Release Notes for Cisco Wireless Control System for Windows or Linux, Release 6.0.196.0

August 2010

These release notes describe open caveats for the Cisco Wireless Control System 6.0.196.0 for Windows or Linux, which comprises part of the Cisco Unified Wireless Network Solution (Cisco UWN).

The Cisco Wireless Control System is hereafter referred to as *Cisco WCS*.

Contents

These release notes contain the following sections:

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

Cisco Unified Wireless Network Solution Components

The following components are part of the Cisco UWN Solution and are compatible in this release:

- Operating system (Wireless LAN Controller and Cisco Aironet Lightweight Access Point)
- Cisco Wireless Control System (Cisco WCS)
- Cisco Mobility Services Engine
- Cisco WCS Navigator
- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers
- Cisco Aironet 1000, 1100, 1130, 1140, 1200, 1230, 1240, 1250, 1310, 1500, and 1524 Series Lightweight Access Points
- Cisco Aironet 1310 and 1410 Bridges
- Cisco Aironet Access Points running Lightweight Access Point Protocol (LWAPP) or Control and Provisioning of Wireless Access Points protocol (CAPWAP)

Requirements for Cisco WCS

The following server hardware and software is required to support Cisco WCS for Windows or Linux.

Server Hardware Requirements

Cisco WCS can be run on a workstation or server, and access points can be distributed unevenly across controllers.

- High-end server—Supports up to 3000 Cisco Aironet lightweight access points, 1250 standalone access points, and 750 Cisco wireless LAN controllers.
  - 3.16-GHz Intel Xeon Quad processor.
  - 8-GB RAM.
  - 200 GB minimum free disk space is needed on your hard drive.
- Standard server—Supports up to 2000 Cisco Aironet lightweight access points, 1000 standalone access points, and 450 Cisco wireless LAN controllers.
  - 3.2-GHz Intel processor.
  - 2.13-GHz Intel Quad Core X3210 processor.
  - 2.16-GHz Intel Core2 processor.

  - 4-GB RAM.
  - 80 GB minimum free disk space is needed on your hard drive.
- Low-end server—Supports up to 500 Cisco Aironet lightweight access points, 200 standalone access points, and 125 Cisco wireless LAN controllers.
  - 3.06-GHz Intel processor.
  - 1.86-GHz Intel Dual core processor.
  - 2-GB RAM.
  - 50 GB minimum free disk space is needed on your hard drive.

Note For all server levels, AMD processors equivalent to the listed Intel processors are also supported.

Note The free disk space listed is a minimum requirement, but several variables (such as backups) impact the disk space.

Operating Systems Requirements

The following operating systems are supported:

- Windows 2003/SP2 and Windows 2003 R2/SP2 32-bit installations with all critical and security Windows updates installed.

  Windows 2003/SP2 64-bit installations are not supported. A 32-bit operating system running on a 64-bit capable hardware is supported.

  Windows 2003 32-bit installations provide support for up to 64 GB of RAM if Physical Address Extension (PAE) is enabled. See the Windows documentation for instructions on enabling this mode.
- Red Hat Linux Enterprise Server 5.X 32-bit operating system installations.

  Red Hat Linux Enterprise Server 5.X 64-bit operating system installations are not supported. A 32-bit operating system running on a 64-bit capable hardware is supported.
- Windows 2003 and Red Hat Linux version support on VMware ESX version 3.0.1 and above with either local storage or SAN over fiber channel.

  Individual operating systems running Cisco WCS in VMware must follow the specifications for the size of Cisco WCS that you intend to use.

Client Requirements

Cisco WCS 6.0.196.0 requires Microsoft Internet Explorer 6.0/7.0/8.0 with the Flash plugin, or Mozilla Firefox 3.0 or later releases.

Using a web browser running on Windows 2003 to access the Cisco WCS web GUI is not recommended because Windows 2003 security settings may cause browsing problems.

The client running the browser must have a minimum of 1 GB of RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

Note The minimum screen resolution recommended for both Cisco WCS and Navigator use is 1024 x 768 pixels.

