

CA Enterprise Log Manager

Agent Installation Guide



This documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2010 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Product References

This document references the following CA products:

- CA Access Control
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Log Manager
- CA Identity Manager
- 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

Contact CA Support

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

- 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

Provide Feedback

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

If you would like to provide feedback about CA 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:

- Added the Prerequisite topic to the Installing an Agent on HP-UX Systems chapter
- Added the Installing an Agent on HP-UX Itanium Systems chapter

Contents

Chapter 1: Introduction 11

About This Guide	11
About Agents and Log Collection	11

Chapter 2: Installing an Agent on a Windows System 13

Workflow for Agent Installation on Windows	14
Agent Deployment Flowchart for Windows Platforms	16
Least-Privileged User Requirements	17
How to Install Manually	17
View or Set the Agent Authentication Key	18
Create a User Account for the Agent	18
Grant the Agent-User Access to Windows Security Logs	19
Download Agent Binaries	20
Install the Agent	21
(Optional) Verify the Agent Installation	23
Export a Connector Configuration	23
How to Install Silently	24
Review Setup Checklist	25
Create a Response File	26
Invoke the Silent Install	27
View the Agent Status Details	27
Prepare a Response File for Re-use	28
Install Silently with a Customized Response File	29
Maintenance Considerations	29
Updating an Agent with New User Credentials	30
Uninstall an Agent	33
Installing an Agent with CA Software Delivery	33

Chapter 3: Installing an Agent on Linux Systems 35

Least-Privileged User Requirements	35
How to Install Manually	35
Create an Authorized User for an Agent	36
View or Set the Agent Authentication Key	36
Download Agent Binaries	37
Install the Agent	38
How to Install Silently	39

Review Setup Checklist	40
Set Up a Response File	41
Invoke the Silent Install	41
View the Agent Status Details	42
Prepare a Response File for Re-use	42
Install Silently with a Customized Response File	43
Maintenance Considerations	43
Uninstall an Agent	44

Chapter 4: Installing an Agent on Solaris Systems 45

Least-Privileged User Requirements	45
Agent Deployment Flowchart for UNIX Platforms	46
Planning Agent Deployment	47
Deploying the First Agent	48
View or Set the Agent Authentication Key	48
Download Agent Binaries	49
Create a Low Privileged User for a Planned Agent	49
Installing an Agent Interactively	50
Verify Locally that the Agent is Running	52
Examine Self-Monitoring Events for Agent Startup	53
View the Agent Status Details	54
Preparing Files and Testing Silent Installation	54
Create and Export Connectors	55
Prepare a Host for Testing Silent Installation	55
Create the Response File	55
Install an Agent Silently	56
Validate Results of the Silent Installation	57
Deploying All Other Planned Agents	57
Edit the Response File	58
Preparing New Agents for Use	59
Maintaining Agents	59
Troubleshooting Agent Installation	59
Change the Low Privileged User for an Agent	60
Uninstall an Interactively Installed Agent	61
Uninstall a Silently Installed Agent	62

Chapter 5: Installing an Agent on HP-UX Systems 63

Prerequisite	63
Least-Privileged User Requirements	63
Agent Deployment Flowchart for UNIX Platforms	64
Planning Agent Deployment	65

Deploying the First Agent	66
View or Set the Agent Authentication Key	66
Download Agent Binaries	67
Create a Low Privileged User for a Planned Agent.....	67
Installing an Agent Interactively	68
Verify Locally that the Agent is Running	70
Examine Self-Monitoring Events for Agent Startup	71
View the Agent Status Details	71
Preparing Files and Testing Silent Installation	72
Create and Export Connectors	72
Prepare a Host for Testing Silent Installation	73
Create the Response File	73
Install an Agent Silently	74
Validate Results of the Silent Installation	75
Deploying All Other Planned Agents	75
Edit the Response File	76
Preparing New Agents for Use	77
Maintaining Agents	77
Troubleshooting Agent Installation	77
Determine Whether an Agent Exists on a Specified Host	78
Change the Low Privileged User for an Agent	79
Uninstall an Agent	79

Chapter 6: Installing an Agent on AIX Systems 81

Least-Privileged User Requirements	81
Agent Deployment Flowchart for UNIX Platforms	82
Planning Agent Deployment	83
Deploying the First Agent	84
View or Set the Agent Authentication Key	84
Download Agent Binaries	85
Create a Low Privileged User for a Planned Agent.....	85
Installing an Agent Interactively	86
Verify Locally that the Agent is Running	88
Examine Self-Monitoring Events for Agent Startup	89
View the Agent Status Details	90
Preparing Files and Testing Silent Installation	90
Create and Export Connectors	91
Prepare a Host for Testing Silent Installation	91
Create the Response File	91
Invoke an Agent Silently	92
Validate Results of the Silent Installation	93

Deploying All Other Planned Agents	93
Edit the Response File	94
Preparing New Agents for Use	95
Maintaining Agents	95
Troubleshooting Agent Installation	95
Change the Low Privileged User for an Agent	96
Uninstall an Agent	97

Chapter 1: Introduction

This section contains the following topics:

[About This Guide](#) (see page 11)

[About Agents and Log Collection](#) (see page 11)

About This Guide

The *Agent Installation Guide* is designed for system or network administrators who install CA Enterprise Log Manager agents. Agents enable the collection and routing of events from configured event sources to a CA Enterprise Log Manager server. Before you begin using this guide, we recommend you read "Agent Planning" in the *Implementation Guide*.

For your ease of use, this guide is divided into sections by operating environment, so you can refer just to the section that applies to the operating environment on which you are doing the installation.

About Agents and Log Collection

You can install an agent directly on an event source. An event source is a host where an application, database, or operating system generates raw events. Or, you can install an agent on a collection point and collect events generated on remote event sources.

When you install the agent, you specify the target server. If you dedicate CA Enterprise Log Manager servers to different roles, the target server is a collection server. During the initial agent startup, the agent registers with the collection CA Enterprise Log Manager you identify during installation.

Event collection begins after you configure connectors on the agent. Each connector collects events from a single event source, performs preliminary event refinement, and then sends them to a CA Enterprise Log Manager server. If an event source is in close network proximity to the CA Enterprise Log Manager server, configure connectors on the resident default agent to collect events.

Chapter 2: Installing an Agent on a Windows System

This section contains the following topics:

- [Workflow for Agent Installation on Windows](#) (see page 14)
- [Agent Deployment Flowchart for Windows Platforms](#) (see page 16)
- [Least-Privileged User Requirements](#) (see page 17)
- [How to Install Manually](#) (see page 17)
- [How to Install Silently](#) (see page 24)
- [Maintenance Considerations](#) (see page 29)
- [Installing an Agent with CA Software Delivery](#) (see page 33)

