Release Notes for Cisco Wireless Control System for Windows or Linux, Release 7.0.164.0

June 2010

These release notes describe open caveats for the Cisco Wireless Control System 7.0.164.0 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, 1040, 1100, 1130, 1140, 1200, 1230, 1240, 1250, 1260, 1310, 1500, 1524, 3500i, and 3500e Series Lightweight Access Points
- Cisco Aironet 801, 1100, 1130, 1200, 1240, 1250, 1141, and 1142 Autonomous Access Points
- Autonomous Access Points for 1801, 1802, 1803, 1811, 1812, 851, 857, 871, 876, 877, and 878 Cisco Integrated Services Routers

  Note Autonomous APs that are integrated in ISR will be supported.

- Cisco Aironet 1310 and 1410 Bridges

  Note Only bridges in autonomous modes are supported.

- 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.

Hardware Requirements for Server

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 X5406 or better.
- 8-GB RAM.
- 200 GB minimum free disk space is needed on your hard drive.

Note If you choose a CPU configuration that is different from what is provided above as a guidance, you may use a website like the following to perform the benchmark tests and assess whether the alternate CPU meets the WCS minimum requirements:
http://www.cpubenchmark.net

Note If you use multiple CPU configurations, the benchmarking sites (like the above website) also allow you to make comparisons based on the number of cores that are being selected per CPU.

Note The free disk space listed is a minimum requirement but may be different for your system, depending on the number of backups.

Unified Computing System

The following Cisco Unified Computing System(UCS) C-Series servers provide guidance to plan your system requirements for either UCS or equivalent hardware platform. Any server can be used if it meets the minimum requirements.

Cisco UCS C-Series M1 Server

The following are the recommended specifications for the Cisco UCS C-Series M1 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5500 series processor X5570 (4-core 2.93-GHz).

  Note If your processor speed is less than the one mentioned above, we recommend you to use two processors.

- 8-GB RAM.
- 200-GB minimum free disk space on your hard drive.

Cisco UCS C-Series M2 Server

The following are the recommended specifications for the Cisco UCS C-Series M2 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5600 series processor X5680 (6-core 3.33-GHz) or one Intel Xeon 5600 series processor X5670 (6-core 2.93-GHz).
- 8-GB RAM.

- 200-GB minimum free disk space 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 Dual Core processor or better.
- 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.

Note If you choose a CPU configuration that is different from what is provided above as a guidance, you may use a website like the following to perform the benchmark tests and assess whether the alternate CPU meets the WCS minimum requirements:
http://www.cpubenchmark.net

Unified Computing System

The following Cisco Unified Computing System(UCS) C-Series servers provide guidance to plan your system requirements for either UCS or equivalent hardware platform. Any server can be used if it meets the minimum requirements.

Cisco UCS C-Series M1 Server

The following are the recommended specifications for the Cisco UCS C-Series M1 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5500 series processor X5570 (4-core 2.93-GHz) or one Intel Xeon 5500 series processor X5550 (4-core 2.66-GHz) or one Intel Xeon 5500 series processor E5540 (4-core 2.53-GHz).
- 4 GB of RAM.
- 80-GB minimum free disk space on your hard drive.

Cisco UCS C-Series M2 Server

The following are the recommended specifications for the Cisco UCS C-Series M2 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5600 series processor X5650 (6-core 2.66-GHz) or one Intel Xeon 5600 series processor X5670 (6-core 2.93-GHz).
- 4 GB of RAM.
- 80-GB minimum free disk space 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 or better.
- 1.86-GHz Intel Dual core processor.
- 2-GB RAM.
- 50 GB minimum free disk space is needed on your hard drive.

Note If you choose a CPU configuration that is different from what is provided above as a guidance, you may use a website like the following to perform the benchmark tests and assess whether the alternate CPU meets the WCS minimum requirements:
http://www.cpubenchmark.net

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.

Unified Computing System

The following Cisco Unified Computing System(UCS) C-Series servers provide guidance to plan your system requirements for either UCS or equivalent hardware platform. Any server can be used if it meets the minimum requirements.

Cisco UCS C-Series M1 Server

The following are the recommended specifications for the Cisco UCS C-Series M1 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5500 series processor X5550 (4-core 2.66-GHz).
- 2 GB of RAM.
- 50-GB minimum free disk space on your hard drive.

Cisco UCS C-Series M2 Server

The following are the recommended specifications for the Cisco UCS C-Series M2 Server, but you can choose higher processing capabilities:

- One Intel Xeon 5600 series processor X5650 (6-core 2.66-GHz).
- 2 GB of RAM.
- 50-GB minimum free disk space on your hard drive.

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 WCS in VMware must follow the specifications for the size of WCS that you intend to use.

Client Requirements

The Cisco WCS user interface requires Internet Explorer 7.0 or later with the Flash plugin or Mozilla Firefox 3 or later releases. Internet Explorer 6.0 is not supported.

Note You are strongly advised not to enable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing Tools > Internet Options and unselecting the Enable third-party browser extensions check box from the Advanced tab.

Using a web browser running on Windows 2003 to access the 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 that is recommended for both WCS and Navigator use is 1024 x 768 pixels.

