



Release Notes for the CiscoWorks Wireless LAN Solution Engine, Release 2.0

These release notes are for use with the CiscoWorks Wireless LAN Solution Engine (WLSE).

These release notes provide:

- [New Features, page 2](#)
- [Product Documentation, page 2](#)
- [Documentation Updates, page 5](#)
- [Known Problems, page 12](#)
- [Browser-Related Problems, page 25](#)
- [Resolved Problems, page 26](#)
- [Obtaining Documentation, page 33](#)
- [Obtaining Technical Assistance, page 35](#)
- [Obtaining Additional Publications and Information, page 37](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

New Features

The WLSE Release 2.0 contains management support for:

- IOS-based platforms
- Up to 2500 access points

It also includes features:

- Configuration archive
- Conversion of non-IOS to IOS during firmware image upgrade for AP1200's
- EAP authentication monitoring of AAA servers

Product Documentation

Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review the WLSE documentation on Cisco.com for any updates.

On Cisco.com, WLSE documentation is located at **Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine**.

You can access the WLSE online help by clicking the **Help** button in the top right corner of the screen or by selecting an option and then clicking the **Help** button. You can access the user guide from the online help by clicking the **View PDF** button.

The following product documentation is available for the WLSE and is available on Cisco.com:

Table 1 *Product Documentation*

Document Title	Description
<i>User Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<p>Describes WLSE features and provides instructions for using it. Available in the following formats:</p> <ul style="list-style-type: none"> • From the WLSE online help. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com at Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Technical Documentation. • Printed document available by order.
<i>Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine</i>	<p>Describes how to install and configure the WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> • PDF on the WLSE Recovery CD-ROM. • On Cisco.com at Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Technical Documentation. • Printed document available by order.

Table 1 *Product Documentation (continued)*

Document Title	Description
<i>Quick Start Guide for the CiscoWorks 1130 Wireless LAN Solution Engine</i>	<p>Helps you get the WLSE installed and ready to use as quickly as possible. Available in the following formats:</p> <ul style="list-style-type: none"> • Printed document shipped with the WLSE. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com at Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Technical Documentation.
<i>Regulatory Compliance and Safety Information for the CiscoWorks 1130 Wireless LAN Solution Engine</i>	<p>Provides regulatory compliance and safety information for the WLSE. Available in the following formats:</p> <ul style="list-style-type: none"> • Printed document shipped with the WLSE. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com at Products and Services > Network Management CiscoWorks > CiscoWorks Wireless LAN Solution Engine > Product Literature.

Documentation Updates

The latest version of the online help and/or User Guide for the CiscoWorks Wireless LAN Solution Engine does not include additions and corrections to the following sections:

- [Performing Administrative Tasks, page 5](#)
- [Using Reports, page 7](#)
- [Configuring Devices, page 7](#)
- [Naming Guidelines, page 12](#)

Performing Administrative Tasks

The following topics require additions or corrections:

- [Managing System Parameters](#)
- [Exporting Devices to a CSV File](#)

Managing System Parameters

The following items are missing from the System Parameters online help and the user guide.

Wireless Client Poll Interval

The following additional tip regarding setting the Wireless Client Poll Interval is missing:

If you will be frequently polling a set of devices, rather than changing the poll interval for all devices, run a scheduled inventory for those devices to obtain up-to-date information.

Truncation Parameters

Fault History Truncation and Job History Truncation Parameter default is 30 days, not 15 days.

Exporting Devices to a CSV File

The documented procedure is missing a few additional steps. The procedure should be as follows:

- Step 1** Select **Administration > Discover > Export Devices > To CSV File**. Device credentials are exported to the file in plain text.
- For added security during the transmission of credentials, click **Warning: Device credentials will also be exported. For added security, switch to HTTPS**. HTTPS will be used for the file download.

**Note**

The following steps are required only if you have not imported a certificate before attempting to export devices to a CSV file using HTTPS.

When the Security Client window appears:

- a. Click **Yes**.
 - b. Click **View Certificate**.
 - c. Click **Install Certificate**.
 - d. Click **Next** on each screen in the Certificate Import Wizard, then click **Finish**.
 - e. Click **OK**.
 - f. Log out of the HTTP session on the client browser.
 - g. Launch a security enhanced HTTPS session on the client browser, then click **Yes** on the Security Client window that appears after login.
- Step 2** Select **Administration > Discover > Export Devices > To CSV File**.