Workflow for Agent Installation on Windows

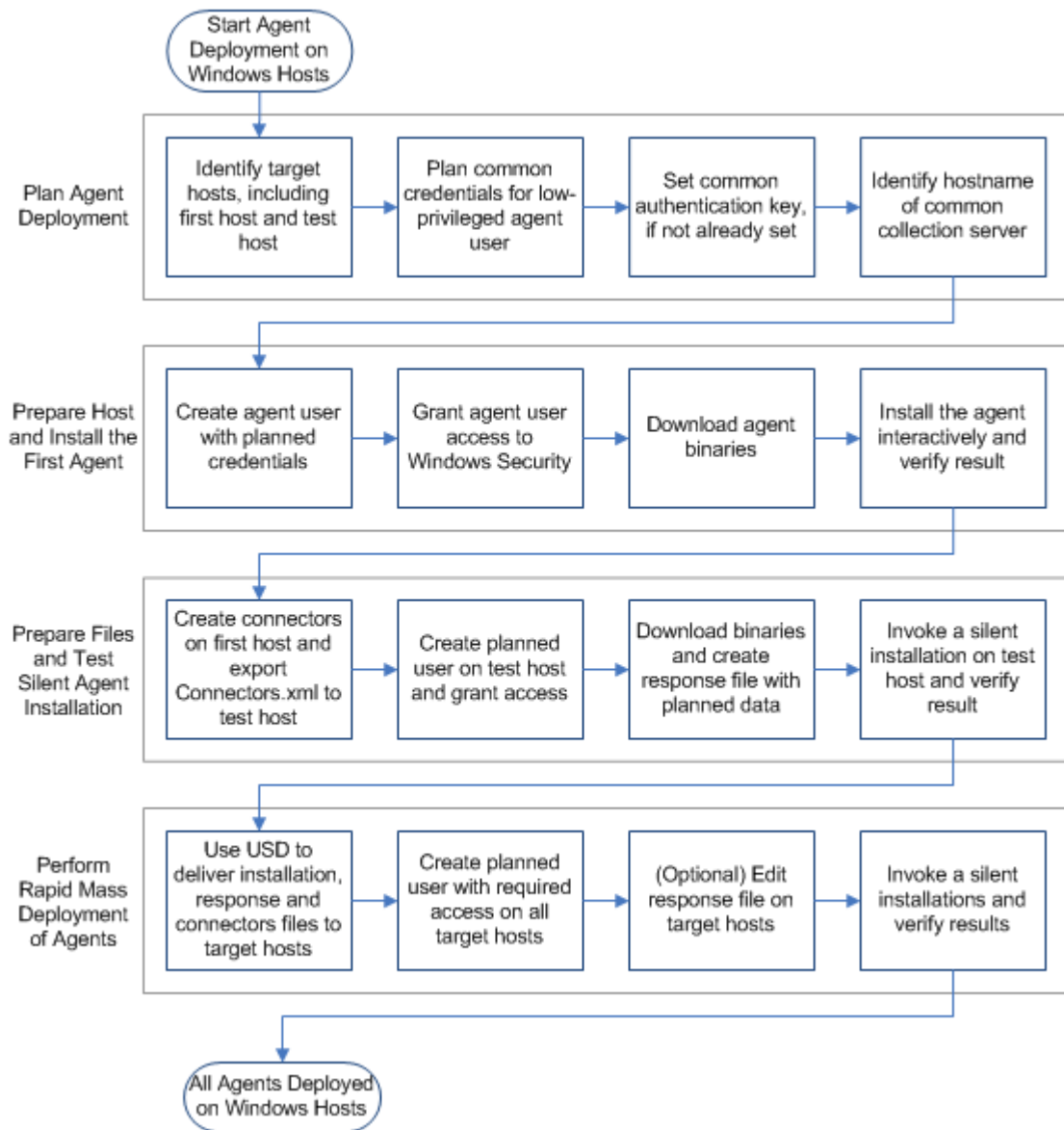
Use the following workflow as a guide:

1. Plan agent deployment on Windows in a way that makes it possible to use the same response file for multiple silent installations without modification..
 - a. Identify the Windows hosts to target for agent installation. Identify a host for first installation and connector export, and then one for testing silent installation.
 - b. Plan a common user name and password to define on each target host for the low-privileged user.
 - c. View or set the agent authentication key to use for all installations.
 - d. Identify the host name or IP address of a common collection server for Windows agents. (Those agents can be installed with the same response file.)
 - e. (Optional) Create a setup checklist with these values.
 - Installation path for installed agent: C:\Program Files\CA\elmagent\.
 - FIPS mode: enable or disable
 - Collection server hostname or IP address
 - Agent authentication key
 - Agent user name and password
 - Name of the connectors file you plan to export: Connectors.xml.
2. Prepare a host and install the first agent.
 - a. Create a low-privileged agent-user account with the planned credentials.
 - b. Grant the agent-user access to Windows Security.
 - c. Download the agent binaries to the desktop for interactive installation.
 - d. Install the agent interactively and verify successful agent installation.
3. Prepare files for broad deployment and test a silent installation
 - a. Identify a test host, that is, a host on which to create a response file and test silent installation.
 - b. Create connectors on the first installed agent, test them, then export the connectors. Save the Connectors.xml file to the %WINDIR% directory on the test host.
 - c. Download agent binaries to %WINDIR%.
 - d. Create a low-privileged user with the planned credentials and grant the agent-user access to Windows Security.
 - e. Create a response file, using the values you recorded in the setup checklist.
 - f. Invoke a silent installation on the test host.

- g. Confirm that results are desired results for remaining agents. If not, make the needed adjustments before continuing.
 - 4. Prepare remaining target hosts and deploy agents with tested files.
 - a. Identify the rest of the target hosts for agent installation.
 - b. Prepare each host for silent installation. If installing with the low-privileged user credentials, add the user and assign required access.
 - c. Use CA Software Delivery to get the agent package; unseal the package and replace the sample response file with the response file you tested, and also add the Connectors.xml file. The package already contains the binaries.
 - d. Distribute and deploy the packages to the target hosts with the CA Server interface.

Agent Deployment Flowchart for Windows Platforms

The following flowchart represents graphically the typical workflow for agent deployment to hosts with Windows operating environments.



Least-Privileged User Requirements

While you can run the agent as a Windows Administrator user, it is a better security practice to create a least-privileged account for the agent to use. This user account is referred to as the agent-user. You can give the agent-user any account name you like, such as *elmagentsr*. Create an agent-user account and grant this account access to Windows security logs before you install the agent.

Note: You will specify the agent-user name and password during agent installation. The install program automatically assigns the minimum-required privileges on the agent installation directory and the agent service to the agent-user you specify. If you choose to specify an Administrator account during installation, you can create the agent-user account later, grant it access to the security logs, and assign the required privileges by running the *AgentAuthUtil* utility.

The base requirements for the least-privileged agent-user are the following:

- Can modify, read, execute, write, delete, and list contents of all files and folders in the agent installation directory.
- Can start, stop, pause or continue (resume), and query the status of the agent service, *caelmagent*, on the Windows server where the agent is installed
- Can access Windows security logs

To create the agent-user account, grant this account required permissions, and install the agent, you must be an administrator on the Windows server. To perform other agent-related tasks, you must log on to the CA Enterprise Log Manager server with an Administrator account.

More information

[Updating an Agent with New User Credentials](#) (see page 30)

How to Install Manually

To install an agent, you must log onto the target server with Windows administrative privileges. The following sequence is the recommended way to prepare for installation and install the agent:

1. Create a Windows user account for the agent.
2. View or set the agent authentication key.
3. Download the agent installer (agent binaries) on the server where you plan to install the agent.
4. (Optional) Export a connector configuration to the server where you plan to install the agent.

5. Install the agent with the agent installer.

During installation, you enter the agent user account name and password, domain name, and the agent authentication key. If you exported the connector file, browse for and select it.

More information:

[Create a User Account for the Agent](#) (see page 18)

[View or Set the Agent Authentication Key](#) (see page 18)

[Download Agent Binaries](#) (see page 20)

[Export a Connector Configuration](#) (see page 23)

[Install the Agent](#) (see page 21)

[Updating an Agent with New User Credentials](#) (see page 30)

View or Set the Agent Authentication Key

If you are a CA Enterprise Log Manager Administrator, you can set the agent authentication key or view the current setting.

To view or set the agent authentication key

1. Click the Administration tab and then click the Log Collection subtab.
The Log Collection Explorer displays in the left pane.
2. Select the Agent Explorer folder.
A toolbar appears in the main pane.
3. Click Agent Authentication Key.
4. Take one of the following actions:
 - Record the configured name so you have it ready to enter during agent installation.
 - Set or reset it by entering and confirming the agent authentication key to be used for the agent installation.

Note: The default value is: `This_is_default_authentication_key`.
5. Click Save.

