CA User Activity Reporting Module

Overview Guide

Release 12.5.04

CA Technologies Product References

This document references the following CA Technologies products:

- CA ControlMinder
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA User Activity Reporting Module
- CA IdentityMinder
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- CA Security Command Center (CA SCC)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- Quick Start Overview—This existing topic has been updated to reference additional types of events, besides syslogs, that can be collected by the default agent on the CA User Activity Reporting Module server.
- Policy Violation Alerting—This existing topic has been updated to reference the ability to send alerts as SNMP traps to network security monitoring systems and to direct alerts to run an IT PAM event/alert output process, such as one to create help desk tickets.
- Explore the Bookshelf of Documentation—This existing topic has been updated to reference the new API Programming Guide, which now appears on the CA User Activity Reporting Module bookshelf.

More information:

Quick Start Overview (see page 13)
Policy Violation Alerting (see page 49)
Explore the Bookshelf of Documentation (see page 59)

Contents

Chapter 1: Introduction

This section contains the following topics:

About this Guide

This *Overview Guide* introduces CA User Activity Reporting Module. It begins with quick tutorials that give you hands on experience with the product right away. The first tutorial walks you through getting a single-server CA Enterprise Log Manager up and running and viewing syslogs collected from UNIX devices in close network proximity. The second tutorial walks you through installing an agent on a Windows operating system, configuring log collection, and viewing resulting events logs. It then describes the major features and where to go to learn more. This guide is intended for all audiences.

A summary of the contents follows:

Section	Describes how to
About CA Enterprise Log Manager	Integrate CA User Activity Reporting Module into your current network environment
Quick Start Deployment	Install a single-server system, configure syslog event sources, update the syslog connector for the default agent, and view refined events
Windows Agent Deployment	Prepare for agent installation, install an agent for the Windows operating system, configure one connector for agent-based collection, update the event source, and view generated events
Key Capabilities	Benefit from key features, including log collection, log storage, compliance reporting and alerting
Learning More about CA User Activity Reporting Module	Get the information you need through tooltips, online help, and the documentation bookshelf

Note: For details on operating system support or system requirements, see the *Release Notes*. For step-by-step procedures on installing CA User Activity Reporting Module and performing initial configuration, see the *Implementation Guide.* For details on installing an agent, see the *Agent Installation Guide*. For details on using and maintaining the product, see the *Administration Guide.* For help on using any CA User Activity Reporting Module page, see the online help.

About CA User Activity Reporting Module

CA User Activity Reporting Module focuses on IT compliance and assurance. It lets you collect, normalize, aggregate, and report on IT activity, and generate alerts requiring action when possible compliance violations occur. You can collect data from disparate security and non-security devices.

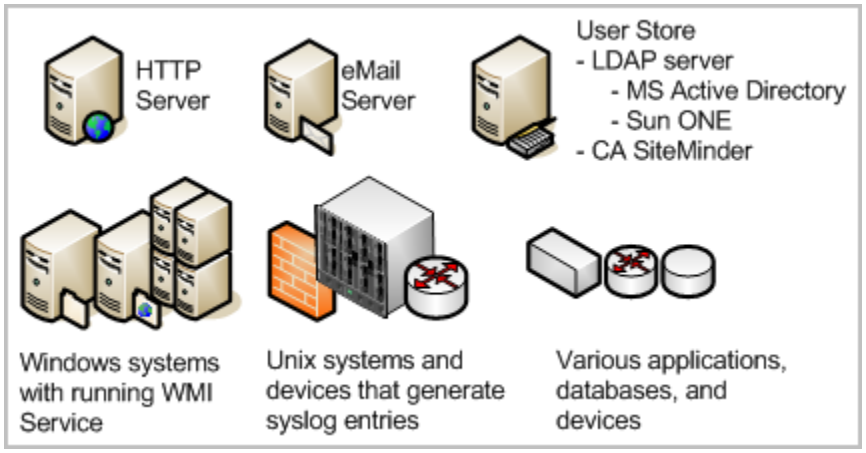
Your Network--Before Installation

Federal regulations and mandates require log record management. To comply, you must:

- Make logs available for auditing.
- Store logs for years.
- Restore logs upon request.

What makes log records difficult to manage is their large number, their location, and their temporary nature. Logs are generated continuously by user and process activity on software. The rate of generation is measured in events per second (eps). Raw events are recorded on every active system, database, and application in your network. Backing up log records for storage must be done at each event source before they are overwritten. Restoring event logs is difficult when backups from different event sources are stored separately.

What makes raw events tedious to interpret is their string format where the event severity does not stand out. Also, similar data from different systems varies.



Operational efficiency demands a solution that consolidates all logs, makes logs easy to read, automates archiving to storage, and simplifies log restoration. CA User Activity Reporting Module offers these benefits, and lets you send alerts to individuals and systems when critical events occur.

What You Install

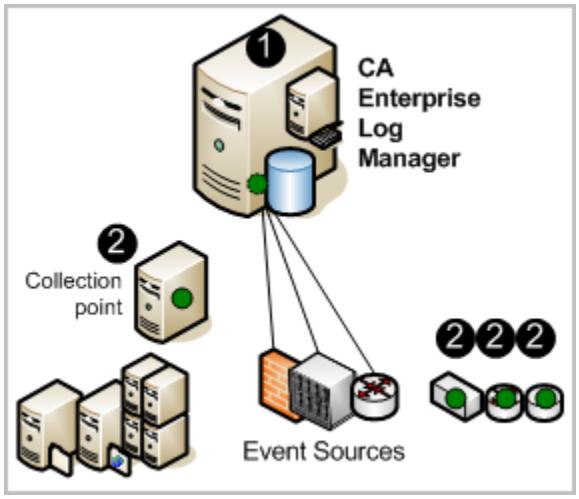
It does not take long to set up a single-server solution and begin collecting events.

The installation disks include these components:

- Operating system (Red Hat Enterprise Linux) for the soft appliance
- CA User Activity Reporting Module Server
- CA User Activity Reporting Module Agent (hereafter referred to as the agent)

In the following illustration, CA User Activity Reporting Module is depicted as a server containing a small server, a dark (green) circle, and a database. The small server represents the local repository that stores application-level content. The dark circle represents the default agent, and the database represents the event log store where incoming event logs are processed and made available to queries and reports.

The dark (green) circles on the collection point and the other event sources represent separately installed agents. Installing agents is optional. You can collect syslogs from UNIX-compatible event sources with the default agent after completing the required configuration.



The numbers on the illustration refer to these steps:

1. You install the operating system for the soft appliance and then you install the CA User Activity Reporting Module application. As soon you configure your sources to push syslogs to CA User Activity Reporting Module and indicate the syslog targets in the configuration of the connector for the default agent, syslogs are collected and refined for easy interpretation.
2. (Optional) You can install an agent on a host you dedicate as a collection point or you can install agents directly on the hosts with sources that are generating events you want to collect.

Note: See the *Implementation Guide* for details on installing the soft appliance. See the *Agent Installation Guide* for details on installing agents.

More information:

Install an Agent (see page 35)

Chapter 2: Quick Start Deployment

This section contains the following topics:

Quick Start Overview

You can achieve a simple, functioning CA User Activity Reporting Module deployment with one soft appliance. The predefined syslog connector makes it possible for the default agent to receive generated syslog events. All you need to do is configure your syslog sources to push syslog events to CA User Activity Reporting Module and edit the syslog connector configuration to identify the syslog targets. What is received depends on the bandwidth between the server and the syslog sources and latency.

Log sensors, including WinRM and ODBC, support direct log collection from over twenty non-syslog event sources. The WinRM log sensor lets you collect events directly from servers running Windows operating systems, such as Forefront Security for Exchange server, Forefront Security for SharePoint Server, Microsoft Office Communication Server, and Hyper-V virtual server and services such as Active Directory Certificate Services. The ODBC log sensor lets you capture events generated by Oracle9i or SQL Server 2005 databases. For details, see the CA Enterprise Log Manager Product Integration Matrix.

You need EiamAdmin credentials to install CA User Activity Reporting Module. As the EiamAdmin superuser, you configure an Administrator account which you use to do the configuration. If you log on with the Administrator credentials, you can verify that the setup is functioning by viewing self-monitoring events.

Install a Single-Server System

The simplest deployment that lets you view queried events is a single-server system. Be sure to select a machine that meets or exceeds the minimum hardware requirements for a CA User Activity Reporting Module soft appliance.

Note: See the *Release Notes* for the certified hardware list, operating system support, and system software and service requirements.

To install a CA User Activity Reporting Module for a single-server system

1. Have the following information at hand:
   - A password to be used as the root password
   - Host name for your appliance
   - If not using DHCP, the static IP address, subnet mask, and default gateway for your appliance
   - Domain for the appliance

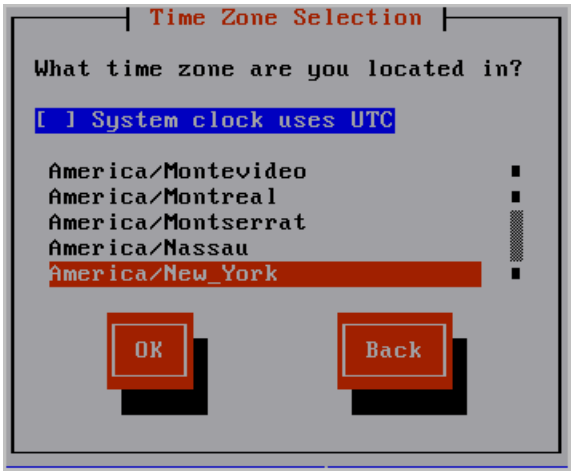
     Note: The domain must be registered with the DNS Servers in your network for the installation to complete.
   - IP addresses of the DNS servers
   - (Optional) IP address of your NTP time server
   - A password for the default installation superuser name, EiamAdmin
   - CAELM.

     This is the default application name for the CA User Activity Reporting Module application.

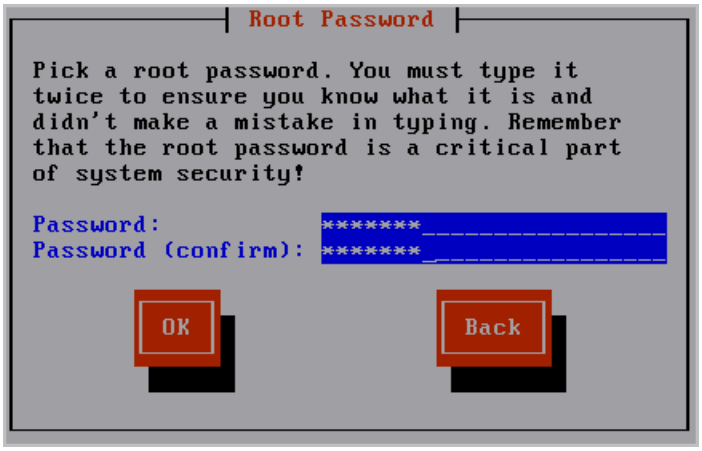
2. Install the preconfigured operating system using the media you created from the CA User Activity Reporting Module download package. During the operating system installation, do the following:

   a. Choose a keyboard type. The default is U.S.

   b. Choose a time zone, for example, America/New York and select OK.



   c. Type the password to be used as the root password, then retype it to confirm. Select OK.



Installation progress information appears.

d. Remove the operating system installation disc and press Enter to reboot the system.

