



Cisco CallManager System Issues

This chapter covers solutions for the following most common issues related to a Cisco CallManager system.

- [Cisco CallManager System Not Responding](#)
- [Replication Fails Between the Publisher and the Subscriber](#)
- [Slow Server Response](#)
- [Security](#)
- [Virus Protection](#)

Cisco CallManager System Not Responding

This document covers the following issues for a Cisco CallManager system not responding:

- [Cisco CallManager System Stops Responding](#)
- [Cisco CallManager Administration Page Does Not Display](#)
- [Errors Occur When Attempting to Access the Cisco CallManager Administration Page from the Browser](#)
- [A Virus is Affecting the Server Performance](#)
- [You Are Not Authorized to View This Page](#)
- [Errors Occur When Attempting to Access the Cisco CallManager Administration Page from a Browser on a Remote Server](#)
- [Name to Address Resolution Failing](#)
- [Default Web Site Under IIS Has Improper Setting](#)
- [Port 80 Is Blocked in One or More Routers Between Your Local Browser and the Cisco CallManager Server](#)
- [You Attempt to Access a Machine Where Access Is Explicitly Denied](#)
- [Improper Network Setting Exists in the Remote Machine From Where You Are Browsing](#)
- [Replication Fails Between the Publisher and the Subscriber](#)

Cisco CallManager System Stops Responding

Symptom

The Cisco CallManager system does not respond.

Probable Cause

Problem may be any of, but not limited to, the following causes:

- Cisco CallManager service stopped.
- The Internet Information Service (IIS) stopped.
- A virus has affected the server.
- The Network Administrator changed the security policy.
- Improper Configuration settings exist.

Corrective Action

Begin troubleshooting the problem locally on the same server where the Cisco CallManager is installed.

If the following procedures do not solve your system problem, contact TAC for a more detailed investigation:

- [Cisco CallManager Administration Page Does Not Display](#)
- [Errors Occur When Attempting to Access the Cisco CallManager Administration Page from the Browser](#)
- [A Virus is Affecting the Server Performance](#)
- [You Are Not Authorized to View This Page](#)
- [Errors Occur When Attempting to Access the Cisco CallManager Administration Page from a Browser on a Remote Server](#)
- [Name to Address Resolution Failing](#)
- [Default Web Site Under IIS Has Improper Setting](#)
- [Port 80 Is Blocked in One or More Routers Between Your Local Browser and the Cisco CallManager Server](#)

- [You Attempt to Access a Machine Where Access Is Explicitly Denied](#)
- [Improper Network Setting Exists in the Remote Machine From Where You Are Browsing](#)

Cisco CallManager Administration Page Does Not Display

Symptom

Administration web page does not display.

Probable Cause

The Cisco CallManager service stopped.

Corrective Action

Use the following procedure to verify that the Cisco CallManager service is active on a server that is local or remote.

Procedure

- Step 1** From Cisco CallManager Administration, choose **Application > Cisco CallManager Serviceability**.
The Cisco CallManager Serviceability window displays.
- Step 2** Choose **Tools > Service Activation**.
- Step 3** From the Servers column, choose a server.
The server that you chose displays next to the Current Server title, and a box with configured services displays.
Activation Status column displays either Activated or Deactivated in the Cisco CallManager line.
If Activated, the Cisco CallManager is active on the chosen server and you need to contact TAC for further assistance.
If Deactivated, continue with the following steps.

Step 4 Check the **Cisco CallManager** check box.

Step 5 Click the **Update** button.

The Activation Status column displays Activated in the Cisco CallManager line. Cisco CallManager is now active for the chosen server.

Perform the following procedure if the Cisco CallManager has been in service and you want to check if it is currently active.

Procedure

Step 1 From Cisco CallManager Administration, choose **Application > Cisco CallManager Serviceability**.

The Cisco CallManager Serviceability window displays.

Step 2 Choose **Tools > Control Center**.

Step 3 From the Servers column, choose the server.

The server that you chose displays next to the Current Server title, and a box with configured services displays.

The Activation Status column displays Activated in the Cisco CallManager line.

Cisco CallManager is active for the chosen server. Contact TAC for further assistance.

If Deactivated, continue with the following steps.

Step 4 Check the **Cisco CallManager** check box.

Step 5 Click the **Update** button.