Create a User Account for the Agent

Before installing the agent, you can create a new, low-privilege user account for the agent in the Windows Users folder. Although the use of low-privileged accounts is considered a best practice, it is not mandatory.

When you supply the agent user credential information during a manual install or in a response file, you can enter local credentials of the new agent user account.

To create a Windows user account for the agent

1. Log on to the host where you plan to install the agent, using Administrator credentials.
2. Click Start, Program Files, Administrative Tools, Computer Management.
3. Expand Local Users and Groups.
4. Right-click Users and select New User.
5. Enter a user name.
6. Enter and confirm the password.

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

7. Click Create, and then click Close.

You will use the user name and password you set for this agent when performing the following tasks:

- Installing the agent
- Creating a response file

If you create an agent user account with a different agent-user name and password on other computers, you must update that data when preparing a response file for re-use.

More information:

[Updating an Agent with New User Credentials](#) (see page 30)

[Install the Agent](#) (see page 21)

[Create a Response File](#) (see page 26)

[Prepare a Response File for Re-use](#) (see page 28)

Grant the Agent-User Access to Windows Security Logs

Administrator-level access for the agent-user is not necessary or recommended. For access to local *and* remote WMI events, the agent-user should be a least-privileged user account which has the user right, Manage auditing and security log. (This user right is also known as the SeSecurityPrivilege.) You can set this user right for the agent-user in the Local Security Settings, Local Policies area.

To set the local security policy

1. Access the Control Panel.
2. Open the Administrative Tools folder.
3. Double-click the Local Security Policy utility.
4. Expand the Local Policies node.
5. Select the User Rights Assignment node, and scroll down through the alphabetical list to the option, Manage auditing and security log.
6. Double-click Manage auditing and security log.
7. Click Add User or Group....
The Select Users or Groups appears.
8. Enter the name of the agent-user account you created and click Check Names.
This action verifies that the user account name is populated correctly in the list.
9. Click OK.

Download Agent Binaries

You can place the agent installation program on the target Windows server in one of the following ways:

- Download the agent binaries from the CA Enterprise Log Manager user interface.
- Copy the agent binaries from the CA Enterprise Log Manager Application DVD or ISO image to the target server. The directory for the Windows agent is `\CA\ELM\Agent\Windows_x86_32`.

You must be an Administrator or have a role that grants you write access to the Administrative tab and Log Collection subtab of the CA Enterprise Log Manager interface.

To download the agent installer from CA Enterprise Log Manager

1. Log on to the computer where you want to install the agent, connect to the CA Enterprise Log Manager interface and log on with Administrator credentials.
2. Click the Administration tab.
The Log Collection subtab displays the Log Collection Explorer in the left pane.
3. Select the Agent Explorer folder.
A toolbar displays in the main pane. The downward-pointing arrow button is Download Agent Binaries.
4. Click Download Agent Binaries.
Links for the available agent binaries appear in the main pane.

5. Select the desired Windows platform.

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

6. Select the location based on the type of installation you want:
 - Select the desktop as the location to download the installation program, if you want to install the agent manually with the wizard.
 - Select the C:\WINDOWS (or C:\WINNT) directory if you want to install the agent silently. This is the default location where the installer will create or modify, and then execute, a response file from the command line.
7. Click Save.

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

8. Click OK.

If you downloaded to the desktop, the agent installation setup launcher appears there.

Install the Agent

You must be a Windows Administrator on the computer on which you plan to install the agent. Before you begin the installation, gather the following information:

- IP address or host name of the CA Enterprise Log Manager server to which the agent is to return events
- Agent authentication key that is configured in the CA Enterprise Log Manager server

Note: The agent authentication key is called the *authentication code* in the installation wizard.

- Name and password for the agent user account you created, or the Windows domain administrator credentials you want the agent to use
- (Optional) An exported connector XML file you can use as a template for configuring connectors

To install a Windows agent

1. Double-click the agent installation launcher.

The installation wizard starts.

2. Click Next, read the end user license agreement, indicate your acceptance of the terms to continue, and click Next.
3. Accept the installation path or change it, and click Next.
4. Choose whether to install in FIPS mode when prompted.

The agent FIPS mode you choose should match the FIPS mode for the CA Enterprise Log Manager server which manages it. The agent, by default, starts in that mode. However, the agent automatically detects the server FIPS mode and restarts itself as needed regardless of the mode you choose.

5. Enter the IP address or host name for the CA Enterprise Log Manager server to which this agent is to forward the logs it collects, and then enter the agent authentication key in the Authentication Code field.

Important! Enter the host name if the CA Enterprise Log Manager is assigned its IP address dynamically.

6. Enter one of the following for the Agent user credential information, and then click Next.
 - The name and password for the local user account you created for the agent. Accept the dot (.) for the domain.
 - The name, domain, and password of the Windows domain administrator you want the agent to use when it runs.
7. (Optional) If you downloaded the Connector.XML file on this host, browse and select it, and then click Next.

The Start Copying Files page appears.

8. Click Next.

The agent installation process completes.

9. Click Finish.

The host name where the agent is installed appears in the Default Agent Group folder on the CA Enterprise Log Manager server.

More information:

[Updating an Agent with New User Credentials](#) (see page 30)

(Optional) Verify the Agent Installation

You can use this procedure to verify the agent installation.

To verify the installation

1. Open the browser and enter the URL for the CA Enterprise Log Manager.
2. Log on as a user with the Administrator role.
3. Click the Administration tab.
4. The Log Collection subtab displays the Log Collection Explorer.
5. Expand Agent Explorer and then expand the Default Agent Group.

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


Export a Connector Configuration

You can export a connector configuration, allowing reuse as a template on different servers of the same platform. This streamlines connector configuration in subsequent agents.

The first time you create an agent on a given platform, you must configure connectors from CA Enterprise Log Manager in order to collect events. When you create subsequent agents on different servers of the same platform, you can export your initial connector configuration to that target server before installing the new agent.

You can enter the name of that connector list file during the agent installation. After agent installation, you can customize this connector for the new agent, rather than configuring an entirely new one.

To export a connector configuration to use as a template

1. From the Windows server where you plan to install the agent, connect to the CA Enterprise Log Manager interface, and log on with Administrator credentials.
2. Click the Administration tab. Expand Agent Explorer and then expand the agent group with the agent where the connector you want to export is deployed.
3. Select the agent with the configured connectors, select one or more connectors, and click Export Connector configuration(s) .

The Select location for download dialog appears with Connectors.xml as the File name.

4. For Save in, navigate to the directory where ca-elmagent-x.x.x.x.exe exists and click Save.

Note: If doing a silent install, the responsefile.iss should also be in this directory.

A message that the integration file has been exported successfully appears.

5. Click OK.
6. Click Save and Close for the New Saved Configuration.

A success message appears.

7. Click OK.

How to Install Silently

If the silent installation is to include a reference to an exported connector, you must manually install an agent first and create the connector. Create a connector for the Windows platform using a domain account for the credentials and local host for the hostname. Export this connector to create a connector configuration file, Connectors.xml.

Installing silently involves the following procedures:

1. Create a user account for the agent.
2. Review the setup checklist, and record the following values for the response file:
 - Installation directory path, where the default is C:\Program Files\CA\elmagent\
 - IP address or host name of the CA Enterprise Log Manager for this agent
 - Agent authentication key
 - Windows User account credentials created for the agent
 - (Optional) A downloaded connector configuration file
3. Load the agent installer in the default directory for the response file, %WINDIR%.
4. Create a response file.
5. Invoke the silent install.
6. (Optional) Verify the silent installation.