Table 1 lists the WCS supported versions of controller, location, and mobility service engine (MSE),

Table 1 WCS Versions

WCS Version	Supported Controller Versions	Supported Location Server Versions	Supported MSE Versions	Release Date	Upgrade Supported From	Operating System Requirement
7.0.164.0	7.0.98.0 6.0.202.0 6.0.199.4 6.0.196.0 6.0.188.0 6.0.182.0 6.0.108.0 5.2.193.0 5.2.178.0 5.2.157.0 4.2.209.0 4.2.207.0 4.2.205.0 4.2.176.0 4.2.173.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0	6.0.103.0	7.0.105.0	June 2010	6.0.181.0 6.0.170.0 6.0.132.0 5.2.148.0 5.2.130.0 5.2.125.0 5.2.110.0	Windows 2003 SP2 32-bit RHEL 5.x Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
6.0.181.0	6.0.196.0 6.0.188.0 6.0.182.0 6.0.108.0 5.2.193.0 5.2.178.0 5.2.157.0 5.1.163.0 5.1.151.0 4.2.207.0 4.2.205.0 4.2.176.0 4.2.173.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0	6.0.101.0	6.0.103.0	17 Feb 2010	6.0.170.0 6.0.132.0 5.2.148.0 5.2.130.0 5.2.125.0 5.2.110.0 5.1.65.4 5.1.64.0 4.2.128.0 4.2.110.0 4.2.97.0 4.2.81.0 4.2.62.11 4.2.62.0	Windows 2003 SP2 32-bit RHEL 5.x Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit

Table 1 WCS Versions (continued)

WCS Version	Supported Controller Versions	Supported Location Server Versions	Supported MSE Versions	Release Date	Upgrade Supported From	Operating System Requirement
6.0.170.0	6.0.188.0 6.0.182.0 6.0.108.0 5.2.193.0 5.2.178.0 5.2.157.0 5.1.163.0 5.1.151.0 4.2.207.0 4.2.205.0 4.2.176.0 4.2.173.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0	6.0.97.0	6.0.97.0	8 Nov 2009	6.0.132.0 5.2.148.0 5.2.130.0 5.2.125.0 5.2.110.0 5.1.65.4 5.1.64.0 4.2.128.0 4.2.110.0 4.2.97.0 4.2.81.0 4.2.62.11 4.2.62.0	Windows 2003 SP2 32-bit RHEL 5.x Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
6.0.132.0	6.0.182.0 6.0.108.0 5.2.178.0 5.2.157.0 5.1.163.0 5.1.151.0 4.2.205.0 4.2.176.0 4.2.173.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0	6.0.85.0	6.0.85.0	11 June 2009	5.2.130.0 5.2.125.0 5.2.110.0 5.1.65.4 5.1.64.0 4.2.128.0 4.2.110.0 4.2.97.0 4.2.81.0 4.2.62.11 4.2.62.0	Windows 2003 SP2 32-bit RHEL 5.x Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
5.2.148.0	5.2.193.0 5.2.178.0 5.2.157.0 5.1.151.0 5.0.148.2 5.0.148.0 4.2.207.0 4.2.205.0 4.2.176.0 4.2.173.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0	5.2.100.0	5.2.100.0	25 June 2009	5.2.130.0 5.2.125.0 5.2.110.0 5.1.65.4 5.1.64.0 5.0.72.0 5.0.56.2 5.0.56.0 4.2.128.0 4.2.110.0 4.2.97.0 4.2.81.0 4.2.62.11 4.2.62.0	Windows 2003 SP2 32-bit RHEL 5.x Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit

Table 1 WCS Versions (continued)

WCS Version	Supported Controller Versions	Supported Location Server Versions	Supported MSE Versions	Release Date	Upgrade Supported From	Operating System Requirement
5.2.130.0	5.2.178.0 5.2.157.0 5.1.151.0 5.0.148.2 5.0.148.0 4.2.176.0 4.2.173.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0	5.2.91.0	5.2.91.0	21 Feb 2009	5.2.125.0 5.2.110.0 5.1.65.4 5.1.64.0 5.0.72.0 5.0.56.2 5.0.56.0 4.2.110.0 4.2.97.0 4.2.81.0 4.2.62.11 4.2.62.0	Windows 2003 SP2 32-bit RHEL 5.x Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
5.2.125.0	5.2.178.0 5.2.157.0 5.1.151.0 5.0.148.2 5.0.148.0 4.2.176.0 4.2.173.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0	5.2.91.0	5.2.91.0	10 Feb 2009	5.2.110.0 5.1.65.4 5.1.64.0 5.0.72.0 5.0.56.2 5.0.56.0 4.2.110.0 4.2.97.0 4.2.81.0 4.2.62.11 4.2.62.0	Windows 2003 SP2 32-bit RHEL 5.x Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
5.2.110.0	5.2.157.0 5.1.151.0 5.0.148.2 5.0.148.0 4.2.176.0 4.2.173.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0	5.2.91.0	5.2.91.0	24 Nov 2008	5.1.64.0 5.0.72.0 5.0.56.2 5.0.56.0 4.2.110.0 4.2.97.0 4.2.81.0 4.2.62.11 4.2.62.0	Windows 2003 SP2 32-bit RHEL 5.1 RHEL 5.0 Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
5.1.65.4	5.1.163.0 5.1.151.0 5.0.148.2 5.0.148.0 4.2.176.0 4.2.173.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0	5.1.35.0	5.1.35.0	9 Jan 2009	5.1.64.0 5.0.72.0 5.0.56.2 5.0.56.0 4.2.110.0 4.2.97.0 4.2.81.0 4.2.62.11 4.2.62.0	Windows 2003 SP2 32-bit RHEL 5.x RHEL 5.x Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit

Table 1 WCS Versions (continued)

WCS Version	Supported Controller Versions	Supported Location Server Versions	Supported MSE Versions	Release Date	Upgrade Supported From	Operating System Requirement
5.1.64.0	5.1.151.0 5.0.148.2 5.0.148.0 4.2.176.0 4.2.173.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0	5.1.30.0	5.1.30.0	21 July 2008	5.0.56.2 5.0.56.0 4.2.97.0 4.2.81.0 4.2.62.11 4.2.62.0	Windows 2003 SP2 32-bit RHEL 5.1 RHEL 5.0 Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
5.0.72.0	5.0.148.2 5.0.148.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0 4.1.185.0 4.1.171.0	4.0.38.0	Not Applicable	5 Aug 2008	5.0.56.2 5.0.56.0 4.2.62.11 4.2.62.0 4.1.91.0 4.1.83.0	Windows 2003 SP2 32-bit RHEL 5.1 RHEL 5.0 Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
5.0.56.2	5.0.148.0 4.2.61.0 4.1.x.x	4.0.33.0	Not Applicable	14 Apr 2008	5.0.56.0 4.2.62.11 4.2.62.0 4.1.91.0 4.1.83.0	Windows 2003 SP2 32-bit RHEL 5.0 Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
5.0.56.0	5.0.148.0 4.2.61.0 4.1.x.x	4.0.32.0	Not Applicable	16 Feb 2008	4.2.62.11 4.2.62.0 4.1.91.0 4.1.83.0	Windows 2003 SP2 32-bit RHEL 5.0 Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit

Table 1 WCS Versions (continued)

WCS Version	Supported Controller Versions	Supported Location Server Versions	Supported MSE Versions	Release Date	Upgrade Supported From	Operating System Requirement
4.2.128.0	4.2.207.0 4.2.205.0 4.2.176.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0 4.1.185.0 4.1.171.0 4.0.216.0 4.0.206.0 4.0.179.11 4.0.179.8 4.0.155.0	3.1.43.0	Not Applicable	13 May 2009	4.2.110.0 4.2.97.0 4.2.81.0 4.2.62.11 4.2.62.0 4.1.91.0 4.1.83.0 4.0.100.0 4.0.97.0 4.0.96.0 4.0.87.0 4.0.81.0 4.0.66.0	Windows 2003 SP2 32-bit RHEL 4.0 RHEL 5.0 (5.1 and later no supported) Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
4.2.110.0	4.2.176.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0 4.1.185.0 4.1.171.0 4.0.216.0 4.0.206.0 4.0.179.11 4.0.179.8 4.0.155.0	3.1.42.0	Not Applicable	29 Sep 2008	4.2.97.0 4.2.81.0 4.2.62.11 4.2.62.0 4.1.91.0 4.1.83.0 4.0.100.0 4.0.97.0 4.0.96.0 4.0.87.0 4.0.81.0 4.0.66.0	Windows 2003 SP2 32-bit RHEL 4.0 RHEL 5.0 Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
4.2.97.0	4.2.176.0 4.2.130.0 4.2.112.0 4.2.99.0 4.2.61.0 4.1.185.0 4.1.171.0 4.0.216.0 4.0.206.0 4.0.179.11 4.0.179.8 4.0.155.0	3.1.38.0	Not Applicable	3 Jun 2008	4.2.81.0 4.2.62.11 4.2.62.0 4.1.91.0 4.1.83.0 4.0.100.0 4.0.97.0 4.0.96.0 4.0.87.0 4.0.81.0 4.0.66.0	Windows 2003 SP2 32-bit RHEL 4.0 RHEL 5.0 Windows/RHEL on ESX 3.0.1 and above No support for 64 bit

Table 1 WCS Versions (continued)

WCS Version	Supported Controller Versions	Supported Location Server Versions	Supported MSE Versions	Release Date	Upgrade Supported From	Operating System Requirement
4.2.81.0	4.2.99.0 4.2.61.0 4.1.185.0 4.1.171.0 4.0.216.0 4.0.206.0 4.0.179.11 4.0.179.8 4.0.155.0	3.1.36.0	Not Applicable	17 Mar 2008	4.2.62.11 4.2.62.0 4.1.91.0 4.1.83.0 4.0.100.0 4.0.97.0 4.0.96.0 4.0.87.0 4.0.81.0 4.0.66.0	Windows 2003 SP2 32-bit RHEL 4.0 RHEL 5.0 Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
4.2.62.11	4.2.61.0 4.1.185.0 4.1.171.0 4.0.216.0 4.0.206.0 4.0.179.11 4.0.179.8 4.0.155.0	3.1.35.0	Not Applicable	25 Jan 2008	4.2.62.0 4.1.91.0 4.1.83.0 4.0.100.0 4.0.97.0 4.0.96.0 4.0.87.0 4.0.81.0 4.0.66.0	Windows 2003 SP2 32-bit RHEL 4.0 Update 5 Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit
4.2.62.0	4.2.61.0 4.1.185.0 4.1.171.0 4.0.216.0 4.0.206.0 4.0.179.11 4.0.179.8 4.0.155.0	3.1.35.0	Not Applicable	9 Nov 2007	4.1.91.0 4.1.83.0 4.0.100.0 4.0.97.0 4.0.96.0 4.0.87.0 4.0.81.0 4.0.66.0	Windows 2003 SP2 32-bit RHEL 4.0 Update 5 Windows/ RHEL on ESX 3.0.1 and above No support for 64 bit

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 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 WCS is already installed and connected, verify the software release by choosing **Help > About the Software**.