**Note**

Device credentials are exported to a plain text file.

- Step 3** Click **Download CSV File**, then click **Save**. Specify the filename and location if it differs from the default.

The file is saved to your desktop.

Using Reports

Report accuracy, especially for client-related reports, is determined by polling frequency.

If you use the following client-related reports often, rather than increasing the wireless client poll interval for all devices, you might want to use Scheduled Inventory under **Administration > Discover > Inventory > Scheduled Inventory** for a set of devices: Client Detail Report, Client Historical Associations Report, Per VLAN Client Report (Group), Per VLAN Client Report (AP), Top N Client Error Rate, Top N Busiest Clients, and Client Statistics Report.

Configuring Devices

The following sections are missing information:

- [Creating a Startup Configuration Template, page 7](#)
- [Assigning a Startup Configuration, page 7](#)
- [Using the Templates., page 8](#)

Creating a Startup Configuration Template

The following information is missing from the online help and the user guide:

In the instructions for creating a startup configuration template, step 3 instructs you to enable SSH. However, enabling SSH is only supported on version 12.2(11)JA. For any version lower, you will have to manage the access points, then create and upload a template that enables SSH on those access points.

Assigning a Startup Configuration

The **Before You Begin** section does not include information on configuring a router as DHCP server, it only includes instructions for a DHCP server.

To configure a router as a DHCP server, enter the following commands:

```
ip dhcp pool (name)
network (network address) (subnet mask)
bootfile (startup file)
```

```
next-server (WLSE IP address)  
default-router (default router)  
domain-name (domain name)  
dns-server (DNS IP address)
```

In this example, use the **next-server** command instead of option 66 or option 150.

In addition, the example given in the user guide and online help has incorrect information. If you have an associated startup template with the Bootfile Name "newap1200.ini", you would use the exact same name when you set the Scope option 067 (Bootfile Name). The user guide and online help incorrectly show the name as new-ap1200.ini instead of newap1200.ini

Using the Templates.

The online help and user guide for the IOS templates is missing fields for the following template selections:

- [Services > IP Filters, page 9](#)
- [Services > VLAN, page 11](#)
- [Services > MAC Address Filters, page 11](#)
- [Services > Ethertype Filters, page 11](#)

Services > IP Filters

The following fields and descriptions are missing:

Field	Description
Version	<p>Select one of the following:</p> <ul style="list-style-type: none"> • 12.(4)JA, 12.2(4)JA1—Use this option if you are configuring filters for either version. <p>When this option is selected, the command format generated by the WLSE is not the same as the command format generated by the access point. This causes the access point UI to display the following alert, “The commands were changed via CLI and not via the AP UI.” Even though the message format is different, and an alert is displayed, the commands generated by the WLSE work on the access point.</p> <ul style="list-style-type: none"> • 12.2(8)JA—Use this option if you are configuring filters for this version. <p>When this option is selected, the command format generated by the WLSE is not the same as the command format generated by the access point. This causes the UI to display the following alert, “ The commands were changed via CLI and not via the AP UI.” Even though the message format is different, and an alert is displayed, the commands generated by the WLSE work on the access point.</p> <ul style="list-style-type: none"> • 12.2(11)JA—Use this option if you are configuring filters for this version.
Destination Address	<p>Enter the IP address that you want to filter.</p> <p>Note This is not valid for versions 12.2(4) or 12.2(4)JA1.</p>

Field	Description
Mask	<p>Enter the mask for the destination IP address. Enter the mask with periods separating the three groups of four characters (255.255.255.240, for example).</p> <p>If you enter 255.255.255.255 as the mask, the access point accepts any IP address.</p> <p>If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered.</p> <p>The mask you enter in this field behaves the same way that a mask behaves when you enter it in the CLI.</p>
Source Address	Enter the IP address you want to filter.
Mask	<p>Enter the mask for the source IP address. Enter the mask with periods separating the three groups of four characters (255.255.255.240, for example). The method for entering the mask depends on the release.</p> <p>If you are using the 12.2(4)JA release, entering 0.0.0.0 as the mask causes the access point to accept any IP address.</p> <p>If you enter 255.255.255.255, the access point looks for an exact match with the IP address you entered in the IP Address field.</p> <p>If you are using the 12.2(8)JA or later release, entering 255.255.255.255 as the mask causes the access point to accept any IP address.</p> <p>If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered in the IP Address field.</p>