After you create an initial response file, you can also install silently using a customized response file with the following steps:

1. Prepare a response file for re-use.
2. Install silently with a customize response file.

More information:[Review Setup Checklist](#) (see page 25)[Create a Response File](#) (see page 26)[Invoke the Silent Install](#) (see page 27)[View or Set the Agent Authentication Key](#) (see page 18)[Download Agent Binaries](#) (see page 20)[Prepare a Response File for Re-use](#) (see page 28)

Review Setup Checklist

You need to supply the same values in the agent installation wizard whether you install an agent manually or set up a response file for silent installation. Before you install, gather the data in the following checklist.

Field	Description
Installation directory path	Path where the agent is installed, where the default is C:\Program Files\CA\elmagent\
Server IP (or Name)	IP address or host name of the CA Enterprise Log Manager server Enter the host name rather than the IP address if the CA Enterprise Log Manager server is assigned its IP address dynamically through DHCP.
Authentication Code	The Agent Authentication Key
Username	The user name for the agent as defined in the Windows Users folder under Computer Management
Password	The password associated with the agent Username
File	(Optional) The name of the exported XML file, typically, Connector.XML.

Create a Response File

Running the agent installer in record mode from a command line creates a response (*.iss) file and installs an agent. You can use the response file to install the agent silently on remote systems after recording it.

Note: You must be an Administrator on the Windows server operating system to set up a response file.

The naming convention for the agent installer is ca-elmagent-x.x.x.x.exe, where the x.x.x.x represents the build number for the agent. The response file is created in %WINDIR% if you do not specify the absolute path with the /f1 option.

To create a response file

1. Open the command prompt.
2. Navigate to the location of the agent installer.

Note: If you do not know where it is, do a Search for it through Windows Explorer as "ca-elmagent*"

3. Enter the following command:

```
ca-elmagent-x.x.x.x /r /f1 "<path>\responsefile.iss"
```

/r indicates record mode and "responsefile.iss" can include the path. Be sure to leave no space between /f1 and the response file name. An example of this is:

```
ca-elmagent-12.0.37.10 /r /f1 "C:\elmagentresponse.iss"
```

The Welcome page of the agent installation wizard appears, click Next.

4. Complete the agent installation wizard. Supply the values you recorded when reviewing the setup checklist.

The response file is generated at the specified path. If you specified no path, it can be found in the %WINDIR% directory.

More information:

[Download Agent Binaries](#) (see page 20)

Response File Command Line Examples

Consider the following response file command line examples for use with the agent installer for Windows systems.

This example command line creates the file, `agentresponsefile.iss`, in the `C:\WINDOWS` or `C:\WINNT` directory:

```
ca-elmagent-12.0.37.8.exe /r /f1"agentresponsefile.iss"
```

This example command line creates the file, `agentresponsefile.iss`, in the `C:\` directory:

```
ca-elmagent-12.0.37.8.exe /r /f1"C:\agentresponsefile.iss"
```

Invoke the Silent Install

You can invoke the silent installation of the agent on a Windows server using the response file (*.iss) with appropriate values for this agent installation. You must be an Administrator to run the silent install program.

To invoke a silent install

1. Open a command prompt.
2. Navigate to the directory where the response file is saved.
The default directory is `C:\WINDOWS` (or `C:\WINNT`).
3. Verify the agent installer is in the current directory. You should see a response similar in format to `ca-elmagent-12.0.37.10.exe`.
4. Run the following command to silently install an agent:

```
ca-elmagent-x.x.x.x /s /f1"responsefile.iss"
```

An example command line is, `ca-elmagent-12.0.37.10 /s /f1"elmagentresponse.iss"`

The agent is installed.

View the Agent Status Details

The Agent Explorer lists new agents as they are installed. The Agent Status Details for a selected agent displays whether the agent service is Running.

To view the agent status details

1. Log on to the CA Enterprise Log Manager interface with Administrator credentials.
2. Click the Administration tab.

The Log Collection subtab displays the Agent Explorer.

3. Expand Agent Explorer and then expand the Default Agent Group.

The name of the computer on which you installed the agent appears.

4. Click the agent name and verify on Agent Status Details that the Status is displayed as Running.

Note: The status of Not Responding indicates that the agent, watchdog, or dispatcher process is not running. Take remedial action specific to the operating environment.

Prepare a Response File for Re-use

Setting up a response file minimizes installation time when installing many agents. You do not have to type in each parameter manually for each installation. For example, if you want to install an agent on 1000 systems, you can automate the process by reusing the first response file you create as a template.

When you create a new agent user account on a target server, keeping the same name and password specified in the response file may offer an advantage. When the account credentials match the response file, you can reuse it without change, because the agent registers with the same CA Enterprise Log Manager server. This means that the authentication key does not change.

To prepare to reuse the response file

1. Log on to the Windows server where you created the response file.
2. Navigate to the directory where the original response file resides.

The default directory is %WINDIR%, for example, C:\WINDOWS or C:\WINNT or it may be on the C:\ drive.

3. Copy the response file and give it a different name.

Ensure that the file has the extension, *.iss. (You will later copy the new file to the target server.)

4. Log in to a different Windows server.
5. Create a Windows user account for the agent.
6. Copy the response file to the %WINDIR% directory.
7. Edit the file to customize it for your requirements. Examples of the response file data that you can modify includes the following:

- Change the installation directory path, where the path to change is displayed in bold type.

szDir=**C:\Program Files\CA\elmagent**

- Change the IP address of the CA Enterprise Log Manager server or the agent authentication key.

szEdit1=**127.0.0.1**

szEdit2=**This_is_default_authentication_key**

- Change the User account credentials for the agent

szEdit1=**elmagentusr**

szEdit1=**elmagentpwd**

More information:

[Invoke the Silent Install](#) (see page 27)

Install Silently with a Customized Response File

Use this procedure to install an agent silently using a customized response file.

Note: This procedure assumes that you have created a response file and customized it.

To install silently with a custom response file

1. Copy the customized response file to the target server, if it is not already there.
2. Invoke the silent install with the following command:

```
ca-elmagent-x.x.x.x /s /f1"customizedresponsefile.iss"
```

In this command, replace x.x.x.x with the actual release number for your agent installation package. Replace the sample file name with your actual file name.

More information

[Prepare a Response File for Re-use](#) (see page 28)

Maintenance Considerations

After you have an agent installed, started, and configured, you may need to perform the following tasks:

- Update an existing agent with new user credentials
- Uninstall an agent

More information:

[Prepare a Response File for Re-use](#) (see page 28)

[Updating an Agent with New User Credentials](#) (see page 30)

[Uninstall an Agent](#) (see page 33)

Updating an Agent with New User Credentials

You can update user credentials for an agent after installation by running the AgentAuthUtil utility. You might need to do this if you are moving to a user account with lower privileges, or if an employee who is responsible for overseeing the account leaves your company.

You can change user credentials for an agent without needing to re-install the agent. If you did not set up a dedicated agent user account before installing the agent, you could run this utility to allow the agent to run as a non-Administrator or non-root user.

Updating an agent with new user credentials involves the following steps:

1. Run the utility, AgentAuthUtil, from a command line.
2. Edit the agent details in the CA Enterprise Log Manager interface.
3. Restart the agent.

More information

[Create a User Account for the Agent](#) (see page 18)

Run the AgentAuthUtil Utility

Use this procedure to update user credentials for the agent.

Important! This procedure is not part of the normal installation process.

To update the agent with new low-privilege user account credentials

1. Log onto a Windows server where you have installed an agent.
2. Access the command prompt and navigate to ...\\CA\\elmagent\\bin.

This is the directory that contains the AgentAuthUtil program that you use to perform the update.

3. Enter the following command:

```
agentauthutil -dir "<agent install directory>" <agent-username>
```

Note: For a local user account, do not specify a domain, not even a dot (.).

The default agent install directory is C:\Program Files\CA\elmagent, and the agent-username is the name you assigned to the user account you created in the Users group for this Windows server.

