Syslog Message Interface

- The Cisco Log Message Format, on page 1
- Configure Syslog Destinations, on page 2

The Cisco Log Message Format

The Cisco Log message format is:

```
<PRI>SEQNUM: HOST: MONTH DAY YEAR HOUR:MINUTES:SECONDS.MILLISECONDS TIMEZONE:
%APPNAME-SEVERITY-MSGID:
%TAGS: MESSAGE
```

An example of a CiscoLog formatted syslog event follows. An entry displays on a single line.

```
<134>25: host-w3k: Feb 13 2007 18:23:21.408 +0000: %ICM_Router_CallRouter-6-10500FF:
[comp=Router-A][pname=rtr][iid=acme1][mid=10500FF][sev=info]: Side A rtr process is OK.
```

The following table describes the Cisco Log message fields:

Table 1: Cisco Log Message Fields

Field	Description
PRI	Encodes syslog message severity and syslog facility. Messages are sent to a single syslog facility (that is, RFC-3164 facilities local0 through local7). For more information, see RFC-3164.
SEQNUM	Number used to order messages in the time sequence order when multiple messages occur with the same time stamp by the same process. Sequence number begins at zero for the first message fired by a process since the last startup.
HOST	Fully qualified domain name (FQDN), hostname, or IP address of the originating system.
MONTH	Current month represented in MMM format (for example, “Jan” for January)
DAY	Current day represented in DD format. Range is 01 to 31.
YEAR	Current year represented in YYYY format.
HOUR	Hour of the timestamp as two digits in 24-hour format; range is 00 to 23.
MINUTE	Minute of the timestamp as two digits; range is 00 to 59.

Field	Description
SECOND	Second of the timestamp as two digits; range is 00 to 59.
MILLISECONDS	Milliseconds of the timestamp as three digits; range is 000 to 999.
TIMEZONE	Abbreviated time zone offset, set to +/-#### (+/- HHMM from GMT).
APPNAME	Name of the application that generated the event. APPNAME field values are: PRODUCT_COMPONENT_SUBCOMPONENT PRODUCT – such as ICM COMPONENT – such as Router SUBCOMPONENT – such as CallRouter
SEVERITY	Supported severity values are: 3 (Error) 4 (Warning) 6 (Informational) 7 (Debug)
MSGID	Hexadecimal message id that uniquely identifies the message, such as 10500FF.
TAGS	(Optional) Supported tags are: [comp=%s] - component name including side, such as Router-A [pname=%s] - process name, such as rtr [iid=%s] - instance name, such as acme1 [mid=%d] - message id, such as 10500FF [sev=%s] – severity, such as info
MESSAGE	A descriptive message about the event.

Configure Syslog Destinations

You can configure syslog destinations using the Cisco SNMP Agent Management Snap-in. The syslog feed is available only on the Unified ICM/Unified CCE Logger Node.

