Release Notes for Cisco Wireless Control System for Windows or Linux, Release 7.0.172.0

First Published: April 14, 2011
OL-19998-06

These release notes describe open caveats for the Cisco Wireless Control System 7.0.172.0 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 2500 Series Wireless Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless Controllers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless Services Module 2 (WiSM2) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless Controller on SRE for ISR G2 Routers
- Cisco Flex 7500 Series Wireless Controllers
- 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, 3500e, and 3500p Series Lightweight Access Points
- Cisco Aironet 801, 1040, 1100, 1130, 1141, 1142, 1200, 1240, 1250, and 1260 Autonomous Access Points
- Autonomous Access Points for 1801, 1802, 1803, 1811, 1812, 801, 802, 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 600 Series OfficeExtend Access Points
- Cisco Aironet Access Points running Lightweight Access Point Protocol (LWAPP) or Control and Provisioning of Wireless Access Points protocol (CAPWAP)

Cisco WCS Requirements

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 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 for 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 that you 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 for 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 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 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 for 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 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 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 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 We strongly advise that you do not 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 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 services 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
7.0.172.0	7.0.116.0 7.0.98.218 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	6.0.202.0	7.0.201.0	April 2011	7.0.164.3 7.0.164.0 6.0.202.0 6.0.196.0 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
7.0.164.3	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	December 2010	7.0.164.0 6.0.196.0 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

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
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
6.0.202.0	6.0.202.0 6.0.199.4 6.0.199.0 (pulled from CCO) 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 4.2.209.0 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	6.0.202.0	6.0.202.0	April 2011	6.0.196.0 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 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
6.0.196.0	6.0.199.4 6.0.199.0 (pulled from CCO) 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 4.2.209.0 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	6.0.102.0	6.0.105.0	15 July 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 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
6.0.181.0	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 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 6.

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.

Removing and Reconfiguring HA

After removing and reconfiguring high availability, the primary and secondary WCS does not work. This is caused if you open any file under the <WCSROOT> while an HA operation is performed. During normal HA operation in windows environment, do not open any file or directory under <WCSROOT> directory.

CleanAir

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

Upgrading the Controllers

When upgrading controllers from the prior releases to the 7.0.172.0 version, we recommend that you perform a refresh of configuration from controller to obtain all 7.0.172.0 new features updated into WCS database. This is to avoid configuration mismatches with upgraded controller. This can be performed manually using the *Refresh Config from Controller* command from the Controller list page or using the *Auto refresh After Upgrade* option from Administration > Settings > Controller Upgrade Settings.

New Features

The following new features are available in WCS software release 7.0.172.0.

wIPS ELM

wIPS now includes the ability to visualize, analyze, and prevent attacks on customer networks and equipment. The objective of the ELM (Enhanced Local Mode) is the ability to detect on-channel attacks while simultaneously providing client access and services. The feature offers full 802.11, nonstandard channel and non-Wi-Fi threat detection. It uses an extensive threat library and supports forensics and reporting. Pre-processing at the access points minimizes the data backhaul because it works over very low bandwidth links.

Voice Diagnostics

The Voice diagnostic tool is an interactive tool to diagnose the voice calls in real time (VoWLAN Client). This tool reports call control related errors, roaming history of the clients, and the total active calls accepted and rejected by an associated AP. This tool enables you to start or stop the voice diagnostic feature.

RF Grouping

This feature provides wireless controller enhancements to Radio Resource Management (RRM). An RF grouping algorithm provides optimal channel allocation and power settings for access points in a network.

This feature enables you to configure RF Group leaders based on two criteria:

- Static leader: You can select an RF Group leader rather than have the leader chosen automatically by the grouping algorithm.
- Type-based leader: Type-based leadership is a configuration where the controller with a lower version should not be allowed to be made a leader for higher version controller.

You can statically select a controller as RF Group Leader with the best physical capabilities and the most recent software load. Load balancing between group leaders when you have different coverage areas allows the controllers to communicate effectively.