Services > VLAN

The following field is missing:

Field	Description
Bridge-group	<p>Enter the bridge group number.</p> <ul style="list-style-type: none"> If the VLAN ID you entered is less than 255, and you do not enter a value in this field, then the same number for the bridge group is automatically assigned. If the VLAN ID you entered is 255 or greater you will need to know what bridge group numbers are unused on the access point and enter one of them. <p>When a VLAN is created directly on the access point, the access point dynamically assigns a bridge group to the VLAN. So, if you create a VLAN ID of 123, then the bridge group is 123.</p> <p>If the VLAN is larger than 255, the access point starts at 255 and decrements the count until it gets to an unused bridge group number. So, if you create a VLAN ID of 500, the access point assigns a bridge group of 255 if that number is unused. If it is used, it will then try 254, and so on until it finds an unused number for the bridge group.</p>

Services > MAC Address Filters

The following field is missing:

Field	Description
Bridge-group	Enter a valid bridge group number used by the interface for which you want to create or delete filters.

Services > Ethertype Filters

The following field is missing:

Field	Description
Bridge-group	Enter a valid bridge group number used by the interface for which you want to create or delete filters.

Naming Guidelines

The online help and user guide for the Naming Guidelines contains incorrect information in the table describing Allowable Characters for Names and Descriptions.

The following characters should not be included in the table as allowed:

- # number or pound sign
- & ampersand
- \ reverse solidus (backward slash)
- + plus sign

Known Problems

- [Table 2](#) describes the problems known to exist in this release.
- [Table 3](#) describes configuration-specific problems in this release.



Note

To obtain more information about known problems, access the Cisco Software bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. (You will be prompted to log into Cisco.com.)

Table 2 WLSE Known Problems

Bug ID	Summary	Explanation
CSCdz34064	The number of clients seen in the AP Associations report and the Group Client Association report do not match.	<p>The data in the Number of Clients Connected field in the Group Client Association report is collected using the performance inventory. The client information displayed in the AP Associations Report is collected using the client inventory.</p> <p>Because the inventory polling frequencies for client and performance inventory are mismatched, the data in these reports do not always match.</p> <p>There is no workaround for this problem.</p> <p>However, in the case of some access points, you can use the Run Inventory Now and Scheduled Inventory features to synchronize the data.</p>
CSCea61722	The 1200 access point Cisco IOS images do not show up when importing from Cisco.com.	<p>When you try to import a Cisco IOS image for the AP 1200 from Cisco.com by selecting Firmware > Import > From Cisco.com, the image does not show up.</p> <p>To work around this problem, download the firmware image from Cisco.com, then import it to the WLSE by selecting Firmware > Import > From Desktop.</p>

Table 2 WLSE Known Problems (continued)

Bug ID	Summary	Explanation
CSCea87369	The IP Address and Name fields of the monitored device do not appear correctly in the Hot Standby report.	The device corresponding to the monitored MAC Address is not managed by the WLSE. To work around this problem, select Administration > Discover > Managed Devices > Manage/Unmanage to have the WLSE manage the monitored device.
	The IP Address and Name fields in the Hot Standby report are empty, and the MAC Address field displays 000000000000 (zeros) despite having configured the MAC Address for monitoring.	The access point for which the report is being viewed is running Cisco IOS 12.2(11)JA or 12.2(8)JA. There is no workaround for this problem. Refer bug CSCeb30121, which is related to these IOS versions.
CSCea88793	A non-IOS to Cisco IOS access point conversion job is successful but is reported as not verified.	When you run a non-IOS to IOS conversion job, the results are displayed as not verified even though the job is successful. The timeout and retries values need to be increased. To work around this problem, and to ensure that future jobs are successful, do the following: <ol style="list-style-type: none"> 1. Access the Job Properties dialog box by entering the following URL: <code>http://wlse IP address:1741/debug/jobprops.jsp</code>. 2. Increase the value for <ul style="list-style-type: none"> – Vxworks to IOS SNMP timeout. – Vxworks to IOS SNMP retries. – Device reboot wait timeout.