The Activation Status column displays Activated in the Cisco CallManager line. Cisco CallManager is now active for the chosen server.

Verification

Repeat the preceding procedure to verify that the Cisco CallManager service is activated

Errors Occur When Attempting to Access the Cisco CallManager Administration Page from the Browser

Symptom

One of the following error messages displays when you are trying to access the administration page from the same server where the Cisco CallManager resides.

- Internet Explorer—The page cannot be displayed.
- Netscape—Warning box displays: There was no response. The server could be down or is not responding.

Probable Cause

The IIS Admin service or the WWW publishing service does not start automatically as expected. One of these services stopping represents the most frequent reason for the pages not displaying locally.

Corrective Action

Use the following procedure to start the IIS.



Note If the IIS is stopped, the WWW publishing services may also be stopped. Start the WWW publishing services, which starts the IIS automatically.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

A window displays listing IIS Administration.

Step 2 Right-click **IIS Admin Service**.

Step 3 Choose **Start**.

Step 4 Click **Yes**.

The IIS starts.

Start the other services using the following procedure.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

Step 2 Right-click the service.

Step 3 Choose **Start**.

Step 4 Click **Yes**.

The service starts.

Verification

Use the following procedure to verify that IIS is started.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

Step 2 Right-click the service.

Step 3 Verify the status, which should display Started.

Step 4 If any service is stopped, perform the following procedures to start the service(s).

Use the following procedure to start the IIS.



Note If the IIS is stopped, WWW publishing services may also be stopped. Start the WWW publishing services, which starts the IIS automatically.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

A window displays listing IIS Admin Service.

Step 2 Right-click **IIS Admin Service**.

Step 3 Choose **Start**.

Step 4 Click **Yes**.

The IIS starts.

Start the other services using the following procedure.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

Step 2 Right-click the service.

Step 3 Choose **Start**.

Step 4 Click **Yes**.

The service starts.

A Virus is Affecting the Server Performance

Symptom

The symptom changes with every virus. The IIS may stop, which results in web pages not displaying. Strange messages may display. Server performance varies or stops.

Probable Cause

Viruses that have affected Microsoft products in turn have infected the Cisco CallManager server.

Corrective Action

Use the following procedure to ensure that you have the necessary patches to protect the Cisco CallManager and Cisco CallManager Applications Servers.

Procedure

- Step 1** Verify that you have the necessary patches to protect your system.
- Step 2** If you do not have the correct patches, go to the following URLs to see if your system may be infected:
- CERT Advisory CA-2001-23 Continued Threat of the “Code Red” Worm
<http://www.cert.org/advisories/CA-2001-23.html>
- CERT Advisory CA-2001-26 Nimda Worms
<http://www.cert.org/advisories/CA-2001-26.html>
- Step 3** If you are affected, continue to the next procedure.
-

Use the following procedure to clean the Nimda and Code Red Virus from the Cisco CallManager and Cisco CallManager Applications Servers.

Procedure

-
- Step 1** Perform an MCS Backup using Cisco-provided Cisco MCS Backup Utility. If you already have a known good backup, continue to the next step.
- Step 2** Ensure you do not have shared drives to any machines that are infected, because the worm can spread via shared drives.
- Step 3** Stop the IIS Admin service on the machine that is infected. (This will also stop the WWW publishing services.)
- Step 4** Download and run the **win-OS-Upgrade.3-1-1.EXE** that is available on CCO. This will require a reboot.



Note To see the link to the download, you must be a registered user to log in.

- Step 5** As a precaution for possible Code Red II vulnerabilities, download the Code Red II Cleanup tool from Microsoft at:
<http://download.microsoft.com/download/iis50/Tool/1.0/NT45/EN-US/CodeRedCleanup.exe>



Note Several antivirus companies have produced tools to eliminate Nimda; however, Cisco has tested the following tool and confirmed that it cleans a Cisco CallManager with no damaging side effects.