Wireless LAN Controller Requirements

Cisco WCS 6.0.196.0 supports management for controllers running the following software releases:

- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 4.2.176.0
- 4.2.205.0
- 4.2.207.0
- 4.2.209.0
- 5.1.151.0
- 5.1.163.0
- 5.2.157.0
- 5.2.178.0
- 5.2.193.0
- 6.0.182.0
- 6.0.188.0
- 6.0.196.0
- 6.0.199.4

Location Server, Mesh, and MSE

Cisco WCS 6.0.196.0 supports management for the following location server, mesh, and mobility services engine (MSE) software:

- MSE release and Context Aware Software 6.0.105.0

  Note Client and tag licenses are required in order to retrieve contextual (such as location) information within the Context Aware Software. See the *Release Notes for Cisco 3300 and 3350 Series Mobility Services Engine, Release 6.0.105.0* for more information.

- Location server 6.0.102.0

  Note See the *Release Notes for Cisco 2700 and 2710 Location Appliances, Release 6.0.102.0* for more information.

- WLC running mesh release 4.1.192.35M and later releases.

Cisco WCS on WLSE Appliance

Cisco WCS on a WLSE appliance supports up to 1500 Cisco Aironet lightweight access points and 161 Cisco wireless LAN controllers. The required processor is a 3.16-GHz Intel Xeon processor (or AMD equivalent) with 3 GB of RAM and 38 GB of free hard drive space.

The Windows operating system is not supported with the Cisco WCS on the WLSE appliance.

Finding the Software Release

To find the software release that Cisco WCS is running, see the *Cisco Wireless Control System Configuration Guide*. If Cisco WCS is already installed and connected, verify the software release by choosing **Help > About the Software**.

Upgrading to a New Software Release

The Cisco WCS release must be the same or more recent than the controller software release. Upgrade the Cisco WCS first to prevent any unexpected problems. Cisco WCS supports database upgrades only from the following official Cisco WCS releases:

- 4.2.62.0
- 4.2.62.11
- 4.2.81.0
- 4.2.97.0
- 4.2.110.0
- 4.2.128.0
- 5.1.64.0
- 5.1.65.4
- 5.2.110.0
- 5.2.130.0
- 5.2.148.0
- 6.0.132.0
- 6.0.170.0
- 6.0.181.0

Note All 5.2.x releases posted after 5.2.148.0 will not be eligible for upgrade to release 6.0.196.0.

Upgrading Cisco WCS

This section provides instructions for upgrading Cisco WCS on either a Windows or Linux server. It handles the steps you would normally follow to accomplish a manual upgrade (shut down Cisco WCS, perform a backup, remove the old Cisco WCS version, install the new version, restore the backup, and start Cisco WCS). If you choose to use the installer, it searches for any previous Cisco WCS versions.

Note You must have software release 4.1.91.0 before you can automatically upgrade to 4.2.

If you choose to use the easy upgrade process, it provides error checking at each step and gives an informative message if an error that causes an exit occurs. An upgrade-*version*.log is also produced and provides corrective measures.

Note For steps on upgrading Cisco WCS in a high availability environment, see Chapter 14, "Performing Maintenance Operations" of the *Cisco Wireless Control System Configuration Guide*.

Using the Installer to Upgrade Cisco WCS for Windows

To upgrade Cisco WCS (on a Windows platform) using the automated upgrade, follow these steps:

Step 1 Insert the Windows Cisco WCS CD into the CD-ROM drive and double-click the WCS-STANDARD-K9-6.0.X.Y.exe file where 6.0.X.Y is the software build. If you downloaded the installer from Cisco.com, double-click the WCS-STANDARD-K9-6-0-X-Y.exe file that you downloaded to your local drive. The Install Anywhere window appears and prepares the system for installation. After a few seconds, the Introduction window appears, followed by the license agreement window.

Step 2 Click the **I accept the terms of the License Agreement** option to continue. At this point, the install wizard detects whether a previous version of Cisco WCS is installed and specifies whether the current version is eligible for an automated upgrade. If your Cisco WCS version cannot participate in the automated upgrade, you receive such a notice.

