Wireless Control System Troubleshooting

Document ID: 70678

Contents

Introduction
Prerequisites
  Requirements
  Components Used
  Conventions
Troubleshoot
  Not Able to Install WCS
  Compatibility Issue Between WLC and WCS Versions
  WCS Fails to Start After Installation in a Non–English Windows 2003 Operating System
  International Characters Not Supported on WCS
  Unable to Start WCS Due to the Corrupted Log Files
  Check the Status of the WCS
  Add a WLC to the WCS
  Refreshing WLC Configuration from WCS
  Firewall Between the WCS and Controller or WCS and the WCS User Interface
  Reset a Controller Back to Factory Defaults using the WCS
  Defragmenting WCS Database
  Check if you have the Appropriate License for the WCS Software
  Use the Security Summary Page for Troubleshooting
  Detect and Locate Rogue Access Points

Use the Access Point (AP) Impersonation Feature on the WCS
  Locate Clients
  Coverage Holes in a WLAN Network
  If you have Difficulties when you Import Maps
  Ping a Network Device from a Cisco WLC
  View Current Cisco WLC Status, Configurations, and Statistics
  Inspect Location Readiness
  Synchronization Issues with the WCS and Location Servers
  Synchronization Issues with the WCS and WLC
  DHCP Configuration Corrupted when Template is Pushed from WCS to WiSM
  WCS Heat Maps Show Incorrect Square Coverage Holes
When does the Rogue AP Template get Applied to the WLC?
  Ports on the WCS Server
  Verify WLANs are set to exclusive–list enable
  Troubleshoot exclusive–list enable
  View and Delete Globally Disabled Clients
  View and Delete Manually Disabled Clients per Controller
  WCS Search for Clients Per Building does not Work
  WCS Reports Incorrect Client Counts Associated to APs in H–REAP Mode
  WCS does not Start if Underscore is Configured in Server/Hostname
  The Error Message "The Procedure Entry Point_FIIfexp_Could Not be Located in the Dynamic Link Library DFORRT.DLL" Displays
  Instructions to Synch the Three Devices
Related Information

Introduction

This document provides troubleshooting procedures for basic problems with the Cisco Wireless Control System (WCS).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of how to configure the Cisco WCS
- Knowledge of how to configure a wireless LAN (WLAN) with the WLAN Controllers (WLCs) and lightweight access points (LAPs)

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Troubleshoot

Not Able to Install WCS

If you experience problems when you try to install WCS, first check to see if the system on which you plan to install WCS meets the minimum system requirements.

This is the prerequisite checklist to use before you install Cisco WCS:

1. Check if the system on which you are about to install the Cisco WCS meets the necessary hardware and software requirements for Cisco WCS. For information on the minimum software and hardware requirements for the installation of the WCS, refer to the System Requirements section of Cisco WCS Configuration Guide, Release 4.0.

2. Ensure that you have updated your system with the necessary critical updates and service packs. Refer to the latest release notes for information on the service packs and patches required for correct operation of the WCS.

   Note: Before you install the WCS on Linux, a full install of Red Hat Linux is required.

3. Backup the existing WCS database. Refer to Backing Up the WCS Database for information on how to perform a Windows backup.

4. Uninstall the older version of the WCS. Refer to Uninstalling Cisco WCS for information on how to perform an uninstall.
Once you ensure that you have the prerequisites, you can install the WCS. Refer to Installing WCS for Windows for information on how to install Cisco WCS for Windows.

Note: WCS only runs on 32-bit Windows; 64-bit operating system installations are not supported.

Refer to Installing WCS for Linux for information on how to install the WCS on Linux.

**Compatibility Issue Between WLC and WCS Versions**

When you install WCS to manage the WLCs, ensure that the WCS and WLC versions are compatible. This information is available in the release notes of the WCS version that you install.

For example, Cisco WCS 5.1.64.0 supports management of these wireless LAN controllers:

- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 5.0.148.0
- 5.1.151.0

This information is available in this document: Release Notes for Cisco Wireless Control System 5.1.64.0 for Windows or Linux

If you use incompatible versions of WCS and WLC, you will not be able add your WLCs to the WCS.

**WCS Fails to Start After Installation in a Non–English Windows 2003 Operating System**

This occurs because WCS is supported only in Windows 2003 with English or Japanese versions. If you use operating systems translated to other languages, it causes WCS to fail after installation. In order to avoid this, use WCS on Windows 2003 English or Japanese versions.

**International Characters Not Supported on WCS**

WCS and location appliances do not support international characters in general. If you use non–English characters for map names, asset information, etc., it can generate display errors (wrong characters displayed) and errors on search functions.

**Unable to Start WCS Due to the Corrupted Log Files**

Sometimes we are not able to start WCS and open its web interface. Even if you try to open WCS with the ".exe" file in the WCS\bin\ folder, it can fail. This message can display while you try to start WCS.

```
Starting WCS
Checking for Port 21 availability... OK
Checking for Port 8456 availability... OK
Checking for Port 8457 availability... OK
..............................
..............................
..............................
```


Starting database server ...

The Nms_Server service is starting........
The Nms_Server service could not be started.

The service did not report an error.

More help is available by typing NET HELPMSG 3534.

Failed to start WCS server.

One possible reason for this issue can be the bug CSCse17963 (registered customers only).