- Step 6** Download the Nimda Cleanup tool from Network Associates
<http://www.mcafee2b.com/naicommon/avert/avert-research-center/tools.asp#NimdaScn>
 Scroll to the bottom of the page and download **Nimdascn.zip** (440 Kb).
- Step 7** Navigate to the directory where the CodeRedCleanup.exe was placed and run it: **CodeRedCleanup.exe**.
- Step 8** Unzip the Nimda Cleanup Tool and place the files along with the Code Red II Cleanup tool on the hard drive of the affected machine.
- Step 9** Choose **Start > Run** and enter **cmd.exe**.
 Navigate to the directory where you placed the Nimda and Code Red II Cleanup tools.
- Step 10** Run the Nimda Cleanup Tool by entering: **nimdascn c:*.***

- Step 11** After this action completes, do the same for the E drive: **nimdasen e:*.***
Cisco CallManager should only have a C and E drive as hard drives with D being the CD-ROM drive.
- Step 12** If the server has any other hard drives, run **nimdasen** for those drives, as well.
-

Find more details on viruses, their effect on Cisco equipment, as well as vulnerabilities on the PSIRT Advisories web page at the following URL:

<http://www.cisco.com/warp/public/707/advisory.html>

For more information on quick recovery from the Code Red II virus, see the [Virus Protection](#) section.

Verification

The Cisco CallManager service performs properly.

As a long-term solution, Cisco recommends the use of Cisco Host IDS Sensor and McAfee Netshield antivirus on the Cisco CallManager server. Both have been tested and approved for installation with the Cisco CallManager. Follow the recommended configuration settings to avoid undesired effects in the processor time.

You Are Not Authorized to View This Page

Symptom

When accessing the administration page, the following error message displays.

Error Message You Are Not Authorized to View This Page
and other similar error messages that may occur include

- You do not have permission to view this directory or page using the credentials you supplied.
- HTTP 401.3 Access denied by ACL on resource Internet Information Services.

- Server Application Error. The server has encountered an error while loading an application during the processing of your request. Please refer to the event log for more detailed information. Please contact the server administrator for assistance.
- Error: Access is Denied.

Probable Cause

The NTFS permissions have been modified on your C drive off the root directory to propagate into child directories on the Cisco CallManager server.

NTFS permissions have been changed from the default settings on the server and are no longer sufficient for IIS to run properly.

Corrective Action

Visit the Microsoft site for details on the issue: Q271071 “Minimum NTFS Permissions Required for IIS 5.0 to Work” at the following URL:

<http://support.microsoft.com/default.aspx?ln=EN-GB&pr=kbinfo&>

Verification

Use the following procedure to verify that IIS is started.

Procedure

-
- Step 1** From the Start menu, choose **Start > Programs > Administration Tools > Services**.
 - Step 2** Right-click the service.
 - Step 3** Verify the status, which should display Started.
 - Step 4** If any service is stopped, perform the following procedures to start the service(s).
-

Use the following procedure to start the IIS.



Note If the IIS is stopped, the WWW publishing services may also be stopped. Start the WWW publishing services, which starts the IIS automatically.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

A window displays listing IIS Admin Service.

Step 2 Right-click **IIS Admin Service**.

Step 3 Choose **Start**.

Step 4 Click **Yes**.

The IIS starts.

Start the other services using the following procedure.

Procedure

Step 1 From the Start menu, choose **Start > Programs > Administration Tools > Services**.

Step 2 Right-click the service.

Step 3 Choose **Start**.

Step 4 Click **Yes**.

The service starts.

Errors Occur When Attempting to Access the Cisco CallManager Administration Page from a Browser on a Remote Server

If you can access the Administration Web page locally on the Cisco CallManager server, but not when you browse from a remote machine, verify whether one of the following situations applies to you. They appear in order, from the most frequent reason to the least frequent reason.

Name to Address Resolution Failing

Symptom

One of the following error messages displays when you try to access the following URL:

`http://your-cm-server-name/ccmadmin`

- Internet Explorer: This page cannot be displayed
- Netscape: Not Found. The requested URL /ccmadmin was not found on this server.

If you try to access the same URL using the Cisco CallManager IP address (`http://10.48.23.2/ccmadmin`) instead of the name, the page displays.

Probable Cause

The name that you entered as "your-cm-server-name" is mapping to the wrong IP address in DNS or hosts file.

Corrective Action

Procedure

-
- Step 1** If you have configured the use of DNS, check in the DNS to see whether the entry for the *your-cm-server-name* has the correct IP address of the Cisco CallManager server. If it is not correct, change it.

Step 2 If you are not using DNS, your local machine will check in the "hosts" file to see whether there is an entry for the *your-cm-server-name* and an IP address associated to it. Open the file and add the Cisco CallManager server name and the IP address.