Step 3 If your Cisco WCS version is eligible for an automated upgrade and the previous qualifying version of Cisco WCS is detected, choose **Upgrade** and continue to Step 4. This method is preferred. If your Cisco WCS version is ineligible for an automated upgrade, choose **Install** to end the installer and switch to a manual upgrade. (See the *Cisco Wireless Control System Configuration Guide* for manual upgrade instructions.)

Several of the values from the previous installation are retained as part of the upgrade. These include the following:

- The ports
- The root password
- The root FTP password
- The TFTP server file location
- The FTP server file location
- The multi-homed server interfaces

Step 4 In the Choose Install Folder page, choose a folder in which to install the Cisco WCS. It must be a different location than the previous installation. Click **Next** to continue.

Step 5 Choose a folder location in which to store the shortcuts. It must be a different location than the previous installation.

Note If shortcuts should be installed for all users on the server, select the **Install shortcuts for all users** check box.

Step 6 Continue to follow the prompts that appear. You are notified when the system checks for required space, uninstalls previous versions, backs up files, restores, and so on. A prompt appears asking if you are ready to start Cisco WCS as a service. Click **Yes**.

Note The upgrade log is located in the standard log directory (\webnms\logs) if the automated upgrade completes. If the automated upgrade did not complete, the upgrade log is located in the user home directory.

Note If Cisco WCS is configured to use TACACS+ or RADIUS for external authentication, you must update the custom vendor attribute list in the TACACS+ or RADIUS server with any new permissions and virtual-domain information. The attribute list for the appropriate UserGroup can be found at Administration > AAA > UserGroups. Click the **Export** link for the appropriate user group. See Chapter 14 "Performing Maintenance Operations" of the *Cisco Wireless Control System Configuration Guide* for additional information regarding upgrading.

Using the Installer to Upgrade Cisco WCS for Linux

To upgrade Cisco WCS (on a Linux platform) using the automated upgrade, follow these steps:

Step 1 Using the command-line interface, perform one of the following:

a. If you are installing from a CD, switch to the /media/cdrom directory.

b. If you are installing from Cisco.com, switch to the directory in which the install file was downloaded. For example, if the install file was placed in /root/Desktop, enter **cd /root/Desktop**.

Step 2 Enter ./WCS-STANDARD-K9-6.0.X.Y.bin (for CD or Cisco.com users) to start the install script. The Install Anywhere message appears and prepares the system for installation. After a few seconds, the Introduction appears, followed by the license agreement statement.

Step 3 Accept the license agreement to continue.

At this point, the install wizard detects whether a previous version of Cisco WCS is installed and specifies whether the current version is eligible for an automated upgrade. You receive a notification whether or not your most recent Cisco WCS version is eligible for the automated upgrade.

Step 4 If your Cisco WCS version is eligible for an automated upgrade and the previous qualifying version of Cisco WCS is detected, choose **Upgrade** and continue to Step 6. This method is preferred. If your Cisco WCS version is ineligible for an automated upgrade, choose **Install** to end the installer and switch to a manual upgrade. (See the *Cisco Wireless Control System Configuration Guide* for manual upgrade instructions.)

Several of the values from the previous installation are retained and carried over as part of the upgrade. These include the following:

- The ports
- The root password
- The root FTP password
- The TFTP server file location
- The FTP server file location
- The multi-homed server interfaces

Step 5 Choose a folder in which to install the Cisco WCS. It must be a different location than the previous installation. Click **Next** to continue.

Step 6 Choose a folder location to store the shortcuts. It must be a different location than the previous installation.

Step 7 Continue to follow the prompts that appear. You are notified when the system checks for required space, uninstalls previous versions, backs up files, restores, and so on. A prompt appears asking if you are ready to start Cisco WCS as a service. Click **Yes**.

Note The upgrade log is located in the standard log directory (\webnms\logs) if the automated upgrade completes. For an incomplete automated upgrade, the upgrade log is located in the user home directory.