As per this bug, WCS database can fail to start because of corrupted log files. In order to resolve this issue, go to the subdirectory **standalone** through the path **webnms\eval_kit\standalone** within WCS directory. In that subdirectory, find the highest numbered **sol####.log file**, where #### is a four digit number. Delete it and reboot the server. Attempt to start WCS. If WCS does not start, repeat for the next sol###.log file, and so on. This workaround will resolve the issue.

**Check the Status of the WCS**

If the WCS does not function as expected, first check the status of the WCS. Complete these steps in order to check the status of the WCS when it is installed as a Windows application or Windows service. You can check the status at any time.

1. Log into the system as administrator.
2. Perform one of these actions:
   - Go to the Windows Start menu and choose **Programs > Wireless Control System > WCSStatus**.
   - From the command prompt, navigate to the WCS installation directory (C:\Program Files\WCS32\bin) and enter **WCSAdmin status**.

The WCSAdmin window appears and displays messages that indicate the status of the WCS:

![WCSAdmin Window](image)

3. Click **Close** in order to close the WCSAdmin window.
If the WCS is installed on a Linux system, complete these steps in order to check the status of the WCS:

1. Log into the system as root.
2. Use the Linux CLI in order to perform one of these tasks:
   - Navigate to the `/opt/WCS32` directory (or the directory chosen during installation) and enter `. /WCSStatus`.
   - Navigate to the `/opt/WCS32/bin` directory and enter `WCSAdmin status`.
   The CLI displays messages that indicate the status of the WCS.

Add a WLC to the WCS

When a new WLC is added to the WCS, ensure that the SNMP version configured on the controller matches with the SNMP version on the WCS. If the versions do not match, the WCS does not detect the controller and this error appears on the WCS:

No response from device, check SNMP.

Also ensure that SNMP write access privilege is enabled on the controller. If you enter read-only access parameters then the controller is added to the WCS, but the WCS is not able to modify the configuration on the controller.

In summary, check these items if there is a problem adding the controller to the WCS:

- The controller service port IP address might be set incorrectly. Check the service port setting on the controller.
- The WCS might not be able to contact the controller. Make sure that you can ping the controller from the WCS server.
- The SNMP settings on the controller might not match the SNMP settings that you entered in the WCS. Make sure that the SNMP settings configured on the controller match the settings that you entered in the WCS.
- When you upgrade the WCS to the latest version, you need a license from Cisco. If your WCS is not licensed, you are not able to add a new WLC. In order to obtain a license, you need to call TAC Support.

Note: If you make any changes on the WCS, then make sure you forward the changes to your controllers. Then refresh the configurations of the controller in order to make it up to date. See the Refreshing WLC Configuration from WCS section of this document to know how to refresh WLC from the WCS.

Refreshing WLC Configuration from WCS

Perform these steps in the WCS in this order to refresh the controller configuration from WCS.

1. Choose `Configure > Controllers`.
2. The Controllers page lists all the added WLCs. From the list of WLCs, choose the WLC to be refreshed.
3. In the resultant controller page, from the `Select a command` drop-down menu, choose `save configuration to flash` and click `Go`.
4. After the configuration is saved in Flash, you receive a successful message on the screen. After the successful screen appears, choose the same controller whose configuration was saved to Flash and, on the `Select a command`, choose `Refresh config from controller`.
5. This prompts you to retain or delete the old configuration. Choose `Delete` and press `OK`.
Firewall Between the WCS and Controller or WCS and the WCS User Interface

When a WCS server and a WCS user interface are on different sides of a firewall, they cannot communicate unless these ports on the firewall are open to two-way traffic:

- 80 (for initial http)
- 69 (tftp)
- 162 (trap port)
- 443 (https)

Open these ports in order to configure your firewall to allow communications between a WCS server and a WCS user interface.

Reset a Controller Back to Factory Defaults using the WCS

Complete these steps to reset the controller to factory defaults using the WCS:

1. Choose Configure > Controllers in order to display the All Controllers page. This page lists all of the controllers that are discovered by the WCS.

2. Click on the IP address of the controller that you want to reset to factory defaults. The Controller Properties window appears.

3. From the left side menu, choose System > Commands.

The Controller Commands window appears.
4. Under Administrative commands select **Reset to factory default** and click **Go**.
5. Choose **Reboot** from the Administrative Commands menu in order to reboot the controller without saving the configuration on the controller. This resets the controller to factory defaults.

   **Note:** Once the controller is reset to factory defaults, the WCS is not able to discover the controller unless it is configured with the management IP address. For this, you need to configure the controller using the start up configuration wizard on the controller.

### Defragmenting WCS Database

All regular WCS operations, such as the deletion of alarms, events, adding/deleting controllers, etc. involve SQL operations internally with the WCS database (DB). Such internal SQL operations naturally increase the database size, which, in turn, have an impact on the performance of WCS.

For example, a delete operation in WCS leaves empty space in the deleted portions of the database. This can result in the discontiguous location of data in the database, which, in turn, affects the WCS performance. Defragment WCS database to overcome this issue.

Defragmentation makes all used and unused space contiguous. The contiguous unused/unused space improves...
performance. If you defragment the database, you can reclaim allocated but unused disk space. A database defragmentation can be beneficial if free disk space on the system runs low due to a large database size or if the response time of the WCS application is noticeably slower when data is requested from it.