When this command completes, the agent user named *agent-username* has full control (modify, read, execute, write, delete, list contents) over the agent installation folder, subfolders, and files.

4. Enter the following command:

```
agentauthutil -srv caelmagent <agent-username>
```

The service name is caelmagent, and the *agent-username* is the name you assigned to the user account you created in the Users group for this Windows server.

When this command completes, the agent user named *agent-username* can start, stop, pause, or continue (resume) the CA Enterprise Log Manager Agent service on the Windows agent host.

5. Verify that the response messages indicate that each operation completed successfully.

In this example, *agent-username* is elmagentusr. Example response messages from running this utility follow:

```
C:\Program Files\CA\elmagent\bin>agentauthutil -dir "C:\Program Files\CA\elmagen
t" elmagentusr
CHECKING FOR USER ACCOUNT.....
ACCOUNT LOOK UP FINISHED
SETTING FOLDER PERMISSIONS.....
FOLDER DACL UPDATED SUCCESSFULLY
OPERATION SUCCESSFUL.....
UTILITY EXITING.....

C:\Program Files\CA\elmagent\bin>agentauthutil -srv caelmagent elmagentusr
CHECKING FOR USER ACCOUNT.....
ACCOUNT LOOK UP FINISHED
SETTING SERVICE PRIVILEGES.....
SERVICE DACL UPDATED SUCCESSFULLY
SUCCESSFULLY GRANTED LOG ON AS SERVICE PRIVILEGES
OPERATION SUCCESSFUL.....
UTILITY EXITING.....
```

More information

[Create a User Account for the Agent](#) (see page 18)

AgentAuthUtil Command Examples

To assign permissions to the agent installation directory

The following command gives the agent account, *elmagentusr*, full control over the *elmagent* folder, its subfolders, and all of the files they contain:

```
agentauthutil -dir "C:\Program Files\CA\elmagent" elmagentusr
```

To assign permissions for the caelmagent service

The following command gives the agent account, *elmagentusr*, the ability to change the state of the *caelmagent* service:

```
agentauthutil -srv caelmagent elmagentusr
```

Edit the Agent Details in CA Enterprise Log Manager

You can edit the agent details in the CA Enterprise Log Manager interface to use the new user credentials.

To edit the agent details

1. Click the Administration tab.
2. Expand the Agent Explorer.
3. Expand the Default Agent Group or the user-defined agent group to which the agent belongs, and select the agent.
4. Click Edit Agent Details.
5. Enter the new user credentials.
6. Click Save.

Restart the Agent

Use this procedure to restart the agent from the CA Enterprise Log Manager interface after changing the user credentials.

To restart the agent

1. Click the Administration tab.
2. Expand the Agent Explorer.
3. Expand the Default Agent Group or the user-defined agent group to which the agent belongs, and select the agent.
4. Click Status and Command and select View Status of Agents.

5. Select the Select check box for the agent and click Restart.
A confirmation message states that the command is placed in the queue.
6. Click Status and Command. You can view the status change from stopped to running.

Uninstall an Agent

You can uninstall an agent on a Windows host server.

To uninstall an agent on a Windows host

1. Access the Add or Remove Programs utility from the Windows Control Panel.
2. Select the CA Enterprise Log Manager Agent and click Change/Remove.
The install wizard appears with a message to confirm deletion.
3. Click Yes.
The wizard uninstalls the agent.
4. Reboot the host server when the wizard finishes to complete the uninstallation process.

Installing an Agent with CA Software Delivery

Packages are available to deliver CA Enterprise Log Manager agents with the CA Software Delivery program. The required packages are located in the CA Enterprise Log Manager Application ISO image.

Use the Windows-only program, SDRegister.exe, to register software delivery packages with the Software Delivery Manager. These packages contain pre-recorded sample response files that are only for use as *templates*. The sample response files (*.iss and *.rsp) reside in separate directories identified by operating system name.

You can run SDRRegister.exe from its current location lower in the directory structure to register one package at a time, or it can be run from a root directory to see and register all available packages at one time.

To deliver CA Enterprise Log Manager agents to Windows hosts through a USD/DSM server, you need:

- A DSM/USD server.
- A DSM/USD agent on each host where you plan to install an agent, where the DSM/USD agent points to your DSM./USD server.

To use USD packages for Unicenter Software Delivery

1. Access a Windows server and open the CA Enterprise Log Manager Application ISO image, or access the Application DVD's file list.
2. Navigate to the directory, \USDPackages.
3. Run the SDRRegister.exe program.
4. Select products to register, view and acknowledge the related license files, and register the necessary installation, update, or uninstall files with the Software Delivery Manager. These sealed packages are not yet ready for deployment or distribution.
5. Unseal the packages and update the sample response files using one of the following methods:
 - (Recommended) Record the customized response file (.iss) using the instructions detailed in the applicable procedure listed below.
 - Modify the existing sample response files to reflect your local environment.
6. Install one agent using the custom response file to verify your settings, then re-seal the package.
7. Distribute and deploy the packages to the appropriate systems using the CA Server interface.

For more information about this method of software delivery, consult a CA Software Delivery administrator.

More information

[Create a Response File](#) (see page 26)

[Set Up a Response File](#) (see page 41)

Chapter 3: Installing an Agent on Linux Systems

This section contains the following topics:

[Least-Privileged User Requirements](#) (see page 35)

[How to Install Manually](#) (see page 35)

[How to Install Silently](#) (see page 39)

[Maintenance Considerations](#) (see page 43)

Least-Privileged User Requirements

The agent installation for CA Enterprise Log Manager agents does not offer automatic user or user group creation. Use a root account to install the agent.

While you can run the agent as a root user, it is a better security practice to create a least-privileged account for the agent to use. You can give this user any account name you like, such as *elmagentsr*.

The agent installation adjusts the permissions on the existing user account you specify during installation. The folder permissions include the following:

- Permission 775 (rwxrwxr-x) over the CA Enterprise Log Manager Agent installation folder, its sub-directories, and files.
- As owner, the account has full permissions for all of the files and directories in the agent install directory.
- Other accounts have read and execute permissions.
- The caelmupdatehandler executable has the setuid bit set.

How to Install Manually

Use the following procedures to install an agent:

1. Create an authorized user for the agent.
2. View or set the agent authentication key.
3. Load the agent installer on the server where you plan to install the agent.
4. Install the agent with the provided shell script.

More information:

[Create an Authorized User for an Agent](#) (see page 36)

[View or Set the Agent Authentication Key](#) (see page 18)

[Download Agent Binaries](#) (see page 37)

[Install the Agent](#) (see page 38)

Create an Authorized User for an Agent

The agent installation for CA Enterprise Log Manager agents on Linux systems does not offer automatic user or user group creation. We recommend that you create an authorized user with the lowest set of privileges required to run the agent before you install.

You must have root access to add a user, and you need to have, or create, a group to contain that user first.

Note: The following procedures assume that the directory, `/usr/sbin` is in the system path.

To add a group and a user account

1. Log into the target agent host as a root user and access a command prompt.
2. Run the following command:

```
groupadd <groupname>
```

This creates the group in the `/etc/group` file.

3. Run the following command:

```
adduser <username> -g <groupname>
```

This adds the user specified by `<username>` to the group, `<groupname>`.

4. Set the new user's password with the following command:

```
password <username>
```

This command prompts you to enter and to confirm a new password for this user.

View or Set the Agent Authentication Key

If you are a CA Enterprise Log Manager Administrator, you can set the agent authentication key or view the current setting.

To view or set the agent authentication key

1. Click the Administration tab and then click the Log Collection subtab.

The Log Collection Explorer displays in the left pane.


2. Select the Agent Explorer folder.
A toolbar appears in the main pane.
3. Click Agent Authentication Key.
4. Take one of the following actions:
 - Record the configured name so you have it ready to enter during agent installation.
 - Set or reset it by entering and confirming the agent authentication key to be used for the agent installation.

