutes.

Table 16-10 Redundancy Parameters (continued)

Field	Description
Seconds between check of other node	How often to check to make sure both nodes are functioning. Default is 60 seconds. Can be set between 15 seconds and 5 minutes.
Seconds between check of system	How often to check the status of the database and the process daemon manager on the active node.

- To change a node's IP address, first turn off redundancy, then configure the IP addresses, then turn on redundancy.

Step 6 Click **Reset** to remove your current settings.

Step 7 Click **Verify** to verify that your settings are correct. The Redundancy Settings Verified screen appears.

- If there are errors, click **Fix Errors** to return to the Redundancy Settings screen to fix the errors.
- If there are no errors:
 - Click **Yes** to apply your changes. Redundancy mode will be turned on. A full backup begins; the backup will be restored to the standby node. Regular backups and restores will now begin, and the standby node will begin regular checking to make sure the active node is functioning.
 - Click **No** to return to the Redundancy Settings screen.

Related Topics

- [Checking Redundancy Settings, page 16-48](#)
- [Viewing the Redundancy Log, page 16-49](#)
- [About Redundancy, page 16-41](#)
- [Redundancy Email Messages, page 16-43](#)
- [Performing Manual Failover to the Standby Node, page 16-50](#)
- [Upgrading Software on Redundant WLSEs, page 16-50](#)
- [TReplacing a Node, page 16-50](#)
- [Backing Up and Restoring on Redundant WLSEs, page 16-51](#)
- [Changing the Web Timeout Period on Redundant Nodes, page 16-52](#)

Checking Redundancy Settings



Note Your login determines whether you can use this option.

Procedure

- Step 1** Log in to the WLSE web interface of either the primary (active) node or the secondary (standby) node.
- Step 2** Select **Admin > Appliance > Redundancy > Redundancy Status**.
- Step 3** The redundancy settings described in [Table 16-11 on page 16-48](#) are displayed. If a field is blank, it has not been configured.

Table 16-11 Redundancy Settings

Field	Description
Redundancy Status	Active—Redundancy is enabled. This is the active node at the current time. Standby—Redundancy is enabled. This is the standby node at the current time. Not Configured—Redundancy is not enabled.
HTTP Port	HTTP port configured on both systems.
Notification Email	Email address to which notifications are sent.
Virtual IP eth0	Virtual IP address of Ethernet interface 0.
Virtual IP eth1	Virtual IP address of Ethernet interface 1 (if in use). For more information on virtual IPs, see Table 16-10 on page 16-45 .
This Node IP	Static IP address of the current system.
Other Node IP	Static IP address of the other system.
Minutes between sync	Synchronization interval (data copied from the active node to the standby node).

Table 16-11 Redundancy Settings

Field	Description
Seconds between check of primary	How often the standby system checks the active system to find out if the primary system is functioning.

Related Topics

- [Configuring Redundancy, page 16-44](#)
- [Viewing the Redundancy Log, page 16-49](#)
- [About Redundancy, page 16-41](#)
- [Redundancy Email Messages, page 16-43](#)
- [Performing Manual Failover to the Standby Node, page 16-50](#)
- [Upgrading Software on Redundant WLSEs, page 16-50](#)
- [TReplacing a Node, page 16-50](#)
- [Backing Up and Restoring on Redundant WLSEs, page 16-51](#)
- [Changing the Web Timeout Period on Redundant Nodes, page 16-52](#)

Viewing the Redundancy Log

The event log contains a listing of all significant redundancy events since the WLSE was started.

**Note**

Your login determines whether you can use this option.

Procedure

Select **Admin > Appliance > Redundancy > Event Log**.

The redundancy log is displayed; for example:

```
02:24:13 02/13/2004 Lost connectivity with standby on 192.161.98.53
02:24:13 02/13/2004 Regained connectivity with standby on
192.161.98.53
02:24:13 02/13/2004 Redundancy active mode
02:24:13 02/13/2004 Shipped file S0000147.LOG
02:24:12 02/13/2004 Shipped file wlse-configs.tgz
```

Related Topics

- [About Redundancy, page 16-41](#)
- [Redundancy Email Messages, page 16-43](#)

Performing Manual Failover to the Standby Node

If you reboot the active node or stop services on it (preferred method), the standby node will automatically become active.

To reboot a WLSE, see [Restarting the WLSE, page 16-9](#).

To stop services on a WLSE, Telnet or SSH to the WLSE and enter the following CLI command:

```
services stop
```

To restart services, enter the following CLI command:

```
services start
```

Once restarted, the formerly active node will automatically become the standby node.

Related Topics

- [About Redundancy, page 16-41](#)

Upgrading Software on Redundant WLSEs

Both the active and standby node must run the same software release. For information on upgrading software in a redundant cluster, see *Upgrading the CiscoWorks Wireless LAN Solution Engine, 2.11* on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_11/index.htm.

Replacing a Node

If you need to replace a node:

- Turn off redundancy.
- Configure the replacement node.
- Turn on redundancy.

See [Configuring Redundancy, page 16-44](#) for information on turning redundancy on and off.