The system reboots and enters non-interactive startup. It displays messages describing installation progress. Detailed information about this installation is saved in the following file: /tmp/pre-install_ca-elm.log.

The following prompt appears:

```
Please insert the CA Enterprise Log Manager r12 - Application Install disk and press enter.
```

3. Insert the CA User Activity Reporting Module Application disc. Press Enter.

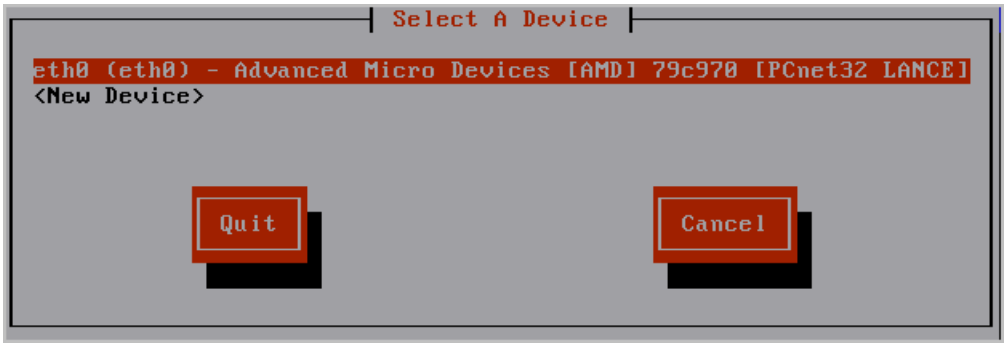
   Your system is reviewed for whether it meets the minimum recommended specifications for optimal performance. If it does not, a prompt appears asking whether you want to stop the installation process.

   The following prompt appears:

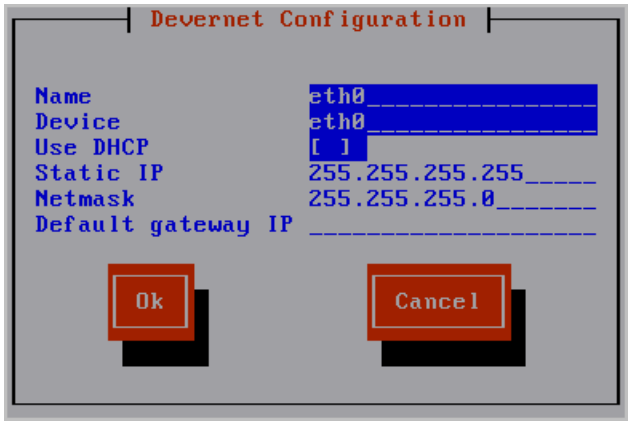
   ```
   Please enter a new hostname :
   ```

4. Enter the host name for this CA User Activity Reporting Module soft appliance. For example, enter CALM1.

5. Accept the default device, eth0. Press Enter to go to the next screen.



6. Do one of the following and then select OK.
   - Select Use DHCP, an acceptable option only for a standalone test system.
   - Enter the static IP address, subnet mask, and default gateway IP address to be associated with the hostname you entered.



   The network services are restarted with the new settings, which are displayed.

   The following message appears:

   ```
   Do you want to change the network configuration? (n):
   ```

7. Review the network settings. If satisfactory, type n, or press Enter, when the message appears allowing you to change the network settings.

   The following message appears:

   ```
   Please enter the domain name for this system :
   ```

8. Enter your domain name, such as <yourcompany>.com.

   The following message appears:

   ```
   Please enter a comma separated list of DNS servers to use:
   ```

9. Enter the IP addresses of your internal DNS servers separated by commas with no spaces.

   Your system date and time is displayed with the following message:

   ```
   Do you want to change the system date and time? (n)
   ```

10. Review the displayed system date and time. If satisfactory, type n or press Enter.

    The following message appears:

    ```
    Do you want to configure the system to update the time through NTP?
    ```

11. If you want to use a Network Time Protocol (NTP) server, continue as follows. Otherwise, specify no and continue with the next step.

    a. Respond yes to the message.

       If you specify yes, the following message appears:

       ```
       Please enter the NTP Server name or IP Address
       ```

    b. Enter the host name or the IP address of the NTP server.

       A confirmation message similar to the following appears: "Your system has been configured to update the time at midnight using the NTP server located at <yourntpserver>."

12. Read the end user license agreements (EULAs) presented and respond as follows:

    a. Read the EULA for the Sun Java Development Kit (JDK).

       At the end of the EULA, the following message appears:

       ```
       Do you agree to the above license terms? [yes or no]
       ```

    b. Type yes if you agree to the terms.

       Product registration information is displayed followed by this message:

       ```
       Press Enter to continue.....
       ```

    c. Press Enter.

       Messages state that in preparation for CA User Activity Reporting Module installation, the system settings are being configured. The CA end user license agreement displays.

    d. Read the CA EULA.

       At the end of the license, the following message appears:

       ```
       Do you agree to the above license terms? [Yes or no]:
       ```

    e. Type Yes if you agree to the license terms.

       CA EEM server information appears.

13. Respond to the following prompts to configure CA EEM.

    ```
    Do you use a local or remote EEM server?
    Enter l (local) or r (remote) :
    ```

    a. To create a standalone test system, enter l for local.

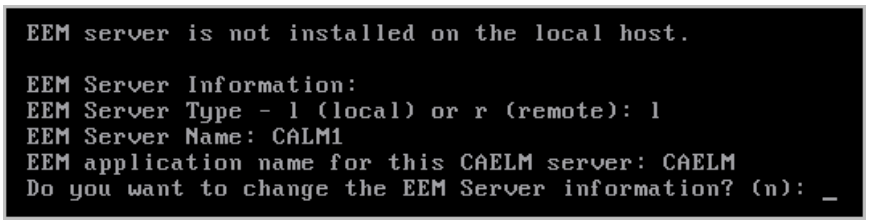
       ```
       Enter the password for the EEM server EiamAdmin user :
       Confirm the password for the EEM server EiamAdmin user :
       ```

    b. Type the password you want to assign to the EiamAdmin default superuser; type it again.

       ```
       Enter an application name for this CAELM server (CAELM):
       ```

c. Press Enter to accept CAELM, the default application name for CA User Activity Reporting Module.

The EEM Server information you entered so far appears with a message that asks if you want to make changes.



d. Press Enter or enter n for no to accept the CA EEM server information you entered.

The installation process begins. Messages appear showing the progress as each CA User Activity Reporting Module component is successfully installed, registrations completed, certificates acquired, files imported, and components configured. The message CA ELM Installation succeeded appears. When the installation completes, the system displays the console logon address.

14. Respond to the following prompt:

```
Do you want to run CAELM Server in FIPS mode?
Enter Yes or No
```

If you enter y, the CA User Activity Reporting Module server will start up in FIPS mode. If you enter n, it will start up in non-FIPS mode.

15. Make note of this address. This is the address you enter in a browser to access this CA User Activity Reporting Module server. That is, https://<hostname>:5250/spin/calm.

A <hostname> login prompt appears. You can ignore this.

Note: If, for any reason, you want to display the operating system prompt from this login prompt, you can do so by entering caelmadmin and the default password, which is the password you assigned to the EiamAdmin user account. You use the caelmadmin account to log in to the appliance on the console or through SSH.

16. Continue as follows:

- If you configured a static IP address, be sure to register this IP address with the DNS servers specified in step 9.
- If you configured DHCP, update your hosts file on the machine from which you intend to browse to this server.
- Browse to the URL you made note of in step 14 and configure the first Administrator.

Update Your Windows Hosts File

During CA User Activity Reporting Module installation, you can identify one or more DNS servers or select Use DHCP. If you selected DHCP, you must update your Windows hosts file on the computer from which you plan to access the CA User Activity Reporting Module with your browser.

To update your hosts file on the host with your browser

1. Open Windows Explorer and navigate to C:\WINDOWS\system32\drivers\etc.
2. Open the hosts file with an editor, for example, Notepad.
3. Add an entry with the IP address of the CA User Activity Reporting Module server and the corresponding hostname.
4. Select Save from the File menu, then close the file.

Configure the First Administrator

After installing a single-server CA User Activity Reporting Module, you prepare for configuration by browsing to the URL of the CA User Activity Reporting Module from a remote workstation, logging on, and creating an Administrator account you can use to perform the configuration.

Note: For the purpose of this Quick Start deployment, we accept the default user store, and the default password policies. Typically, these are configured before adding the first Administrator.

To configure the first Administrator

1. Connect to the following URL from your browser, where hostname is either the host name or IP address of the server where you installed the CA User Activity Reporting Module.

   `https://<hostname>:5250/spin/calm`

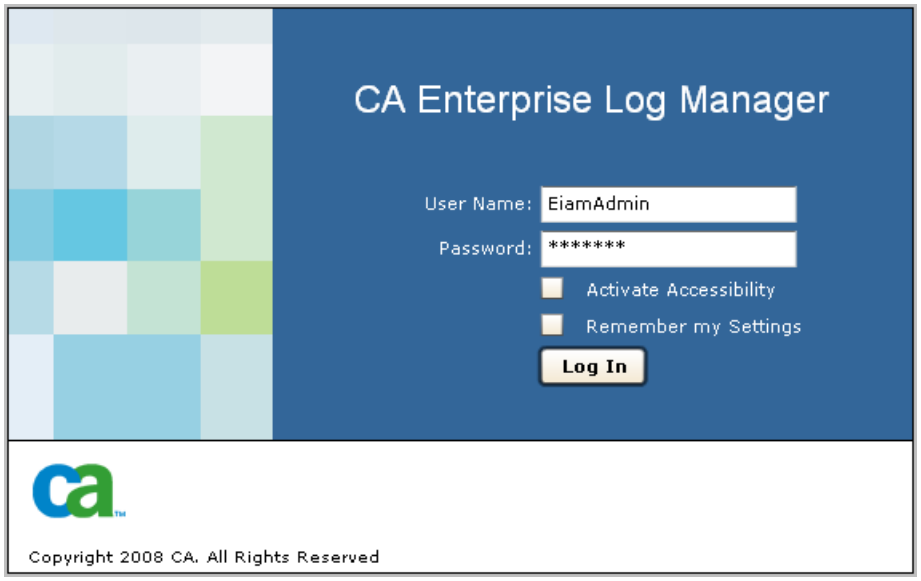
2. If a security alert appears, do the following:
   a. Click View Certificate.
   b. Click Install Certificate, accept the defaults, and finish the import wizard.

      A security warning appears stating you are about to install a certificate claiming to represent the host name of the CA User Activity Reporting Module server.
   c. Click Yes.

      The root certificate is installed and a successful import message appears.
   d. Click OK.

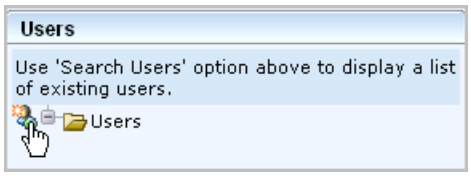
      The trusted certificate dialog appears.
   e. (Optional) Click the Certification Path and verify the certificate status says this certificate is OK.
   f. Click OK, and then click Yes.

      The logon page appears.
3. Log on with the EiamAdmin user name and the password you creating when you used to install the software. Click Log In.