Table 2 *WLSE Known Problems (continued)*

Bug ID	Summary	Explanation
CSCea91955	Fault Notification Syslog messages from WLSE are displayed in a truncated form on the Resource Manager Essentials (RME) 3.4 Syslog Standard Report.	<p>The RME 3.4 Syslog Standard Report displays fault notification syslog messages sent in XML message format or in plain text message format in a truncated form.</p> <p>To work around this problem and view the syslog messages in an untruncated form, see the following flat syslog file located in:</p> <ul style="list-style-type: none"> • On the Solaris 2.8 based RME 3.4 server: /var/log/syslog_info • On the Windows 2000 based RME 3.4 server: C:/Program Files/CSCOPx/log/syslog.log

Table 2 WLSE Known Problems (continued)

Bug ID	Summary	Explanation
CSCeb19507	<p>An error message appears in the Install Software Updates window in two possible circumstances:</p> <ul style="list-style-type: none"> • After having upgraded to Release 2.0 from a previous release of the WLSE. • On a newly installed WLSE, Release 2.0. 	<p>After having upgraded to a WLSE 2.0 or after newly installing a WLSE 2.0, if you either:</p> <ol style="list-style-type: none"> 1. Use the CLI command <code>hostname</code> to change the hostname to one that is not configured under IP Name Server on the WLSE. 2. Use the CLI commands <code>services stop</code> then <code>services start</code> to stop then start services. <p>then the WLSE will not accept the host name change, and the following problems occur:</p> <ul style="list-style-type: none"> • An error message appears in the Install Software Updates window. • You cannot e-mail any log files (e.g. tomcat.log) in the View Log File window. • The “AAA Server is Not Available” fault is erroneously generated and stays in active state indefinitely even though the AAA servers are actually available. • Fault notification e-mails display the previous hostname, not the current one. <p>To work around this problem, use the CLI command <code>reload</code> after having executed foregoing two steps.</p>

Table 2 WLSE Known Problems (continued)

Bug ID	Summary	Explanation
CSCeb32794	Specific trap host configuration using IOS configuration templates removes previously configured trap host configurations.	<p>Whenever a specific trap host is defined using the IOS configuration template, all previous specific trap host configuration commands are removed from the access point by the WLSE.</p> <p>For example, if you use the WLSE to configure host xxx.xxx.xxx.xxx to be the trap receiver for receiving hot standby switchover type traps, then push it to the access point, the access point will have this host as the trap receiver for switchover type traps. If the access point already has another trap receiver, yyy.yyy.yyy.yyy, configured to receive association and disassociation type traps, it will be removed.</p> <p>This is because the WLSE generates commands to disable all non switchover type traps (because this is the only type we selected in the template) from being generated.</p> <p>To work around this problem, select trap types that are already configured on the access point, in addition to the new trap type.</p> <p>Using the example above, if switchover and associate and disassociate type traps are selected, then the WLSE will not disable the associate and disassociate type traps.</p> <p>You can also use commands in the custom templates to work around this problem.</p>

Table 2 WLSE Known Problems (continued)

Bug ID	Summary	Explanation
CSCeb36372	The Client Historical Association report does not contain a disassociation time.	<p>The Client Historical Association report does not have the information about last time a client associated with the access point, the time it disconnected from the access point, the duration of the association, or the association state.</p> <p>There is no workaround for this problem.</p> <p>Note In the current release, only association times of a client are supported. Dissociation time of the client is not available in this release.</p>
CSCeb40356	When you rediscover an already-discovered device, inventory is not run automatically.	<p>When discovery is run on an already-discovered device, even though it is auto-managed, the inventory feature is not triggered.</p> <p>To work around this problem, you must run an on-demand inventory by selecting Administration > Discover > Inventory > Run Inventory Now, or wait for the next available inventory cycle.</p>
CSCeb44234	The Failed Authentication report display 0's (zeros).	<p>The number of failed authentications always show up as 0.</p> <p>There is no workaround for this problem; the problem is on the access point. Please refer to CSCeb46160.</p>
CSCeb46145	The non-IOS to Cisco IOS upgrade images are not available from Cisco.com.	<p>When you try to download an upgrade image from Cisco.com, the image does not show up.</p> <p>To work around this problem, download the firmware image from Cisco.com to your desktop, then import it to the WLSE by selecting Firmware > Import > From Desktop.</p>

Table 2 WLSE Known Problems (continued)