Related Topics

- [About Redundancy, page 16-41](#)
- [Checking Redundancy Settings, page 16-48](#)
- [Viewing the Redundancy Log, page 16-49](#)

Backing Up and Restoring on Redundant WLSEs

This section contains the following information:

- General information about backup and restore on redundant nodes—[About Backup and Restore on Redundant Nodes, page 16-51](#).
- How to restore on redundant nodes—[Restoring on Redundant Nodes, page 16-52](#).

About Backup and Restore on Redundant Nodes

When backing up and restoring on redundant nodes:

- If redundancy is not enabled, backup and restore are allowed.
- On the active node, backup is allowed; but restore fails and generates an error message asks you to first turn off redundancy.
- On the standby node, neither backup nor restore is allowed. If you try to run backup, an error message asks you to run backup on the active node.
- When restoring, if the backup was performed on the active node, redundancy will be automatically turned off after the restore. You will have to re-enable redundancy.

Restoring on Redundant Nodes

When restoring data from a previous backup on WLSEs that have been configured for redundancy, use the following procedure.

Procedure

- Step 1** Turn off redundancy.
- Step 2** Restore data on the primary WLSE, following the procedure in [Restoring Data, page 16-34](#).
- Step 3** Turn on redundancy
-

Related Topics

- [About Redundancy, page 16-41](#)
- [Redundancy Email Messages, page 16-43](#)
- [Configuring Redundancy, page 16-44](#)
- [Checking Redundancy Settings, page 16-48](#)
- [Viewing the Redundancy Log, page 16-49](#)

Changing the Web Timeout Period on Redundant Nodes

If WLSE redundancy is in effect, you should stop and restart services on the standby WLSE. Otherwise, resetting the timeout will cause a switchover from the active server to the standby server and the new timeout period will not take effect.

Procedure

- Step 1** Telnet or SSH to the standby WLSE.
- Step 2** Enter the following CLI command on the standby server:
- ```
services stop
```

**Step 3** Change the web timeout period on the active server. For more information, see [Set the Web Timeout Period, page 16-61](#).

**Step 4** Enter the following CLI command on the standby server:

```
services start
```

---

## Controlling Access via HTTP/HTTPS on Redundant Nodes

If you are implementing HTTP/HTTPS access control by using the **http-server accept** CLI command, you must add each server to the other server's access list.

Assuming that the redundant WLSEs have IP addresses 209.165.202.100 and 209.165.202.200, enter the following CLI command on the WLSE with IP address 209.165.202.100:

```
http-server accept 209.165.202.200
```

Enter the following CLI command on the WLSE with IP address 209.165.202.200:

```
http-server accept 209.165.202.100
```

## Using WLSE Diagnostics Options

The Diagnostics option provides tools to aid in troubleshooting. You can use these tools when you have a problem that might require assistance from the Cisco Technical Assistance Center (TAC).

The options under **Admin > Appliance > Diagnostics** are:

- **WLSE Info**—Gather troubleshooting information about the WLSE status and create status reports (see [Viewing and Creating a Status Report, page 16-54](#)).
- **Self Test**—Create and display self tests (see [Viewing and Creating a Self-Test Report, page 16-54](#)).
- **Processes**—View WLSE process status, stop and start processes (see [Managing Processes, page 16-55](#)).

## Viewing and Creating a Status Report

This option provides a tool to aid in troubleshooting. The WLSE information and status report shows general WLSE status, log files, package information, database status, process status, web server information, Java class information, and log files.




---

**Note** Status reports show **UTC** time.

---




---

**Note** Your login determines whether you can use this option.

---

### Procedure

---

- Step 1** Select **Admin > Appliance > Diagnostics > WLSE Info**. Any existing reports are listed.
- Step 2** To display a report, click its name.
- Step 3** To create a new report, click **Create**. It will take five to seven minutes for the report to be complete. To display the new report, click its name. If the new report is not listed, click **Refresh**.
- Step 4** To delete a report, select it and click **Delete**.
- 

### Related Topics

- [Viewing and Creating a Self-Test Report, page 16-54](#)
- [Managing Processes, page 16-55](#)

## Viewing and Creating a Self-Test Report

This option provides a tool to aid in troubleshooting. Self-tests show the status of WLSE memory, database, DNS setup, and backup location configuration. Reports indicate whether the tests passed or failed. Self-tests are used mainly by the TAC when diagnosing problems.



---

**Note** Self-test reports show timestamps as [UTC](#) time.

---



---

**Note** Your login determines whether you can use this option.

---

### Procedure

---

- Step 1** Select **Admin > Appliance > Diagnostics > Self Test**. Any existing report is listed.
- Step 2** To display the report, click its name.
- Step 3** If no report is listed, you can create a new report by clicking **Create**.
- Step 4** To display the new report, click its name. If the report is not displayed, click **Refresh**.
- Step 5** To delete a report, select it and click **Delete**.
- 

### Related Topics

- [Viewing and Creating a Status Report, page 16-54](#)
- [Managing Processes, page 16-55](#)

## Managing Processes

This option provides a tool to aid in troubleshooting. You can view the status of the major processes running on the WLSE, start and stop processes, and access complete reports.