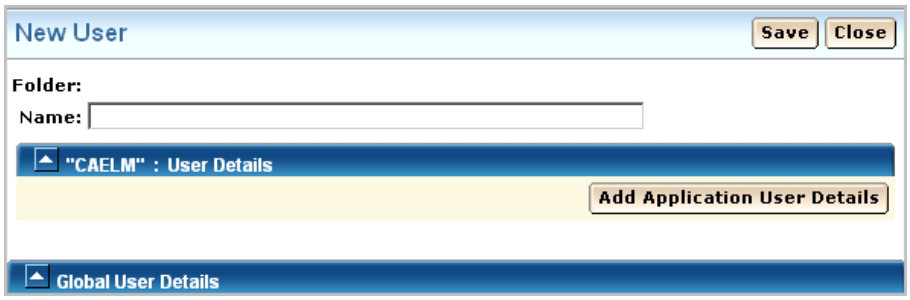


   The application opens with only the Administrator tab and the User and Access Management subtab active.
4. Click Users.

5. Click Add New User.

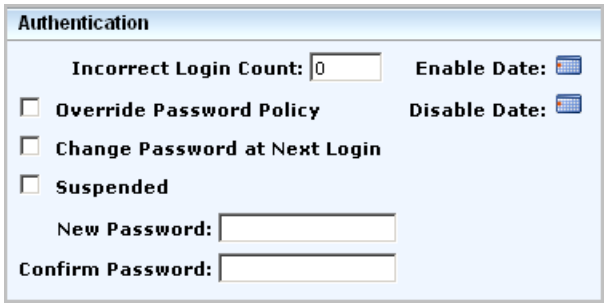


6. Enter your name in the Name field and click Add Application User Details.



7. Select Administrator and move it to the Selected User Groups list.

8. Under Authentication, enter a password for this new account in the two fields for entry and confirmation.



9. Click Save and then click Close. Click Close.

10. Click the Log out link on the toolbar.

    The logon page appears.

11. Log back into CA User Activity Reporting Module with the Administrator credentials you just defined.

    CA User Activity Reporting Module opens with all functionality enabled. The Queries and Reports tab and Queries subtab is displayed.

12. (Optional) View your login attempts as follows:

    a. Select the System Access from the query tag list.

    b. Select System Access Detail from the query list.

    The query results show your two login attempts, first as EiamAdmin, then with your Administrator name where the login attempts are marked with S for successful.

CA Severity	Date ▲	Ac...	Performer	Host	Log Na...	Category	Action	Result
Information	Wed Oct 8 2008 09:30:37 AM		EiamAdmin		CALM	System Access	Login Attempt	S
Information	Wed Oct 8 2008 09:31:38 AM			127.0.0.1	EiamSdk	System Access	Login Attempt	S
Information	Wed Oct 8 2008 09:31:38 AM			127.0.0.1	EiamSdk	System Access	Authorization	S
Information	Wed Oct 8 2008 09:31:48 AM		Administrator1		CALM	System Access	Login Attempt	S

Configure Syslog Event Sources

To enable direct collection of syslog events by the default agent that exists on each CA User Activity Reporting Module server, you begin by identifying the syslog event sources from which you want to collect events and determining the associated integration. Then you do the following two things in either order.

- Configure the syslog event sources. Log on to each host where a syslog event source is running and configure it as documented in the connector guide for that syslog integration.
- Configure the syslog connector on the default agent to add the target syslog integrations associated with the configured event sources.

As soon as you complete this two-step configuration, event collection and refinement begins. Then, you can use CA User Activity Reporting Module to view or report on events you care about in a standardized format. You can also generate alerts when specific events occur.

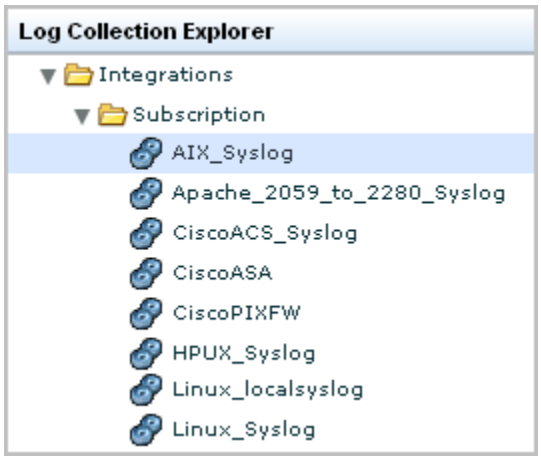
To configure a selected syslog event source

1. Log on to the host with a target syslog event source.
2. Launch CA User Activity Reporting Module from a browser on this host.
3. Click the Administration tab and Log Collection subtab.

   The Log Collection Explorer appears.

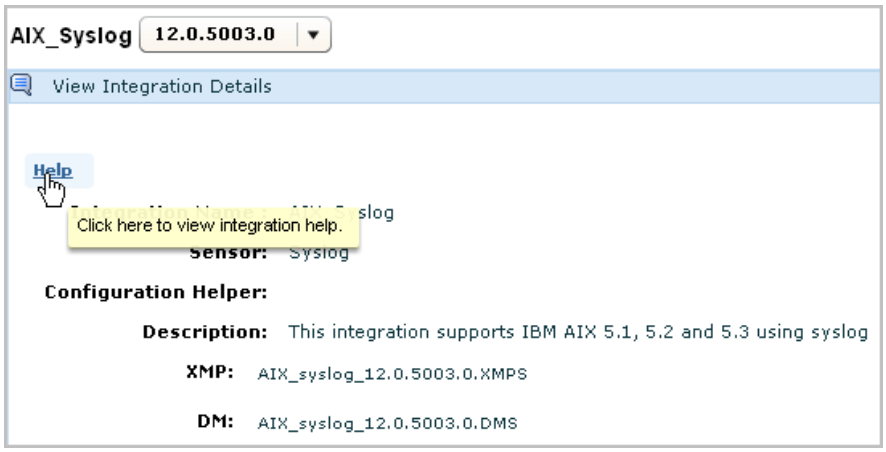
4. Expand Event Refinement Library, Integrations, Subscription.

   The list of predefined integrations displays. An abbreviated example follows:



5. Select the integration for the event source you need to configure. For example, if you wanted to collect syslogs generated by an AIX operating system, you would select AIX_Syslog.

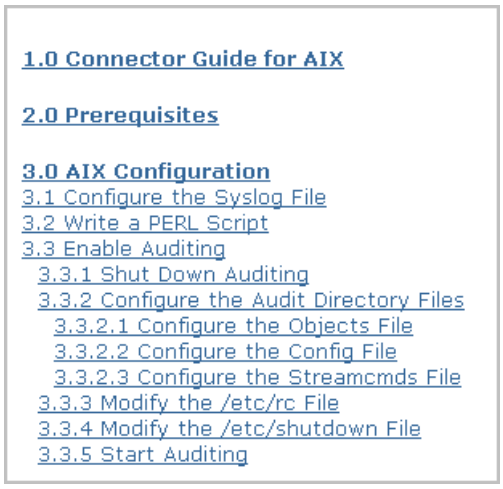
   The integration details appears.



6. Click the Help button located just above the Integration name on the right hand pane.

   The connector guide for the selected integration appears.

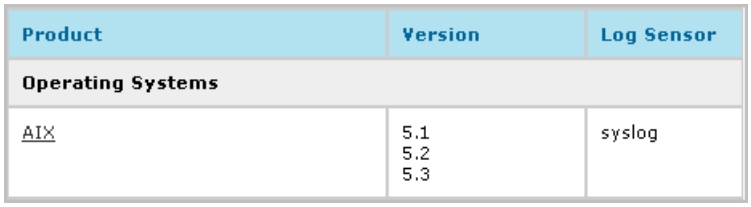
7. Click the section on the event source configuration requirements. In this example, the documentation describes how to configuring the AIX operating system event source to send its syslogs to CA User Activity Reporting Module.



Example--Alternative Source for Connector Guides: Support Online

You can open a selected connector guide from within the CA User Activity Reporting Module user interface or from CA Support Online. Following is an example that shows how to open a connector guide from this alternative source.

1. Log on to CA Support Online.
2. Select CA Enterprise Log Manager from the Select a Product page drop-down list.
3. Scroll to Product Status and select CA Enterprise Log Manager Certification Matrix.
4. Select Product Integration Matrix.
5. Find the category for the integration associated with the event source you are configuring. For example, if the event source is the AIX operating system, scroll to the Operating Systems category and click the AIX link.



Product	Version	Log Sensor
Operating Systems		
AIX	5.1 5.2 5.3	syslog

Edit the Syslog Connector

Each CA User Activity Reporting Module has a default agent. When a CA User Activity Reporting Module is installed, its default agent has a partially configured connector called Syslog_Connector, which is based on the listener, Syslog. This listener receives raw syslog events on the default ports as soon as you configure the event sources to send syslogs to CA User Activity Reporting Module. However, for CA User Activity Reporting Module to refine these raw events, you must edit this Syslog_Connector. Certain edits are mandatory; others are optional.

- You must identify the syslog targets when you edit this connector. You select as syslog targets each integration that corresponds to one or more event sources you have configured or plan to configure. Your identification of syslog targets enables CA User Activity Reporting Module to properly refine the events.
- Optionally, you can apply suppression rules, limit the acceptance of syslogs to trusted hosts, specify ports to listen on other than 514, the well-known syslog UDP port, and 1468, the default TCP port, and/or add a new time zone for a trusted host.

To edit the syslog connector for a default agent

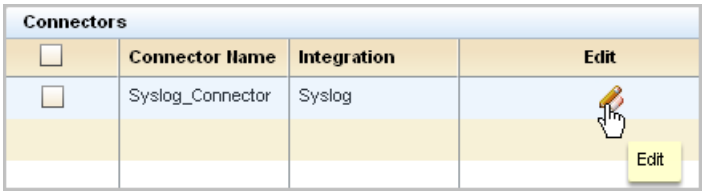
1. Click the Administration tab.

   The Log Collection subtab is displayed.

2. Expand Agent Explorer and then expand the Default Agent Group or the user-defined group with the CA User Activity Reporting Module to be configured.

3. Select the name of a CA User Activity Reporting Module server.

   The connector named Syslog_Connector is displayed.



4. Click Edit.

   The Edit Connector wizard appears with the Connector Details step selected.

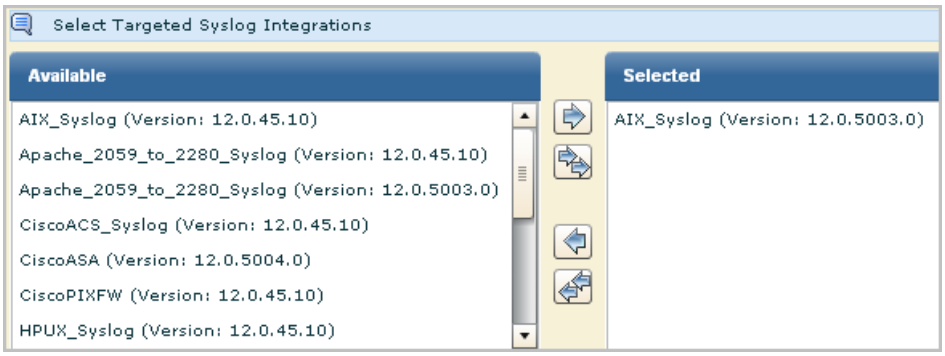
5. (Optional) Click Apply Suppression Rules. If there is any syslog event type that you want suppressed, that is, *not* collected, move that event type from the available list to the selected listed. Select the event to move and click the move button.