In order to perform defragmentation manually in WCS, stop the WCS application. In order to do this, click Start > Programs > Wireless Control System > Stop WCS. Then open a command line box, change to the C:\Program Files\WCS4.0\bin directory (the default directory where WCS is installed), and run the command DBAdmin defrag. This initiates the defragmentation process. Once the process is completed, restart WCS with the Start > Programs > Wireless > Control System > Start WCS operation.

**Note:** Defragmentation works automatically after the database restores. Still, in some cases, manual defragmentation is done to free up some disk space. A manual defrag is not really necessary. That space likely is regained within a few days when WCS starts to create and delete alarms.

### Check if you have the Appropriate License for the WCS Software

Cisco Unified Wireless Network Software Release 4.0 enforces software–based licensing. Customers are prompted to enter license certificates by all new Cisco WCS SKU families (except the Cisco WCS Demonstration License). Current customers that migrate to release 4.0 are also affected by licensing. Cisco WCS licensing enforcement is tied to these parameters:

- **Host name** The host name of the Cisco WCS server is now required during the registration process. Licenses issued are tied to the original host name designated during the registration process.
- **Feature option** The Cisco WCS feature option purchased, Base or Location, is now tracked by the Cisco WCS licensing system.
- **Access points** The number of access points supported in set increments of 50, 100, 500, 1000, or 2500 is now tracked by the Cisco WCS licensing system.
- **Demonstration license** This free, location–enabled Cisco WCS demonstration license supports 10 access points for up to 30 days.

Refer to the Cisco WCS Licensing and Ordering Guide for more detailed information about the Cisco WCS license and the different types of licenses available.

Select the correct license based on your deployment situation, the number of access points to be supported, and Cisco WCS options (Base or Location). All SKUs within a SKU family can be combined with equivalent option levels such as Base–to–Base or Location–to–Location. Unequal option levels (Base and Location) cannot be mixed. Only one type of license can be used on the WCS at one time.

For example, if your computer has a location license, you cannot add a base license. You can add to the current license by purchasing a license to increase the access point count. For example, if you have a location license with an access point count of 50 and in a year you need to add more access points, you can buy another location license with an access point count of 100, apply it to the WCS, and have a WCS with a location license for 150 access points. You can add a license to increase the number of access points in increments of 50, 100, 500, 1000, 2500, or unlimited.

If you have a base license and want to upgrade to a location, you need to purchase a location upgrade license. You need to purchase a location upgrade license equivalent to the total number of access points with a base license. For example, if you have three base licenses with support for 50, 100, and 200 access points (for a total of 350 access points), you must purchase a single location upgrade license with support for 350 access points.

All Cisco WCS SKUs require a PAK certificate to register the Cisco WCS license. The PAK is a paper certificate sent via U.S. mail from Cisco Systems upon purchase of the Cisco WCS license. The PAK certificate allows customers to receive a Cisco WCS license. It is used to register the Cisco WCS and generate
license files. All customers must go to the PAK registration site listed on their PAK certificate to complete their Cisco WCS registration. The PAK certificate provides clear instructions on how to complete the Cisco WCS licensing process.

All customers that purchase Cisco WCS from Cisco.com via download or CD must activate their Cisco WCS license by registering at the PAK site. Customers will receive the PAK via U.S. mail. Cisco WCS is not activated until the PAK registration process is completed. Refer to WCS Licenses for information on how to install and manage a WCS license.

**Use the Security Summary Page for Troubleshooting**

The Security Summary page provides the user with information about all security related events. This page provides information about rogue access points, information on signature attacks, information on attacks on the access points, and information related to client security.

This page is an effective troubleshooting tool specifically if the problem is related to security threats. This page also provides information on the most recent security alerts.

Here is an example of the Security Summary page:

**Detect and Locate Rogue Access Points**

When the Cisco LAPs are powered up and associated with Cisco WLCs, the Cisco WCS built into the Operating System immediately starts to listen for rogue access points. When a Cisco WLC detects a rogue access point, it immediately notifies Cisco WCS, which creates a rogue access point alarm. WCS considers any access point which is not part of its wireless network as a rogue access point.
When Cisco WCS receives a rogue access point message from a Cisco WLC, Cisco WCS generates an alarm, with an indicator visible in the lower left corner of all Cisco WCS User Interface pages. This example shows 72 Cisco WCS rogue access point alarms.

Complete these steps in order to detect and locate rogue access points:

1. Click the **Rogues** indicator in order to display the Rogue AP Alarms page. This page lists the severity of the alarms, the rogue access point MAC addresses, the rogue access point types, the date and time when the rogue access points were first detected, and their SSIDs.

2. Click any Rogue MAC Address link in order to display the associated Alarms > Rogue – AP MAC Address page. This page shows detailed information about the rogue access point alarm.
3. Choose one of these commands from the Select a Command menu and click **GO** in order to modify the alarm.