---

**Note** Your login determines whether you can use this option.

---

### Procedure

---

- Step 1** Select **Admin > Appliance > Diagnostics > Processes**. The Process Report displays the following information.

| Column       | Description                                                                                                                                                                                                                     |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process name | How a process is registered. For information on the processes displayed, see <a href="#">Processes Displayed, page 16-57</a> .                                                                                                  |
| State        | Process status and a summary of the log file entries for the process.                                                                                                                                                           |
| Pid          | Process ID. A unique number by which the operating system identifies each running program.                                                                                                                                      |
| RC           | Return code. “0” means normal program operation. Any other number typically represents an error. Refer to the error log.                                                                                                        |
| Signo        | Signal number. “0” means normal program operation. Any other number is the last signal delivered to the program before it terminated.                                                                                           |
| Start Time   | Time (UTC) and date the process was started.                                                                                                                                                                                    |
| Stop Time    | Time (UTC) and date the process was stopped.                                                                                                                                                                                    |
| Core         | “Not applicable” means the program is running normally.<br>“Core file created” means the program is not running normally and the operating system has created a core file. The core file stores important data about processes. |
| Information  | What the process is doing. “Not applicable” means the program is not running normally.                                                                                                                                          |

**Step 2** From the process table, you can do the following:

| Task                           | Procedure                                                                                                                                           |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| View details.                  | Click process name. See <a href="#">Daemon Information, page 16-58</a> .                                                                            |
| View process status.           | Click process state. See <a href="#">Process Status, page 16-58</a> .                                                                               |
| Stop process.                  | Select process and click <b>Stop</b> . New status and other process information is displayed. The WebServer and Tomcat processes cannot be stopped. |
| Start process.                 | Select process and click <b>Start</b> . New status and other process information is displayed.                                                      |
| Update table with latest data. | Click <b>Refresh</b> . The table does not automatically update.                                                                                     |
| View all processes.            | Click <b>Complete Report</b> . The system status is displayed.                                                                                      |

### Related Topics

[Administering Management Services via CLI, page 17-22](#)

## Processes Displayed

The Process Report table displays the status of the following major WLSE processes:

| Process Name   | Description                                           |
|----------------|-------------------------------------------------------|
| WirelessSvcMgr | Process that manages internal radio management tasks. |
| WLSEjobvm      | Job virtual machine.                                  |
| WLSEFaults     | Fault manager.                                        |
| WebServer      | Web server.                                           |
| Tomcat         | Java servlet engine.                                  |

| Process Name  | Description                                                            |
|---------------|------------------------------------------------------------------------|
| Snmpttrapd    | Trap processes.                                                        |
| ExcepReporter |                                                                        |
| CDPbrdcast    | CDP daemon that identifies Cisco devices to their immediate neighbors. |
| PerfMon       | Process that monitors performance.                                     |

## Daemon Information

The Daemon Information dialog box displays the following:

| Field        | Description                                                   |
|--------------|---------------------------------------------------------------|
| Process      | Process name.                                                 |
| Path         | File location.                                                |
| Flags        | Flags used to register the process with the Daemon Manager.   |
| Startup      | Method used to start the process.                             |
| Dependencies | Other processes that must be running for this process to run. |

## Process Status

The system log, which describes the status of the processes running in the system, displays the following:

| Field       | Description                                    |
|-------------|------------------------------------------------|
| Timestamp   | Date and time the message is logged.           |
| Process     | Process that logged the message.               |
| Type        | Message type: INFO, WARNING, CRITICAL.         |
| Information | Process status as known by the Daemon Manager. |

## Specifying a Splash Screen Message

The Splash Screen option allows you to set up a message that is displayed when a user logs in. After viewing the message, the user clicks **Agree** to continue logging in or **Disagree** to log out.

**Note**

---

Your login determines whether you can use this option.

---

**Procedure**

- 
- Step 1** Select **Admin > Appliance > Splash Screen**.
- Step 2** Enter the message to be displayed.
- Step 3** Check the **Enable** check box, then click **Apply**. The splash screen message is enabled.

**Note**

---

You *must* check **Enable** for the message to appear.

---

## Setting Time, Time Servers, Name Servers, and Web Session Timeout

The **Admin > Appliance > Time/NTP/NAME** option allows you to:

- [Set the Current Local and UTC Time, page 16-59](#)
- [Specify NTP Time Servers, page 16-60](#)
- [Specify Name Servers, page 16-61](#)
- [Set the Web Timeout Period, page 16-61](#)

### Set the Current Local and UTC Time

Current local (browser) time appears in most WLSE displays. Universal Coordinated Time (**UTC**) is the system time and appears in log files.

To set the time that appears in the Web interface, use the following procedure. Because there is a single system clock, setting the time here also updates the UTC time.

**Note**


---

Your login determines whether you can use this option.

---

**Procedure**

- 
- Step 1** Select **Admin > Appliance > TIME/NTP/NAME/WEB TIMEOUT**.
- Step 2** In the Current Time area, select the new time and date parameters from the lists and click **Update**.
- 

**Related Topics**

[Setting the System Clock Manually via CLI, page 17-17](#)

## Specify NTP Time Servers

This option allows you to maintain the current time on the WLSE by using [NTP](#) (Network Time Protocol) servers.

**Note**


---

Your login determines whether you can use this option.