You can find the "hosts" file at `C:\WINNT\system32\drivers\etc\hosts` on your Windows station.

Default Web Site Under IIS Has Improper Setting

Symptom

One of the following error messages displays when you try to access the following URL:

`http://your-cm-server-name/ccmadmin`

- Internet Explorer: This page cannot be displayed
- Netscape: Not Found. The requested URL /ccmadmin was not found on this server.

If you try to access the same page using the Cisco CallManager IP address (`http://10.48.23.2/ccmadmin`) instead of the name, the page displays.

Probable Cause

An incorrect setting in the **Default Web Site** tab for the IIS has been set on the server.

Corrective Action

Procedure

Step 1 Verify in the Internet Service Manager on the Cisco CallManager machine the **Default Web Site**. In the **Web Site** tab, choose **All Unassigned** and not the IP address of the machine.

You can verify that setting by choosing **Start > Programs > Administrative tools/Internet Service Manager**. Expand the icon that shows your server name.

- Step 2** Right-click **Default Web Site**. You have option properties that you must choose. Look for the **Web Site** tab and verify the **All Unassigned** setting.

**Note**

If you need to keep the specific IP address setting for any reason, you will not be able to use the name instead of IP address from a remote web browser.

Port 80 Is Blocked in One or More Routers Between Your Local Browser and the Cisco CallManager Server

Symptom

One of the following error messages displays when the port that is used by the web server or the http traffic is being blocked by a firewall:

- Internet Explorer: This page cannot be displayed
- Netscape: There was no response. The server could be down or is not responding

Probable Cause

For security reasons, the http access from your local network to the server network has been blocked.

Corrective Action

Procedure

- Step 1** Verify whether other types of traffic to the Cisco CallManager server are allowed, such as ping or Telnet. If any of them are successful, it will show that http access to the Cisco CallManager Web server has been blocked from your remote network.
- Step 2** Check the security policies with your network administrator.
- Step 3** Try again from the same network where the Server is located.
-

You Attempt to Access a Machine Where Access Is Explicitly Denied

Symptom

One of the following error messages displays:

- Internet Explorer: This page cannot be displayed
- Netscape: Not Found. The requested URL / ccmadmin was not found on this server.
- From both browsers without **show friendly http error messages** advance setting configured: Access to this server is forbidden.

Probable Cause

This represents a security policy that is applied by the network administrator.

Corrective Action

Procedure

- Step 1** Check the security policies with your network administrator. Try again from a different machine.
 - Step 2** If you are the network administrator, check the **Directory Security** tab of the **Default Web Site** in the Internet Service Manager on the Cisco CallManager server.
 - Step 3** You can verify the setting by choosing **Start > Programs > Administrative tools/Internet Service Manager**.
 - Step 4** Expand the icon that shows your server name.
 - Step 5** Right-click **Default Web Site**. You have the option properties from which you must choose.
 - Step 6** Look for the **Directory Security** tab and verify the setting.
-

Improper Network Setting Exists in the Remote Machine From Where You Are Browsing

Symptom

There is no connectivity, or there is no connectivity to other devices in the same network as the Cisco CallManager.

When you attempt the same action from other remote machines, the Cisco CallManager Administration Page displays.

Probable Cause

Improper network configuration settings on a station or on the default Gateway can cause a web page not to display because partial or no connectivity to that network exists.

Corrective Action

Procedure

- Step 1** Try pinging the IP address of the Cisco CallManager server and other devices to confirm that you cannot connect.
- Step 2** If the connectivity to any other device out of your local network is failing, check the network setting on your station, as well as the cable and connector integrity.
- Step 3** If the connectivity to any other device out of your local network is failing, check the network setting on your station, as well as the cable and connector integrity. Refer to the appropriate hardware documentation for detailed information.
- If you are using TCP-IP over a LAN to connect, continue with the following steps to verify the network settings on the remote station.
- Step 4** Choose **Start > Setting > Network and Dial-up connections**.
- Step 5** Choose **Local Area Connection**, then **Properties**.
- The list of communication protocols will appear checked.
- Step 6** Choose **Internet Protocol (TCP-IP)** and click **Properties** again.
- Step 7** Depending on your network, choose either **Obtain an ip address automatically** or **set manually your address, mask and default Gateway**.
- The possibility exists that a browser-specific setting could be improperly configured.
- Step 8** Choose the Internet Explorer browser **Tools > Internet Options**.
- Step 9** Choose the **Connections** tab and then verify the LAN settings or the dial-up settings.
- By default, the LAN settings and the dial-up settings are not configured. The generic network setting from Windows is used.
- Step 10** If the connectivity is failing only to the Cisco CallManager network, a routing issue probably exists in the network. Contact the network administrator to verify the routing that is configured in your default gateway.