- **Assign to me** Assigns the selected alarm to the current user.
- **Unassign** Unassigns the selected alarm.
- **Delete** Deletes the selected alarm.
- **Clear** Clears the selected alarm.
- **Event History** Enables you to view events for rogue alarms.
- **Detecting APs** (with radio band, location, SSID, channel number, Wired Equivalent Privacy (WEP) state, short or long preamble, Receive Signal Strength Indicator (RSSI), and SNR) Enables you to view the access points that currently detect the rogue access point.
- **Rogue Clients** Enables you to view the clients associated with this rogue access point.
- **Set State to `Unknown − Alert'** Tags the rogue access point as the lowest threat, continues to monitor the rogue access point, and turns off containment.
- **Set State to `Known − Internal'** Tags the rogue access point as internal, adds it to the known rogue access points list, and turns off containment.
- **Set State to `Known − External'** Tags the rogue access point as external, adds it to the known rogue access points list, and turns off containment.
- **1 AP Containment through 4 AP Containment** When you select level 1 containment, one access point in the vicinity of the rogue unit sends deauthenticate and disassociate messages to the client devices that are associated to the rogue unit. When you select level 2 containment, two access points in the vicinity of the rogue unit send deauthenticate and disassociate messages to the rogue's clients and so on up to level 4. That is, the access point chosen for containment prevents clients from communicating to the rogue access point. This effectively neutralizes the function of the rogue access point.

4. Go to the Select a Command drop-down menu, choose **Map (High Resolution)** and click **GO** in order to display the current calculated rogue access point location on the Maps > Building Name > Floor Name page.
If you use WCS Location, WCS compares the RSSI signal strength from two or more access points in order to find the most probable location of the rogue access point and places a small skull–and–crossbones indicator at its most likely location. In the case of an under–deployed network for location with only one access point and an omni antenna, the most likely location is somewhere on a ring around the access point, but the center of likelihood is at the access point.

Here is an example that shows a rogue access point on a map:

If you use WCS Base, WCS relies on RSSI signal strength from the rogue access point and places a small skull–and–crossbones indicator next to the access point that receives the strongest RSSI signal from the rogue unit.

With the location appliance, rogues can be tracked, are shown in the Monitor > Map drop–down menu, and have the Show Rogue AP and Show Rogue Clients options. Without the location appliance, these options are not present, and you can only see the location of the rogues when you go to the rogue alarm and select the MAP (high resolution) command from the drop–down menu.

On the WCS Base, the rogue is shown next to the detecting AP (not the closest), without location information. For more detailed information on the features that are supported in WCS Base and WCS Location, refer to Comparison of WCS Base and WCS Location.

Note: Firmware release 4.0 has Cisco bug IDs CSCse96812 (registered customers only) and CSCsf17545 (registered customers only) that always show rogue client counts at zero in the rogue access point list. The workaround for this problem is to see the rogue access point list directly on the controller for correct counts.
Use the Access Point (AP) Impersonation Feature on the WCS

The AP Impersonation feature improves the detection of rogue APs that attempt to impersonate valid Cisco 1000 Series LAPs. This feature creates a radio frequency (RF) network group, and the Cisco 1000 Series LAPs in the same group distribute radio resource management (RRM) neighbor packets to each other. If a Cisco 1000 Series LAP hears packets from another Cisco 1000 Series LAP from which it has not received any RRM neighbor packets, then the Cisco 1000 Series LAP can assume that the new AP is impersonating a Cisco 1000 Series LAP and therefore reports it as a rogue AP.

When the WCS finds an AP that attempts to impersonate another AP on the WLAN, you see this alert on the WCS server:

```
AP Impersonation with MAC '00:14:1b:62:4e:42' is detected by authenticated AP '00:14:1b:62:4e:40' on '802.11b/g' radio and Slot ID '0'
```

On the controller, this trap log message shows the source MAC address that causes the issue:

```
```

Refer to Cisco bug ID CSCsbf90622 (registered customers only) for more information on AP impersonation related WCS error logs.

AP impersonation is reported by IDS when you see an AP that advertises a Cisco MAC address that does not communicate through Lightweight Access Point Protocol (LWAPP) or Wireless LAN Context Control Protocol (WLCCP). In the LWAPP model, WCS can map an approximate location of a rogue AP from the controller interpretation of all AP readings.

**Locate Clients**

The Cisco WCS allows system operators to locate clients in the enterprise. Complete these steps:

1. Choose **Monitor > Devices > Clients** in order to navigate to the Clients Summary page.
2. On the Clients Summary page, in the left sidebar, search for All Clients in order to have Cisco WCS display the Clients page.
From the Clients page, click the User Name of the client you want to locate. Cisco WCS displays the corresponding Clients <client name> page.

3. From the Clients <client name> page, you have two choices for locating the client:

- In the drop-down menu, select **Recent Map** (high/low resolution) in order to locate the client without disassociating it.
- In the drop-down menu, select **Present Map** (high/low resolution) in order to disassociate and then locate the client after reassociation. If you make this choice, Cisco WCS displays a warning message and asks you to confirm that you want to continue. Here is an example:

4. From the Clients <client name> page, you have two choices for locating the client:

- In the drop-down menu, select **Recent Map** (high/low resolution) in order to locate the client without disassociating it.
- In the drop-down menu, select **Present Map** (high/low resolution) in order to disassociate and then locate the client after reassociation. If you make this choice, Cisco WCS displays a warning message and asks you to confirm that you want to continue. Here is an example:
Refer to this illustration for a Heat Map that shows client locations.
Note: Cisco WCS Location compares RSSI signal strength from two or more Cisco 1000 Series LAPs in order to find the most probable location of the client, and places a small Laptop icon at its most likely location. Cisco WCS Base compares RSSI signal strength from the client, and places a small Laptop icon next to the Cisco 1000 Series LAP that receives the strongest RSSI signal from the client.