6. Click the Connector Configuration step.

   All available integrations are selected by default.

7. Select syslog targets by moving the syslog integrations to target from the available list to the selected list.

   For example, if you have configured the AIX operating system on a host in your network, you would move the syslog target, AIX_Syslog, from the available list to the selected list.



8. (Optional) Identify the trusted hosts from which the syslog connector is to accept incoming events. Enter the IP address in the entry field and click Add. Repeat for each trusted host. Then, when an event is received from a host not configured as trusted, that event is rejected.

   Note: It is a good practice to configure trusted hosts. Typically, you configure all the hosts on which you have configured event sources to send syslogs to CA User Activity Reporting Module. Specifying trusted hosts ensures the default agent does not accept events from rogue systems that an attacker has configured to send events to the syslog listener.

9. (Optional) Add ports.

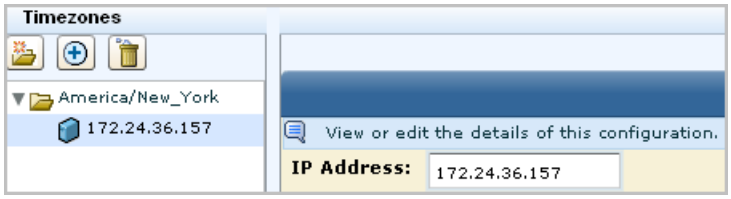
   You can typically accept the default UPD and TCP ports for the default agent.

   Note: You can gain performance improvements by defining a syslog connector for different event types and specifying different ports for each. Be sure to select unused ports when making new port assignments.

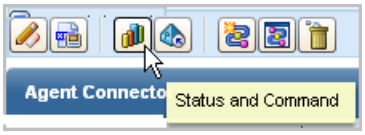
10. (Optional) Add a time zone only if collecting syslogs from machines in a different time zone from the soft appliance.

    a. Click Create Folder and expand the folder.

    b. Highlight the blank entry under the folder. Enter the IP address of either a trusted host you configured for this connector or the NTP time server you specified at installation of the CA User Activity Reporting Module.



11. Click Save and Close.
12. View the status.
    a. Click Status and Command



    View Status of Agents is selected. The host name of the server you installed appears in the Agent column, since the default agent is on this server. The status is shown as running.

    b. Click the Running link to view details.

    c. Click the Connectors button to view the status of connectors.

    d. Click the Running link.

    The percentage CPU, memory usage, average events per second (EPS), and filtered event count appear.

View Syslog Events

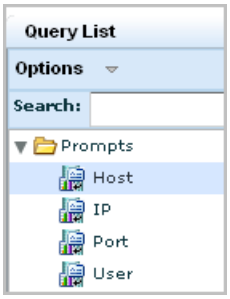
One of the quickest ways to view query results on events collected by a syslog listener is to use the Prompt for Host.

To view syslog events

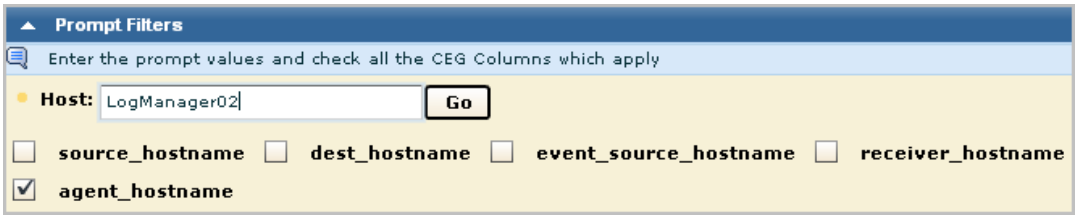
1. Select the Queries and Reports tab.

   The Queries subtab displays.

2. Expand Prompts under Query List and select Host.



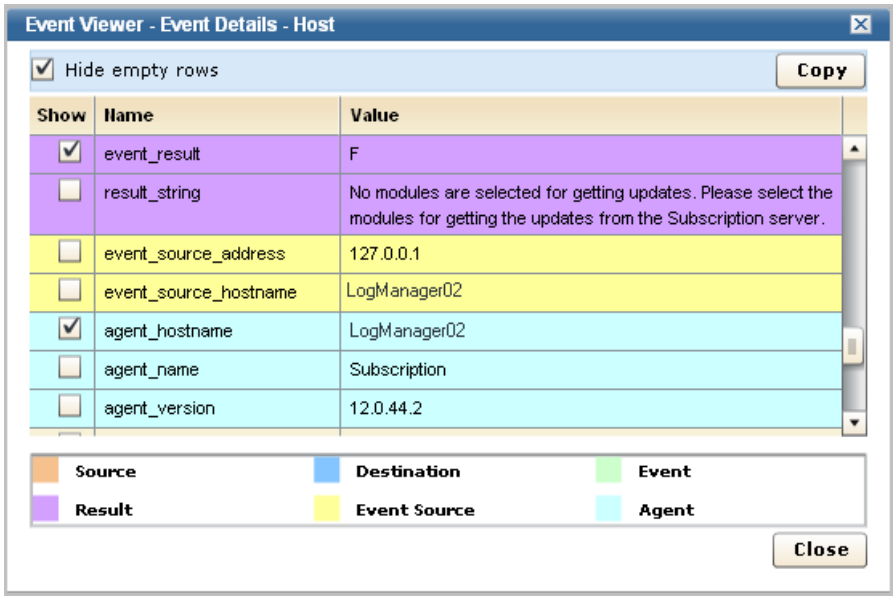
3. Submit a query for events collected by the default agent.
   a. Enter the default agent host name in the Host field, which is also the name of the CA User Activity Reporting Module on which it resides.
   b. Select agent_hostname.
   c. Click Go.



4. Display the results to examine.
   a. Click the Results column to sort by results.
   b. Scroll to the first result of F for failure. Assume it is a configuration warning in the category Configuration Management.
   c. Double-click to select the row to view in detail.

   The Event Viewer appears.

5. Scroll to the area where the Result is displayed. In the example, the error is a warning that you need to configure the subscription module. This is a warning you should ignore until you have finished installing all of the CA User Activity Reporting Module servers you plan to install.



Chapter 3: Windows Agent Deployment

This section contains the following topics:

Create a User Account for the Agent

Before installing an agent on a Windows operating system, you create a new account for the agent in the Windows Users folder. The purpose of creating this low-privileged account for the agent is to allow it to run with the lowest possible privileges. You supply the user name and password you create here when you install the agent.

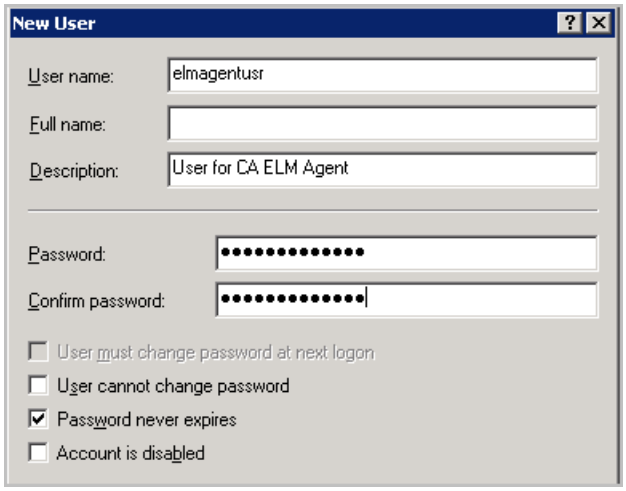
Note: You can bypass this step and specify the domain credentials of an Administrator for the agent when you do the installation, but this is not considered a good practice.

To create a Windows user account for the agent

1. Log on to the host where you plan to install the agent. Use Administrative credentials.
2. Click Start, Program Files, Administrative Tools, Computer Management.
3. Expand Local Users and Groups.
4. Right-click Users and select New User.

   The Windows dialog, New User appears.
5. Enter a user name and enter a password twice. A strong password has mix of alpha, numeric, and special characters. For example, calmr12_agent. Optionally, enter a description.

   Important! Remember this name and password or record it. You will need to enter it when you install the agent.



6. Click Create. Click Close.

More information:

Install an Agent (see page 35)

Set the Agent Authentication Key

Before you install the first agent, you must know the agent authentication key. You can use the default, if no key has been set, use the current key, if one is set, or set a new key. The agent authentication key configured here must be entered during the installation of each agent. Only an Administrator can perform this task.

To set the agent authentication key

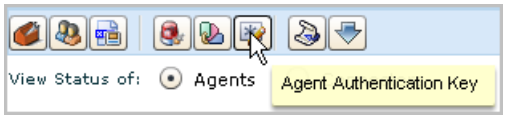
1. Open the browser on the host where you plan to install the agent and enter the URL for the CA User Activity Reporting Module server for this agent. An example follows.

   `https://<IP address>:5250/spin/calm/`

2. Log on to the CA User Activity Reporting Module. Enter your name and password and click Logon.
3. Click the Administration tab.

   The Log Collection Explorer displays in the left pane.
4. Select the Agent Explorer folder.

   A toolbar appears in the main pane.
5. Click Agent Authentication Key



6. Enter the agent authentication key to be used for agent installation or take note of the current entry.

   Important! Remember or record this key. You will need it to install the agent.

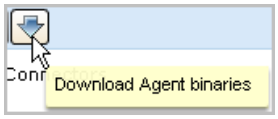
7. Click Save.
8. Continue with the next step, Download the Agent Installation Program.

Download the Agent Installation Program

If you just set the agent authentication key, you are positioned to download the agent installation program onto the desktop.

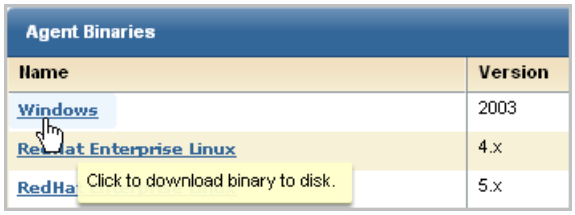
To download the agent installation program

1. Click Download Agent binaries from the toolbar displayed for Agent Explorer.



   Links for the available agent binaries appear in the main pane.

2. Click the Windows link to install the agent on a server with a Window Server 2003 operating system.



   The dialog, Select location for download by <IP address>, appears.

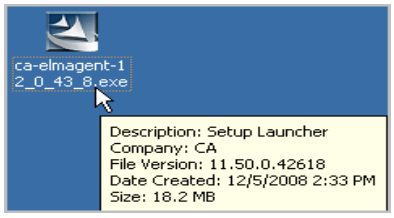
3. Select the desktop and click Save.

   A message showing the progress of the download of the selected agent binary appears, followed by a confirmation message.

4. Click OK.

5. Minimize the browser but leave the connection open so you can quickly verify the installation after it completes.

   The Setup Launcher for the agent installation program appears on the desktop.



Install an Agent

Before you begin, have at hand the following:

- IP address of the CA User Activity Reporting Module server from which you downloaded the agent program
- User name and password from the user account you created for the agent
- Agent authentication key you set

To install an agent for a Windows host

1. Double-click the agent installation launcher.

   The installation wizard starts.