Note: The default value is: `This_is_default_authentication_key`.
5. Click Save.

Download Agent Binaries

You can download the agent binaries directly from the management CA Enterprise Log Manager server.

To download the agent binaries

1. Log on to the target host computer where you want to install the agent.
2. Open a browser, connect to the CA Enterprise Log Manager interface, and log on with Administrator credentials.
3. Click the Administration tab.
The Log Collection subtab displays the Log Collection Explorer in the left pane.
4. Select the Agent Explorer folder.
A toolbar displays in the main pane.
5. Click Download Agent binaries .
Links for the available agent binaries appear in the main pane.
6. Click the link for the desired platform.
The dialog, Select location for download by <IP address>, appears.
7. Select a directory to which the CA Enterprise Log Manager server downloads the installation files.

8. Click Save.

The CA Enterprise Log Manager server downloads an installation file for the agent. A message showing the download progress of the selected agent binary appears, followed by a confirmation message.

9. Click OK.

If you downloaded to the desktop, the agent installation launcher appears there.

Install the Agent

Use this procedure to install an agent on Red Hat Linux, SuSe Linux, and VMware ESX Server systems. Before you begin, gather the following information:

- Host name of the CA Enterprise Log Manager server to which the agent is to return events
 - Agent authentication key that is configured in the CA Enterprise Log Manager server
- Note:** The agent authentication key is called the authentication code in the installation wizard.
- The root credentials on the target agent host server
 - The agent installation tar file location on the host server
 - (Optional) An exported connector file

To install a Linux agent

1. Log in as root on the computer on which you want to install the agent.
2. Access a command prompt and navigate to the directory where you saved the agent tar file.
3. Extract the tar file with the following command.

For Red Hat Enterprise Linux 4.x:

```
tar -xvf elm_agent_linux_k24_32_x_x_x.tar
```

For Red Hat Enterprise Linux 5.x:

```
tar -xvf elm_agent_linux_k26_32_x_x_x.tar
```

For VMware ESX Server 3.x:

```
tar -xvf elm_agent_linux_k24_32_x_x_x.tar
```

For SuSe Linux 11.x:

```
tar -xvf elm_agent_linux_k26_32_x_x_x.tar
```

4. Run the installation script, `sh install_ca-elmagent`.

5. Press Enter, read the end user license agreement, indicate your acceptance of the terms to continue by entering Yes, and press Enter.
6. Enter the IP address or host name for the CA Enterprise Log Manager server to which this agent forwards the log it collects, and then enter the authentication code.
7. Enter the IP address or host name for the CA Enterprise Log Manager to which this agent forwards the logs it collects, and then enter the authentication key.

Important! Enter the host name if the CA Enterprise Log Manager is assigned its IP address dynamically.

8. Enter the authorized user credentials for the Agent user credential information and press Enter.
9. Enter yes or no to choose whether to install in FIPS mode, and press Enter.

The agent FIPS mode you choose should match the FIPS mode for the CA Enterprise Log Manager server which manages it. However, the agent automatically detects the server FIPS mode and restarts itself as needed regardless of the mode you choose.

10. Accept the default installation path, or change it, and click Next.
11. (Optional) If you want to configure default connectors, enter yes and press Enter. Type the path and file name for the connector configuration and press Enter.

The agent installation process completes.

How to Install Silently

Installing a CA Enterprise Log Manager agent silently on Red Hat Linux, SuSe Linux, and VMware ESX systems involves the following steps:

1. Review the setup checklist.
2. Set up a response file.
3. Invoke the silent install.
4. (Optional) Verify the silent installation.

After you create an initial response file, you can also install silently using a customized response file with the following steps:

1. Prepare a response file for re-use.
2. Install silently with a customize response file.

Review Setup Checklist

While installing an agent on Linux systems, you may need to edit the following parameters in the response file, `ca-elmagent.rsp`, to fit your requirements:

Field	Description
ELM_SERVER	<p>The Host name or IP address of the CA Enterprise Log Manager server.</p> <p>Enter the host name rather than the IP address if the CA Enterprise Log Manager server is assigned its IP address dynamically through DHCP.</p>
AGENT_AUTHKEY	<p>The Agent Authentication Key in the Agent Explorer UI under the Administration tab. Select the Agent Authentication Key button to display the panel.</p> <p>The agent authentication key displays as clear text. Take precautions not to divulge the key to persons not authorized to use it.</p> <p>Note: The agent service will not start after installation if the key value you enter during installation is invalid.</p>
AGENT_USER	<p>The user name with which you want to run the CA Enterprise Log Manager agent. The default name is root.</p> <p>We recommend that you create a lower-privilege user account to run the agent before starting the agent installation.</p>
INSTALL_DIR	<p>The directory in which agent is to be installed. The default directory is <code>opt/CA/ELMAgent</code>.</p>
DEFAULT_CONNECTORS	<p>The path and file name of an XML file for a default connector.</p> <p>You can create a default connector in the CA Enterprise Log Manager Agent Explorer by exporting an existing connector configuration to XML. After you create the export file, move it to the target host before running the installation script.</p> <p>Leave this field blank if you do not plan to install a default connector.</p>

Set Up a Response File

On Linux and VMware ESX systems, you can create a response file for installing an agent using this procedure. Creating the silent response file does not actually install an agent on the local server.

You only have to create the silent response file once. After that, you can use it for any agent you want to install with the same set of configuration parameters.

Note: You may want to edit the response file for reuse to change the installation directory, user name, or password so that it is specific to the target agent host.

To create a silent response file for an agent

1. Log on to a Linux computer as a root user.
2. Open a browser, log into the CA Enterprise Log Manager server, and download the agent binary files.
3. Log off the CA Enterprise Log Manager server.
4. Access a command prompt and navigate to the directory that contains the installation files.
5. Run the following command to create a silent response file:

```
./install_ca-elmagent -g <name of response file>
```

6. Respond to the prompts exactly as if you were installing the agent locally.

When you finish creating the file, you are ready to install agents silently on another host.

More information:

[Prepare a Response File for Re-use](#) (see page 42)

Invoke the Silent Install

You can invoke a silent installation of an agent on a Linux server. Use the response file that you created, or updated, with values for this agent installation. You must be logged in as a root user to run a silent installation.

To invoke a silent install

1. Navigate to the directory where you saved the binary and response file.
2. Run the following command to install an agent silently:

```
./install_ca-elmagent -s <name of response file>
```

The agent is installed using the settings you provided when you recorded in the response file.

View the Agent Status Details

The Agent Explorer lists new agents as they are installed. The Agent Status Details for a selected agent displays whether the agent service is Running.

To view the agent status details

1. Log on to the CA Enterprise Log Manager interface with Administrator credentials.
2. Click the Administration tab.

The Log Collection subtab displays the Agent Explorer.

3. Expand Agent Explorer and then expand the Default Agent Group.

The name of the computer on which you installed the agent appears.

4. Click the agent name and verify on Agent Status Details that the Status is displayed as Running.

Note: The status of Not Responding indicates that the agent, watchdog, or dispatcher process is not running. Take remedial action specific to the operating environment.

Prepare a Response File for Re-use

Setting up a response file minimizes installation time when installing many agents. You do not have to type in each parameter manually for each installation. For example, if you want to install an agent on 1000 systems, you can automate the process by reusing the first response file you create as a template.

When you create a new agent user account on a target server, keeping the same name and password specified in the response file may offer an advantage. When the account credentials match the response file, you can reuse it without change, because the agent registers with the same CA Enterprise Log Manager server. This means that the authentication key does not change.

To prepare to reuse the response file

1. Log into the Linux server where you created the response file.
2. Navigate to the directory where the original response file resides.
3. Copy the response file and give it a different name.
4. Log into a different Linux system.
5. Create a user account for the agent.