Note If Cisco WCS is configured to use TACACS+ or RADIUS for external authentication, the custom vendor attribute list should be updated in the TACACS+ or RADIUS server with any new permissions. The attribute list for the appropriate UserGroup can be found at Administration > AAA > UserGroups. Click the **Export** link for the appropriate user group. See Chapter 14, "Performing Maintenance Operations" of the *Cisco Wireless Control System Configuration Guide* for additional information regarding upgrading.

Restoring the Cisco WCS Database in a High Availability Environment

During installation, you are prompted to determine if a secondary Cisco WCS server would be used for high availability support to the primary Cisco WCS server. If you opted for this high availability environment and enabled it in the Administration > High Availability page, the status appears as *HA enabled*. Before performing a database restore, you must convert the status to *HA not configured*.

Note If the restore is performed while the status is set to *HA enabled*, unexpected results may occur.

Choose the desired option from the following choices to change the status from *HA enabled* to *HA not configured*:

- Click **Remove** in the HA Configuration page (Administration > High Availability).
- Restart the primary server. Go to the secondary HealthMonitor GUI (https://<SecondaryWCS>:8082) and click **Failback**.

This procedure is used when one of the following instances has occurred:

- The primary server is down and a failover has not been executed, so the secondary server is in the SecondaryLostPrimary state.
- The primary server is down and a failover is already executed, so the secondary server is in the SecondaryActive state.

The primary server will now be in HA Not Configured mode, and you can safely perform a database restore.

Important Notes

This section describes important information about Cisco WCS.

If you change the report repository path under Administration > Settings > Report, then the existing saved download report will no longer work. To fix this problem, manually move the files to the new directory by cutting and pasting the files.

If you are upgrading between different releases of the WCS and Controller, check the SNMP MIBs or OID structures on running controller versions for affected changes of features. Controller should be applying commands based on right MIB versions.

Duplicate AP Name

If you see access points with the same name while applying controller templates or adding them to the map, perform a refresh config. The duplicates in the database will be eliminated.

High Availability

An e-mail address is now optional when you configure high availability. However, if you enter a properly formatted e-mail address, you must also configure a Cisco WCS e-mail server.

Note High availability is supported on Linux, Windows 2003, and VMware environments. Specific operating system support is listed in the "Operating Systems Requirements" section on page 3.

Client Session Report

The new client session report replaces the existing Client Association and Client Detail Report. If you perform an upgrade, Client Association no longer appears on the Reports menu. The data pertaining to these reports migrates successfully, and saved report entries for Client Association and Client Detail reports are migrated. However, the new ClientSessionInfo table is not populated with data from the previous reporting period; the table is populated with client-related data that occurred after the upgrade. The new client detail report contains the details of association time, disassociation time, and session timeout with details of VLAN, session length, client location, Megabit information used, SNR, RSSI, and throughput.

Cisco WCS Supported on Windows 2003 English and Japanese Operating Systems Only

Cisco WCS is supported only on English or Japanese versions of the Windows 2003 operating system. Display problems sometimes occur when you install and run Cisco WCS on operating systems translated to other languages or with locale settings other than English or Japanese.

Notifications in Junk E-mail Folder

If a domain name is not set in the e-mail settings, notifications may end up in the junk e-mail. When the primary device is down, no e-mail notifications are received, but the log message indicates that an e-mail was successfully sent.

Internet Explorer Error

When you click certain links that call JavaScript code, you may get an Internet Explorer error as follows:

Problems with this web page might prevent it from being displayed properly or functioning properly. In the future, you can display this message by double-clicking the warning icon displayed in the status bar.

This problem appears if another program has deregistered the dynamic-link library (DLLs). Reregistering them corrects the problem.

To reregister the DLLs, follow these steps:

Step 1 Open a command-line window in Windows XP (Start > All Programs > Accessories > Command Prompt).

Step 2 Run these commands one at a time in the following order. After each command successfully runs, you should receive a pop-up message that the DllRegisterServer in_*something*.dll succeeded.