---

**Procedure**

- 
- Step 1** Select **Admin > Appliance > TIME/NTP/NAME/WEB TIMEOUT**.
- Step 2** To remove an NTP server, select it from the Current Servers list and click **Remove**.
- Step 3** To add an NTP server, enter the server's IP address in the NTP Server IP Address text box and click **Enable**.
-

### Related Topics

[Setting the System Clock Using NTP via CLI, page 17-16](#)

## Specify Name Servers

You can specify the addresses of up to three name servers for name and address resolution.



### Note

---

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1** Select **Admin > Appliance > TIME/NTP/NAME/WEB TIMEOUT**.
  - Step 2** To remove a name server, select it and click **Remove**.
  - Step 3** To add a name server, enter its IP address in the Name Server IP Address textbox and click **Enable**.
- 

## Set the Web Timeout Period

The default timeout period for the Web interface is 30 minutes. If there is no input for 30 minutes, you will be logged out.

If WLSE redundancy is in effect, you should stop and restart services on the standby WLSE. Otherwise, resetting the timeout will cause a switchover from the active server to the standby server and the new timeout period will not take effect. For the procedure to reset the web timeout when using redundancy, see [Changing the Web Timeout Period on Redundant Nodes, page 16-52](#).



### Note

---

Your login determines whether you can use this option.

---

To reset the timeout period for the Web interface:

### Procedure

---

- Step 1** Select **Admin > Appliance > TIME/NTP/NAME/WEB TIMEOUT**.
- Step 2** To change the timeout period:
- a. Enter the new timeout setting (in seconds) in the **New Timeout** field.
  - b. Click **Set**.



**Note** After you click **Set**, the Web server will be restarted for the new timeout to take effect and you will be logged out.

---

- Step 3** To reset the timeout period to the default (30 minutes), click **Restore Default**.
- 

## Configuring the Mail Route

To ensure that WLSE email notifications reach their destinations, you can configure the WLSE's mail route by specifying an **SMTP** mail server. This setting affects emailing notifications about firmware and configuration jobs, emailing reports, and emailing fault notifications.



**Note** Your login determines whether you can use this option.

---

### Procedure

---

- Step 1** Select **Admin > Appliance > Configure Mailroute**.
- Step 2** Enter the hostname or IP address of an SMTP mail server on your network and click **Save**.
- Step 3** To remove the mail route, click **Remove**.
- 

### Related Topics

[Configuring the Mail Route via CLI, page 17-21](#)

## Managing Files for the WLSE TFTP Server (WLSE Express Only)

**Note**

---

Your login determines whether you can use this option. This option is available on the WLSE Express only.

---

You can manage files in the /tftpboot/public directory of the WLSE Express by using the TFTP Management option. For example, you can download images for routers, switches, and other devices in the network and load the images on the devices. The space available in this directory for managing files is 1 gigabyte.

The root directory for the TFTP server is /tftpboot. However, when sending files to the WLSE TFTP server, use a pathname starting with /public (instead of /tftpboot/public).

The following file management operations are permitted:

- Uploading files from the desktop or other systems and downloading files to the desktop or other systems.
- Deleting files.
- Creating an empty file to allow file *put* operations from TFTP clients and importing files from devices.

**Note**

---

User files in the /tftpboot/public directory will be backed up and restored by the normal WLSE backup/restore processes and files will be synchronized when operating in redundancy mode.

---

**Procedure**

---

**Step 1** Select **Admin > Appliance > TFTP Management**. A listing of files currently in the /tftpboot/public directory is displayed.

**Step 2** To import a file from the desktop:

- a. Enter the path in the text box or click **Browse** to locate the file.
- b. Click **Upload**.

Result: The file will be copied to the /tftpboot/public directory and listed in the file table. The file table includes information about the total amount of space that has been used and contains the following fields for each stored file:

| Field         | Description                              |
|---------------|------------------------------------------|
| Name          | Filename                                 |
| Size          | Size of file                             |
| Last Modified | Date and time created or last modified   |
| Trashcan icon | Deletes the file.                        |
| Rename icon   | Allows you to rename the file.           |
| Save icon     | Allows you to view or download the file. |

**Step 3** To create an empty file for TFTP *put* operations:

- a. Enter the filename in the text box.
- b. Click **Create**.

Result: An empty file will be created in the /tftpboot/public directory and listed in the file table.



**Note** The /tftpboot directory is the root directory for the TFTP server. Therefore, to transfer a file to the WLSE, include the subdirectory in the command: `tftp://wlse_ip_address/public/filename`.

**Step 4** To download a file to the desktop:

- a. Click the save icon in the file table.
- b. In the Downloading dialog box, click **Open** or **Save**.
- c. Browse to the location where you want to save the file.

**Step 5** To rename a file:

- a. Click the Rename icon in the file list.
- b. Enter the new name, then click **OK**.

**Step 6** To delete a file, click the trashcan. To delete all files, click **Select All**, then click **Delete**.

To deselect a file, click its checkbox in the file table. To deselect all files, click **Deselect All**.

## Using Connectivity Tools

When you select **Admin > Appliance > Connectivity Tools**, the following options for testing device connectivity and reachability are displayed:

- **Network Tools**—ping, traceroute, nslookup, TCP port scan, SNMP reachability (see [Using Network Tools, page 16-65](#)).
- **SNMP Query Tool**—query a device’s SNMP variables (see [Using the SNMP Query Tool, page 16-66](#)).