Bug ID	Summary	Explanation
CSCeb50004	The View current faults for this setting link under Faults > Manage Profiles cannot be used to clear Vlan WEP key length policy violation faults.	<p>When you display WEP Encryption per VLAN security policy profile under Faults > Manage Profiles, then click View current faults for this setting, the window for the previously selected link in a different policy window appears. This means that the VLAN WEP key length policy violation fault cannot be cleared using this link.</p> <p>To work around this problem:</p> <ol style="list-style-type: none"> 1. Select Faults > Display Faults 2. Select the Vlan WEP key length policy violation faults for the affected access points 3. Click Clear. <hr/> <p>When you select the WEP Key Length security policy window under Faults > Manage Profiles, then click View current faults for this setting, the window for the previously selected link in a different policy window appears. This means the WEP key length policy violation fault cannot be cleared using this link.</p> <p>To work around this problem:</p> <ol style="list-style-type: none"> 1. Select Faults > Display Faults 2. Select the Vlan WEP key length policy violation faults for the affected access points 3. Click Clear.
CSCeb52919	Initial configuration of RADIUS TACACS+, or MS NT Domain authentication fails.	<p>When you configure the RADIUS, TACACS+, or MS NT Domain authentication modules for the first time, the WLSE does not accept the configuration; it retains the original Local Authentication module.</p> <p>To work around this problem, configure the RADIUS, TACACS+, or MS NT Domain authentication modules a second time.</p>

Table 3 WLSE Configuration-Specific Problems

Bug ID	Summary	Explanation
CSCea64667	There is no way to remove the Wireless Domain Services Priority and IP address in the Global Properties.	<p>If you want to remove an access point's wireless domain services priority there is no way to do so using an IOS template under Wireless Services > WDS.</p> <p>To work around this problems, create a custom template with the following command:</p> <pre>no wlccp wds priority (priority number) interface BVI1</pre>
CSCeb09196	If you click Finish for an IOS configuration job before you select a template and assign it to devices, the job is saved as a non-IOS job.	<p>When creating an IOS configuration job, if you click Finish before you have assigned a template to any devices, the job will be saved as a non-IOS job. (The protocol given is HTTP and SNMP.) This happens even if you select the template and IOS devices after clicking Finish.</p> <p>To work around this problem, do not click Finish until you have assigned a template and selected the devices.</p>

Table 3 *WLSE Configuration-Specific Problems (continued)*

Bug ID	Summary	Explanation
CSCeb24253	Imported template values cannot be validated by the WLSE.	<p>When you import a full configuration from a device, configuration parameters not supported through the Templates appear in the custom key values. By design, version validation does not validate these extra parameters.</p> <p>However, even when you delete all the custom parameters, the configuration is still not validated.</p> <p>To work around this problem save the configuration template with version checking disabled, which means that when the configuration template is selected to be applied to a set of devices, the WLSE will not validate the device versions against the template's valid device versions.</p> <p>Note Since a configuration template is a generic set of configuration parameters than can be applied to several devices, it is recommended that you delete the device-specific configuration parameters from an imported configuration that appear under custom values section.</p>

Table 3 WLSE Configuration-Specific Problems (continued)

Bug ID	Summary	Explanation
CSCeb30067	The following options are missing from the IOS Template under Services > QoS policy : filter and default classification for packets on the VLAN.	<p>The options to configure filter and default classification for packets on the VLAN are present only when there is a VLAN or filter configured on the access point.</p> <p>Enter the commands in the IOS Custom Values template.</p> <p>To configure QoS on defined filters, enter:</p> <pre>class-map match-all _class_(QoS policy name) (unused index) match access-group (filter name for IP filter and access-list number for MAC and EtherType filter) policy-map (QoS policy name) class _class_ (QoS policy name) set cos (class of service)</pre> <p>For example,</p> <pre>class-map match-all _class_test10 match access-group 200 policy-map test class _class_test0 set cos 0</pre> <p>To configure QoS on Default Classification for Packets on the VLAN, enter the following:</p> <pre>policy-map (QoS policy name) class class-default set cos (class of service)</pre> <p>For example:</p> <pre>policy-map test2 class _class-default set cos 1</pre>

Table 3 WLSE Configuration-Specific Problems (continued)

Bug ID	Summary	Explanation
CSCeb32801	Hot standby cannot be configured on a dual mode access point.	<p>When an access point is set as dual mode, the hotstandby template is missing a field for the second radio.</p> <p>To work around this problem, create a custom template with the following command:</p> <pre>iapp standby mac-address (MAC address of radio 11b) (MAC address of radio 11a)</pre>
CSCeb37296	The interfaces to which QoS policies are assigned are not displayed in the GUI.	<p>Interfaces that have QoS policies assigned to them are not shown in the GUI.</p> <p>To work around this problem click Preview to see to which interfaces the QoS policies are assigned. This also applies to deleted policies on the interfaces.</p>
CSCeb39374	During IOS template validation for Proxy Mobile IP, the WLSE displays that only the AP1210 is a valid version.	<p>Proxy Mobile IP template validation indicates that only the AP1210 is valid, even though this template can be applied to all IOS versions and device types.</p> <p>To work around this problem, disable version checking when using a Proxy Mobile IP template.</p>