1. regsvr32 msscript.ocx
2. regsvr32 dispex.dll
3. regsvr32 vbscript.dll
4. regsvr32 scrrun.dll
5. regsvr32 urlmon.dll
6. regsvr32 actxprxy.dll
7. regsvr32 shdocvw.dll

Step 3 Restart the computer.

Notes About Google Earth

When you launch Google Earth, this message appears:

```
Google Earth could not write to the current cache or myplaces file location. The values
will be set as follows:
My Places Path:"C:\Document and Settings\userid\Application Data\Google\GoogleEarth"
```

```
Cache Path: "C:\Documents and Settings\userid\Local Settings\Application
Data\Google\GoogleEarth"
```

This behavior is expected.

Also, if you visit the AP Details page a second time, you get an "invalid path / googleArthLradDetails was requested" HTTP status message. This Google Earth problem can be resolved by deleting the first AP Details occurrence.

Windows XP Cannot Load CAD Files

Internet Explorer 7 running on Windows XP cannot load CAD files because of missing DLLs (C:\Windows\system\DWMAPI.DLL). These DLLs are present only on Windows Vista.

Take one of the following actions:

- Uninstall IE7 and install IE6.
- Leave IE7 and install the missing DLLs.

Deletion of TFTP Server is not Updated in the Configuration Backup

To add a TFTP server, choose **Configure > Controller Templates**, choose **TFTP server** from the left sidebar menu, and choose **Add TFTP Server** from the drop-down list. To add the TFTP server, enter the name and IP address and click **Save**. If you later delete this TFTP server and back up the configuration (Administration > Background Task > Configuration Backup), the IP address of the TFTP server still appears in the TFTP Server page when only the default server appears.

Conflicting Ports Interrupt Cisco WCS Start

Cisco WCS fails to start if there is a conflicting port in use. You receive a "Failed to start WCS server" message, but you do not receive a list of conflicting ports. Go to WCS/webnms/logs/wcs-0-0.log and view the conflicting ports. Enter the following to get a list of the process IDs associated with each connection:

In Windows XP and Windows Server 2003, enter **netstat -na0**.

In Linux, enter **netstat -nlp**.

In the Task Manager, you see the respective PID and can stop the process using the port that Cisco WCS requires.

New Features

There are no new features in this maintenance release.

Caveats

The following sections list open and resolved caveats in Cisco WCS 6.0.196.0 for Windows and Linux. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are taken directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

http://tools.cisco.com/Support/BugToolKit/.

To become a registered cisco.com user, go to the following website:

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

Open Caveats

Table 1 lists the open caveats in Cisco WCS 6.0.196.0.

Table 1 Open Caveats

ID Number	Caveat Title
CSCte50763	WCS TFTP Server stops an existing transfer if an unreachable message is received about the previous transfer.
CSCtg65340	After sync up, the primary WCS failed, and the secondary WCS is having license issue.
CSCth08840	The controller license information appears blank for non-root users
CSCtf51758	Session cookie and scripting code issues.
CSCtf69799	WCS allows user to access devices outside the partition.

Resolved Caveats

Table 2 lists caveats resolved in Cisco WCS 6.0.196.0.

Table 2 Resolved Caveats

ID Number	Caveat Title
CSCsx20463	Impossible to differentiate lower L and upper I on guest credentials.
CSCsx96043	Client count graph in the home page does not show Autonomous clients.