## Using Network Tools

The Network Tools option offers several tools for testing device connectivity.



### Note

Your login determines whether you can use this option.

### Procedure

**Step 1** Select **Admin > Appliance > Connectivity Tools**.

**Step 2** Enter a device name or IP address in the Device text box.

When you select an option button, the results window tells you whether the connectivity test was successful. Pressing **Enter** will not work. You *must* click a button.

**Table 16-12 Connectivity Tools**

| Button | Description                | Results                                                                          |
|--------|----------------------------|----------------------------------------------------------------------------------|
| Ping   | Tests device reachability. | If successful, statistics are displayed on the packets transmitted and received. |

Table 16-12 Connectivity Tools (continued)

| Button         | Description                                                                                                                                                                                                                                               | Results                                                                                                                                                                                                                                                                                             |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Traceroute     | Detects routing errors between the WLSE and a device.                                                                                                                                                                                                     | If successful, the routes to the device are displayed.                                                                                                                                                                                                                                              |
| NSLookup       | Looks up hostname or IP address information via the name server.                                                                                                                                                                                          | If successful, displays the name server name and IP address and the device name and IP address.                                                                                                                                                                                                     |
| TCP Port Scan  | Finds the active ports on a device.                                                                                                                                                                                                                       | Displays the active ports.                                                                                                                                                                                                                                                                          |
| SNMP Reachable | Tries to reach a device by using <a href="#">SNMP</a> . To reach a device by using SNMP, the device's credentials must be in the WLSE database. To check credentials, select <b>Devices &gt; Discover &gt; Device Credentials &gt; SNMP Communities</b> . | <p>If the device is reachable, its sysObjID is displayed.</p> <p>If no sysObjID is returned:</p> <ul style="list-style-type: none"> <li>• The query may be timing out because the device is busy or is remotely located.</li> <li>• The SNMP agent in the device may not be functioning.</li> </ul> |

**Step 3** Click **Close** to close the results window.

## Using the SNMP Query Tool

This tool allows you to find the value of a specified SNMP variable. Normally, this tool is used under the direction of Cisco TAC when they are assisting you with troubleshooting a problem.



**Note** Your login determines whether you can use this option.

### Procedure

**Step 1** Select **Admin > Appliance > Connectivity Tools > SNMP Query Tool**.

**Step 2** Enter the device's IP address or hostname and the OID of the SNMP variable.

- Step 3** Click **Get** to display a single-value variable.
- Step 4** Click **Get Table** to display a variable that consists of a table.
- Step 5** Click **Clear** to clear your entries.
- 

## Managing Firmware Version Support

You can use the WLSE to upgrade and update the firmware on one or more access points, either as a scheduled operation or on demand. To accomplish this, information about supported firmware versions is stored on the WLSE. You can:

- View the versions currently supported by the WLSE.
- Update the version support on the WLSE.

The topics covered in this section are:

- [Updating Supported AP Firmware Versions, page 16-67](#)
- [Viewing Supported AP Firmware Versions, page 16-68](#)

## Updating Supported AP Firmware Versions

To provide incremental support for minor updates to currently-supported IOS firmware versions, an incremental update package may be posted on Cisco.com. You can download this file and import it into the WLSE to update versions supported by the WLSE firmware module.

**Note**

Incremental updates are not intended for supporting major firmware versions; they are only for incremental version support. For example, if you have version 12.2(15)XR, you can use the WLSE to download and import subsequent incremental versions such as 12.2(15)XR, 12.2(15)XR1 and 12.2(15)XR2.

---

**Note**

Your login determines whether you can use this option.

---

To import new firmware support information:

### Procedure

- 
- Step 1** To download the firmware version update file to your desktop or another network computer from Cisco.com, enter this URL in the browser:  
<http://www.cisco.com/cgi-bin/tablebuild.pl/wlan-sol-eng>
- The firmware version update file is listed along with the WLSE software update files.
- Step 2** Select **Admin > System > New Version Support**.
- Step 3** Enter the path to the device support file or click **Browse**.
- Step 4** Click **Import**.
- Step 5** To display the firmware versions currently supported by the WLSE, see [Viewing Supported AP Firmware Versions, page 16-68](#).
- 

### Related Topics

[Viewing Supported AP Firmware Versions, page 16-68](#)

## Viewing Supported AP Firmware Versions



### Note

Your login determines whether you can use this option.

To display firmware versions currently supported by the WLSE:

- 
- Step 1** Select **Admin > System > Firmware Supported Versions**.
- Step 2** The access point firmware versions that are supported by this WLSE are displayed.
- Step 3** To import updated firmware support, see [Updating Supported AP Firmware Versions, page 16-67](#).
-

**Related Topics**

[Updating Supported AP Firmware Versions, page 16-67](#)

## Managing GUI Users

The options displayed when you select **Admin > User Admin** allow you to manage user roles and logins:

- [Managing Roles, page 16-69](#)—Add, modify, and delete user roles.
- [Managing User Accounts, page 16-71](#)—Add, modify, and delete user accounts.