Note: Usually, when you shut down your laptop, it takes a long time (in minutes) before the WLC or WCS removes the client from the Clients list. It continues to show "associated". This is because there are two timers that control the users association information called Idle Timeout and Session Timeout. Both of these timers can be changed. These are the default timers:

- **Idle Timeout** (300 seconds)
- **Session Timeout** (1800 seconds)

**Coverage Holes in a WLAN Network**

Coverage holes are areas where clients cannot receive a signal from the wireless network. The Operating System Radio Resource Management (RRM) identifies these coverage hole areas and reports them to Cisco WCS. This allows the IT manager to fill holes based on user demand.

When Cisco WCS displays the Top 5 Coverage Holes, click the **Coverage** indicator on the bottom left of the Cisco WCS User Interface page (or choose **Monitor > Alarms** and then search for **Alarm Category − Coverage**) in order to have Cisco WCS display the Coverage Hole Alarms page. On the Coverage Hole Alarms page, choose **Monitor > Maps** and then search for Access Points by Cisco 1000 Series LAPs Name...
(this search tool is case-sensitive). Cisco WCS displays the Maps > Search Results page, which lists the Floor or Outdoor Area where the Cisco 1000 Series LAP is located. Click the link to display the related Maps > <building name> > <floorname> page.

On the Maps > <building name> > <floor name> page, look for areas of low signal strength near the Cisco 1000 Series LAP that reported the coverage hole. Those are the most likely locations of coverage holes. If there do not appear to be any areas of weak signal strength, make sure that the floor plan map is accurate. Also, if you have used the Floor Plan Editor to create .FPE files, that you have not left out any metal obstructions, such as walls, elevator shafts, stairwells, or bookcases. If so, add them to the .FPE floor plan file and replace the old floor plan with the new floor plan.

### If you have Difficulties when you Import Maps

Cisco WCS enables the user to view the managed WLAN network on realistic campus, building, and floor plan maps. You can import the floor, campus, or building plan to the Cisco WCS as an image file and you can add devices at the appropriate locations. Cisco WCS supports these image types:

- .PNG format
- .JPG format
- .JPEG format
- .GIF format

If you face an issue when you import maps to Cisco WCS, it could be due to an unsupported image format. In order to resolve this issue, open the image with Microsoft Paint and save the file as `<filename>.GIF`. Then try to import the image again.

At times, the imported image file can display in WCS with very poor quality, even though the original image file is of high quality. One possible reason for this problem is with the image itself. WCS incorporates the white space that surrounds the image under the assumption that it is part of the map; this can lead to poor display quality in the WCS map editor. Try to crop the image file to remove the white space and then import the new image into WCS.

Refer to Adding and Using Maps for detailed information on adding maps to the Cisco WCS.

### Ping a Network Device from a Cisco WLC

Complete these steps in order to ping other devices from a Cisco WLC:

1. Choose **Configure > Controllers** and click an IP address under the IP Address column to have Cisco WCS display the <IPaddress> > Controller Properties page.
2. On the <IPaddress> > Controller Properties page, go to the left sidebar and choose **System > Commands** to have Cisco WCS display the <IPaddress> > Controller Commands page.
3. On the <IPaddress> > Controller Commands page, choose **Administrative Commands > Ping** from Switch and click **GO**.
4. In the Enter an IP Address (x.x.x.x) to Ping window, enter the IP address of the network device that the Cisco WLC is to ping, and click **OK**.
5. Cisco WCS displays the Ping Results window which shows the packets sent and received. Click **Restart** in order to ping the network device again, or click **Close** in order to stop pinging the network device and close the Ping Results window.
View Current Cisco WLC Status, Configurations, and Statistics

After you add Cisco WLCs and Cisco 1000 Series IEEE 802.11a/b/g LAPs to the Cisco WCS database, you can view the Cisco WLAN Solution status.

Note: When you search for clients or tags without a location appliance, you need to specify WLC Controllers in the WCS database. This is because the WCS always defaults to "location servers".

Note: The WCS application must be manually stopped/shutdown before you make any changes to the server IP address. If you reboot the server without stopping the application, then there are chances that the database might get corrupted.

In the Cisco WCS User Interface, choose **Monitor > Network** in order to display the Monitor Network Summary. Here is an example:

![Cisco WCS Network Summary](image)

Cisco WCS periodically collects statistics, such as RSSI, SNR, profile failures, client counts, rogue access point trends, and busy clients, and organizes them into reports. Use the **Monitor > Reports** windows in order to view these reports.
Here is an example of the client count report for the 802.11a/b/g clients for the last seven days:

These reports can also be used as an effective troubleshooting tool.

**Inspect Location Readiness**

The Inspection of Location readiness is a feature introduced in Location Appliance version 2.1.34.0. With this feature, WCS can verify the ability of the existing access point deployment to estimate the true location of an element within 10 meters at least 90% of the time. The Location readiness calculation is based on the number and placement of access points.

In order to inspect Location readiness from WCS, choose **Inspect Location Readiness** from the menu found on the Monitor > Maps page. A color-coded map appears that shows those areas that do (Yes) and do not
Synchronization Issues with the WCS and Location Servers

Sometimes there might be problems with the WCS getting synchronized with the location appliance. The network diagram in the WCS might not synchronize with the location appliance. There are quite a few reasons for this synchronization problem.

- The size of the network design might have exceeded the maximum limit of 30 Mb. Cisco bug ID CSCse60657 (registered customers only) addresses this issue more clearly.

