CISCO CONFIDENTIAL

CHAPTER 23

Using the Diagnostic and Support Utilities

CWCS provides diagnostic and customer-support utilities that:

- Help customers collect data about their CWCS installations and the applications installed with them.
- Give Cisco developers and technical support staff the information they need to resolve customer problems more quickly.

The following topics describe these utilities:

See this Topic	For Information on this Utility
Using Collect Server Info	Collect Server Info: Gathers all-in-one information about the state of the CWCS Server.
Using the MDC Support Utility	MDCSupport: Collects diagnostic output into a zip file.
Using SNMP Set and Walk	SNMP Set and Walk: SNMPwalks a device to troubleshoot or gather information about that device.
Using Packet Capture	Packet Capture: Captures live data from the CiscoWorks Server.
Using Logrot	Logrot: Rotates log files.

Using Collect Server Info

The Collect Server Info utility allows customers to quickly collect all-in-one information about the state of their CWCS Servers.This module is implemented as a Perl script. This script uses all OS-specific commands to get system information, process information and memory information. The following topics describe how to use this utility:

- What Data Does Collect Server Info Gather?
- Customizing Collect Server Info
- Running CollectServerInfo

What Data Does Collect Server Info Gather?

Collect Server Info collects the following information:

- System identity, including name, type, network data.
- System configuration. This includes:

CISCO CONFIDENTIAL

  - Network settings
  - CWCS Server name
  - Shared secret
  - TIBCO RVRD IP address
  - Root account enable/disable
  - Notification settings (where CWCS sends its notifications)
  - Cluster management
  - SMTP server name
  - NTP configuration
  - Security configuration
  - Backup history configuration
  - Application settings
- Software installed on the system, with detailed information about packages.
- Web server configuration and status.
- Servlet engine configuration and status.
- Database status and configuration with the sizes of database files.
- Process status and service status log files. If log files are very big, only the last portions could be collected (for example, the last 300 records).

Customizing Collect Server Info

To add your application's troubleshooting information to the Collect Server Info utility:

Step 1 Create and add a shell script or perl file to the $*NMSROOT*/collect directory. This file will collect your application-specific information. For example, myInfo.exe.

Step 2 Add a text file named myInfo.txt containing the following lines to the $*NMSROOT*/collect directory:

```
Name=My
Option=my
Descr=My Status
Order=A3
```

Running CollectServerInfo

To run CollectServerInfo:

Step 1 From the CWHP, select **Server > Diagnostics > Collect Server Info**. The Collect Server Information page displays.

Step 2 Click **Create** to view a list of options such as web server, operating system, and process status.

CISCO CONFIDENTIAL

Step 3 Select the options by clicking in the appropriate boxes, then **Finish**. To collect your application-specific information, click on the checkbox for MY Information. If MY Information does not appear, perform the steps in the "Customizing Collect Server Info" section on page 23-2.

The Collect Server Information page refreshes with a link to the server information report.

Step 4 Click on the hyperlink to view the report.

Using the MDC Support Utility

The MDC support utility is a console application written in C++. It allows users enter an optional command line argument (the output path/location of where the zip file should be located) to collect diagnostic output into a zip file.

The resulting zip file consists of SQL DB files, Core Client Registry (CCR) files, configuration and log files of Apache and Tomcat, Core log file, WinNT event logs and System information like host details, memory, disk, and network details. The utility can also:

- Run other support utilities registered by applications with CCR.
- Register these other utilities with the CCR.

MDCSupport in Core provides the same information as the Collect Server Info utility, and also provides information by executing the application-specific executables registered with CCR.

The following topics describe how to use this utility:

About the MDC Support Utility Requirements

There are no disk space requirements for MDC Support other than the room required for the zip file.

What Data Does the MDC Utility Collect?

The MDC Support utility collects the following information:

- SQL database files under <CoreRoot>\Sybase\Db*
- CCR file <CoreRoot>\etc\regdaemon.xml
- Schema files under <CoreRoot>\etc
- Apache (web server) configuration and log files located at:
  - <CoreRoot>\apache\conf*
  - <CoreRoot>\apache\log*
- Tomcat configuration and log files (the servlet container technology standard at Cisco, currently deployed on the CCI environment), and the XML file located at:

CISCO CONFIDENTIAL

  - <CoreRoot>\tomcat\conf*
  - <CoreRoot>\tomcat\log*
  - <CoreRoot>\tomcat\mdc\web-inf\web.xml
  - <CoreRoot>*.log: Log file created when Tomcat crashes, containing a stack trace.
- Log files registered with CCR for Core under <CoreRoot>\MDC\log, including the audit and operation logs
- Installation log files of the form cw*.log found in the System drive
- Registry subtree: [HKEY_LOCAL_MACHINE][SOFTWARE][Cisco][MDC]
- Windows NT event logs:
  - System event log file
  - Application event log file
- Host environment information:
  - OS version/NT service packs
  - Physical RAM
  - Disk Space on all volumes
  - Computer Name
  - Virtual Memory size

Note The MDCSupport utility also queries CCR for any other, alternative support utilities and runs them automatically if they are registered. For more information, see the "Registering Alternative MDC Support Utilities" section on page 23-4.

Registering Alternative MDC Support Utilities

You can have the MDC Support utility automatically run other, alternative MDC support utilities and include their output in the *MDCSupportInformation.zip* file. To do this, register the alternative support utility with the Core Client Registry using the following command:

Name	ccraccess
Runtime Location	The location of the support utility.

Syntax	`ccraccess -addMDC mdcName mdc_root_dir`
	
	`ccraccess -addResource mdcName Custom Custom support_utility_path EMPTYSTRING MDCSupportExecutable`

Arguments	The utility registered takes two arguments: • The first argument is the core installation directory (usually $*NMSROOT*/MDC). • The second argument is the directory in which the MDC's support utility needs to add all the data it wants zipped by the MDCSupport utility. **Tip** To make it easier to identify the files coming from each MDC, it is highly recommended that each MDC create a temporary directory inside this directory and put all the files there.

CISCO CONFIDENTIAL

Name	ccraccess

Example	If SampleMDC is installed at C:\apps\MDC\SampleMDC:
	1. Register MDC with CCR:
	`ccraccess -addMDC SampleMDC C:\\apps\\MDC\\SampleMDC`
	2. Register support utility with CCR:
	`ccraccess -addResource SampleMDC Custom Custom C:\\apps\\MDC\\SampleMDC\\bin\\SampleSupport.exe EMPTYSTRING MDCSupportExecutable`

When MDCSupport is run (with no arguments):

1. MDCSupport creates a temporary directory: <CoreRoot>\etc\mdcsupporttemp
2. MDCSupport collects all requested data
3. MDCSupport queries CCR and finds that SampleMDC has a utility registered, and creates a process: C:\\apps\\MDC\\SampleMDC\\bin\\SampleMDCSupport.exe and passes it the two arguments <CoreRoot> and <CoreRoot>\etc\mdcsupporttemp. (Note that the two arguments are full paths).
4. SampleMDCSupport creates a SampleMDC directory under mdcsupporttemp dir, and adds all the files it needs to this directory.
5. MDCSupport zips the contents of mdcsupporttemp and then deletes mdcsupporttemp and all of its contents.

Running MDC Support

The *MDCSupport.exe* utility is a console application that takes one optional command-line argument: the output path and location where the resulting zip file should be created. If you do not specify a value for this argument, the output is created in <CoreRoot>\etc.

The output consists of an *MDCSupportInformation.zip* file. An MDCSupport.log text file in the zip package acts as a log of what has been collected and notes any errors encountered. Other information in the file includes:

- The time the support tool was run.
- The Core version installed.
- The installation location of Core.
- The System path.
- Host environment information.
- Other MDCs support utilities executed.

To run MDCSupport.exe:

Step 1 If there is enough space on the disk where the MDC suite is installed, enter the following on the command line (with no arguments):

MDCSupport.exe

The file *MDCSupportInformation.zip* file is created in the <CoreRoot>\etc directory.

CISCO CONFIDENTIAL

Step 2 If you use another disk to store the temporary files and the output, enter the output path and location where the resulting zip file should be created. For example:

MDCSupport D:\temp

The file *MDCSupportInformation.zip* is created in the D:\temp directory.

Using SNMP Set and Walk

Use SNMP Set and Walk to troubleshoot or gather information about a device. The following topics describe how to use this utility:

- About the SNMP Set and Walk Requirements
- Running SNMP Set and Walk
- Updating the MIBs for SNMP Walk

Note This tool is intended for customers running CiscoWorks and is designed to integrate with CWCS.