**Related Topics**

[Modifying Your Profile, page 16-77](#)

[Overview: Authentication Modules, page 16-23](#)

## Managing Roles

Use this option to add, modify, and delete user-defined roles and to modify predefined roles. A user's role determines the tabs and subtabs the user can access. Users who have access to a subtab can perform all of the tasks under the subtab.

This section contains the following topics:

- Adding, modifying, and deleting roles—See [Adding, Modifying, and Deleting Roles, page 16-70](#).
- About roles—See [Overview: Roles, page 16-69](#).

### Overview: Roles

A user's role determines the tabs and subtabs the user can access. Users who have access to a subtab can perform all of the tasks under the subtab.

The XML API privileges are for users who will be using the XML application programming interface (API). If you are using the API, you should create different users for this purpose, and grant such users access to the API only. Access to the API is authenticated and authorization is checked. For more

information about the XML API, see the *Developer Guide for the CiscoWorks Wireless LAN Solution Engine*. This guide is included with the XML API SDK (Software Developer Kit) in the Software Center on Cisco.com.

Although you cannot delete predefined roles, you can modify them. The predefined roles and their default privileges are:

- System administrator—Allows access to all WLSE tasks. You can change the password using the console or the WLSE's Manage Users option (see [Managing User Accounts, page 16-71](#)).
- Network administrator—Monitoring authority, device configuration authority, and discovery configuration authority.
- Network operator—Monitoring and device configuration authority.
- Help desk—Monitoring authority only.

You can use these predefined roles to control which features staff members are allowed to access. Less skilled, front-line technical support can be assigned the Help Desk role. More skilled and experienced support staff might be given the Network Operator or Network Administrator roles. The most skilled and experienced staff with direct responsibility for the WLSE should be given the System Admin role.

You cannot modify the privileges of the System Admin role. A user who has the System Admin role can modify other user roles.

## Adding, Modifying, and Deleting Roles

You can edit the predefined roles, or you can create new, user-defined roles. You can modify or delete any user-defined roles.



### Note

---

Your login determines whether you can use this option.

---

### Procedure

- 
- Step 1** To access the role management window, select **Admin > User Admin > Manage Roles**. Role names are displayed in the center pane. To view the subtabs to which the role has access, select the role.
- The admin user and System Admin users can view all roles.

- The admin user and a System Admin user can modify all of the other roles.
- Other users can only view the roles assigned to them and any roles that they have created.

**Step 2** To add a role:

- a. Replace the text *New Role* with the name you have chosen for the new role.
- b. Select the check boxes next to the features the role will access. Click **Add**.



---

**Note** When you select a feature (for example, Display Faults), the role is granted access to the corresponding subtab (for example, **Faults > Display Faults**).

---

- c. The new role appears in the list of roles.

**Step 3** To modify a role, select the role. Select the check boxes for the features you want to add to the role and deselect the check boxes next to the features you want to remove from the role. Then click **Modify** to save the changes.

**Step 4** To delete a user-defined role, select the role, then click **Delete**.

---

#### Related Topics

- [Naming Guidelines, page B-1](#)
- [Managing User Accounts, page 16-71](#)

## Managing User Accounts

Using the options under this tab, you can create new user accounts, modify existing users, and delete users. The topics in this section are:

- [Add Users, page 16-72](#)
- [Modify Users, page 16-75](#)
- [Delete Users, page 16-77](#)
- [Overview: User Accounts, page 16-72](#)

**Related Topics**

- [Overview: Authentication Modules, page 16-23](#)
- [Modifying Your Profile, page 16-77](#)
- [Naming Guidelines, page B-1](#)
- [User Management via CLI, page 17-4](#)

**Overview: User Accounts**

Each new user must be assigned at least one role and assigned a privilege level for accessing the WLSE CLI. There are three possible privilege levels for the WLSE CLI:

- None—No access to the CLI.
- Level 0—Access to a small subset of CLI commands.
- Level 15—Full WLSE CLI access. Typically, level 15 privileges should only be given to the most skilled systems administration level users.

The default user (admin) is created when the setup script is run. The admin user has the System Administrator role and level 15 CLI privileges. This user cannot be deleted.

User accounts that you add by using the CLI commands do not have Web interface privileges. You can modify such users in the Web interface and add the appropriate roles to give them access to the Web interface.

Except for the admin user and users with the System Admin role, only the logins created by you are displayed. If logins were created by another user, they are not visible; only their creator can display them. However, the admin user and any user with the System Administrator role can view all users, no matter who created them.

**Add Users****Note**

---

Your login determines whether you can use this option.

---

## Procedure

- Step 1** Select **Admin > User Admin > Manage Users**. The Users list displays the current users.
- The admin user can view and modify all existing users.
  - Users who have the System Admin role can view all users that have been created, no matter who created them. Other users can view their own logins and any users they have created.
  - When creating other users, a user can only assign his role or a role with lesser privileges. For example, userA has only the network administrator role. Users created by userA can have only the network administrator role or roles with fewer privileges.
- Step 2** Enter the following information, in the order shown in [Table 16-13 on page 16-73](#).

