



Installing the Remote Syslog Analyzer Collector on Windows

The Syslog Analyzer Collector can be installed on a remote UNIX or Windows 2000 or Windows NT machine to process syslog messages. If necessary, it can also filter the syslog messages before forwarding them to the Syslog Analyzer process on the Essentials server. You can uninstall the Syslog Analyzer Collector later, if you do not want to run it on the remote UNIX or Windows server.



Note

Do not install Remote Syslog Analyzer Collector on a machine that has CiscoWorks2000 and Resource Manager Essentials already installed, or stop the CRM logger service before installing Remote Syslog Analyzer Collector. This is because CRM logger will hook to the UDP port and read all the syslog messages. When the SacNTService tries to connect to the same port, it gets a 'address not found' exception, and does not read any syslog messages arriving on the port.

The Syslog Analyzer Collector uses CORBA, an Essentials system service, to communicate with the Essentials server. It functions as follows:

1. At startup, the Syslog Analyzer Collector tries to connect to the Syslog Analyzer on the Essentials server through CORBA (RmeOrb process), which runs on the Essentials server.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

AREA FOR BAR CODE

Copyright © 2001. Cisco Systems, Inc. All rights reserved.

2. After it is connected, the Syslog Analyzer Collector:
 - a. Obtains the filters it needs from the Essentials server to filter syslog messages.
 - b. Sends status to the Syslog Analyzer process about the collected syslog messages, including the number of messages read, number of messages filtered, and number of messages with bad syntax. It also forwards unfiltered messages to the Syslog Analyzer process.

You can install the Syslog Analyzer Collector on a UNIX system or on a Windows system.

This document contains:

- [Preparing to Install the Syslog Analyzer Collector](#)
- [Installing the Syslog Analyzer Collector](#)
- [Configuring the Syslog Analyzer Collector to Run Automatically](#)
- [Uninstalling the Syslog Analyzer Collector](#)
- [Obtaining Documentation](#)
- [Obtaining Technical Assistance](#)

Preparing to Install the Syslog Analyzer Collector

-
- Step 1** Make sure Internet Explorer 4.01. or later is installed on the remote server.
 - Step 2** Obtain the installation file from the Essentials server:
 - Through FTP from the /opt/CSCOPx/htdocs/rdist/sysloga directory of the Essentials server.
 - or
 - Through a browser on the remote server. The URL is:
<http://CiscoWorks2000-server/sysloga/SAC.html>
 - Step 3** Download SacNTService.exe or NT Remote Collector.
 - Step 4** Obtain the SAenvProperties.ini file from the same location from where you obtained the SacNTService.exe file.

- Step 5** Place the file in any directory you want. You will need to specify its location when you start the Syslog Analyzer Collector, so make sure to remember the location.
- Step 6** Update each variable in this file with the appropriate values from the [Properties Variables Table](#).

Properties Variables Table

Table 1 *Properties Variables Table*

Variable	Description
FILE	File from which syslog messages are read. Set a value if a syslog daemon is running on the server.
SAC_PORT	Number of the port on which syslog messages are coming in, typically, port 514. Specify the number of the port from which Syslog Analyzer Collector reads syslog messages.
SAC_SERVER	Essentials server to which Syslog Analyzer Collector forwards parsed and filtered messages.
SAC_SERVER_PORT	Number of port used by RmeOrb process on Essentials server. To check port number: <ol style="list-style-type: none"> Using a browser, log in to the Essentials server. Select Server > Administration > Process Management > Process Status. The Process Status table appears. Scroll down and click RmeOrb. The Process Details window appears. In the Flags row, note the port number (after the -p option).
VERSION	Syslog Analyzer Collector version. Recommended version is 1.0.

Table 1 Properties Variables Table

Variable	Description
BINDAME	<p>Name used by Syslog Analyzer Collector to bind to OSAgent process. Value should be the same as value set for SAC_SERVER variable and followed by ::SaReceiver.</p> <p>For example, if SAC_SERVER variable is set to nm_bgdemo.cisco.com, then BINDNAME variable should be set to nm-bgdemo::SaReceiver.</p> <p>Make sure the name you enter for this variable matches the Essentials server name exactly.</p> <p>To find out the name under which the Essentials server is registered, refer to the value set for PX_HOST in the file, md.properties. This file is located in <i>install_dir/lib/classpath</i>, where <i>install_dir</i> is the directory in which CiscoWorks2000 is installed (C:\Program Files\CSCOpX by default).</p>
DEBUG_LEVEL	<p>Debug level in which you run the Syslog Analyzer Collector.</p> <p>Note It is recommended that you retain the default value which is 4, as this reports ERRORS. Setting it to any other value might result in a large number of debug messages being reported.</p>
SA_APP_NAME	<p>Name Syslog Analyzer Collector uses for printed ERROR or DEBUG messages. It is recommended that you retain the default value, SyslogAnalyzer.</p>

Installing the Syslog Analyzer Collector

Step 1 From the command line, enter **SacNTService /install** to install the SAC service.