**Note**

If you cannot browse from the remote server after following this procedure, contact TAC to have the issue investigated in more detail.

Refer to the following URL for more information on configuration settings:
http://www.cisco.com/warp/public/63/initial_config.shtml

Replication Fails Between the Publisher and the Subscriber

Symptom

Error Message Cannot update data because the publisher is not available. Please try again later. (58)

Probable Cause

The subscriber build failed.

Corrective Action

Procedure

- Step 1** Ensure that the NetBIOS name resolution is working between all servers.
- Step 2** Ensure (by editing) that the hosts and LMHOSTS are filled in on the publisher and subscriber servers, so each one can resolve the other's host name and NetBIOS name.
- Hosts is used for DNS resolution. LMHOSTS uses NetBIOS for name resolution. Also, SQL uses NetBIOS for name resolution.

If the Cisco CallManager fails to update, the database layer on the subscriber cannot find the publisher.

- Step 3** Check the SQL “distribution agent” on the publisher for history and errors.
- Step 4** Choose **Start > Programs > Administrative Tools > Local Security Policy**.
- Step 5** Choose **Audit Policy**.
- Step 6** Enable **Failure auditing for all events**.

For SQL, enable **Authentication**.



Note Users get replicated in the DC Directory, not in SQL.

- Step 7** From the web, upgrade the Cisco CallManager for the software version on your publisher.

The software will download the SQL database to the subscriber(s).

Slow Server Response

Symptom

Slow response from the server occurs.

Probable Cause

Slow response could result if the duplex of the switch does not match the duplex port setting on the Cisco CallManager server.

Corrective Action

Procedure

- Step 1** For optimal performance, set both switch and server to **100/Full**.
Cisco does not recommend using the Auto setting on either the switch or the server.
- Step 2** You must restart the Cisco CallManager server for this change to take effect.
-

Security

This section covers the following security issues and provides information on where to find detailed documentation regarding the security process:

- [Changing IIS Parameters for Security](#)
- [Near-Term Security Solutions](#)
- [Long-Term Security Solutions](#)
- [Related Information](#)

Changing IIS Parameters for Security

Symptom

You lose settings for locking down the IIS servers to protect the Cisco CallManager from hackers, attacks, or threats.

Probable Cause

Whenever you upgrade or reinstall the Cisco CallManager, all the IIS settings revert to the Cisco CallManager defaults.

Corrective Action

Test all your settings on a non-production Cisco CallManager before changing the settings on your production server.

Note the settings, because they will change every time that you perform an upgrade or reinstall, and you will have to reset them.

**Caution**

Ensure that you do not change any settings within the Cisco web directory, or you run the risk of losing a Cisco CallManager service due to a missing or moved file.

Near-Term Security Solutions

Refer to the following documents to ensure that you have quality of service (QoS) configured properly throughout your network to help ensure voice quality is affected as little as possible during the remainder of cleanup operations:

- *Cisco IP Telephony QoS Design Guide*
- *Cisco IP Telephony Network Design Guide*
- *IP Telephony Solutions Guide*

The following URL provides the guides:

http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/index.htm

Refer to the *Cisco IP Telephony Network Design Guide* to establish separate Voice/Data VLANs.

**Note**

This could provide a long-term solution depending on the size and complexity of the network involved.

Long-Term Security Solutions

Once the immediate emergency is over, look at the *Cisco IP Telephony Solution Guide: Security Considerations for IP Telephony Networks* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/solution/4_design.htm

The subsection “Securing CallManager Servers” provides details on how to properly secure an IP Telephony solution for long term. The *Cisco IP Telephony Solution Guide* provides measures that would prevent Code Red issues on the Data network from affecting the IP telephony network.