  Hence, while you attempt to synchronize a campus diagram whose overall size, including the number of buildings inside that campus and the number of floors on each building, on a whole might have exceeded the maximum limit of 30 Mb, this synchronization process fails.

  This problem can be further verified when you view the logs of the location appliance for this message.

    TRACE[com.aes] THROW com.aes.server.cmn.AesServerException:  
    Server Exception: Message size exceeded: 37176782

  This limitation in size is overcome in the upcoming WCS version.

- Another possible reason is that the resolution of the image loaded into the WCS is too high, and probably exceeds the acceptable resolution of 1024x768. While trying to synchronize such an image with the location appliance, the synchronization process fails. In such cases, reduce the resolution in order to help this issue.

- Ensure that you run the latest version on your WCS and location server. Also ensure that the time and date match exactly on all the devices.

  This can be verified when you look at these outputs.

    ♦ Output of the date and time command on the WCS
    ♦ Output of the date on the locserver
    ♦ Output of the show time command on the WLC

- Another possible remedy is to stop the location−server, and remove the database using this command at the location server console:

    rm −rf /opt/locserver/db/linux/server−eng.db where /opt/locserver/db/linux/server−eng.db is the directory for location−server db.

  Restart the location server with the command /etc/rc.d/init.d/locserver restart.

  Then try to resynchronize the devices.

Synchronization Issues with the WCS and WLC

Synchronization problems might occur between the WCS and the WLC. Because of this issue, the number of active clients might be different on the WLC and the WCS. In order to synchronize the controllers and the WCS, complete these steps:

1. Choose Configure > Controllers, and click the check box at the top of the IP Address list to choose all controllers.
2. From the Select a Command drop−down list, choose Save Config to Flash.
3. Click OK.
This is a basic test to verify that SNMP works correctly, and the controllers will do as the WCS tells them.
4. Choose **Configure > Controllers**, and click the check box at the top of the IP Address list to choose all controllers.
5. From the Select a Command drop-down list, choose **Refresh Config from Controllers**.
6. Click **OK**.

This action tells the WCS to believe the new information from the controllers over anything it previously had known.

**DHCP Configuration Corrupted when Template is Pushed from WCS to WiSM**

When a general template is pushed from the WCS to the Wireless Services Module (WiSM), the Dynamic Host Configuration Protocol (DHCP) configuration in the controller becomes corrupted. The template can have exactly the same options that are present in the WiSM.

The main effect is that DHCP offer messages are dropped, so clients do not receive a DHCP address. This message is logged in the controller:

```
Thu Jul 13 05:05:07 2006 [VERBOSE] dhcpd.c 164: Dropping packet from 192.168.80.23 (unable to match to a dhcp scope)
```

This problem is due to Cisco bug ID CSCse98623 (registered customers only). Do not use general templates in the WCS. The configuration has to be restored manually in order to recover the DHCP forwarding. This bug is fixed in WCS firmware version 4.0.87.0 and later.

**WCS Heat Maps Show Incorrect Square Coverage Holes**

WCS Heat Maps show incorrect square coverage holes. The coverage holes should never be square or rectangle. The heat map radiation pattern is circular. This issue is a specific square hole on the map, which should not be possible. No trace editing has been performed on the map. With the use of a site surveyor tool, it is verified that no coverage hole exists. The connection is very strong in these areas.

This is related to Cisco bug ID CSCsf19291 (registered customers only). Choose the option **Recompute Prediction** from the drop-down menu and recompute the prediction. The heat map becomes circular and no square coverage holes exist. This issue is fixed in version 4.0, but if you migrate from version 3.0 then the issue might exist for small size floors.

**When does the Rogue AP Template get Applied to the WLC?**

The rogue access point (AP) template gets applied to the controller only if these two conditions are true:

- The AP on that controller has discovered the rogue AP.
- The rogue AP schedule task is completed.

**Ports on the WCS Server**

When you run a firewall on the server where the WCS application runs, you need to open up some ports in order to communicate with the WLC. There are some services that run on the WCS servers such as Apache.exe, JavaService.exe, and Solid.exe. In TCPView, the output appears similar to this output:

```
Apache.exe:1712 TCP 0.0.0.0:443 0.0.0.0:0 LISTENING
JavaService.exe:1680 TCP 0.0.0.0:21 0.0.0.0:0 LISTENING
```
In order to work with the WLC, open up only a few ports like UDP 161 (SNMP), UDP 162 (SNMP Trap), and TCP 443 (HTTPS). This table shows a list of ports which might be useful if some of the traffic is blocked.

<table>
<thead>
<tr>
<th>Service</th>
<th>Ports</th>
<th>Port Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>UDP</td>
<td>161</td>
</tr>
<tr>
<td>SNMP Trap</td>
<td>UDP</td>
<td>162</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
</tr>
<tr>
<td>Advent Net</td>
<td>TCP</td>
<td>2000</td>
</tr>
<tr>
<td>Database</td>
<td>TCP</td>
<td>1315</td>
</tr>
<tr>
<td>FTP</td>
<td>TCP</td>
<td>21</td>
</tr>
<tr>
<td>HTTP Connector</td>
<td>TCP</td>
<td>8457</td>
</tr>
<tr>
<td>HTTP Connector Redirect</td>
<td>TCP</td>
<td>8457</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP</td>
<td>80</td>
</tr>
<tr>
<td>RMI</td>
<td>TCP</td>
<td>1299</td>
</tr>
<tr>
<td>TFTP</td>
<td>UDP</td>
<td>69</td>
</tr>
<tr>
<td>Web Container</td>
<td>TCP</td>
<td>8009</td>
</tr>
</tbody>
</table>

**Verify WLANs are set to exclusive-list enable**

Complete these steps in order to verify that WLANs are set to `exclusive-list enable`.