Additionally, when access points see each other, they are aware of the controllers they are associated with, which enables you to make predictable decisions.

This enhancement minimizes the limitations of the current approach to RF group management and reporting tools for predictability of RF group forming.

3500p AP Support

Support for the 3500p AP has been added in WCS. The 3500p APs are 802.11n access points designed for use in high density deployments utilizing narrow beam, highly directional antennas.

HREAP: Local Authentication

When a client associates to a hybrid-REAP access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration.

In order to meet association/authentication timeouts of wireless clients, you can connect HREAP and the controller with a link that can provide less than 100msec latency and 128Kbps throughput. To remove the requirement of 100msec latency on the network connection, local authentication of HREAP is used.

VLAN Select

Integration of the VLAN Select feature in 7.0.114.82 release enables WLAN to be mapped to multiple interfaces using an interface group. Wireless clients associating to this WLAN will get an IP address from pool of subnets identified by the interfaces in round-robin fashion.

This feature extends the current access point group and AAA override architecture where access point groups and AAA override can override the interface group WLAN that the interface is mapped to, with multiple interfaces using interface groups.

This feature also provides the solution to guest anchor restrictions where a wireless guest user at a foreign location can get an IP address from multiple subnets on the foreign locations/foreign controllers from same the anchor controller.

Web Auth Proxy

This feature enables clients that have manual web proxy enabled in the browser to facilitate authentication with the controller. If the user's browser is configured with manual proxy settings with a configured port number as 8080 or 3128 and if the client requests any URL, the controller responds with a web page prompting the user to change the Internet proxy settings to automatically detect the proxy settings. This process prevents the browser's manual proxy settings from getting lost. After configuring this feature, the user can get access to the network through the web authentication policy. This functionality is provided for port 8080 and 3128 because these are the most commonly used ports for web proxy server.

FIPS Support

Cisco Controller Release 7.0.98.0 has been awarded Federal Information Processing Standard (FIPS) 140-2 validation. The following Cisco WLAN controllers and access points have received FIPS 140-2 Level 2 validation: the Cisco 5508 WLAN Controller; the Cisco Wireless Integrated Services Module (WiSM); the Cisco 4400 Series WLAN Controllers; the Cisco 3750G WLAN Controller; the Cisco Aironet Lightweight Access Points: 3502i, 3502e, 1262, 1142, 1252, 1524, 1522, 1131, and 1242. The NIST Security Policies and FIPS certificates for these modules can be downloaded at the NIST website: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

Non-Cisco WGB Support

Starting in release 7.0.114.82, the controller software has been updated to accommodate non-Cisco workgroup bridges so that the controller can forward ARP, DHCP, and data traffic to and from the wired clients behind workgroup bridges. This process is accomplished by enabling the passive client feature. To configure your controller to work with non-Cisco workgroup bridges, you must enable the passive clients feature. All traffic from the wired clients is routed through the work group bridge to the access point.

Reporting Enhancements

The following new reports are available in WCS 7.0.172.0:

- PCI Reports
- Client Traffic Report

PCI Reports

The PCI DSS Compliance report summarizes your Wireless LAN Security components with reference to the Payment Card Industry (PCI) Data Security Standard (DSS) requirements. PCI DSS compliance is required for all merchants and service providers that store, process, or transmit cardholder data. You can find PCI DSS standards at https://www.pcisecuritystandards.org.

Client Traffic Report

This report displays the traffic used by the wireless clients on your network.

Preferred Call Support

The Preferred Call feature enables you to specify highest priority to SIP calls made to some specific numbers. The high priority is achieved by allocating bandwidth to such preferred SIP Calls even when there is no available voice bandwidth in the configured Voice Pool. This feature is supported only for those clients that use SIP based CAC for bandwidth allocation in WCS or WLC.

CDP Over Air

CDP is used between network devices to discover properties of the other end of an interface and the device. When CDP is enabled on an interface, the device sends its properties and interface information to the device at the other end of the interface. This information is useful for debugging and troubleshooting problems in a network. Though revealing the network device information via CDP does not pose significant security risks, some customers are averse to reveal any network information to clients that connect to network.