About the SNMP Set and Walk Requirements

- Supported versions: CiscoWorks CD One, CD One 2nd edition, CD One 2nd Edition Patch 1, CD One 3rd Edition, CD One 4th Edition, CD One 5th Edition, or CiscoWorks Common Services 2.2 and 3.0.
- Supported platforms:
  - Windows2000 Server with SP2 (Pentium III & 4)
  - Windows2000 Advanced Server (not configured as either a Domain Controller or a Terminal Server) (Pentium 4)
  - Sun Solaris 7 and 8 (2.7 and 2.8) (UltraSPARC II, IIi, IIe, III, and IIIc)
- *All* prerequisites for CiscoWorks must be met for both client and server.

Running SNMP Set and Walk

SNMP Set and Walk fetches credentials from the CWCS Device Credentials Repository (DCR), if available. Otherwise, it assumes the default credentials for SNMP v1/v2c.

Step 1 Using your web browser, log in to CiscoWorks as local administrator.

Step 2 You must launch the SNMP Set and Walk tools from the Device Center:

To launch SNMP Set:

a. Select **CiscoWorks HomePage > Device Trouble Shooting > Device Center**.

b. Enter an IP address or select one from the Device Selector list.

c. Select **Go**. The Tools column shows the list of available tools.

CISCO CONFIDENTIAL

d. Select **SNMP Set**.

To launch SNMP Walk:

a. Select **CiscoWorks HomePage > Device Trouble Shooting > Device Center**.

b. Enter an IP address or select one from the Device Selector list.

c. Select **Go**. The Tools column shows the list of available tools.

d. Select **SNMP Walk**.

Step 3 Enter the following information:

Field	Description
Object ID, Instance ID or number	Either an IP address or a hostname. If it is a hostname, the hostname *must* resolve correctly either through DNS, local hosts file, or NIS. **Note** WINS has not been tested and is *not* supported. **Note** The device does not need to be in RME's inventory or discovered on the Campus Manager topology map.
community string	This can be either a read-only community string, a read-write string, or a read-write-all string. Remember, it is case-sensitive! **Note** Do not use this field if you are using SNMPv3.
SNMPv3 user, password, and authentication protocol	For SNMPv3 users only. If you are not using SNMPv3, leave these fields blank. **Note** SNMPv3 support is for authNoPriv only at this time.
starting object ID	Optional: The point in the MIB tree where you want to start the walk. If this field is left blank, SNMP Walk will start the walk from: • For SNMP Set, you can specify multiple OIDs. • For SNMP Walk, you can enter only one OID.
translate results	Optional: If you check this box, all OIDs will be shown numerically instead of translated. This can help troubleshoot issues that require the sysObjectID.
SNMP timeout	Optional: The SNMP timeout (default = 10 seconds).
version	The version of SNMP to use. Anything that is a 64-bit counter must be queried with v2c or v3.

Step 4 To run SNMP Walk, select **Ok**. SNMP Walk will start the walk based on the parameters you entered. A full walk may take a *long* time, so be patient.

SNMP Set requires two additional fields:

Field	Description
object type	The type of object to be set. You can select the object type from the drop-down list.
new value	The new value to be set for the object.

CISCO CONFIDENTIAL

To set multiple objects, fill in all the required fields, then click **Next**. Repeat this until you are ready to send the SETs to the device. At this point, each SET goes into its own packet.

Updating the MIBs for SNMP Walk

By default, SNMP Walk uses the MIBs found in the installed nmidb.jar. This jar file is found in $*NMSROOT*/nmim/nmidb.

If a newer nmidb jar file is downloaded from CCO, you can run the $*NMSROOT*/bin/upgradeJTMibs.pl script to add those MIBs to SNMP Walk.

To run the script:

- On Windows platforms, enter:

  ```
  C:\> $NMSROOT\bin\perl $NMSROOT\bin\updateJTMibs.pl <path to nmidb.zip>
  ```

  (where $*NMSROOT* is the path where CiscoWorks is installed)

  For example:

  ```
  C:\> C:\Progra~1\CSCOpx\bin\perl C:\Progra~1\CSCOpx\bin\updateJTMibs.pl
  C:\nmidb.1.0.025.zip
  ```

- On UNIX platforms, enter:

  ```
  # /opt/CSCOpx/bin/updateJTMibs.pl <path to nmidb.zip>
  ```

  For example:

  ```
  /opt/CSCOpx/bin/updateJTMibs.pl /tmp/nmidb.1.0.025.zip
  ```

Using Packet Capture

Use the Packet Capture utility to capture live data from the CiscoWorks machine. This utility is intended for customers running CiscoWorks and is designed to integrate with CWCS.