1. Choose **Configure > Controller**.
2. Click on an IP address under the IP Address column.
3. Click **WLAN** on the left.
4. Click on each WLAN ID in order to verify that it is not set to **Checked**.

**Troubleshoot exclusive-list enable**

Complete these steps in order to troubleshoot `exclusive-list enable`.

1. Track the client.
2. Verify the WLAN for the exclusion client.
3. Select the exclusive client to **Delete**.
4. Delete the clients from the exclusive-list under the specified controller.

**View and Delete Globally Disabled Clients**

Complete these steps in order to view and delete globally disabled clients.

1. Choose **Monitor > Devices > Clients**.
2. Click **Manually Disabled Clients**.
3. Select the MAC Address to access this page.
4. Click **Delete**.

**View and Delete Manually Disabled Clients per Controller**

For security purposes and several other reasons, certain clients can be blacklisted as "Manually Disabled Clients".

Complete these steps in order to view manually disabled clients individually on each controller added to the WCS:

1. Go to the WCS GUI.
2. Choose **Configure > Controllers**.
3. Click on the IP address under the IP Address column for the controller to which manually disabled clients need to be viewed.
4. On the page that appears, choose **Security** and click **Manually Disabled Clients** in order to display the list of Manually Disabled Clients for this particular controller.

From the drop-down menu on the left, choose **Delete Manually Disabled Clients** in order to delete manually disabled clients.

**WCS Search for Clients Per Building does not Work**

This problem can be due to Cisco bug ID CSCse97619 (registered customers only). A WCS search for clients on a floor on a building works correctly, but a search for clients on all floors in a building does not work. The fix for this bug is available with WCS version 4.0.87.0. If you use WCS versions earlier than 4.0.87.0, the workaround is to search for clients in a floor area.

**WCS Reports Incorrect Client Counts Associated to APs in H–REAP Mode**

This problem is due to Cisco bug ID CSCsg48059 (registered customers only). WCS reports client counts that are way too high when H–REAP is enabled on the controller. The workaround to find out how many clients are associated to the APs or the given controller is to use the WCS Monitor > Clients feature, search by the AP or controller, which is limited by the radio type to avoid duplicates, and use the total number of items found as your true population number. The bsnMobileStation table also has the correct number of rows for the number of clients. You can also use the WLC to find the correct client count.

**WCS does not Start if Underscore is Configured in Server/Hostname**

Underscore characters '_' are not supported in the WCS server name. If you use an underscore in the Server/Host name on a WCS installation, WCS fails to start. The installation of the software does not report any issues and installs as normal, but the RFC–952 states that the underscore is an unsupported character, which is why this causes the WCS software to fail.


It is essential that the controllers, location servers, and WCS all use Network Time Protocol (NTP) to ensure accurate local time. The location server drops any date from the controller that is outside of its 15 minutes window.
The controller keeps only one time internally but modifies it for display if an offset is specified. If you specify an offset, you tell the controller that the time which was entered was UTC time [local time for London, UK] and that you want the controller to display your local time with the addition of the offset. NTP is always in UTC time, and an offset is required if you want the controller to display it in your local time. For example, EST has an offset of −5. If you have NTP configured, the controller gets UTC time but adds the offset to get local time for the timestamps in the logs.

The controller, location server, and WCS must all be within 15 minutes internal time (not local time [internal time with offset]), or the location server does not display or track clients; instead it shows this error message in the location server log:

```
Failed as the RSSI list is empty after time pruning
```

The location server only has enough real time storage for the last 15 minutes of stored data. Remember that the location server tracks clients in real time, while the WCS archives the data over longer periods of time. WCS can track clients but updates only every few minutes – not real time. If the clocks are off between the devices, there is no client data after the location server removes the ones outside the specified time interval in the request. In fact, if the location server receives data from the controller with the internal timestamp more than 15 minutes outside its internal time, it tosses the data into the bit bucket.

You must turn on NTP for the WLC, WCS, and location server to automatically synchronize the internal time to UTC.

**The Error Message "The Procedure Entry Point_FIIfexp_Could Not be Located in the Dynamic Link Library DFORRT.DLL" Displays**

If WCS uses a third party application, such as MATLAB Compiler, and MATLAB uses a specific version of the DFORRT.dll library, when an application has already installed the DFORRT.dll library in c:\windows\system32, the WCS is not correctly installed. As a result, when you start WCS, this error message displays:

```
The procedure entry point _FIIfexp_ could not be located in the dynamic link library DFORRT.DLL
```

In order to correct the problem, remove the DFORRT.dll file in c:\windows\system32 and reinstall WCS.

**Instructions to Synch the Three Devices**

**For the location server:** Refer to the Installation and Configuration Guide for information within the initial configuration.