Table 3 WLSE Configuration-Specific Problems (continued)

Bug ID	Summary	Explanation
CSCeb44384	You cannot delete RADIUS servers if their authentication ports have changed	<p>The WLSE will not allow you to delete a RADIUS server if its authentication port has changed.</p> <p>To work around this problem, do the following:</p> <ol style="list-style-type: none"> 1. Create a template to remove the RADIUS server. 2. Copy the template. 3. Create a custom template. 4. Paste the commands from the copied template into the custom template. 5. Append the following command to the end of every line of the IP address of the RADIUS server you want to delete: <code>auth port (port number)</code> <p>For example:</p> <pre>no server 10.10.10.100 auth port 2323</pre>
CSCeb47024	Validation for SSID templates that have no VLANs fails.	<p>When a template is created for SSIDs without VLANs, the validated, a message appears indicating that no device versions for the template are supported.</p> <p>To work around this problem, disable version checking.</p>
CSCeb49336	The server manager template does not display all of the configured fields.	<p>When you view a configured server manager template, not all of the data is displayed.</p> <p>To work around this problem, click Preview to view the configured fields.</p>

Browser-Related Problems

Table 4 describes the browser problems known to exist in this release.

Table 4 *WLSE Browser-Related Problems*

Bug ID	Summary	Explanation
None.	Window resizing in Netscape Navigator causes page reloads.	<p>When a window whose content is not cached is resized, Netscape Navigator sends a page request to the server.</p> <p>This can cause any of the following problems:</p> <ul style="list-style-type: none"> • Work that is in progress could be interrupted, and the default page of the last module accessed from the navigation bar could be displayed. • Any data that was being entered in a dialog box could be lost. • Some of the pages may not show correct information, particularly those containing the date and time.
None	Reports in PDF format do not display the far right column when using the Japanese Netscape Navigator 4.79.	<p>When you view a report and export it as a PDF file, the rightmost column does not appear.</p> <p>To work around this problem, use the Japanese Microsoft Internet Explorer.</p>

Resolved Problems

Table 5 describes the problems resolved since the last release.

Table 5 *WLSE Resolved Problems*

Bug ID	Summary	Explanation
CSCdy67138	Large configuration files cause SNMP jobs to fail on versions prior to 12.00T.	Access points fail to upload configuration files greater than 4Kbytes. To work around this problem create several small configuration templates to upload.
CSCdz19851	The values for the 11a radio data rates in a template imported from an AP1200 are blank.	When you import a configuration from a 1200 AP, the 11a radio's data rates are not imported correctly, and are displayed as blank. There is no workaround for this problem.
CSCdz24905*	Substituting devices on the network creates duplicate entries for the devices. If you restore your WLSE from 1.3 into a 2.0 and had already devices with duplicate IP conflicts then is necessary to delete those devices from the system, otherwise the Duplicate IP Fault might not be generated.	When you: <ol style="list-style-type: none"> 1. Perform an initial discovery of an access point and manage it with the WLSE. 2. Replace that device with another access point using the same IP address. 3. Run discovery again. The new access point shows up as part of the new devices group and the old access point remains listed in the managed group. To work around this problem: <ol style="list-style-type: none"> 1. Delete the device from the managed list before replacing it. 2. Clear arp cache on the connected switches/routers for network connectivity.
	Note New devices, discovered after installing Release 2.0 and which have a duplicate IP conflict, will generate a Duplicate IP fault. Refer to CSCeb37882, which will be fixed in release 2.5).	