Note Do not add the .exe extension to the SacNTService file.

Step 2 Modify the SAenvProperties.ini file, if you have not already done so.

Step 3 To start the service, select **Start > Settings > Control Panel > Services**. The Services window appears.

Step 4 Select Cisco Syslog Collector.

- Step 5** In the Startup Parameters field, enter the location of your SAenvProperties.ini file, for example:

```
-pr c:\directory\SAenvProperties.ini
```



Note

Make sure you use two backslashes (\\) when you specify the pathname, and remember to use the **-pr** argument; otherwise, the Syslog Analyzer Collector will not run. The directory name should be in DOS format. Refer to [Configuring the Syslog Analyzer Collector to Run Automatically](#) for additional control information.

- Step 6** Click **Start**.

The error and debug messages are collected in a log file. You can specify the name and location of this log file. The log file with the specified name is created by the process. The format of the location path is:

```
drive_name:\location_directory\logfile_name
```

It is mandatory to mention the path.

If the directory structure does not exist, then the error and debug messages are put into the event viewer. The default location of the log file is:

```
c:\Program Files\SyslogRemoteCollector.log
```

- Step 7** To run the Syslog Analyzer Collector with different parameters, include additional arguments when you enter the full pathname of the properties file.

Table 2 Arguments

Arguments	
-pr <i>properties file name</i>	properties file name
-sf <i>syslog file name</i>	syslog file name
-sp <i>syslog port #</i>	syslog port number
-bsn <i>bg server name</i>	Essentials server name
-bsp <i>bg server port</i>	Essentials port number
-bnd <i>orb bind name</i>	orb bind name
-dbg [1-6]	debug modes 1-6
-h	print usage information

For example, enter:

```
C:\tmp\SAenvProperties.ini -bsn sbanks-ss20.cisco.com -bsp 420 -bnd  
sbanks-ss20::SaReceiver
```

The [Properties Variables Table](#) contains more information on the arguments.

Step 8 To stop the Syslog Analyzer Collector:

- a. On Windows NT, select **Start > Settings > Control Panel > Services**. The Services window appears.
On Windows 2000, select **Start > Programs > Administration Tools > Services**. The Services window appears.
- b. Select Cisco Syslog Collector.
- c. Click **Stop**.

Configuring the Syslog Analyzer Collector to Run Automatically

You can store the Properties file location in the Windows registry to avoid specifying the Properties file in the start up parameters of the service window. During startup, if no parameters are specified, the Syslog Analyzer Collector will look in the registry for the location of the Properties file.

To store the Properties file in the registry, from the command line, enter:

```
SacNTService /cmd:SacNTService -pr C:\directory\SAenvProperties.ini  
-set
```



Note

You can store only the Properties file location in the registry; any other command line options are ignored.

To run the Syslog Analyzer Collector automatically every time the machine starts up:

-
- Step 1** On Windows NT, select **Start > Settings > Control Panel > Services**. The Services window appears.
On Windows 2000, select **Start > Programs > Administration Tools > Services**. The Services window appears.
 - Step 2** Select Cisco Syslog Collector
 - Step 3** Click **Startup**.
 - Step 4** Select Automatic.
 - Step 5** Click **OK**.
-

Uninstalling the Syslog Analyzer Collector

-
- Step 1** Select **Start > Settings > Control Panel > Services**. The Services window appears.
 - Step 2** Select Cisco Syslog Collector.
 - Step 3** Stop the Syslog Collector service.
 - Step 4** In the directory where you installed the SacNTService.exe file, enter:
`SacNTService / uninstall`
-

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the “Documentation Roadmap” section.

AccessPath, AtmDirector, Browse with Me, CCDE, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0105R)

Copyright © 2001, Cisco Systems, Inc.

All rights reserved.