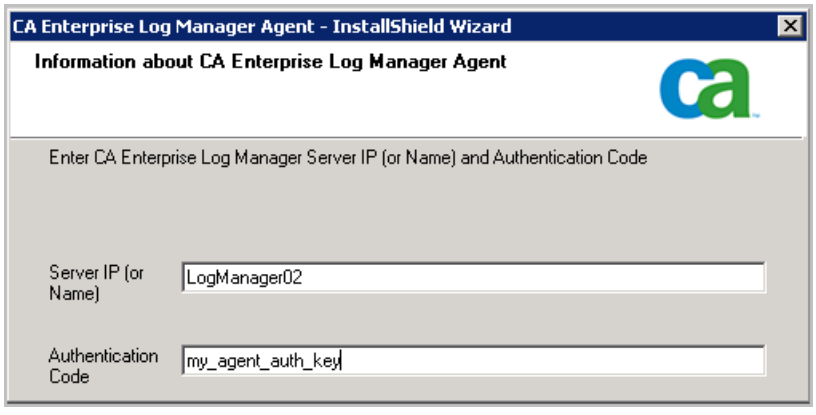
2. Click Next, read the license, click I accept the terms in the license agreements to continue, and click Next.
3. Accept the installation path or change it and click Next.
4. Enter the requested information as follows:

   a. Enter the hostname for the CA User Activity Reporting Module to which this agent is to forward the logs it collects.

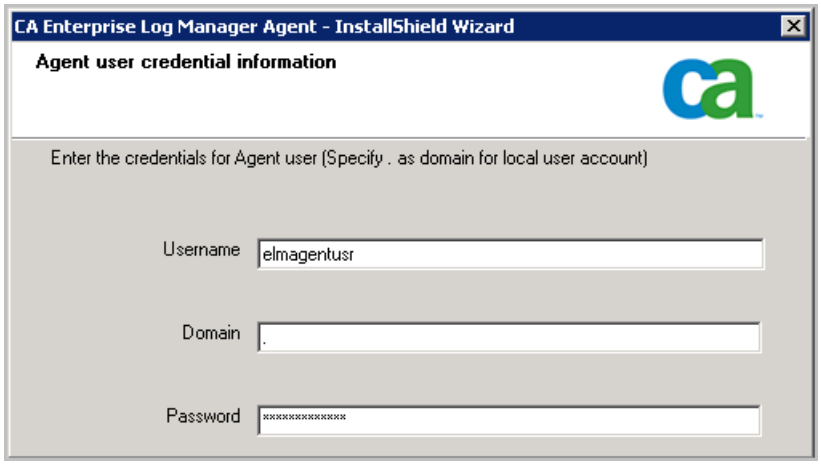
      Note: Since the CA User Activity Reporting Module in this example scenario uses DHCP for IP address assignment, you should not enter the IP address here; doing so introduces the risk of having to reinstall the agent if the IP address of the server ever changes.

   b. Enter the agent authentication key.

   An example follows:



5. Enter the name and password defined in the user account you set up for the agent and then click Next.



6. Click Next. Specifying an exported connector file is optional.

   The Start Copying Files page appears.

7. Click Next.

   The agent installation process completes.

8. Click Finish.

9. Continue with configuring connectors for this agent.

   After connectors are configured, the collected events are sent to the CA User Activity Reporting Module Event Log Store through port 17001.

   Important! If you do not allow outgoing traffic from the host on which you installed the agent and you use the Windows Firewall, you need to open this port on your Windows Firewall.

More information:

Download the Agent Installation Program (see page 34)
Create a User Account for the Agent (see page 32)
Set the Agent Authentication Key (see page 33)

Create a Connector Based on NTEventLog

After installing an agent, you create a connector to specify the event sources for the events you want to collect. Since you installed an agent on a server with a Windows operating system, you create a connector based on the NTEventLog integration and specify settings for the WMILogSensor as described in the connector guide you open from the New Connector Creation wizard. You specify the name of the host on which the agent is installed for agent-based log collection. Optionally, you can add another WMI log sensor for this connector and specify a host other than the one where the agent is installed. This enables agentless log connection. The additional host or hosts must be in the same domain and have the same Windows administrator as the first host you added.

To configure a connector based on NTEventLog

1. Maximize your browser displaying the CA User Activity Reporting Module Agent Explorer.
2. Expand Agent Explorer and then expand the Default Agent Group.

   The name of the computer where you installed the agent appears.

3. Select this agent.

   The Agent Connectors pane appears.

4. Click Create New Connector

   The New Connector Creation wizard appears with the Connector Details step selected.

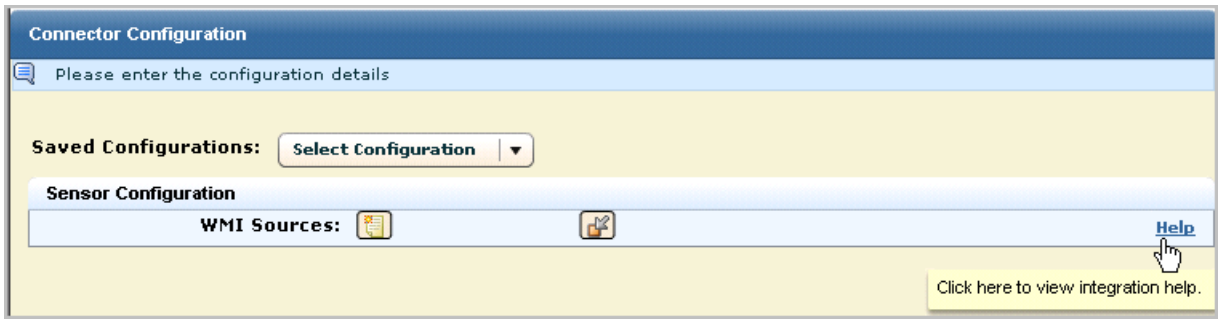
5. Leave Integrations selected, and select NTEventLog from the Integration drop-down list.

   The Connector Name and Description fields are populated based on the selection of Integration.

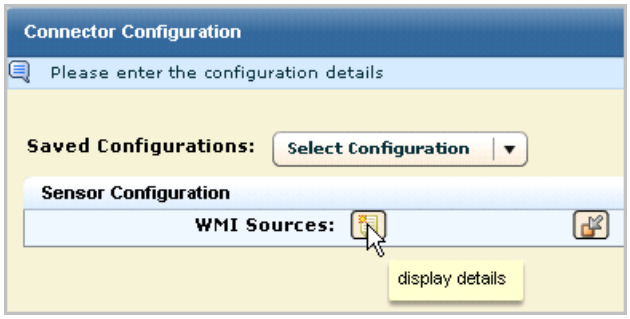
6. Edit the connector name to make it unique. Consider extending this name with the target server name, for example, NTEventLog_Connector_USER001LAB.

7. Select the Connector Configuration step.

The Sensor Configuration pane appears with a Help button to the Connector guide for NTEventLog, which provides help on the fields for sensor configuration.

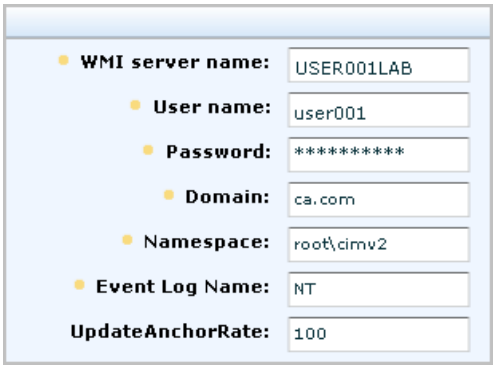


8. Click the display details button for WMI sources.



9. Configure the WMILogSensor settings for the local computer for agent-based log collection. Click the Help link for details.

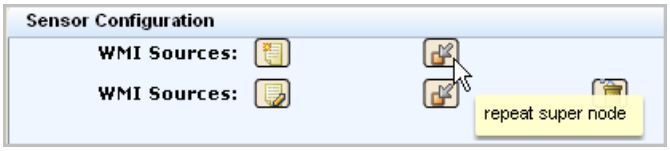
   The following example shows a configuration where the user is a Windows administrator on the specified WMI server. The domain is for the WMI server.



10. (Optional) Configure a WMI sensor for a different computer for agentless log collection using this same connector.

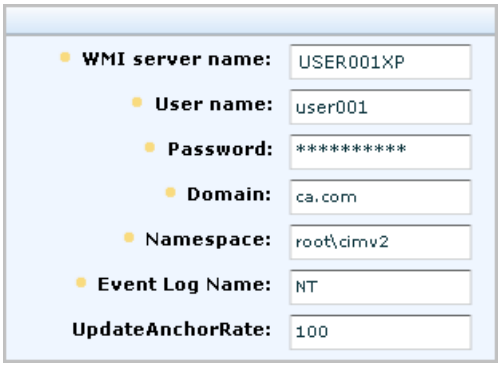
    a. Click the repeat super node button.

       The following illustration shows a configuration with two WMI sources.



    b. Configure the WMILogSensor settings for another computer.

    The following example shows a configuration for a second WMI log sensor in the same domain and with the same administrator credentials.



11. Click Save and Close.

12. To view the status of the connector you configured, do the following:

    a. Select the agent in the left pane.

    b. Click Status and Command.

    c. Select View Status of Connectors.

    The Status Details pane appears.

13. Click the Running link.

    The displayed status of the target configured in the connector includes the CPU percentage, memory usage, and average events per second (EPS).

Configure a Windows Event Source

After configuring a connector using the NTEventLog integration on the agent, you should be able to see events through your Event Viewer. If events are not being forwarded to your event viewer, you should change the Windows settings for your Local Policies on the event source.

To configure local policies on the event source for a NTEventLog connector

1. If the Log Collection Explorer is not already displayed, click the Administration tab.
2. Expand Event Refinement Library, expand Integrations, expand Subscription, select NTEventLog, and click the Help link above the Integration Name on the View Integration Details pane.

   The Connector Guide for NT Event Log (Security, Application, System) appears.
3. Minimize the CA User Activity Reporting Module user interface and follow the directions in the Connector Guide for editing local policies on an event source running on a Windows operating system.

   Note: If your system is Windows Server 2003, select Control Panel, Administrative Tools, Local Security Policy, and then expand Local Policies.
4. (Optional) If you configured a WMI Sensor for a second WMI server, edit the local policies on that server also.
5. Maximize CA User Activity Reporting Module.

View Logs from Windows Event Sources

One of the quickest ways to view query results on incoming events is to use the Prompt for Host. You can also select queries or reports.

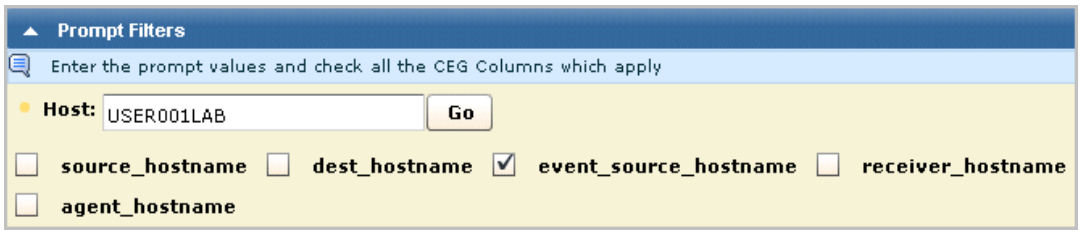
To view incoming event logs

1. Select the Queries and Reports tab.

   The Queries subtab displays.