Table 5 WLSE Resolved Problems (continued)

Bug ID	Summary	Explanation
CSCdz27158*	The FCS Error fault is not needed.	The FCS error counter does not indicate a fault; therefore displaying it as a fault is not necessary. There is no workaround for this problem.
CSCdz42008*	Unable to upgrade from WLSE 1.1 to a 1.3 using the recovery CD due to permission problems.	This is an Internet Explorer 6.0 browser problem. To work around this problem, select Tools > Internet Options > Privacy , then change the privacy setting to low.
CSCdz37464	You cannot add a new policy group to an access point with version 12.00T.	This is a bug in the 12.00T software; not the WLSE. When you try to add a new policy group to an access point with version 12.00T it returns errors. There is no workaround for this problem.
CSCdz41224	Unmanaging or deleting a device while running a firmware job will leave the job pending for that device.	If you create and run a firmware job for a group of devices, then delete or unmanage a device within the group when the job is only partially complete, the job will be listed as completed with a start and end time. However, the device that was unmanaged or deleted will show a status of not verified with a blank end time, and the job remains pending. There is no workaround for this problem.
CSCdz45323*	The use of [] brackets is not allowed in device credentials.	Brackets cannot be used in address ranges with wild cards, despite the guidelines saying they can. There is no workaround for this problem.
CSCdz57223	There is no way to clear unwanted faults from the Faults display.	Unwanted faults cannot be removed from the Faults display. To work around this problem, acknowledge the faults. Acknowledging a fault clears it from the active list, but does not remove it entirely.

Table 5 WLSE Resolved Problems (continued)

Bug ID	Summary	Explanation
CSCdz59384*	Error message is null when attempting to validate a template.	<p>With certain template settings selected, you cannot perform configuration validation for templates.</p> <p>To work around this problem, disable version checking. Note, however that some of the template settings may not be applied to the access point.</p>
CSCdz61105*	The pound (#) sign is not allowed in the password when creating a users in template.	<p>When the password contains the # sign, the template page freezes if you click Preview or Finish.</p> <p>There is no workaround for this problem.</p>
CSCdz64494*	DNS resolution does not function correctly.	<p>The discovery process caches the names/IPs so that new DNS entries are not reflected after the discovery run.</p> <p>There is no workaround for this problem.</p>
CSCdz65469*	The Faults counter does not work with AP resets.	<p>The counter rollover logic is incorrectly applied for cases when the access point resets.</p> <p>There is no workaround for this problem.</p>
CSCdz66597*	When adding or deleting a user in a template, you must enter a unique numeric userid.	<p>Having to remember all the userids that have been created previously is difficult and cumbersome.</p> <p>There is no workaround for this problem.</p>

Table 5 WLSE Resolved Problems (continued)

Bug ID	Summary	Explanation
CSCdz73883*	Connectivity tools return unformatted text.	<p>When you select Administration > Appliance > Connectivity Tools, enter an IP address/hostname, then click any button, the results appear correctly.</p> <p>However, when you do it a second time, the results return unformatted server-side Java errors.</p> <p>To work around this problem:</p> <ol style="list-style-type: none"> 1. Log out of the WLSE. 2. Clear the Web browser's cache. 3. Log in and use the tool again.
CSCCea05699*	Configuration templates do not accept dashes (-) in the VLAN Name field.	<p>When you add a VLAN by selecting Association > VLANs, the VLAN Name field does not accept the dash (-) character. However, 1200 access point do support dashes in VLAN names.</p> <p>To work around this problem, do not use a dash (-) or other special characters in the VLAN Name field.</p>
CSCCea06465*	The Top N percentage errors exceeds 100%	<p>Traffic counters increase and roll over; however, the formula reduces the throughput to zero in most of the cases.</p> <p>There is no workaround for this problem.</p>
CSCCea12144*	There is a syntax error for the mail to command in the WLSE CLI.	<p>The command description in the documentation is incorrect; it does not show that message must end with a period.</p> <p>To work around this problem, enter the CLI command correctly by ending the message with a period.</p>

Table 5 WLSE Resolved Problems (continued)