Note Packet Capture is a troubleshooting tool. It should *not* be used a general-purpose sniffer.

The following topics describe how to use this utility:

- About the Packet Capture Utility Requirements
- Running Packet Capture

About the Packet Capture Utility Requirements

- Supported versions: CiscoWorks CD One, CD One 2nd edition, CD One 2nd Edition Patch 1, CD One 3rd Edition, CD One 4th Edition, CD One 5th Edition, Common Services 2.2 and 3.0

CISCO CONFIDENTIAL

- Supported platforms:
  - Windows2000 Server with SP2 (Pentium III & 4)
  - Windows2000 Advanced Server (not configured as either a Domain Controller or a Terminal Server) (Pentium 4)
  - Sun Solaris 7 and 8 (2.7 and 2.8) (UltraSPARC II, IIi, IIe, III, and IIIc)
- *All* prerequisites for CiscoWorks must be met for both client and server.

Running Packet Capture

To run the Packet Capture utility:

Step 1 If you are using one of the supported Windows platforms: Install winpcap.exe in NMSROOT/objects/jet/bin directory. The version of winpcap.exe is 3.0 and is intended for use with Windows only.

Step 2 Using your web browser, log in to CiscoWorks as Admin.

Step 3 To launch Packet Capture:

a. Select **CiscoWorks HomePage > Device Trouble Shooting > Device Center**.

b. Enter an IP address or select one from the Device Selector list.

c. Select **Go**. The Tools column shows the list of available tools.

d. Select **Packet Capture**.

Step 4 The currently-archived capture files are displayed. (If no capture files have been archived, a message will indicate that there are no capture files.) From this screen, you can:

- Create a new capture
- Delete an existing capture file

Step 5 Select **Create** to configure which packets should be captured.

a. If you have multiple interfaces on the machine, select the interface on which you wish to capture packets. The Address(es) field accepts one or more addresses (separated by a single space) to match when capturing.

b. You can configure the protocol and port on which to capture (the default), or you can select from the pre-configured list of common CiscoWorks applications.
   - Protocols and ports: Select the protocols (TCP, UDP, or ICMP) you would like included in the capture. Then enter the list of ports to capture on for TCP and UDP. The Port(s) field accepts one or more TCP or UDP ports (separated by a single space).
   - Pre-configured list of common CiscoWorks applications: Select **Application**, then select one or more applications from the list.

c. Specify when to stop the packet capture. You can choose to terminate the capture:
   - After a set amount of time. By default, the capture stops after 60 seconds (1 minute).
   - After the filter has captured a certain amount of data.
   - After a certain number of packets have been captured.

Step 6 While the capture is running, an applet will update the number of packets captured and capture size in real time. To stop the capture before the auto-stop condition is met, click **Stop**.

CISCO CONFIDENTIAL

Step 7 Each capture is saved on the server in the *NMSROOT*/htdocs/jet directory. The files are created in binary libpcap format with a .jet extension. You can use your web browser to download these files, then email them to the TAC for further analysis.

Remarks

- On Solaris platforms, Packet Capture installs a setuid root binary in /opt/CSCOpx/objects/jet/bin. This binary is only executable by users in the casusers group, but if this is still too risky, consider revoking its setuid privileges until you need to use it.
- Packet Capture is only accessible to CiscoWorks users that have System Administrator (admin) privileges. It is not recommended that you change this.

Using Logrot

The logrot utility is a log rotation program designed for use with CiscoWorks. While it depends on CiscoWorks being installed on the same machine, logrot is not limited to rotating only CiscoWorks log files. You can use logrot to rotate any file you wish.

The logrot utility has some unique advantages over other log rotation programs:

- It can rotate logs while CiscoWorks is running or it can shut down CiscoWorks before rotating the logs.
- It can optionally archive and compress rotated logs.
- It can be configured to rotate logs only when they have reached a certain size.
- It has a built-in configurator that makes adding new files very easy.

The following topics describe how to use Logrot:

Configuring Logrot

To configure Logrot:

Step 1 Navigate to the logrot directory:

- On Windows platforms, enter:

```
C:\> NMSROOT\bin\perl.exe NMSROOT\bin\logrot.pl -c
```

- On UNIX platforms, enter:

```
# /opt/CSCOpx/bin/logrot.pl -c
```

Step 2 Select **Edit Variables** and enter the following information:

CISCO CONFIDENTIAL

Variable	Description
backup directory	The backup directory must already exist. If you do not set a backup directory, then each log will be rotated in its current directory.
restart delay	Optional: Daemon Manager restart delay.