**Table 16-13 Adding Users**

| Field            | Information to Enter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Name        | <p>Name of the new user. Usernames can be up to 32 characters in length and are case-sensitive. Usernames must begin with a character and cannot begin with a number.</p> <p>The username cannot contain a colon, semi-colon, single quote, double quote, or space.</p> <p><b>Note</b> If the user is <i>not</i> using the CLI (that is, CLI Access is set to 0), the username can begin with a number.</p> <p>For more information on the allowable characters, see <a href="#">Appendix B, “Naming Guidelines.”</a></p> |
| User Password    | Password for the new user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Confirm Password | Passwords are unlimited in length and are case sensitive. You can use any character except for the single quote or double quote.                                                                                                                                                                                                                                                                                                                                                                                          |
| Email            | Email address of the user (optional).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Table 16-13 Adding Users**

| Field      | Information to Enter                                                                                                                                                                                                                                                                                                                        |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CLI Access | User's level of access to the WLSE CLI: None, Level 0, or Level 15. Users with privilege level 15 can use all commands, and users with privilege level 0 can use a small subset of commands. <sup>1</sup>                                                                                                                                   |
| Roles      | One or more roles for the user. Roles determine the user's access to tabs and subtabs in the Web interface. <ul style="list-style-type: none"> <li>To add a role, select it from the pulldown list.</li> <li>To view a role, select it and click <b>show role</b>.</li> <li>To remove a role, select it and click <b>remove</b>.</li> </ul> |

1. For information on CLI commands, see [Appendix A, "Command Line Interface \(CLI\) Commands."](#)

- Step 3** To clear your entries and start over, click **Clear**.
- Step 4** To add the new user, click **Add**. The new username is added to the Users list. To discard your changes, click **Clear**.
- Step 5** After you add users, it is recommended that you run a backup. See [Scheduling and Running Backups, page 16-32](#).

### Related Topics

- [Modifying Your Profile, page 16-77](#)
- [Naming Guidelines, page B-1](#)
- [Managing Roles, page 16-69](#)

## Modify Users



### Note

Your login determines whether you can use these options.

### Procedure

To modify a user:

- Step 1** Select **Admin > User Admin > Add/Modify/Delete**. The Users list displays the current users.



### Note

Except for the admin user and users with the System Administrator role, only the logins created by you are displayed. If logins were created by another user, they are not visible; only their creator can display them. However, the admin user and any user with the System Administrator role can view all users.

- Step 2** Select the user from the Users list and make the desired changes, using the field descriptions in [Table 16-14 on page 16-75](#).

**Table 16-14 Modifying Users**

| Field     | Information to Enter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Name | <p>User's name. Usernames can be up to 32 characters in length and are case-sensitive. Usernames must begin with a character and cannot begin with a number.</p> <p>Usernames cannot contain a colon, semi-colon, single quote, double quote, or space.</p> <p><b>Note</b> If the user is <i>not</i> using the CLI (that is, CLI Access is set to 0), the username can begin with a number.</p> <p>For information on the allowable characters, see <a href="#">Appendix B, "Naming Guidelines."</a></p> |

**Table 16-14 Modifying Users**

| Field            | Information to Enter                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Password    | New password for user.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Confirm Password | Passwords are unlimited in length and are case sensitive. You can use any character except for the single quote or double quote.                                                                                                                                                                                                                                                                                                                              |
| Email            | Enter or change the user's email address.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| CLI Access       | <p>User's access to the WLSE <a href="#">CLI</a>: None, Level 0, or Level 15. By default, Level 15 is selected for the System Administrator role, and None is selected for others.</p> <p>Users with privilege level 15 can use all commands, and users with privilege level 0 can use a subset.</p> <p>For information on commands that are available for each privilege level, see <a href="#">Appendix A, "Command Line Interface (CLI) Commands."</a></p> |
| Roles            | <p>The user's roles. Roles determine the user's access to tabs and subtabs in the Web interface.</p> <ul style="list-style-type: none"> <li>• To add a role, select it from the pulldown list.</li> <li>• To view a role, select it and click <b>show role</b>.</li> <li>• To remove a role, select it and click <b>remove</b>.</li> </ul>                                                                                                                    |

**Step 3** Click **Modify** to save your changes or **Clear** to discard your changes.

#### Related Topics

- [Naming Guidelines, page B-1](#)
- [Managing Roles, page 16-69](#)
- [Modifying Your Profile, page 16-77](#)

## Delete Users

Use the following procedure to delete users.



---

**Caution**

If a user is deleted, all the users created by the deleted user are also removed. For example, if userA creates userB and then userA is deleted, userB is also deleted.

---



---

**Note**

Your login determines whether you can use this option.

---

**Procedure**

---

- Step 1** Select **Admin > User Admin > Manage Users**.
- Step 2** Select the username from the Users list, then click **Delete**. After you click **OK**, the user is deleted.
- 

## Modifying Your Profile

Use the My Profile tab to:

- Change your password—See [Changing Your Password](#), page 16-78.
- Change your email address—See [Changing Your Email Address](#), page 16-78.
- Set your home page preferences—See [Changing the Default Tab and Subtab](#), page 16-79.

## Changing Your Password

The user password is set when the user is created. Use the following procedure to change your password.

**Note**

---

Your login determines whether you can use this option.