Bug ID	Summary	Explanation
CSCea25427*	The WLSE 1.3.1 patch image is not available through the GUI.	<p>If you are trying to upgrade from 1.0 to 1.1, 1.1 to 1.3, and 1.3 to 1.3.1, using an appliance as a repository, the upgrade image is not visible through the GUI.</p> <p>There is no workaround for this problem.</p>
CSCea25814*	Cannot specify timeout/retries when importing devices from file.	<p>The specified timeout/retry values are not used the very first time by the discovery process even though they are specified at the time of import.</p> <p>There is no workaround for this problem.</p>
CSCea61412*	When access point firmware is upgraded, it is not reflected in the reports.	<p>Firmware changes to the access point are not showing up in reports or groups.</p> <p>There is no workaround for this problem.</p>
CSCea63970*	The broadcast WEP key rotation resets to zero (0) for the 11b radio.	<p>The broadcast WEP key rotation interval (sec) can be set from both the 11a and 11b radio configuration screens. If you change the value in the 11b radio screen, the 11a radio remains zero (0) and overrides the changed value.</p> <p>To work around this problem, set broadcast WEP key rotation interval value in the UI, then click the 11a radio screen once and it will use the newer value.</p>
CSCea72423*	No documentation is available for export/import from one WLSE to another.	<p>The GUI implementation will not be made until the next release (2.0), therefore the help for it cannot be written until the next release.</p> <p>To work around this problem, see the documentation at the following URL: bj.cisco.com/targets/ucdit/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_0/inst_gd/ig_adm.htm#1061161</p>

Table 5 WLSE Resolved Problems (continued)

Bug ID	Summary	Explanation
CSCea73121*	The use of a backslash (\) in profile names, renders the Manage Profiles screen unusable.	Under Faults > Manage Profiles , if you enter a profile name that contains a backslash, the screen becomes unusable. To work around this problem, do not use a backslash in a profile name.
CSCea77235*	When you select all the alarms in the Faults display, only 10 at a time are displayed.	To acknowledge all the faults, you can only do so one page at a time. There is no workaround for this problem.
CSCea81454*	Firmware upgrades do not complete before the job timeout.	Firmware upgrade jobs are terminated when an SNMP error or timeout exception occurs, which happens particularly over slow links. There is no workaround for this problem.
CSCea81743*	The Fault Notification settings allow you to save trap settings with no community string.	The Fault Notification Settings UI allows you to save trap settings with no community strings. If the WLSE is rebooted or if services are restarted through the CLI command, the Fault Notification screen displays an error and cannot be used. There is no workaround for this problem.
CSCea87963*	The documented backup command details for Windows2000/XP is incomplete.	When the command is entered as documented, you will see the following error message: Cannot create directory: 550 C:\BACKUP: Access denied. Could not open ftp connection. To work around this problem, include the following step in addition to the other ones listed in the procedure: In the FTP Site Directory, verify that the Write box is checked.

Table 5 WLSE Resolved Problems (continued)

Bug ID	Summary	Explanation
CSCea89516*	You cannot enter a dash (-) or underscore (_) in the name field of the Service Set.	<p>When dash or underscore is entered in the Name field under Templates > Association > Services Sets > Service Set the following error appears: Service Set name is invalid. Alphanumeric only.</p> <p>To work around this problem, use awcDot11AuxSSID.<ssid#>.1 as key, and strings that contain dash or underscore as value in Customer Values instead.</p>
CSCea93444*	The WLSE uses optional RFC commands, which cause backups to fail.	<p>In the WLSE 1.3.1 optional RFC commands for backup transfer cause the backup ftp to fail.</p> <p>There is no workaround for this problem.</p>
CSCea93472*	Unexpected usernames are generated when you modify a user.	<p>If you make changes under User Admin > Manage Users to an existing user, click Modify, then while waiting for the changes to be saved, select other users, when the modification is done, a new user containing all selected usernames with a question mark (?) as separator is generated.</p>

Table 5 WLSE Resolved Problems (continued)

Bug ID	Summary	Explanation
CSCeb00662*	The WLSE admin password recovery procedure has syntax errors.	The WLSE 1.3.1 documentation for the admin password recovery procedure on Cisco.com asks you to boot into the Maintenance image as Step 1. However, the maintenance image requires that you know the admin password to login. To work around this problem, after step 1, do the following: Power the system off and then back on.
CSCeb01974*	Invalid characters in the hostname cause 500 Server Errors in the GUI.	The CLI command hostname allows use of invalid characters such as # which are disallowed in RFC 952. To work around this problem, use the hostname command via CLI (telnet/ssh) and change the hostname of the WLSE to a valid hostname using up to 24 characters (A-Z), digits (0-9), minus sign (-). Then, reinitialize the database using the CLI command reinitdb.

* This bug is a customer-found bug and has a CARE ticket associated with it.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise

- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

<http://tools.cisco.com/RPF/register/register.do>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

<http://www.cisco.com/go/packet>

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

This document is to be used in conjunction with the documents listed in the “[Product Documentation](#)” section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuic Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Copyright © 2003, Cisco Systems, Inc. All rights reserved.