Upgrading WCS

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

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 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 WCS for Windows

To upgrade 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-K9-7.0.X.Y.exe file where 7.0.X.Y is the software build. If you downloaded the installer from Cisco.com, double-click the WCS-STANDARD-WB-K9-7-0-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 WCS is installed and specifies whether the current version is eligible for an automated upgrade. If your most recent WCS version cannot participate in the automated upgrade, you receive such a notice.

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

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 Choose a folder in which to install the Cisco WCS at the Choose Install Folder page. 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.

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 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 WCS is configured to use TACACS+ or RADIUS for external authentication, you should update the custom vendor attribute list 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.

Using the Installer to Upgrade WCS for Linux

To upgrade 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-K9-7.0.X.Y.bin** (for CD users) or **./WCS-STANDARD-LB-K9-7-0-X-Y.bin** (for 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 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 WCS version is eligible for the automated upgrade.

Step 4 If you cannot continue to the automated upgrade because your current WCS version is not eligible, choose **Install** and continue to the manual upgrade (see the *Cisco Wireless Control System Configuration Guide* for manual upgrade instructions). You can also choose to do a manual upgrade rather than the recommended automated upgrade by choosing **Install** and continuing to the manual upgrade, but this action is not recommended. If your current WCS version is eligible for the recommended automated upgrade, choose **Upgrade** and continue to Step 6.

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 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 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 WCS Database in a High Availability Environment

During installation, you are prompted to determine if a secondary WCS server would be used for high availability support to the primary 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.

Follow one of these procedures 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.

WPlus License Features Included in Base License

All features included in a Wireless LAN Controller WPlus license are now included in the base license; this change is introduced in controller release 6.0.196.0. There are no changes to WCS BASE and PLUS licensing.

These WPlus license features are included in the base license:

- Office Extend AP
- Enterprise Mesh
- CAPWAP Data Encryption

The licensing change can affect features on your wireless LAN when you upgrade or downgrade controller software releases, so you should be aware of these guidelines:

- If you have a WPlus license and you upgrade from 6.0.18x to 6.0.195.0, your license file contains both Basic and WPlus license features. You will not see any disruption in feature availability and operation.
- If you have a WPlus license and you downgrade from 6.0.195.0 to 6.0.18x, the license file in 6.0.195.0 contains both Basic and WPlus license features, so you will not see any disruption in feature availability and operation.
- If you have a base license and you downgrade from 6.0.195.0 to 6.0.18x: When you downgrade, you lose all WPlus features.

Note Some references to Wireless LAN Controller WPlus licenses remain in WCS and in the controller CLI and GUI in release 6.0.196.0. However, WPlus license features have been included in the Base license, so you can ignore those references.

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 WCS e-mail server.

Note High availability is supported on Linux, on Windows 2003, and on VMware environments. Specific operating system support is listed in the "Operating Systems Requirements" section on page 5.

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 folder. 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). Re-registering them corrects the problem.

To reregister the DLLs, follow these steps:

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

Step 2 Enter the following commands one at a time in the following order. After each command successfully runs, you should receive a 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, the following 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 the following action:

- 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 navigation pane, 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 WCS Start

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 WCS requires.

New Features

The following new features are available in WCS software release 7.0.164.0.

Cisco CleanAir

Note To enable CleanAir on WCS, you need to have WCS Plus License installed.

The Cisco CleanAir features are as follows:

- Cisco CleanAir Dashboard—Cisco WCS includes a customizable Cisco CleanAir dashboard that displays current and historical business-critical information about wireless air quality, RF interference events, and security alerts. Information available from the Cisco CleanAir dashboard includes:
  - Air Quality summary
  - Network areas with the worst RF conditions
  - Recent security risk interferers
  - Threshold alarms
  - Interferer counts
- Cisco CleanAir Enhancements to Cisco WCS Security Dashboard—The Cisco WCS security dashboard is enhanced to include Cisco CleanAir information about RF interferers that are potential security risks. These enhancements deliver the only integrated security solution available in the industry to provide immediate visibility of security issues at both the logical and physical layer of the network.
- Cisco CleanAir Enhancements to Cisco WCS Radio Resource Management Dashboard—The Cisco WCS Radio Resource Management (RRM) dashboard is enhanced to include information about Cisco CleanAir RF interference alerts and mitigation. This feature helps in tracking RF interference events and correlating Cisco RRM adjustments that were made over the last 24 hours and for up to 7 days.
- Cisco CleanAir Enhancements to Cisco WCS Client Troubleshooting Tool—The Cisco WCS client troubleshooting tool can show the Air Quality at the access point and identify the RF interferers that are affecting the client device.