Table 2 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtb58698	When a permanent MSE license is added for client/tag tracking, the error "Context Aware Service has license expiring in 0 days" appears.
CSCtc56702	Wrong warning appearing for SSH/Telnet template.
CSCtd26408	WCS 4.2.110.0 cannot modify external web auth redirection URL for WLANs.
CSCtd42314	The CLI template should continue operation when one command throws an error.
CSCtd44718	User input for the required commands to CLI template parser needs to be added.
CSCtd53290	Change the default "maximuim row per table" to 40000.
CSCtd65126	The search options that WCS shows for the total client distribution is wrong.
CSCtd74615	WCS Ntp template fails to rewrite/overwrite when three entries exist in WLC.
CSCtd75773	The 802.11 a/n and 802.11 b/g/n parameters template changes AP power level to 1.
CSCtd98538	WCS Lobby administrator cannot login and a HTTP 500 error appears.
CSCtd99328	Migration of Autonomous AP {AIR-AP1131G-A-K9} to LWAPP fails.
CSCte05355	Noticed high memory utilization by Java.
CSCte18212	WCS displays an unexpected error while pushing lag mode with diagnostic WLAN.
CSCte48962	Time differed 1:30 hours between the scheduled run and the view migration report.
CSCte57726	WCS fails to show the ethernet interface for 1510 AP running 4.2.176.51M.
CSCte73143	WCS creates unlimited log files when the secondary WCS is down.
CSCte75474	Issue with template discovery for system general templates.
CSCte81786	The dbadmin remotebackup script generates errors, and it does not perform FTP backup.
CSCte97911	WCS directs to a wrong page when you choose Monitor > Access Points > Mesh Statistics > Security > Mesh Link Alarms.
CSCte98698	The WCS home page takes a long time to load.
CSCtf07885	Need pop-up in the AP Group page that mentions about the HREAP VLAN mapping.
CSCtf12020	Under the Services > Mobility Services > Synchronize WCS and the MSE(s) > Switches tabs, when there records that are more than one page, the buttons to navigate to other pages do not appear.
CSCtf13873	Under Alarms, WCS reports duplicate IPs incorrectly.
CSCtf27124	While searching for clients based on the NAC state, the search is misleading for disassociation clients.
CSCtf30942	WCS Autonomous AP “operationally down” alarm is inaccurate.
CSCtf35333	Reflected XSS issues.
CSCtf40315	A superuser member is unable to expand the chart on the main monitoring page.
CSCtf42584	Export PDF functionality is not working for Accuracy Report.

Table 2 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtf56907	Changes to Standard Signature Frequency, MAC Frequency, and Quiet Time are not pushed.
CSCtf56987	WCS fails to audit configurations for the wireless protection policies.
CSCtf60667	Rogue AP's RSSI value is not updated.
CSCtf64993	Error while installing WCS.
CSCtf84301	Unable to disable "Trace Display Values" once enabled.
CSCtg00319	Newly assigned OUIs are missing from WCS.
CSCth02673	An errors occurs when applying the WLAN template with security as WEP.
CSCtg14415	Potential issue in webacs/monitorMapListAction.do.
CSCtg16331	Loading images greater than 12 mega pixels causes JVM to crash, when map editor is invoked.
CSCtg17101	WCS should generate alarm when config backup fails for a controller.
CSCtg27581	AP template error occurs when changing mesh role
CSCtg29286	The email notification/status change for the scheduled guest template fails.
CSCtg33854	Several XSS on different WCS URLs.
CSCtg38030	WCM Controller is not manageable by WCS.
CSCtg42601	WCS allows "+" (plus sign) in AP Group name that breaks WLC configuration through GUI.
CSCtg47863	WCS does not retain key/certificate across upgrades.
CSCth00531	A servlet exception found on creating a local net user template.
CSCth04157	The report title causes export failure.
CSCte61754	Permission denied for show status filter in Guest Users controller template.
CSCth01325	An advanced search for the autonomous AP with 11n support is not working.
CSCtg62371	General template with Lag mode enabled and push to controller displays SNMP error.
CSCtd01625	An industry-wide vulnerability exists in the Transport Layer Security (TLS) protocol that could impact any Cisco product that uses any version of TLS and SSL.

If You Need More Information

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at the following location:

http://www.cisco.com/cisco/web/psa/troubleshoot.html

Click **Wireless** and **Wireless LAN Management**, and then choose **Autonomous Wireless LAN** and **Unified Wireless LAN Management**.

Related Documentation

For information on the Cisco Unified Wireless Network Solution and for instructions on how to configure and use the Cisco UWN, see the *Cisco Wireless Control System Configuration Guide* and the *Cisco Wireless LAN Controller Configuration Guide.*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.