2. Expand Prompts under Query List and select Host.

3. Enter the WMI server name configured for the sensor in the Host field. Clear the other check marks and click Go.



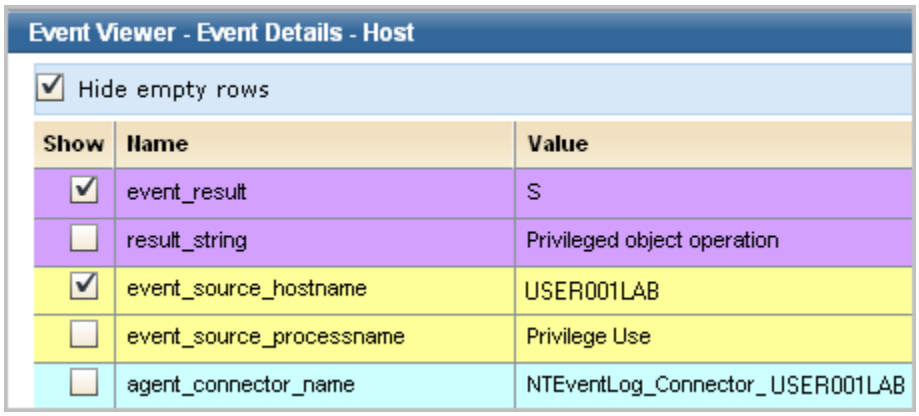
   Events from the WMI server event sources appear.

4. Click the CA Severity and scroll through to find a warning. A compressed example without the Date and Event Source columns follows:

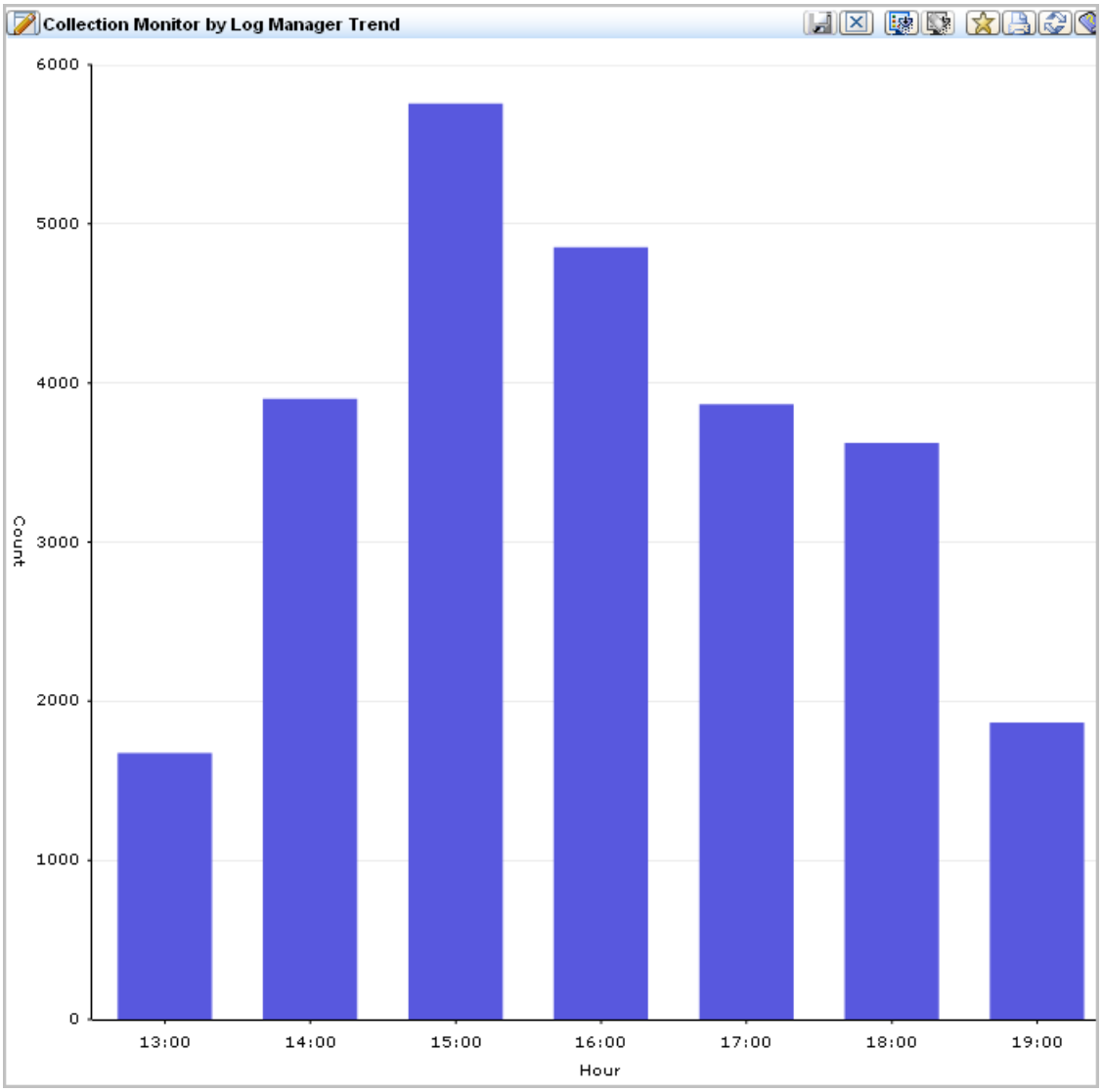
CA Severity ▼	Source User	Result	Category	Action	Log Name
Warning	calm_agent	S	System Access	Privilege Use	NT-Security

5. Click Show raw event to display the raw events for the warning.

6. Double-click the warning to display the Event Viewer with much more data. A few rows of example data follow:



7. Click the Queries and Reports tab, click a query from the Query List, for example, Collection Monitor by Log Manager Trend. View the resulting bar graph.



8. Click Reports. Under Report List, enter self in the Search field to display the report name System Self Monitoring Events. Select this report to display a listing of the events that are generated by the CA User Activity Reporting Module server.

Note: See online help or the *Administration Guide* for details on scheduling reports on information you are interested in analyzing.

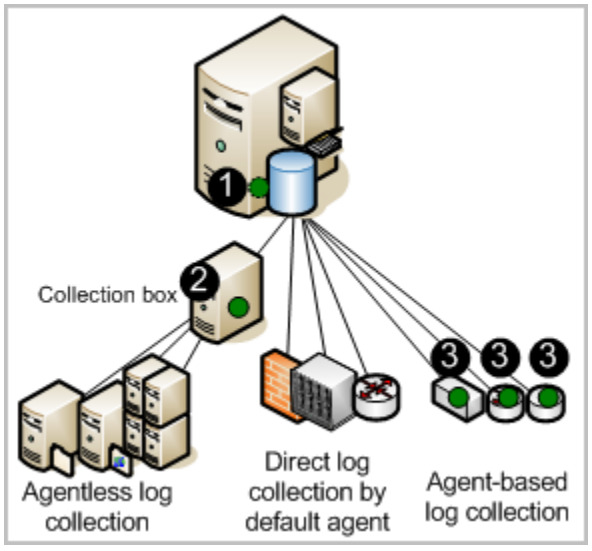
Chapter 4: Key Capabilities

This section contains the following topics:

Log Collection

The CA User Activity Reporting Module server can be set up to collect logs using one or more supported techniques. The techniques differ in the type and location of the component that listens for and collects the logs. These components are configured on agents.

The following illustration depicts a single-server system, where agent locations are indicated with a dark (green) circle.



The numbers on the illustration refer to these steps:

1. Configure the default agent on the CA User Activity Reporting Module to fetch events directly from the syslog sources you specify.
2. Configure the agent installed on a Windows collection point to collect events from the Windows servers you specify and transmit them to the CA User Activity Reporting Module.
3. Configure agents installed on hosts where event sources are running to collect the configured type of events and perform suppression.

Note: Traffic from the agent to the destination CA User Activity Reporting Module server is always encrypted.

Consider the following advantages of each log collection technique:

- Direct log collection

  With direct log collection, you configure the syslog listener on the default agent to receive events from the trusted sources you specify. You can also configure other connectors to collect events from any event source that is compatible with the soft appliance operating environment.

  Advantage: You do not need to install an agent to collect logs from event sources that are in close network proximity to the CA User Activity Reporting Module server.

- Agentless collection

  With agentless collection, there is no local agent on the event sources. Rather, an agent is installed on a dedicated collection point. Connectors for each target event source are configured on that agent.

  Advantage: You can collect logs from event sources running on servers where you cannot install agents, such as severs where corporate policy prohibits agents. Delivery is guaranteed, for example, when ODBC log collection is configured properly.

- Agent-based collection

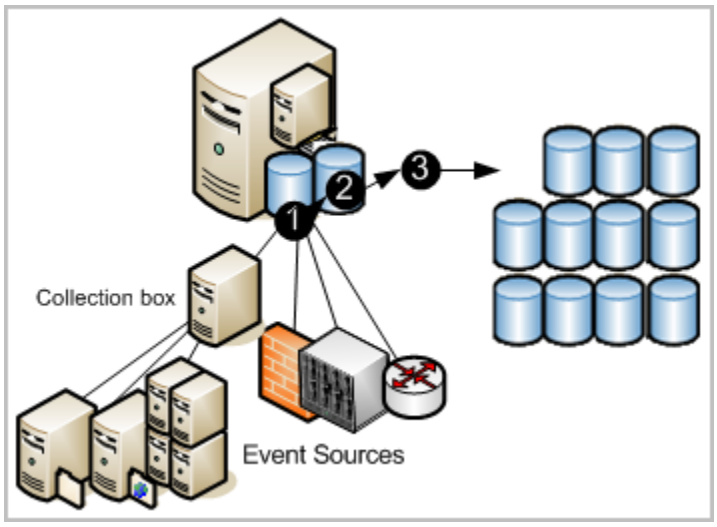
  With agent-based collection, an agent is installed where one or more event sources are running and a connector is configured for each event source.

  Advantage: You can gather logs from a source where the network bandwidth between that source and the CA User Activity Reporting Module is not good enough to support direct log collection. You can use the agent to filter the events and reduce the traffic sent across the network. Event delivery is guaranteed.

Note: See the *Administration Guide* for details on agent configuration.

Log Storage

CA User Activity Reporting Module provides managed embedded log storage for recently archived databases. Events collected by agents from event sources go through a storage lifecycle as illustrated by the following diagram.



The numbers on the illustration refer to these steps:

1. New events collected by any technique are sent to the CA User Activity Reporting Module. The state of incoming events depends on the technique used to collect them. Incoming events must be refined before being inserted into the database.
2. When the database of refined records reaches the configured size, all records are compressed into a database and saved with a unique name. Compressing log data reduces the cost of moving it and reduces the cost of storage. The compressed database can either be moved automatically based on auto-archive configuration or you can back it up and move it manually before it reaches the age configured for deletion. (Auto-archived databases are deleted from the source as soon as they are moved.)
3. If you configure auto-archive to move the compressed databases to a remote server on a daily basis, you can move these backup to off-site long-term log storage at your convenience. Retaining backups of logs enables you to comply with the regulations that state that logs must be securely collected, centrally stored for a certain number of years, and available for review. (You can restore database from long-term storage at any time.)

Note: See the *Implementation Guide* for details on configuring the event log store, including how to set up auto-archiving. See the *Administration Guide* for details on restoring the backups for investigation and reporting.