Media Support Enhancements

The WLAN configuration and template pages have been modified in this release. The 802.11 a/n and 802.11 b/g/n Video Parameter configuration pages have been renamed to 802.11 a/n and 802.11 b/g/n Media Parameter configuration pages and modified to add additional parameters. The controller monitoring feature has been enhanced to include Media Streams. Multicast Direct is a new feature that converts multicast frames to unicast frames in order to ensure multicast delivery of video. On top of Multicast Direct a Resource Reservation system is implemented that will ensure QoS of the video stream.

Caveats

The following sections list open and resolved caveats in Cisco WCS 7.0.172.0 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 7.0.172.0

Table 2 lists the open caveats in Cisco WCS 7.0.172.0.

Table 2 Open Caveats

ID Number	Description
CSCsj23423	The AP template is partially visible when switching between tasks and dates. Symptom: The AP template page is partially visible while switching between task and dates, and the selected dates are not getting refreshed. Conditions: When an already created AP template is opened, the template page is partially visible. Sometimes the AP template page with a faded drop-down menu appears. Workaround: Refresh the page or revisit the link again.
CSCsv34264	An attempt to generate an ID certificate throws an SNMP Error. Symptom: SNMP error thrown while trying to generate ID certificate Conditions: 1. Add a controller to WCS. 2. Choose Configure > Controllers > Security > Ipsec 3. Now, choose the ID certificate option. 4. Choose the paste option. 5. Copy and paste the contents of the .pem file. An error occurs. Workaround: None

Table 2 Open Caveats (continued)

ID Number	Description
CSCsy31225	The left navigation pane of the Access Point Details page disappears. Symptom: Left Navigation Pane disappears for Access Point Detail page, when clicking a Access Point link available under Configure > Controllers > <controller_ip> > Access Points > Cisco APs list page. Conditions: WCS 6.0. Workaround: To navigate to the Controller page from Configure > Access Points > Access Point Detail, click the controller link available for the Registered Controller field.
CSCsm99598	A blank page appears when the ID certificate is downloaded from Configure > Controller > Security > ID Certificate. Symptom: When we download id certificate from configure > controller > Security > ID Certificate, a blank page appears. The certificate download is unsuccessful. Conditions: When we download id certificate from configure > controller > Security > id cert, a blank page appears. The certificate download is unsuccessful. Workaround: ID certificate can be downloaded from controller WEBUI

Table 2 Open Caveats (continued)

ID Number	Description
CSCto27062	WCS import maps feature reports invalid mime type. Symptom: Export Maps: 1. Choose Monitor > Maps > Export Maps from select command. 2. Select all Maps and include map info and calibration. 3. Click Export. Works correctly to export data to .tar file that contains xml data. Import Maps: 1. Choose Monitor > Maps > Import Map > Select XML format and next. 2. Choose file called ImportExportxxxx.tar. 3. Click Next. Conditions: Use Firefox 4.0 and Safari 5. The same errors occur. The following error occurs: `XML Import: 'ImportExport_xxxxxx.tar' has an unsupported Mime Type\n\nMime Type sent by Browser 'application/x-tar'\n\nPossible causes/workarounds\n1. Check File [Associations/Types/Extensions]\n2. Ensure appropriate application launches file\n3. Try a different browser\n4. If File [Associations/Types/Extensions] are correct try closing the browser and relaunch\n\nMaps Import: Supported file format mime types are \n\n'application/gzip-compressed', 'multipart/gzip-compressed', 'multipart/x-zip-compressed', 'application/x-gzip-compressed', 'application/zip', 'multipart/zip', 'application/x-zip-compressed', 'multipart/x-gzip', 'application/x-zip', 'application/gzip', 'application/x-gzip', 'multipart/x-gzip-compressed', 'multipart/gzip', 'multipart/x-zip'\n\n` Workaround: None
CSCto06155	Authenticated client count is incorrect in WCS reports Symptom: Clients that are associated but not authenticated against the anchor controller show as authenticated on the foreign controller. This is misguiding and creates discrepancies in WCS reports. Some WCS reports such as Client Count and Guest Count get client status from foreign controller and total number of authenticated clients count is incorrect. Conditions: WCS 7.0.164.0, MSE 7.0.105, WLC 6.0.199.4 Workaround: None