After the appliance is started, you must stop the location server before you can change the date, time, or time zone. Follow these steps:

1. In order to change the location appliance time zone, copy the appropriate time zone file to /etc/localtime:

   ```
   # cp /usr/share/zoneinfo/<your country>/<your timezone> /etc/localtime
   ```

2. Verify that the file /etc/sysconfig/clock is defined as is this without any ZONE specified:

   ```
   # more /etc/sysconfig/clock
   UTC=true
   ARC=false
   ```

3. Verify the date and time with the `date` command on the location server CLI.
4. Restart the location server with the instructions available at

**Note:** If you want to use the NTP server for the location appliance, refer to Configuring NTP Server.

**For the WCS:** WCS relies on Windows for the correct time. It checks the Windows OS once every 24 hours for the system time. It does not immediately know about system time changes unless you stop and re−start the WCS server. Right click the clock and choose change time/date. Use an NTP time source to set the clock and manually set the offset for your timezone. Typically this is already set.

**For the Controller:** On the controller, use the CLI command `show clock` to verify the time and offset. You can do this through the GUI, as well. Uncheck the DST checkbox or use the command `config time timezone disable −8 0 −8 0`.

After you finish the time synchronization between the devices, you need to synchronize the location server with the WCS (under `location−server > synchronize`). This is done so that they have the same data with the same timestamps.

Notice that the WCS, controller, and location software are released on the same date.

**WLAN Template Does not Apply the Correct "Broadcast SSID" Setting in the WLC**

After you create WLAN templates and load them into the WLC through WCS, the "Broadcast SSID" field remains checked in the individual controller WLAN configuration screen, regardless of the setting in the WCS WLAN template. This always broadcasts the WLAN SSID information.

In order to disable broadcast SSID on the current WLAN template with WCS, perform these steps in WCS with versions earlier than 4.1.83.

**Note:** If you upgrade the WCS to Version 4.1.83, it also resolves this issue. Also, such problems occur mainly when the controller and the WCS are out of sync. In such cases, synchronize the WLC and WCS.

1. In the WCS WLAN template, disable or uncheck the Admin status box and make sure that the Broadcast SSID is unchecked.
2. Save the template.
3. Apply the template to the controller.
4. Reenable the admin box of this WLAN.
5. Save the template
6. Apply the template to the controller again.

Now, you can find the "Broadcast SSID" field as turned off in the individual WLAN configuration of the controller.

**WLAN Templates do not Display the Correct 7920 CAC Checkbox Setting**

When you create WLAN templates to push the WLANs to the controllers, check the 7920 CAC checkbox to enable that feature and save and redisplay that same WLAN. The template shows as unchecked even though it is really checked and does enable that feature on the controller when pushed to it.

This is due to bug CSCsi77521, which is associated with this issue.
Upgrade the WCS to Version 4.1 to resolve this issue.

**Unable to Delete Off-line Controllers from WCS Version 3.2.51.0**

In certain cases, users cannot delete WLCs that are no longer used from the WCS. This is because of issues with the database structure of WCS in Version 3.2.51.0; as a result, WCS tends to lock up resources. The entire database was restructured in Version 4.0 and has enhanced the performance level.

There are two workarounds for this issue:

- Delete the audit reports and then delete the controller or
- Upgrade to WCS 4.0.87.0 and later

With the first option, in order to delete the off-line controllers, do this:

1. When WCS monitors a very large pool of controllers, the best thing is to first delete the audit reports of those controllers, one by one, and then try to delete those controllers. In order to delete the audit reports, follow these steps:
   
   a. Go to **Configure Controller**.
   b. Check the box of the desired controller. Only one controller at a time is allowed.
   c. Choose the command **View Audit Reports** from the drop-down box.
   d. Click the **Go** button.
   e. Delete the audit reports.
   f. Then try to delete the controllers.

2. Try this procedure on all other controllers. Make sure that the user accounts that you use to carry out these tasks are part of the SuperUser group.

   On occasion, it deletes some of the audit reports but not all reports for a specific controller.

3. The audit reports that have the synchronization status of **Same in WCS and Controller** can be successfully deleted, but audit reports with the synchronization status of **Different in WCS and Controller** cannot be deleted.

4. You can see this error message when you try to delete audit reports with the status of **Different in WCS and Controller**.

   The resource you are trying to delete seems to be busy

5. In this case, the controller cannot be deleted. This error message means that the database has locked the resource. This can happen if the user hit the delete button, did not wait long enough, and then hit the **Back** to go to previous page. This was an issue in Version 3.2; just wait and see if the resource frees up.

Alternatively, you can use the second option to upgrade WCS to 4.0.87.0 or above, which has great performance enhancements from 3.2 due to a restructure of the WCS database.

**Cannot Add Web Authentication Template with Type Default Internal From WCS**

In an attempt to push the template, the error message **SNMP operation to Device failed** appears.

This is because of bug CSCsh89306. WCS gives the SNMP error when it pushes a web authentication template to a controller that runs Version 4.0.206.0.

The workaround is to configure a web authentication directly on the controller.
1. Navigate to the web authentication customization template page.
2. Choose the web authentication type as **External**.
3. Enter some dummy URL text.
4. Change the web authentication type to **Default Internal**.
5. Enter a Custom Redirect URL.
6. Save and apply the template.

Basically, the External and Custom Redirect URL must not be left blank on the page even if they are not relevant to the current web authentication application type.

**Related Information**

- Wireless Control System (WCS) Troubleshoot FAQ
- Cisco Wireless Control System Configuration Guide, Release 4.0
- Cisco Wireless Control System
- Wireless Support Page
- Technical Support & Documentation – Cisco Systems