Step 3 Return to the main menu, then select **Edit Log Files**.

Step 4 Enter the following information:

Field	Description
log file location	Enter the full path to the logfile. If the full path is not entered, the default logfile path for your operating system is prepended (for example, /var/adm/CSCOpx/log on UNIX). **Tip** To add multiple logfiles at once, use '*' in the file name. The '*' character matches zero or more characters in a filename. **Note** You must use DOS file names when specifying the logfile path on Windows.
archives to keep	Enter the number of archive revisions to keep. If you don't want to keep any archives, enter 0 for this option.
file size	Enter the maximum file size in kilobytes (KB). The log will not be rotated until this size is reached.
compression option	Allowable options are: Z—The archived file will be compressed using UNIX compress(1). bz2—The archived file will be compressed using bzip2 (available by default on Solaris 8 and above only). gz—The archived file will be compressed with GNU gzip (available by default on Windows only). blank—On Windows platforms, the only valid values are to leave this option blank or set it to gz.
restart delay	How long to wait (in seconds) before proceeding after the Daemon Manager is shut down. This option is only used if logrot is run from the command line using the -s switch (see the "Using Logrot Command Line Switches" section on page 23-12). The default delay is 60 seconds.

Running Logrot

Logrot is typically run as a UNIX cron or Windows AT job.

Step 1 Before automating logrot, verify that it runs on-demand:

- To run logrot on UNIX platforms, enter:

CISCO CONFIDENTIAL

```
/opt/CSCOpx/bin/logrot.pl
```

- To run logrot on Windows platforms, enter:

```
NMSROOT\bin\perl.exe NMSROOT\bin\logrot.pl
```

Step 2 The following commands will run logrot every day at 1:00 AM. The UNIX cron line will also send all output of the command to root via email.

- To set up cron on UNIX, enter:

```
0   1   *   *   *   /opt/CSCOpx/bin/logrot.pl 2>&1 | /usr/lib/sendmail root
```

- To set up AT on Windows, enter (all on one line):

```
at 01:00 /every:M,T,W,Th,F,S,Su C:\progra~1\CSCOpx\bin\perl.exe
C:\progra~1\CSCOpx\bin\logrot.pl
```

This assumes CiscoWorks is installed in the default location on Windows.

Using Logrot Command Line Switches

The logrot utility accepts the following command-line switches:

Switch	Description
-v	Output verbose messages.
-s	Shut down dmgtd (the Daemon Manager) before rotating the logs. This can be a safer way of performing log rotations (see the "Known Problems with Logrot" section on page 23-13). **Note** To specify the restart delay, see the "Configuring Logrot" section on page 23-10.
-c	Re-run the configurator. This option can be specified at any time.

Troubleshooting Logrot

The following topics can help you troubleshoot the logrot utility:

Verifying Files and Time Cycles

You can run the **at** command from the command prompt to see if the files specified and the time cycles are correct. For example:

```
C:\Documents and Settings\Administrator>at
```

CISCO CONFIDENTIAL

will produce output similar to this:

```
Status ID   Day                     Time          Command Line
-------------------------------------------------------------------------------
13   Each M T W Th F S Su    8:22 PM       C:\progra~1\CSCOpx\bin\perl.exe C:\progra~1\CSCOpx\bin\logrot
```

Verifying Scheduled Tasks

To verify scheduled tasks on the server, select **Start > Settings > Control Panel > Scheduled Tasks**. There should be an AT job present, AT<ID> (for example, AT13), that can be verified for correctness.

Viewing the Scheduled Jobs Log File

To look at the scheduled jobs log file:

1. Select **Start > Settings > ControlPanel > Scheduled Tasks**.
2. Select the AT job.
3. Select **Advanced > View Log**.

Verifying Logrot Status

To see if logrot is failing, run it from the command line using the -v (verbose) flag.

Known Problems with Logrot

After shutting down Daemon Manager when rotating daemons.log online, you may find that the daemons.log fills up with a lot of NUL (^@) characters. This is a side-effect of online log rotation. Daemon Managert should archive this file for you when it restarts. This does not cause any application problems, and can be worked around by doing an offline rotation of daemons.log.

When reporting problems, please include the verbose output of logrot (use the -v switch) as well as the logrot.conf file. The logrot.conf file can be found in /opt/CSCOpx/objects/logrot on UNIX and in *NMSROOT*\objects\logrot on Windows.

CISCO CONFIDENTIAL