- Cisco CleanAir Enhancements to Cisco WCS Advanced Search—The Cisco WCS advanced search tool includes options to search for interferers across the entire wireless network. A variety of search options are available to support searches for specific types of interferers and for specific severity, duty cycle, location, and other characteristics.
- Cisco CleanAir Display Tools and Heat Maps—Cisco WCS includes new Air Quality tools, heat map options, and device detail information including:
  - Options to display real-time network air quality by access point, floor, building, or campus
  - Adjustable Cisco WCS heat map display of the average and minimum air quality for each location on the wireless network
  - Mouse-over details about each interferer, including type of interferer, active or inactive status, detected and reported dates, and zone of impact from the floor map
- Cisco CleanAir Reporting—Cisco WCS can monitor, collect, and store Cisco CleanAir information for up to 30 days. Customized reports can be generated based on current or stored information about RF interference and air quality. Cisco CleanAir reports can assist with tracking of Wi-Fi and non-Wi-Fi devices, network trends, and security policy effectiveness and enforcement.

  Cisco CleanAir reports are available for the following features:
  - Air Quality over time
  - Security risk interferers
  - Worst air quality access points
  - Worst interferers
- Ten Most Severe RF Interference Devices—A mouse-over option in the Cisco WCS floor map view displays the ten devices that are causing the most severe RF interference for each Cisco CleanAir access point.
- Cisco CleanAir Enhancements to Cisco Mobility Services Engine—When the Cisco Mobility Services Engine (MSE) is used with Cisco WCS and Cisco CleanAir, the following additional features are available:
  - Cisco CleanAir dashboard listing of the top RF interferers by severity
  - Correlation of RF interference information across multiple access points
  - Reports with historical tracking of devices generating RF interference
  - Location mapping and zone of impact information for each interferer

Maps Import and Export for Cisco WCS Servers and Third-Party Tools

Cisco WCS is significantly enhanced to support exporting and importing of Cisco WCS maps, hierarchies, map-related data, and network designs between one or more Cisco WCS servers.

Information from leading third-party site survey tools can be easily imported and integrated into Cisco WCS to aid in WLAN design and deployment.

Northbound Alarms and Events API

Cisco WCS can forward alarms and events to third-party, northbound receivers and applications that have fault, configuration, accounting, performance, and security (FCAPS) capability, such as HP OpenView or IBM Tivoli Netcool.

Event and alarm notifications are sent via SNMP. Notifications are customizable within Cisco WCS by category and severity.

Enhanced Auto-Provisioning Feature Suite for Wireless LAN Controllers

Cisco WCS simplifies WLAN deployments with support for auto-provisioning of the following Cisco wireless LAN controller parameters: dynamic interface, country regulatory domain, and mobility groups.

Scheduled Wireless LAN Controller Image Upgrades

Cisco WCS makes it easier to schedule wireless LAN controller firmware upgrades and access point pre-image downloads.

You can schedule wireless LAN controller and access point firmware upgrades to occur at the date and time of your choice. FTP or TFTP is supported. A reboot scheduling option is available.

Scheduled Migration of Standalone (Autonomous) Access Points

Cisco WCS templates support user-defined scheduled migration of Cisco Aironet standalone (autonomous) access points running Cisco IOS software to operate as lightweight access points running CAPWAP protocol.

Cisco self-signed certificate (SSC) entries on Cisco Aironet standalone access points can be saved in a CSV file for future reference.

Cisco WCS 7.0.164.0 supports secure shell (SSH).

Serviceability Program

The Cisco WCS Serviceability Program gives organizations the opportunity to provide anonymous usage statistics and wireless operational information to Cisco.

This voluntary “opt-in” program gathers anonymous statistics from Cisco WCS and the network. No confidential data is collected.

For more information about the Wireless Product Improvement Program policy, see the following website:

http://www.cisco.com/en/US/docs/wireless/wcs/pip/improvement_pg.htm

TAC Attachment Tool

Cisco WCS supports the “opt-in” collection of diagnostic data about Cisco Wireless LAN Controllers and Cisco Aironet access points to assist with Cisco Technical Assistance Center (TAC) cases.

Enhanced Web Browser Support

Cisco WCS 7.0.164.0 supports Microsoft Internet Explorer 8.0 and Mozilla Firefox 3.5.

Cisco Secure Access Control Server 5.1

Cisco WCS supports Cisco Secure Access Control Server (ACS) 5.1 for enhanced client troubleshooting.

Ease-of-Use

Cisco WCS ease-of-use is improved by enhancements to the following areas:

- The edit view option (Access Point Details > Current Associated Client) can now be customized to show additional columns such as Received Signal Strength Indicator (RSSI) and display protocol and uptime.
- The edit view option (Clients Details Page > Association History) can now be customized so that you can display the columns that you are interested in.
- Support for multiple MAC address format.
- Redesign of the radio resource management (RRM) dynamic channel assignment (DCA) template.

The following advanced search enhancements are available:

- Search by access point model and location
- Templates search by access point IP address range, name, and MAC address

Reporting

Cisco WCS includes the following reporting enhancements:

- Reports can be built based on the reporting information from the previous month.
- Data can be displayed by the device name for selected reports and charts.
- The Export Now reporting feature allows reports to be immediately exported without the need to run the report.

Rogue Device Management

The following enhancements for rogue device management are available in Cisco WCS:

- Improved refresh of rogue device attributes, such as channel and Service Set Identifier (SSID), as they change over time in the network.
- Details about rogue devices that are seen by multiple controllers can be displayed by each individual controller.
- Several display terms on the rogue device report have been renamed to simplify operations. (For example, “Map Location” is renamed to “Location of Detecting AP.”)

Voice Audit Tool

The Voice Audit Tool best-practices configuration settings have been updated for the aggressive load balancing rule that is now audited per Voice over WLAN.