---

**Procedure**

- 
- Step 1** Select **Admin > My Profile > Change password**.
- Step 2** To change your password, enter a new password in the New Password and Re-enter New Password fields. For information on allowable characters, see [Naming Guidelines, page B-1](#).
- Step 3** Click **Apply** to save your changes or **Reset** to discard your changes.
- 

**Related Topics**

- [Modify Users, page 16-75](#)
- [Naming Guidelines, page B-1](#)

## Changing Your Email Address

The email address is set initially when a user is created. To change your email address, use the following procedure.

**Note**

---

Your login determines whether you can use this option.

---

**Procedure**

- 
- Step 1** Select **Admin > My Profile > Change Email Address**.
- Step 2** Enter a new email address.

**Step 3** Click **Save** to save your changes or **Reset** to discard your changes.

---

#### Related Topics

- [Modify Users, page 16-75](#)

## Changing the Default Tab and Subtab

By default, an overview that provides information about all the main tabs is displayed when you log in. When you select a tab, an overview of the subtabs is displayed.

Use the following procedure to select a tab as your home page and select default subtabs for each main tab.



#### Note

Your login determines whether you can use this option.

---

#### Procedure

---

- Step 1** Select **Admin > My Profile > Set Tab Defaults**.
- Step 2** Select the home page you want displayed when you log in. For example, you may want your most frequently used tab to be displayed first.
- Selecting Overview restores the defaults.
  - Selecting a main tab makes that tab your default home page.
- Step 3** Select default subtabs for any or all main tabs:
- Selecting Overview displays information about the contents of the subtab.
  - Selecting a subtab makes that subtab the default tab that appears first when you select the main tab.
- Step 4** Click **Save** to save your changes or **Reset** to discard them.
-

# Creating Links

You can link to other systems and display their desktops in the right pane or in a separate window. For example, you could link to a CiscoWorks server, to Cisco Secure ACS, or to another WLSE.

The special link called ACS Failed Login Report generates a report about failed logins on an ACS server.

This section contains the following topics:

- Creating a link to another system, such as a CiscoWorks server or another WLSE—See [Creating a Link to Another System, page 16-80](#).
- Configuring the ACS Failed Login Report link and recreating the link if it has been deleted—See [Configuring the ACS Failed Login Report Link, page 16-81](#).
- Running the ACS Failed Login Report—See [Running the ACS Failed Login Report, page 16-83](#).

**Note**

---

This feature is available to all users.

---

## Creating a Link to Another System

**Note**

---

The following characters are unsupported and cannot be entered in this dialog: double quote, single quote, and angle brackets (< >).

---

**Procedure**

- 
- Step 1** Select **Admin > Links**. The Add Links window and current links appear.
- Step 2** To add a link:
- a. Enter the name of the link and the URL of the system in the Add Link window; for example: `http://cw_server:1741` creates a link to the CiscoWorks server called `cw_server`.



- Step 2** On the WLSE, select **Admin > Links**. The Add Links window and current links appear.
- Step 3** Click **Edit** under ACS Failed Login Report and enter the following information:

| Field    | Description                                                                                                                                                                    |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL      | URL of the ACS server, in the format <code>http://ACS_server:port</code> or <code>https://ACS_server:port</code> .<br>For ACS server 3.x for Windows, the port number is 2002. |
| Username | Administrator username created when ACS software was installed on the ACS server.                                                                                              |
| Password | Password for the administrator username.                                                                                                                                       |

- Step 4** To display the report in the right pane of the WLSE interface, deselect **Open in New Window**. Otherwise, the report opens in a separate window.
- Step 5** Click **Save**.

#### Related Topics

[Running the ACS Failed Login Report, page 16-83](#)

## Replacing a Deleted Link

If the link has been deleted, use the following procedure to create it again.

#### Procedure

- Step 1** Navigate to **Admin > Links** and click **Add to Links ...**
- Step 2** In the Name field, enter **ACS Failed Login Report**, then click **Save**. The ACS Failed Login Report link appears in the list of current links.

**Step 3** Click **Edit** under ACS Failed Login Report and enter the following information:

| Field    | Description                                                                                                                            |
|----------|----------------------------------------------------------------------------------------------------------------------------------------|
| URL      | URL of the ACS server, in the format <code>http://ACS_server:port</code> .<br>For ACS server 3.x for Windows, the port number is 2002. |
| Username | Administrator username created when ACS software was installed on the ACS server.                                                      |
| Password | Password for the administrator username.                                                                                               |

**Step 4** To display the report in the right pane of the WLSE interface, deselect **Open in New Window**. Otherwise, the report opens in a separate window.

**Step 5** Click **Save**.

#### Related Topics

[Running the ACS Failed Login Report, page 16-83](#)

## Running the ACS Failed Login Report

The ACS failed login report shows failed logins on a specified Cisco Access Control Server (ACS).



#### Note

Only a single link is supported; therefore, you cannot add a second link that points to a second ACS server.

To run an ACS failed login report:

#### Procedure

**Step 1** Select **Admin > Links**. The ACS Failed Login Report link is displayed in the list of current links:

- If the link is missing, see [Replacing a Deleted Link, page 16-82](#).

- If no report is displayed, see [Configuring the ACS Failed Login Report Link, page 16-81](#).

**Step 2** To run the report, click **ACS Failed Login Report**.

---