Standardized Presentation of Logs

Logs generated by applications, operating systems, and devices all use their own formats. CA User Activity Reporting Module refines the collected logs to standardize the way the data is reported. The standard format makes it easier for auditors and upper management to compare data collected from different sources. Technically, the CA Common Event Grammar (CEG) helps implement event normalization and classification.

The CEG provides several fields which are used to normalize various aspects of the event, including the following:

- Ideal Model (Class of technologies such as antivirus, DBMS, and firewall)
- Category (Examples include Identity Management and Network Security)
- Class (Examples include Account Management and Group Management)
- Action (Examples include Account Creation and Group Creation)
- Results (Examples include Success and Failure)

Note: See the *CA User Activity Reporting Module Administration Guide* for details on the rules and files used in event refinement. See the section on Common Event Grammar in the online help for details on the normalizing and categorizing events.

Compliance Reporting

CA User Activity Reporting Module lets you gather and process security-relevant data and turn it into reports suitable for internal or external auditors. You can interact with queries and reports for investigations. You can automate the reporting process by scheduling report jobs.

The system provides:

- Easy to use query capability with tags
- Near-real time reporting
- Centrally searchable, distributed archives of critical logs

Its focus is on compliance reporting rather than real-time correlation of events and alerts. Regulations demand reporting that demonstrates compliance with industry-related controls. CA User Activity Reporting Module provides reports with the following tags for easy identification:

- Basel II
- COBIT
- COSO
- EU Directive - Data Protection
- FISMA
- GLBA
- HIPAA
- ISO\IEC 27001\2
- JPIPA
- JSOX
- NERC
- NISPOM
- PCI
- SAS 70
- SOX

You can review predefined log reports or perform searches based on criteria you specify. New reports are provided with subscription updates.

Log view capabilities are supported by the following:

- On demand query capability with predefined or user-defined queries, where results can include up to 5000 records

- Quick search, through Prompts, for a specified host name, IP address, port number, or user name
- Scheduled and on demand reporting with out-of-the-box reporting content
- Scheduled query and alerting
- Basic reports with trending information
- Interactive, graphical event viewers
- Automated reporting with email attachment
- Automated report retention policies

Note: For details on using predefined queries and reports or creating your own, see the *CA User Activity Reporting Module Administration Guide*.

Policy Violation Alerting

CA User Activity Reporting Module lets you automate the sending of an alert when an event occurs that requires near-term attention. You can also monitor action alerts from CA User Activity Reporting Module at any time by specifying a time interval, such as from the last five minutes to the last 30 days. Alerts are automatically sent to an RSS feed that can be accessed from a web browser. Optionally, you can specify other destinations, including email addresses, a CA IT PAM process such as one that generates help desk tickets, and one or more SNMP trap destination IP addresses.

To help you get started, many predefined queries are available for scheduling as action alerts, as is. Examples include:

- Excessive user activity
- High CPU utilization average
- Low available disk space
- Security event log cleared in last 24 hours
- Windows audit policy changed in last 24 hours

Some queries use keyed lists, where you supply the values used in the query. Some keyed lists include predefined values that you can supplement. Examples include default accounts and privileged groups. Other keyed lists, such as that for business critical resources, have no default values. After you configure them, alerts can be scheduled for predefined queries such as:

- Group membership addition or removal by privileged groups
- Successful login by default account
- No events received by business critical sources

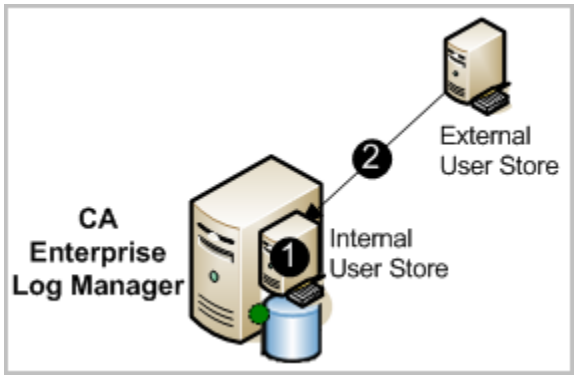
Keyed lists can be updated manually, by importing a file, or by running a CA IT PAM dynamic values process.

Note: See the *CA User Activity Reporting Module Administration Guide* for details on action alerts.

Entitlement Management

When you configure the user store, you choose whether to use the default user store on the CA User Activity Reporting Module for setting up user accounts or reference an external user store where user accounts are already defined. The underlying database is exclusive to CA User Activity Reporting Module and does not use a commercial DBMS.

Supported external user stores include CA SiteMinder and LDAP directories such as Microsoft Active Directory, Sun One, and Novell eDirectory. If you reference an external user store, user account information is automatically loaded in read-only format as shown by the arrow in the following diagram. You define only application-specific details to selected accounts. No data is moved from the internal user store to the referenced external user store.



The numbers on the illustration refer to these steps:

1. The internal user store performs entitlement management by authenticating the credentials supplied by users at login and authorizing users to access different features of the user interface based on the policies associated with the roles assigned to their user accounts. If the user name and password of the user attempting to log in have been loaded by an external user store, the credentials entered must match the loaded credentials.
2. The external user store has no function other than to load its user accounts into the internal user store. These are loaded automatically when the reference to the user store is saved.

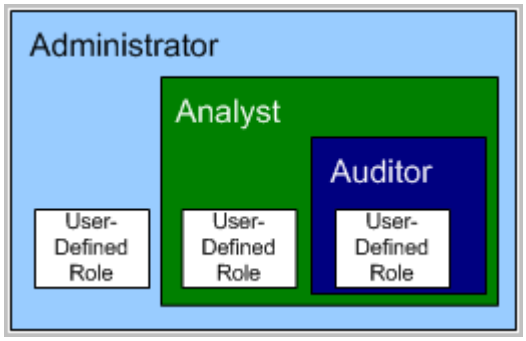
Note: See the *CA User Activity Reporting Module Implementation Guide* for details on configuring basic user access. See the *CA User Activity Reporting Module Administration Guide* for details on policies supporting predefined roles, creating user accounts, and assigning roles.

Role-Based Access

CA User Activity Reporting Module provides three predefined application groups or roles. Administrators assign the following roles to users to specify their access rights to CA User Activity Reporting Module features:

- Administrator
- Analyst
- Auditor

The Auditor has access to few features. The Analyst has access to all Auditor features plus more. The Administrator has access to all features. You can define a custom role with associated policies that limit user access to resources in the way that suits your business needs.



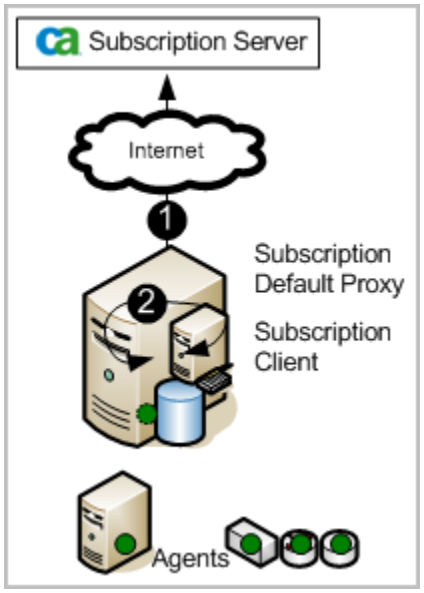
Administrators can customize access to any resource by creating a custom application group with associated policies and assigning that application group, or role, to user accounts.

Note: See the *CA User Activity Reporting Module Administration Guide* for details on planning and creating custom roles, custom policies, and access filters.

Subscription Management

The subscription module is the service that enables subscription updates from the CA Technologies Subscription Server to be automatically downloaded on a scheduled basis and distributed to CA User Activity Reporting Module servers. When a subscription update includes the module for agents, users initiate the deployment of these updates to agents. *Subscription update*s are updates to CA User Activity Reporting Module software components and operating system updates, patches, and content updates such as reports.

The following illustration depicts the simplest direct Internet connection scenario:



The numbers on the illustration refer to these steps:

1. The CA User Activity Reporting Module server, as the default subscription server, contacts the CA Subscription server for updates and downloads any new available updates. The CA User Activity Reporting Module server creates a backup, then pushes content updates to the embedded component of the management server that stores content updates for all other CA User Activity Reporting Modules.
2. The CA User Activity Reporting Module server, as a subscription client, self-installs the product and operating system updates it needs.

Note: See the *Implementation Guide* for details on planning and configuring subscription. See the *Administration Guide* for details on refining and modifying the subscription configuration and for applying updates to agents.

Out-of-the-Box Content

CA User Activity Reporting Module includes predefined content that you can begin using as soon as you install and configure the product. The subscription process regularly adds new content and updates existing content.

Categories of predefined content include:

- Reports with tags
- Queries with tags
- Integrations with associated sensors, parsing files (XMP), mapping (DM) files, and in some cases, suppression rules
- Suppression and summarization rules

Chapter 5: Learning More about CA User Activity Reporting Module

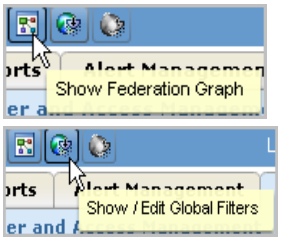
This section contains the following topics:

Display Tooltips

You can identify the purpose of buttons, check boxes, and reports on the CA User Activity Reporting Module page in your current view.

To display tooltips and other help

1. Move your cursor over the buttons to display the description of the button function. You can view the function of any button in this way.

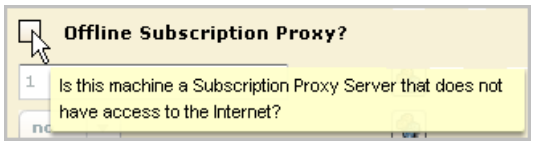


2. Notice the difference between active and inactive buttons.

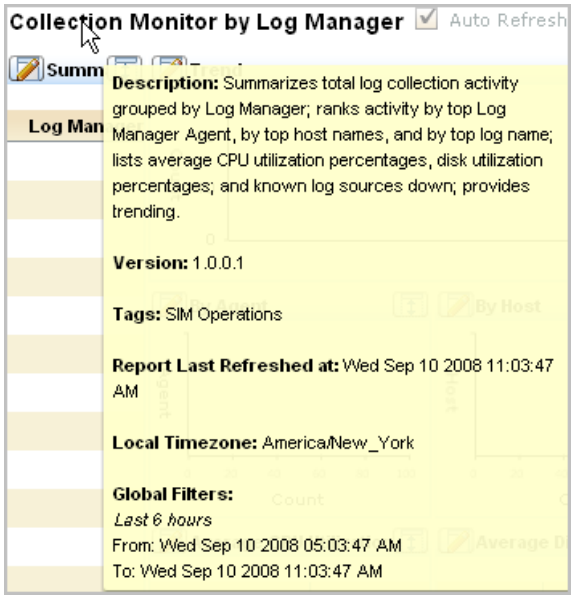
   Enabled, active buttons are displayed in color. For example, Administrators of user and access management view the Access Filter List button in color.

   Disabled, inactive buttons are displayed in black and white. For example, Auditors view the Access Filter List buttons in black and white.