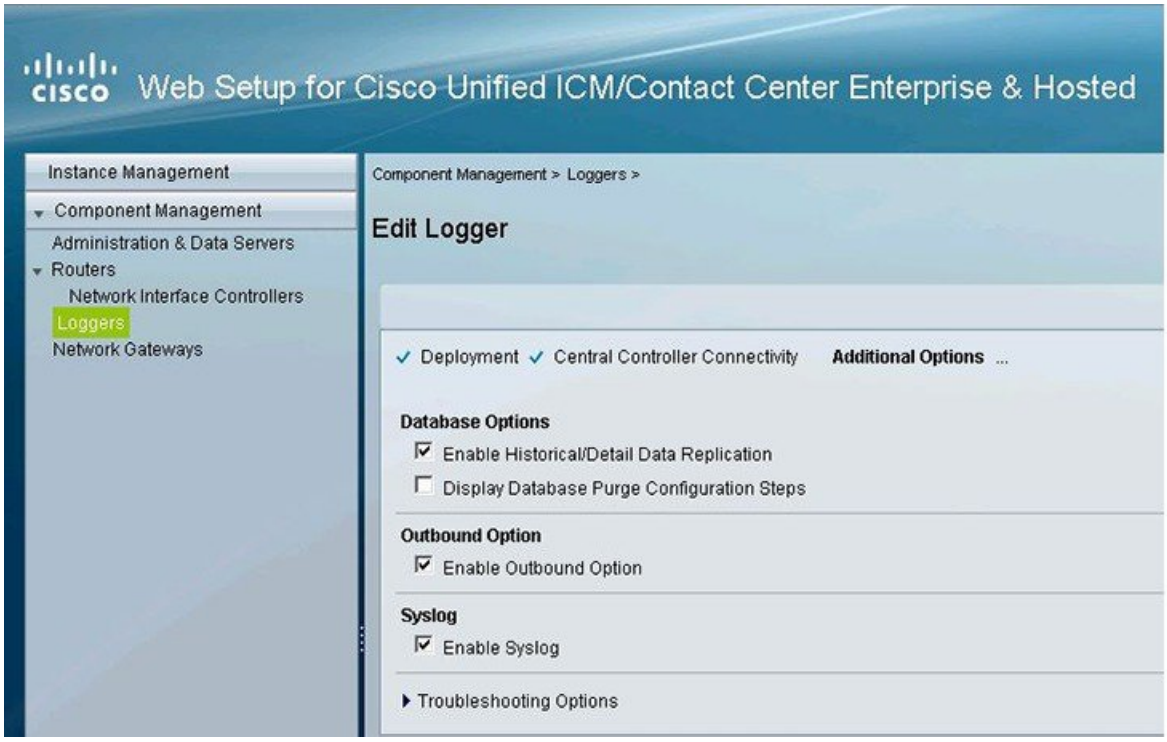
Before you begin

Before you configure the syslog destinations, start the syslog process (cw2kfeed.exe) from the Web Setup tool.

1. Open the Web Setup tool.
2. Select Component Management > Loggers, and then choose the instance of the logger for which you want to enable the syslog event feed.

3. In the Additional Options area, check the **Enable Syslog** check box to enable the syslog event feed process.

Figure 1: Enable Syslog



These steps runs the CW2KFEED process when the logger is started.

Procedure

Step 1 Go to **Start** menu and select **Run**.

Step 2 In the **Start** box, type **mmc / 32** and press Enter key.

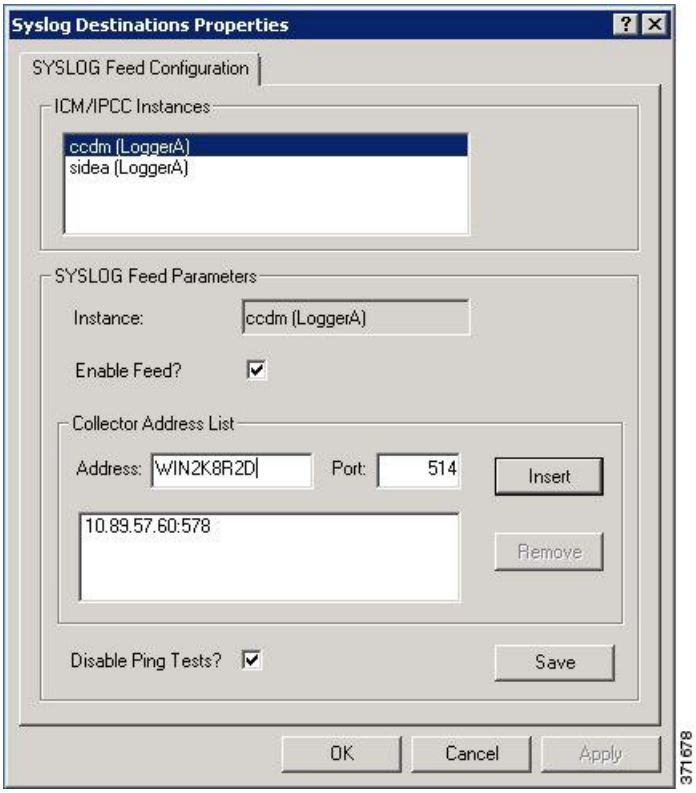
Step 3 Expand **Cisco SNMP Agent Management** in the left pane of MMC snap-in.

Step 4 Highlight **Syslog Destinations** in the left pane under Cisco SNMP Agent Management.
The following columns appear in the right pane:

- ICM Instance Name
- Feed Enabled
- Ping Disabled

Step 5 Right-click the white space in right pane and select **Properties**.
A dialog box appears:

Figure 2: Syslog Destinations Properties Dialog Box



Step 6 From the **ICM/IPCC Instances** list box, select one Unified ICM/Unified CCE instance.
The **Instance** field displays the selected instance.

Step 7 Check **Enable Feed?** check box.

Step 8 In the **Collector Address** field, enter the IP address or Host Name.

Step 9 (Optional) In the **Port** field, enter the collector port number on which syslog collector is listening.

Note The default port is 514.

Step 10 Click **Insert** to add the IP address to the list.

Note You can add up to five IP addresses.

Step 11 (Optional) To remove an existing IP address, select the IP address in the **Collector Address List** area, and click **Remove**.

Step 12 (Optional) Check **Disable Ping Tests?** check box.

Step 13 Click **Save**.

Step 14 Click **OK**.