Serviceability

Cisco WCS serviceability is enhanced in the following areas for the wireless network:

- Critical exceptions logging
- Startup process logging
- Diagnostics
- Usage data collection
- CLI templates error handling

Caveats

The following sections list open and resolved caveats in Cisco WCS 7.0.164.0 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/.

Note To become a registered cisco.com user, go to the following website: http://tools.cisco.com/RPF/register/register.do

Open Caveats

Caveats Associated with Release 7.0.164.0

Table 2 lists the open caveats in Cisco WCS 7.0.164.0.

Table 2 Open Caveats

ID Number	Caveat Title
CSCta77783	WCS does not support backup and upload of third party certificates that are installed on WLC.
CSCta93780	WCS is unable to upload customized web bundle from WLC.
CSCtb82643	While discovering the controllers, if the user selects the telnet/ssh verification option, the discovery result page gets into an infinite loop.

Table 2 Open Caveats (continued)

ID Number	Caveat Title
CSCtc17617	Telnet/ssh credentials are not validated while adding a controller.
CSCte94504	While creating a new floor area (on a Windows platform), WCS incorrectly shows Russian characters.
CSCte94520	Alarm is not generated on WCS when the radio is shut down due to a radar activity.
CSCtf17687	The heatmap does not reflect the option selected from the AP heatmap page.
CSCtg10241	Though troubleshooting a 802.1x results in failure, the results shows "Success".
CSCtg17085	WCS accepts duplicate AP names.
CSCtg23235	WCS displays incorrect IP address under the Monitor > Clients page.
CSCtg24632	An ObjectNotFoundException exception occurs while saving a virtual domain.
CSCtg32645	WCS receives a cold start trap from controller that appears as an internal error.
CSCtg42616	A view-only notification allows modifications as well.
CSCtg42774	A few components in the security tab are taking longer as compare with others.
CSCtg58343	WCS shows sensitive information.
CSCtg65481	Multiple wIPS profiles with same names exists in WCS.
CSCtg80655	The AP pre-image download task does not initiate on WLC from the schedule task.
CSCtg80981	WCS shows unclear message when user tries to push HREAP configuration with a WLAN profile.
CSCtg86035	An error message appears while saving a controller discovered DCA template.
CSCsw66937	Tags cannot be located from non-root Virtual Domain in WCS.
CSCtg79058	The WiFi TDoA receivers and Chokepoint list pages return empty results.
CSCsq17846	An error is received if you download software on a WLC using WCS regardless of whether you use FTP, TFTP, or the GUI. This error occurs only if the access point is already downloading software from the WLC.
CSCth11426	The wIPs report filter is not working properly.
CSCth12617	An error occurs when you click on a wIPs default profile.
CSCth18155	Under rare conditions, Health Monitor triggers a failover when it detects primary WCS is not running.
CSCth20001	Inactive devices do not show up on WCS maps correctly.

Bugs Opened Prior to Release 7.0.164.0

Table 3 lists the caveats that are open in releases prior to Cisco WCS 7.0.164.0 and still remain open.

Table 3 Open Caveats Prior to Release 7.0.164.0

ID Number	Caveat Title
CSCsj23423	The AP template is partially visible when switching between tasks and dates.
CSCsv34264	An attempt to generate an ID certificate throws an SNMP Error.

Table 3 Open Caveats Prior to Release 7.0.164.0 (continued)

ID Number	Caveat Title
CSCsy31225	The Access Point Details page left navigation pane disappears when you click an access point link from Configure > Controllers > <controller_ip> > Access Points > Cisco APs list page.
CSCsy31679	WCS displays an incorrect sorting order for Audit Status located on the Monitor > Controllers page.
CSCsz75691	The coverage hole alarm values for failed clients, total client, and threshold are all 0 on the Home page.
CSCsk01665	If you try to add any template with a negative test case and apply it to a device, the object is not created, but the Apply To field is incremented as expected.
CSCsm99598	A blank page appears when the ID certificate is downloaded from Configure > Controller > Security > ID Certificate. The certificate download is unsuccessful.
CSCso83838	The message that indicates when the current load on the radio is exceeded fails to specify which access point name or radio MAC has exceeded the load.
CSCsq38486	The profile VLAN mapping is not updated correctly on the access point, even though the native VLAN is applied correctly.

Resolved Caveats

Table 4 lists caveats resolved in Cisco WCS 7.0.164.0.

Table 4 Resolved Caveats

ID Number	Caveat Title
CSCsv34781	The user is unable to synchronize WLC to the MSE after the WLC sysname changes.
CSCsw80427	A discovered H-REAP template displays the wrong PAC timeout value.
CSCsx38955	After a database restore and upon synchronization, a controller can be assigned to multiple MSEs that are running wIPS. No error message displays.
CSCsx72413	When you enable the Diagnostic Channel for a WLAN and apply it to a device, audit differences appear in the WLAN.
CSCsx77870	Some configurations are missing from the Audit on Selected Parameters page.
CSCsy07751	When adding a new config group in WCS, the "Copy Templates from Controller" feature does not function properly.
CSCsy31176	When you successfully add a controller in WCS, the controller list page should appear, but instead the add controller page reappears.
CSCsy31617	The Category column under Monitor > Alarms displays an incorrect sorting order.
CSCsy57155	Web passthrough with pre-auth ACL fails to apply to release 5.2, 4.2, and 5.1 WLC.