Related Information

The following URL provides *Cisco CallManager Security Patch Process*:

http://www.cisco.com/warp/public/cc/pd/nemnsw/callmn/prodlit/cmspp_qa.pdf

Cisco highly recommends that you do not install any patches from Microsoft. Download the wrapped versions from CCO.

You can sign up for Microsoft security patch alerts at the following URL:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp>

The alerts include an associated rating, which allows you an approximate time of a HotFix posting to CCO.

Refer to the following URL for security considerations for an IP telephony network:

http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/solution/4_design.htm#22024

Virus Protection

This section covers the [Code Red II Recovery](#) procedures to immediately eliminate most of the effects to Cisco CallManager due to a widespread Code Red II infection.

See the [A Virus is Affecting the Server Performance](#) section for additional information.

Code Red II Recovery

Symptom

The worm can compromise the system and loads malicious commands or code.

Probable Cause

An email attachment carried the worm.

Corrective Action

Procedure

- Step 1** Run **win-OS-Upgrade.3-1-1.exe** (available from the Crypto Site) on all IP telephony servers that are running Windows 2000
- Step 2** Run the appropriate repair utility (Microsoft has a tool available) and/or manually (tool available from McAfee) close the back doors created by Code Red II.
- Step 3** For IP telephony servers that are running NT4.0 IIS, install Service Pack 6a and then the Code Red fix.



Caution

Due to the nature of this worm of creating backdoors, if this server is directly attached to the Internet, someone could have placed more back doors into it while it was compromised. If the possibility of the server being further compromised from within your network exists, the safest action would be to back up the data, and reinstall the server from scratch.

Stop Services

- Step 4** Stop and disable IIS Admin Service and World Wide Web Publishing service on all Cisco CallManager subscribers and any server that does not require the services.



Note

Ensure that these services remain active on the Cisco CallManager publisher server.

- Step 5** Bring up the services applet by choosing **Start > Programs > Administrative Tools > Services**.
- Step 6** Right-click **IIS Admin Service** and choose **Stop**.
This will also stop the World Wide Web Publishing service.
- Step 7** Right-click **IIS Admin Service** and choose **Properties**.
- Step 8** Change **Startup Type** to **Disable** and close the window.
- Step 9** Right-click **World Wide Web Publishing** and choose **Properties**.
- Step 10** Change **Startup Type** to **Disable** and close the window.
- Step 11** Patch/repair all known IIS servers in the network.

Deploy updated phone loads

- Step 12** For 3.0(x) systems, download **cisocm_3-0-11_spA.exe** from CCO.
- Step 13** From Cisco CallManager Administration, go to **System > Device Defaults** and set the 7940/7960 Device Loads to **P003E310**.
- Step 14** Click **Update**.
- Step 15** For 3.1(x) systems, download **cisocm_3-1-1_spA.exe** from CCO.
- Step 16** From Cisco CallManager Administration, choose **System > Device Defaults** and set the 7940/7960 Device Loads to **P00303010100**.
- Step 17** Click **Update**.
- Step 18** Go to **System > CallManager Group**, choose the first group on the left side, and click **Reset Devices**.
- Step 19** When prompted, choose **OK**.
Repeat steps 12 through 19 for each Cisco CallManager Group that is present for the phones to get new loads.
- Step 20** Identify and repair remaining infected IIS servers on the network (this could easily stretch into a near-term solution depending on how many "rogue" IIS servers are on the network).
Two methods follow to locate and repair infected IIS servers.
- Step 21** On the Cisco CallManager publishing server, or any other IIS server with logging enabled, go to C:\winnt\system32\logfiles\w3svc1 and get the most recent logfile. These files have a naming convention of ex000000.log.

Step 22 Look for a line similar to the following

```
2001-08-09 00:11:57 172.20.148.189 - 172.20.225.130 80 GET
/default.ida
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXX
XX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858
%ucbd3%u7801%u9090%u9090%u8190%u
00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a200 -
```

In this case, the IP address 172.20.148.189 represents the attacking server.

Step 23 Patch and clean or disconnect the server from the network.

Step 24 Follow steps 21 through 23 until all remaining Code Red infected servers have been located and repaired.

Step 25 Another method is to use the free utility available from eEye - CodeRedScanner. The utility will scan 1 Class C at a time looking for infected machines and machines that are vulnerable to an .ida based attack. A Class B scanner is available at additional cost.

■ Virus Protection