Table 2 Open Caveats (continued)

ID Number	Description
CSCto19629	Saved search criteria does not save updates. Symptom: While creating a search (client type) and making a change to the criteria, the changes are not saved. It works correctly when you delete and recreate it (in version 5.2). If you want to search for all clients with ssid = guest, you can change it and it will search for that time, but if you go back and select the same search, it goes back and searches with the previous ssid that was mentioned. Conditions: None Workaround: None
CSCto27416	Client associated state search returns disassociated states also. Symptom: When you perform a client search and select associated state only, you get both associated and disassociated states even when you do not select the include disassociated check box. Conditions: None Workaround: None
CSCtf17687	Heatmap does not reflect the option selected from the AP Heatmap page Symptom: Heatmap does not reflect the option selected from the AP Heatmap page Conditions: • When Switching between Avg, and Min AQ values from AP Heatmap menu, heatmap does not change all the time. • Sometimes when going from coverage to AQ, the AQ heatmap does not change unless same option is clicked twice or OK is clicked. Workaround: Sometimes clicking the same option twice changes the heatmap or clicking on OK after selection changes the heatmap accordingly. Alternatively give some time between the selections or wait until the heatmap is completely loaded.
CSCto44190	The controller name masking is not working in the controller audit alarm message. Symptom: For the controller audit alarm that is received via email, the controller name is not masked in the alarm message. Conditions: Whenever there is a configuration mismatch between WCS and controller, performing an audit operation creates an audit mismatch alarm in WCS and corresponding alarm email is sent to the recipient. Workaround: None

Resolved Caveats

Table 3 lists caveats resolved in Cisco WCS 7.0.172.0.

Table 3 Resolved Caveats

ID Number	Caveat Title
CSCsz14861	Virtual Domain broken for maps.
CSCtb65365	The timer for absent data set to 0 everytime log preference changes.
CSCtb91371	Non-root users unable to authenticate for AP timers config list page.
CSCtc49690	Audit mismatch for LAG mode.
CSCtd01625	TLS protocol security update.
CSCtd26408	WCS 4.2.110.0 cannot modify external web auth redirection URL for WLANs.
CSCtd29026	WCS can not create static WEP key with same index number on different WLAN.
CSCtd44718	Add user input required commands to CLI template parser.
CSCtd99328	Migration of Autonomous AP {AIR-AP1131G-A-K9} to LWAPP fails.
CSCte67521	Unable to discover templates from WLC.
CSCte95983	Planning mode does not provide proper data rates for 802.11n.
CSCtf13873	Duplicate IP not reported correctly on WCS under Alarms.
CSCtf17441	Certain APs are missing from the AP Summary Reports.
CSCtf37019	Blind SQL injection in order by clause of Client List screens
CSCtf51758	Session cookie and scripting code issues.
CSCtg26555	WLAN template deletion deleting it from APgroup.
CSCtg29286	Email notification/status change for scheduled guest template fails.
CSCtg33854	Several XSS on different WCS URLs.
CSCtg47863	WCS does not retain key/cert across upgrades
CSCtg97706	Remove the 5 sec option from the auto refresh on the maps.
CSCth35226	Optimization of Client related database queries
CSCth37438	A few WLCs are missing for CLI templates
CSCth53494	Clients/Rogues are not reported in the floor plan for outdoor area.
CSCth59199	RogueRuleGroup has no supported MIB attributes for 7.0.98.0
CSCth60573	Unable to apply WLAN template.
CSCth65673	InSNMPv3, unable to add controllers on WCS and found wrong MAC address.
CSCth70299	untaggedInterfaceWithSamePort error when changing the DHCP server address.
CSCth75384	WCS Audit drops records as their key fields failed validation.
CSCth95281	WCS adds mobility group members using incorrect MAC address.
CSCth97727	WCS not allowing to set Radius auth server shared secret more than 32 characters.
CSCti09924	Port Utilization reports wrong value in WCS report function.
CSCti17527	WCS Guest User Added emails not being sent in 7.0 version.
CSCti28776	WCS map editor may not fully load image.
CSCti35828	WCS > Monitor > Clients > [Select Client] throws error.
CSCti55099	System Error Page on CleanAir dashboard.
CSCti55551	WCS 7.0 Config Guide using old info for General Controller Templates.