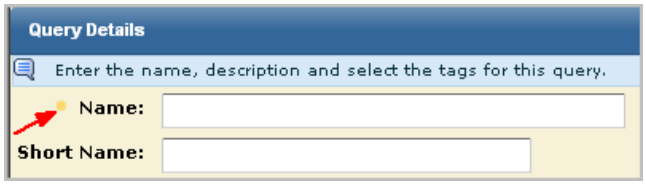
3. View descriptions for entry fields or check boxes by moving your cursor over the field name.



4. View descriptions of reports by moving your cursor over the report name.



5. Notice an orange dot to the left of some fields. This dot indicates that the field is required. For configurations you can save, a save is not allowed until you have entries in all required fields.



Display Online Help

You can display help for the page you are viewing or for any task you want to perform.

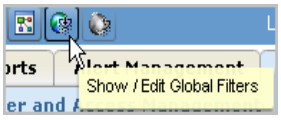
To display online help

1. Click the Help link in the toolbar to display the online help system for CA User Activity Reporting Module.

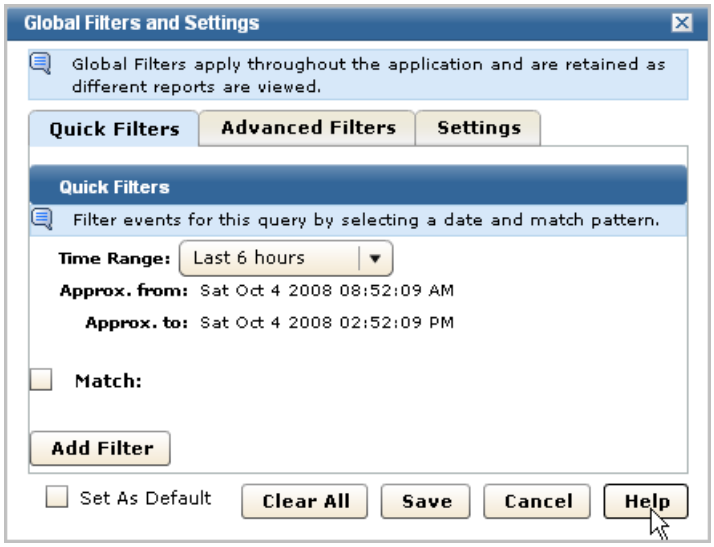
The CA User Activity Reporting Module help system appears, with the contents displayed in the left pane.

2. Access context-sensitive help from a Help button as shown in the following example.

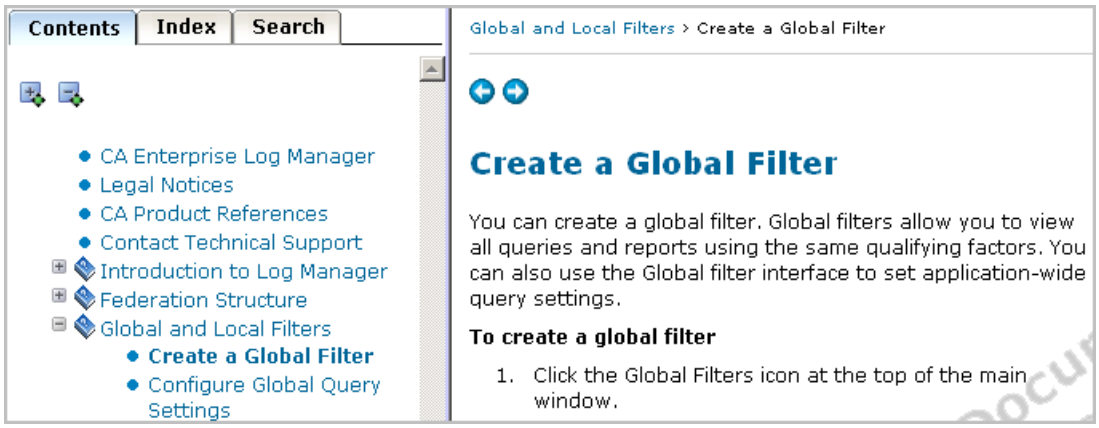
   a. Click the Show / Edit Global Filters button.



   The Global Filters and Settings window appears with a Help button.



b. Click the Help button. Online help for the procedure you can perform on the current page, pane, or dialog appears in a secondary window.



c. If you know the task you want to perform, but do not know how to access the corresponding page in CA User Activity Reporting Module, you may find it listed in the Table of Contents. Clicking the task title displays the page.

Note: If you are unable to find the task you need in the Table of Contents, refer to the bookshelf of documentation.

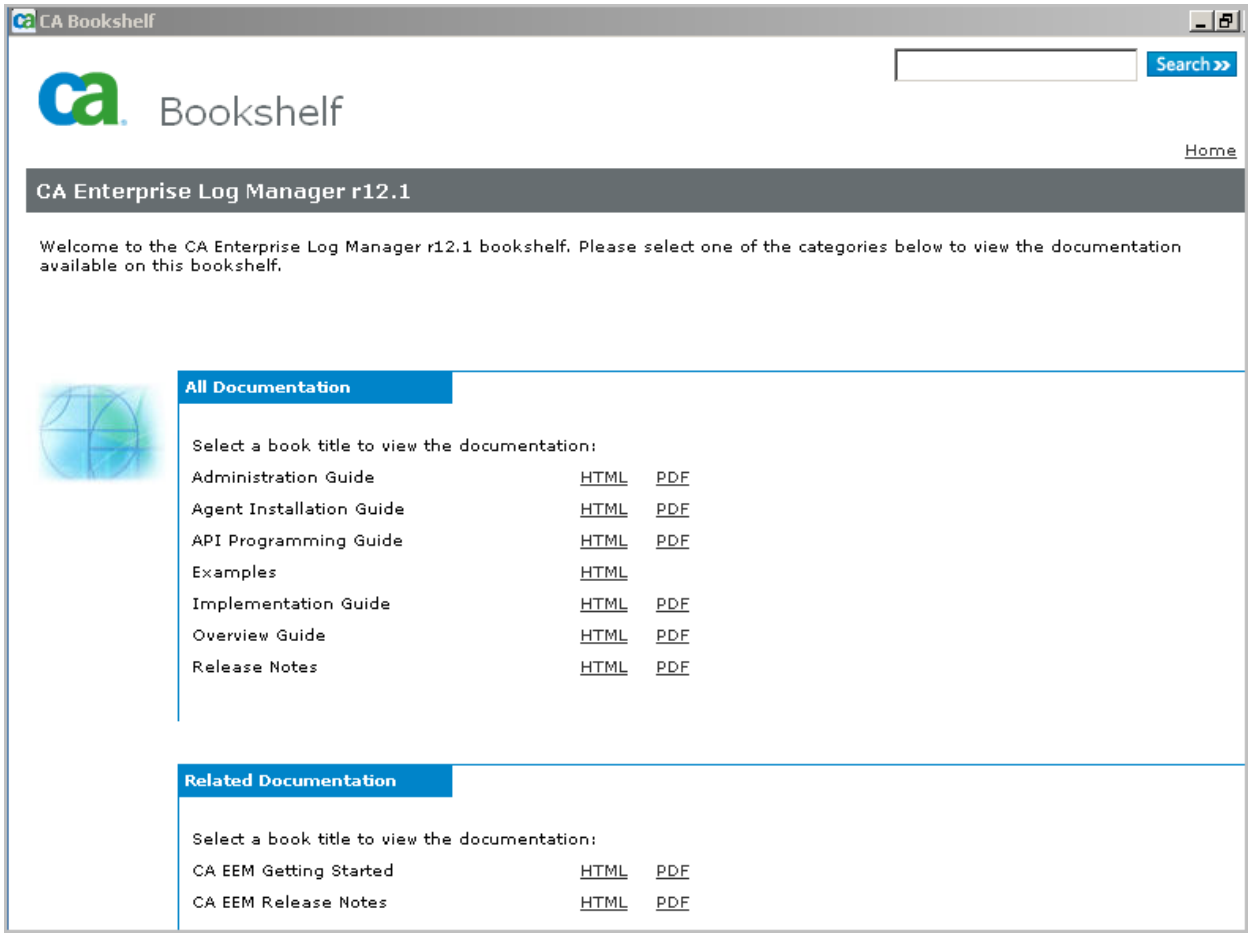
Explore the Bookshelf of Documentation

You can copy the bookshelf to your local drive and open any book in HTML or PDF format. Books in HTML format contain cross-book cross-references.

To explore the bookshelf

1. Copy the Bookshelf to your local drive from the installation DVD for the application or download it from the CA Customer Support website. Double-click Bookshelf.hta or Bookshelf.html to open the bookshelf.

   A page similar to the following appears.

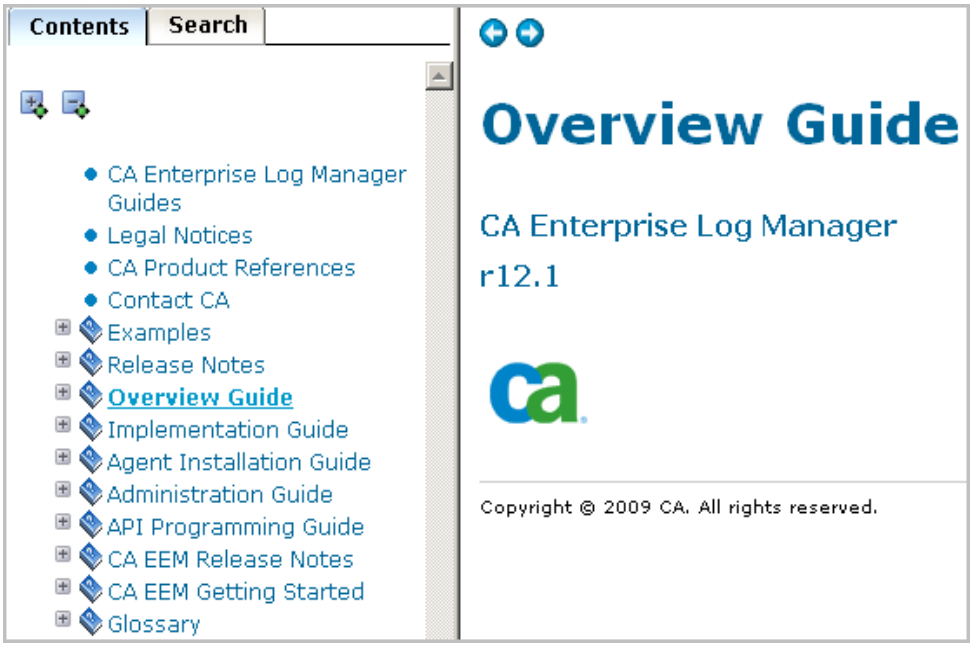


Descriptions of the contents of the major guides and the Examples follows:

Deliverable	Describes how to
Agent Installation Guide	Install agents

Deliverable	Describes how to
Implementation Guide	Install and configure a CA User Activity Reporting Module system.
Administration Guide	Customize the configuration, perform routine administration tasks, and work with queries, reports, and alerts.
API Programming Guide	Use the API to display event data in a web browser or to embed reports in another CA or third-party product.
Examples	Solve common business problems, with links to topics in the documentation.

2. Type a value in the Search entry field and click the Search button to display all documented occurrences that include your entry.
3. Click a Print link to open the PDF of the selected guide.
4. Click an HTML link to open the integrated documentation set. The integrated set includes all guides in HTML format. If you select the HTML link for the Overview Guide, that is the guide that is displayed.



Index