6. Copy the modified response file from the first server to the desired directory on the target agent host.
7. Edit the file to customize it for your requirements. Examples of the data in the response file that you can modify includes the following:
 - Change the installation directory path:
`INSTALL_DIR=/opt/CA/ELMAgent`
 - Change the path of the default connectors, if any:
`DEFAULT_CONNECTORS=/temp/connectors.xml`
 - Change the IP address of the CA Enterprise Log Manager server:
`ELM_SERVER=127.00.0.29`
 - Change the agent authentication key:
`AGENT_AUTHKEY=agent authentication key text`
 - Change the User account credentials for the agent:
`AGENT_USER=root`

Install Silently with a Customized Response File

Use this procedure to install an agent silently using a customized response file.

Note: This procedure assumes that you have created a response file and customized it.

To install silently with a custom response file

1. Copy the customized response file to the target server, if it is not already there.
2. Invoke the silent install with the following command:

```
./install_ca-elmagent -s <name of response file>
```

In this command, replace the sample file name with your actual file name.

Maintenance Considerations

Maintenance considerations involve the following:

- Uninstall an Agent

More information:

[Prepare a Response File for Re-use](#) (see page 42)

[Uninstall an Agent](#) (see page 44)

Uninstall an Agent

You can uninstall an agent on a Linux computer using this procedure.

To uninstall an agent on a Linux system

1. Log in as a root user.
2. Run the following command to remove the agent:

```
rpm -e ca-elmagent
```

The agent is uninstalled.

Chapter 4: Installing an Agent on Solaris Systems

This section contains the following topics:

- [Least-Privileged User Requirements](#) (see page 45)
- [Agent Deployment Flowchart for UNIX Platforms](#) (see page 46)
- [Planning Agent Deployment](#) (see page 47)
- [Deploying the First Agent](#) (see page 48)
- [Preparing Files and Testing Silent Installation](#) (see page 54)
- [Deploying All Other Planned Agents](#) (see page 57)
- [Preparing New Agents for Use](#) (see page 59)
- [Maintaining Agents](#) (see page 59)

Least-Privileged User Requirements

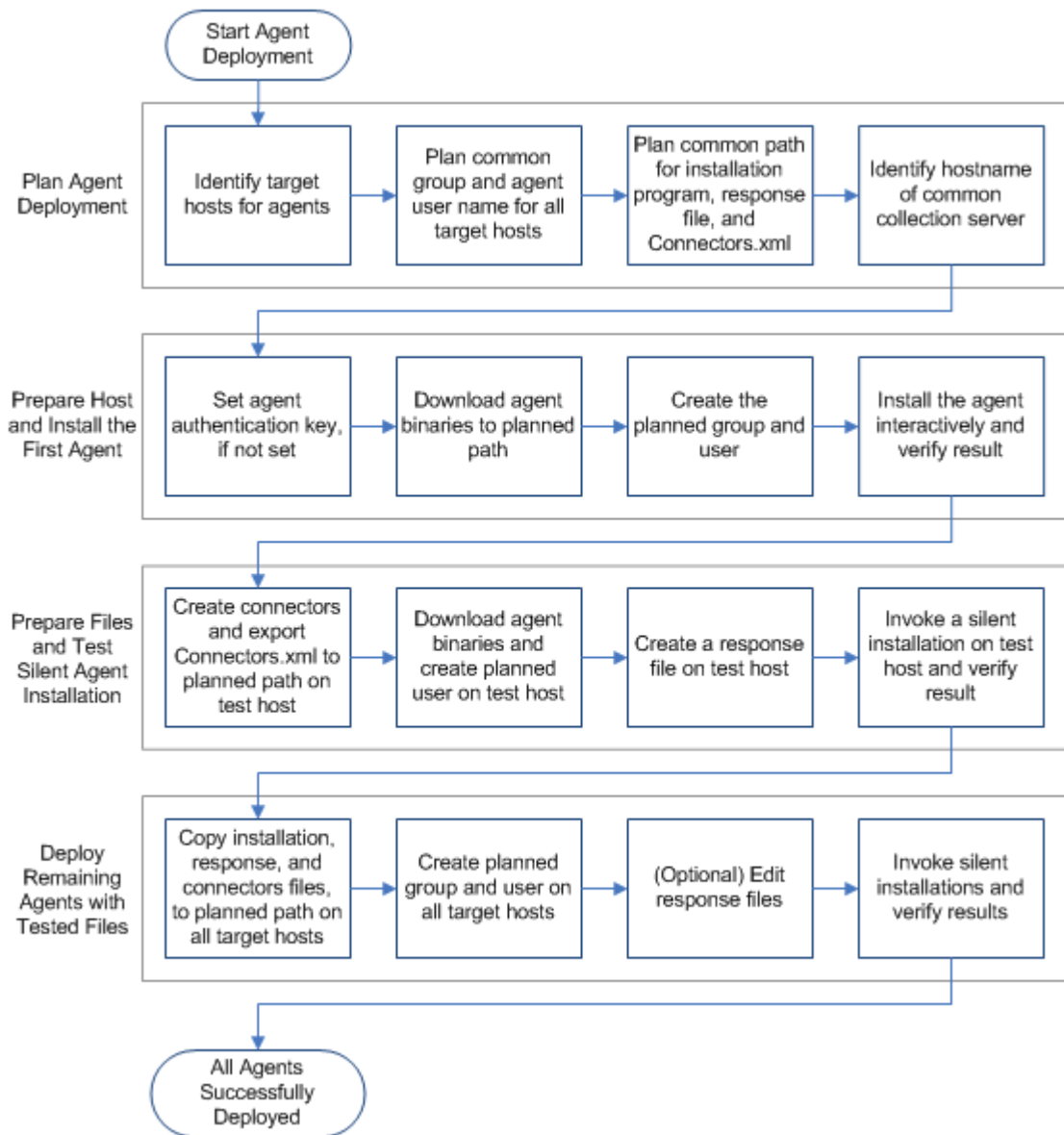
The agent installation for CA Enterprise Log Manager agents does not offer automatic user or user group creation. Use a root account to install the agent.

While you can run the agent as a root user, it is a better security practice to create a least-privileged account for the agent to use. You can give this user any account name you like, such as *elmagentsr*.

The agent installation adjusts the permissions on the existing user account you specify during installation. The folder permissions include the following:

- Permission 775 (rwxrwxr-x) over the CA Enterprise Log Manager Agent installation folder, its sub-directories, and files.
- As owner, the account has full permissions for all of the files and directories in the agent install directory.
- Other accounts have read and execute permissions.
- The caelmupdatehandler executable has the setuid bit set.

Agent Deployment Flowchart for UNIX Platforms



This section is based on the following agent deployment workflow. See online help for tasks related to monitoring and maintaining agents.

Planning Agent Deployment

Before you begin agent deployments, it is a good practice to identify elements that all agent installations can share and elements unique to each installation. The more elements that agents have in common, the easier agent installations become. Elements unique to each installation are the computers on which agents are installed and computers from which the agents collect events. Elements all agents can share include the collection server that manages the agents, the credentials of the low-privileged user under which the agent service runs, and the authentication key.

Common planning tasks include the following:

- Identify event sources from which to collect events.
- Identify computers that meet system requirements for agent installation.
Note: See the CA Enterprise Log Manager [Agent Hardware and Software Certification Matrix](#).
- Determine the IP addresses and host names of the computers that require agents.
- Identify the CA Enterprise Log Manager collection server that each agent is to register with.
- Decide on a common name and group for the low privileged user for agents.
- Set the authentication key to use for all agent installations. If already set, record the current setting for use during installation.
- Identify the host to target for the first agent installation. This agent can be used for creating connectors and exporting Connectors.xml to be referenced in the response file.
- Identify a second host to target for creating a response file and testing silent installation.
- Plan a common path for saving the exported Connectors.xml, the response file, and the installation program. You specify the path for the Connectors.xml file when you create a response file. It is convenient to copy all three files to the same location when preparing for mass deployment.
- Accept the default directory for agent installation, /opt/CA/ELMAgent, or determine another directory to use for all agent installations.