Table 3 Resolved Caveats (continued)

ID Number	Caveat Title
CSCti57522	Refresh Config from Controller should pull in Controller Model.
CSCti61213	WCS does not recognize latest series of Client OUIs.
CSCti69432	AP Summary Report in WCS lists incorrect entries under Associated WLANs.
CSCti71639	WCS config group failure report does not contain details for all failure.
CSCti79553	CleanAir dashboard requires WCS Plus licenses.
CSCti79856	The Guest Account template deleted when trying to de-provision it.
CSCti82207	Autonomous AP migration template becomes disabled after first use.
CSCti83182	Discover templates failing after upgrade from version 6.0 to 7.0.
CSCti93778	Option to disable alerts for Aeroscout Engine.
CSCti94038	Alpha WCS HA Failover Event.
CSCti96265	WCS fails to run Adaptive wIPS Alarm report.
CSCti96524	Antennas are missing from WCS.
CSCtj06880	SSID and channel details missing for rogue/ad hoc rogue controller details
CSCtj09965	Default value for max bandwidth on WCS defined as 0.
CSCtj22801	Empty guest report if a pre-configured time interval is selected.
CSCtj26384	WCS not updating SSC after migrating 1230 AP.
CSCtj44949	Heatmaps stop working in WCS 7.x when CleanAir APs are added to heatmaps
CSCtj65183	Monitor lite users are allowed to disable clients
CSCtj67448	Map export changes the unit from meters to feet.
CSCtj67470	Importing a map exported in meters causes incorrect AP location.
CSCtj76743	Error message 'Provision failure: COMMON-1' seen on WCS.
CSCtj78582	Alarms only show the last user that has too many unsuccessful attempts.
CSCtj81907	WCS switchport tracing error COMMON-1.
CSCtj85409	WCS does not set group name to default-group when pushed in templates.
CSCtj85997	Background task shows warning on WLC backup.
CSCtj87130	Issue with Virtual domain permissions.
CSCtj95292	Count in Alarm summary does not match the list.
CSCtk32910	Creating new trap receiver template returns an unexpected internal error.
CSCtk34563	Unable to change the AP height using LWAPP template.
CSCtk35416	Map displays wrong heatmap with concurrent users.
CSCtk63392	WCS 7.0 should allow upgrade from 6.0.196.0.
CSCtk75438	WCS templates to proceed even if error occurs with a single device
CSCtk94155	Planned AP Association fails if using a valid AP ethernet MAC
CSCtl21436	WCS Allows an Interface with the Same IP Address as its Gateway
CSCtl43831	Template columns on Config Group details page no longer sortable
CSCtl71432	WCS does not push guest name with swedish characters to WLC

Table 3 Resolved Caveats (continued)

ID Number	Caveat Title
CSCtl88067	WCS does not save profile name-VLAN mapping when saving AP template.
CSCtn00982	Error when creating Maps or buildings. An error occurs while updating maps.
CSCtn37360	Domainmap images are not deleted when deleting campus or buildings.
CSCtn61887	ACL basic config operation taking more time in JMR.
CSCtn63486	Failed HA registration dbNetcopyThread failed on setPrimaryActive CATCH
CSCtn77970	AIR-ANTM2050D-R not found in the antenna option for AP801AGN
CSCtn79787	Scheduled reports need to execute at scheduled interval than current interval.
CSCtn84937	Duplicated email notification when rogue AP is detected by multiple APs.

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.