Table 4 Resolved Caveats (continued)

ID Number	Caveat Title
CSCsy72020	WCS returns an exception when saving a WCS CLI template. This occurs when more than 400 WLAN config lines are added and the template is saved.
CSCsy74747	Ethernet switches are not partitioned. All users in all partitions can view all ethernet switches.
CSCsy78058	When you use Advanced Search to search for Telemetry tags and attempt to save the search, WCS fails to save the search and fails to conduct the search.
CSCsy78668	GUI buttons and the table format on the client troubleshooting page need to be updated.
CSCsy79232	WCS fails to save the apply device status to a report if WCS contains more than 25 controllers.
CSCsy84499	GUI buttons and the table format on the logged-in guest user page need to be updated.
CSCsy86778	WCS allows you to assign the same profile name to a WLAN and to a guest LAN. When you search currently logged-in guest users, WCS shows inaccurate results.
CSCsy89181	Sorting doesn't work correctly on some Monitor > Clients page columns.
CSCsy89369	The same page is shown even if you click on different profile statuses.
CSCsy94947	WCS displays an AP Authorization failed trap with the MAC address of the MSE when the NMSP session between WLC and MSE fails. When an MSE attempts to establish an NMSP session with the WLC and the authorization fails, the WLC sends a trap to WCS. This trap does not display enough information for WCS to distinguish this as an MSE-related trap. WCS defaults to an AP authorization failure trap with an MSE MAC address.
CSCsy97570	When you click a client device on the Monitor > Client page, the client detail page takes over one minute to appear.
CSCsy98346	After you configure a WLAN template with customized webauth pages, WLCs are not listed.
CSCsz00316	When 802.11a Status is enabled, WCS sometimes displays this message when you try to edit a data rate setting: Row already updated or deleted by another transaction.
CSCsz02466	Microsoft Internet Explorer version 6 sometimes fails to display accurate results for the Client Count Customization feature.
CSCsz04879	When you use the Detecting APs option, you sometimes see duplicate reports or incorrect RSSI values.
CSCsz05363	The WCS location configuration template might display an incorrect location path loss configuration for the normal client burst interval if you do not check the normal client box.
CSCsz05548	Client List page can sometimes take 30-500 seconds to load.
CSCsz06840	WCS shows a difference for CDP parameters on access points after saving the Switching.
CSCsz11535	On the WLAN configuration scheduled task page, the Selected WLANs table list is not inline with the heading and footer of the table.

Table 4 Resolved Caveats (continued)

ID Number	Caveat Title
CSCsz12395	For omni-directional antennas, WCS shows the access point information with the antenna angle at 90 degrees, which makes a customer think it is a directional antenna.
CSCsz19497	Buildings created under the Root Area appear in all virtual domains including domains to which they are not assigned. The problem happens when there are multiple virtual domains partitioned by campus and buildings, as well as buildings directly created under the Root Area.
CSCsz24278	Downloaded log files do not include all log files.
CSCsz24549	WCS causes an audit mismatch by displaying the wrong attributes for port physical mode or by editing the port speed parameters.
CSCsz28308	The config group template and audit results sometimes show a mismatch, even when you update the config templates from the controller.
CSCsz29526	When you use more than one MSE or location appliance to run an accuracy test on a floor and one of the devices is running a 5.x release and one is running a later release, the accuracy test fails.
CSCsz33239	Under background tasks, the Controller Configuration Backup task sometimes fails with this message: com.cisco.server.common.errors.IllegalOperationException: MEDIATION-5,TransferConfig!171.71.128.75,uploadMode,No access
CSCsz34211	A rogue client discrepancy occurs on the rogue AP page.
CSCsz40279	Prior to version 6.0, the MSE services tracked the maximum allowable elements; starting from 6.0, licensing is enforced. When 6.0 is installed, the services come up in evaluation mode which tracks only 100 elements for CAS and 20 for wIPS. You must install a permanent license for CAS and WIPs.
CSCsz44750	When the WCS search for tags with Telemetry option is enabled, Context Aware notifications are not updated.
CSCsz45064	GUI buttons and the table format on the Monitor Mesh AP page need to be updated.
CSCsz45172	When an ACS server sends a TACACS+ authorization reply with a long list of tasks, WCS sometimes closes the TCP connection and declares the ACS dead.
CSCsz48241	WCS displays Success for WLANs with media session snooping for unsupported controller versions.
CSCsz48609	The MAC address format used in a wired client search field is case sensitive. Also, if a space is added in front of the MAC address, the search fails.
CSCsz51669	On WCS, under the RRM group panel for a controller that is not a group leader, the last update time displays incorrectly.
CSCsz51707	The WCS IE window occasionally displays *Service Temporarily Unavailable* when checking the access points and clients in the WCS map from both local machine and remotely.
CSCsz53023	Upgrading a controller to 5.2.183.0 and above version does not upgrade the WLAN WEP Key size from unsupported 128-bit to 'UnKnown' or any other supported Key size. Because the MIB is not updated when a controller is upgraded, WCS does not update the Key size.

Table 4 Resolved Caveats (continued)

ID Number	Caveat Title
CSCsz54353	The Monitor > Clients > Clients Detected by MSE option does not populate the Controller Name column when the client is associated to the local WLC.
CSCsz58150	When you apply a config group to a controller, an SNMP exception is returned.
CSCsz58626	An audit reveals discrepancies between SNMP communities and AP authorization after a conversion from read-write to read-only.
CSCsz66652	A search of controller licenses using the Type filter criteria yields no results.
CSCsz68873	When you enable or disable the Power over Ethernet (POE) option and run an audit, WCS displays a mismatch for that setting on the controller.
CSCsz69090	WCS displays an SSID string for wired guest LANs on the WLAN list page (Configure > WLC > WLAN), and it should display dashes.
CSCsz69651	A download to WLC using TFTP from WCS fails with an invalid credentials error.
CSCsz72241	When you restore WCS to the controller's configuration, the username is successfully forwarded to the controller but not the password.
CSCsz72799	When you open WCS using Microsoft Internet Explorer and run a scheduled report that contains more than 60 selections, the browser sometimes hangs.
CSCsz73267	Rogue configuration parameters including RLDP (Monitor Mode APs-Only) and auto containment options are missing from WCS.
CSCsz75749	If an SSID contains one or more braces, the report fails to display the TSM information.
CSCsz75902	The wrong interface is used on high availability re-registration during VmWare setup.
CSCsz76058	When the dynamic power control report is run, the wrong power assignment mode is returned for the monitor access point.
CSCsz78329	The online help for scheduled and on-demand accuracy is not mapped correctly.
CSCsz80636	If you delete an AP group template, WCS moves the access points to a default group and then resets.
CSCsz80839	The Rogue AP Event report takes longer than expected to show the results.
CSCsz80919	WCS does not distinguish between voice clients and V5 clients. No alerts are given to the user.
CSCsz82240	The downstream packet delay data is missing from the TSM QoS computation.
CSCsz84382	If discrepancies exist on the rogue AP rule detail page, they do not necessarily appear at the controller level audit.
CSCsz85603	When you delete access points from the default access point group, WCS reboots the access points and they later rejoin the default group.
CSCsz89419	TACACS+ Authorization packet sends PAP as authentication field type, even if set to CHAP.
CSCsz91240	When you search a Client detail report by client username, WCS sometimes takes a long time to display the results. The problem occurs when the client historical database contains over one million records, and when client traps are enabled on the controllers.

Table 4 Resolved Caveats (continued)

ID Number	Caveat Title
CSCsz93996	An incorrect message appears when you try to generate a report for more than 5 access points or radios.
CSCsz95495	If you make modifications to the H-REAP config (such as disabling the least latency controller join option) using access point templates, the OEAP reboots when the template is applied. This is not expected behavior.
CSCsz96369	An "invalid type by" error is returned in the Client Sessions report if you upgraded from version 4.2 or 5.2 to version 6.0.
CSCsz96466	If you create a WLAN with webauth security, create a guest user mapped to the WLAN, and then forward it to WLC, you cannot delete the WLAN on the Configure > Controller > WLAN page. An exception error is returned.
CSCsz96510	If you try to delete a WLAN with a mobility anchor configured, an unknown exception is returned.
CSCsz96549	When a guest user with limited liftetime is discovered from a Discover Templates from Controller function, the wrong expire and end time is shown.
CSCta00548	From version 4.2 to 6.0, all web auth configuration (including internal, external, and customized) returns an SNMP failure across all supported controllers.
CSCta02499	On the Summary > Controller page, WCS incorrectly shows the remaining period of an evaluation license for 5500 series controllers.
CSCta04203	WCS sometimes fails to display clients in a partition that contains the access point to which the client is associated but which does not contain the controller to which the access point is associated.
CSCta05459	WCS creates a guest user template and a local net user for the same config when a guest user that was created on a controller performs a refresh config.
CSCta05909	WCS fails to perform a View History for a guest count graph.
CSCta08270	WCS does not allow email addresses with more than 32 characters.
CSCta18874	In some Windows installations in locales outside of the U.S., WCS startup fails.
CSCsh82165	During the installation and uninstallation of WCS or Navigator, the following error message occasionally appears on Linux devices: Command.run(): process completed before monitors could start.
CSCsj36002	When you troubleshoot a client, the generated logs are not truncated into files of 2-MB size.
CSCsj61673	The event log generated for the Cisco Compatible Extension v5 client is duplicated after time.
CSCsj77046	The controller addition message mentions only WiSMs.
CSCsq35574	The EAP-FAST parameters Authority ID and Server Key do not accept entries of 17 or more characters.
CSCsu39828	Even if activity for an infrastructure client is no longer occurring, the client still remains on the WCS map.
CSCsz28308	Config group template and audit consistently display a mismatch even when the config template is updated from the controller.
CSCsz91711	The copy and replace function does not copy information (such as host name and IP address) to the WLC.

Table 4 Resolved Caveats (continued)

ID Number	Caveat Title
CSCsz95770	When you choose Monitor > Alarms and view the interference alarm detail, it is missing information for the top 5 access points, some exceptions are returned, and some values are not correct.
CSCsz95961	The Voice Parameter template fails when it is applied to controllers.
CSCsz96528	The Mesh AP Detail page (Configure > Access Point and open Mesh access point) displays with an error message.
CSCtg34826	Delete WLC from WCS and check NMSP Connection is still up between MSE and WLC.
CSCtg50685	Modify the location readiness page to reflect new location accuracy.
CSCtf34858	Client cannot transmit traffic if it reassociates to an AP within 20 seconds.

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/en/US/support/index.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.