Deploying the First Agent

Efficient agent deployment takes planning. After determining common and unique elements for planned agents, you are ready to deploy the first agent. The recommended process follows:

1. Get the authentication key and installation software from the collection server.
 - a. View and remember the agent authentication key or set a new value.
 - b. Download agent binaries.
2. Prepare to install the first agent on a new operating environment.
 - a. Copy the binaries to the target host.
 - b. Create an <install directory> and extract binaries.
 - c. Create a low privileged user for the agent.
3. Install the first agent interactively.
4. Verify successful installation or troubleshoot and then verify successful installation.
 - a. Monitor agent installation self-monitoring events.
 - b. Examine agent status detail.
 - c. Troubleshoot the installation.

View or Set the Agent Authentication Key

If you are a CA Enterprise Log Manager Administrator, you can set the agent authentication key or view the current setting.

To view or set the agent authentication key

1. Click the Administration tab and then click the Log Collection subtab.

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

A toolbar appears in the main pane.
 3. Click Agent Authentication Key.
 4. Take one of the following actions:
 - Record the configured name so you have it ready to enter during agent installation.
 - Set or reset it by entering and confirming the agent authentication key to be used for the agent installation.
- Note:** The default value is: `This_is_default_authentication_key`.
5. Click Save.

Download Agent Binaries

Download agent binaries from the collection server that is to manage the agent. Download the binaries to the computer from which you browsed to the CA Enterprise Log Manager.


To download the agent binaries

1. Log on to CA Enterprise Log Manager as an Administrator.
2. Click the Administration tab.

The Log Collection subtab displays the Log Collection Explorer in the left pane.

3. Select the Agent Explorer folder.

A toolbar displays in the main pane.

4. Click Download Agent binaries. 

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

5. Click the link for the desired operating environment and version.
6. Select a directory to download the installation file and click Save.

The CA Enterprise Log Manager server downloads the file. A message showing the download progress of the selected agent binary appears, followed by a confirmation message.

7. Click OK.

Note: Unless you downloaded the agent binaries to the target host, export the downloaded tar file to the target host. Then, log on to this host and extract the tar file. The directory containing the installation file is referred to in this guide as the <install directory>.

Create a Low Privileged User for a Planned Agent

While you can run the agent as a root user, it is a better security practice to create a low privileged account for the agent to use. We recommend that you create a low privileged user and group before installing the agent. Assign required permissions to the group and user.

Determine whether your site policies permit identical account on all agent hosts with passwords that never expire. If so, you can create a response file where the same agent user name can be used for all silent installations.

Note: The following procedures assume that the directory, `/usr/sbin` is in the system path.

To add a group and a user account for use by an agent that is not yet installed

1. Log into the target agent host as root and access a command prompt.
2. Create a group in `/etc/group`.
3. Give the primary group full permissions to support subsequent changes to this low privileged user.
4. Add the name of the planned low privileged user to the group you created.
Consider an easily recognized username, such as *elmagentusr*.
5. Set a password for the new user and re-enter to confirm it.

Installing an Agent Interactively

The prerequisites for installing a CA Enterprise Log Manager agent interactively are the same on any UNIX system.

Prerequisites include:

- The following information for entry during the installation process
 - Host name or IP address of the CA Enterprise Log Manager server to which the agent is to return events.
 - Agent authentication key configured in the CA Enterprise Log Manager server.
 - Name of the low-privileged user defined on the target host.
- The target host location of the agent installation tar file.

When you download the agent binaries from CA Enterprise Log Manager, you save the tar file to the host from which you opened the browser to access CA Enterprise Log Manager. Copy this file to the host where you plan to install the agent. Consider creating a directory on the target host under `/usr` and copying the tar file to `/usr/<mydirectory>`.

Important! In this guide, we refer to the directory containing the file you invoke to install the agent as the *<install directory>*.

The installation program installs the agent and creates the *agent root directory*, `/opt/CA/ELMAgent`. The installation program refers to `/opt/CA/ELMAgent` as the install path.

Install the Agent on a Solaris Host

Installing a CA Enterprise Log Manager agent on a Solaris system is done from the command line.

To install a Solaris agent

1. Log on to the target host as root.
2. From the command prompt, navigate to the directory where you saved the agent tar file and extract the contents of the agent tar file.
3. Navigate to the install directory with the agent package file, ca-elmagent.pkg.
4. Run the following command.

```
pkgadd -d <elmagent_solaris.pkg>
```

A message asking you to select the package to process appears.
5. Press Enter to select the default, all.

The license agreement appears.
6. Read the end-user license agreement. To accept, type Yes.
7. If you selected a custom install, either accept the installation path or change it and click Next.
8. Enter the IP address or host name for the CA Enterprise Log Manager to which this agent forwards the logs it collects.

Important! Enter the host name if the CA Enterprise Log Manager is assigned its IP address dynamically.
9. Enter the authentication key defined in the CA Enterprise Log Manager server.
10. Enter the agent username or, if root, press Enter.
11. Do *one* of the following:
 - If you want to run the Agent in FIPS mode, type YES and press Enter.
 - If you want to run the Agent in non-FIPS mode, type NO and press Enter.
12. Enter the full path to the ca-elmagent root directory, or press Enter to accept the default, /opt/CA/ELMAgent.

A message designed to determine the availability of the Connectors.xml file appears.

13. Do *one* of the following:

- If you did not export the connector configuration file to this host, type No.

Note: No is the typical response for the first installation.

- If you did export Connector.xml, type Yes.

A prompt that requests the default connectors configuration file path appears.

- a. Type the path.

14. Type Y to create the ca-elmagent root directory.

15. Type Y to continue with the agent installation.

The following message appears: Installation of <ca-elmagent> was successful. If you specified a low privileged user as the agent username, the installation process assigned required permissions.

Note: Technically, the agent service starts when the caelmwatcdog process successfully binds with the caelmagent process. To verify that a successful bind occurred or to troubleshoot a bind failure, see Troubleshooting Agent Installation.

More information:

[Troubleshooting Agent Installation](#) (see page 59)

Verify Locally that the Agent is Running

Successful agent installation typically starts the agent service. Technically, the agent service starts when the caelmwatcdog process successfully binds with the caelmagent process.

You can determine whether the agent you installed is running while still logged on to the Solaris host.

To verify locally that the agent service is running

1. Change directories to the agent root directory, /opt/CA/ELMAgent.

2. Enter the following:

```
ps -eaf|grep caelm
```

3. Verify that the agent, caelmagent, is running. If two lines similar to the following example appear in the command results, the agent is running.

```
root 16843 16809 0 17:58:11 ?    0:00 ./caelmwatcdog
root 16809  1 0 17:57:57 ?    0:57 ./caelmagent -b
```

4. If the agent service is not running, see Troubleshooting Agent Installation for remedial action.

More information:

[Troubleshooting Agent Installation](#) (see page 59)

Examine Self-Monitoring Events for Agent Startup

Examine self-monitoring events to determine whether the agent service of the installed agent started successfully. You can monitor the agent installation process, whether installing manually or silently.

To monitor agent registration and startup processing

1. Browse to the CA Enterprise Log Manager server that is managing the agent that you installed.
2. Click the Queries and Reports tab.
3. Type self in the Search field under Query List.
4. Select the query, System Self Monitoring Events Detail.
5. Create a filter that displays only events from the server where you installed the agent:
 - a. Click Show/Edit Local Filters
 - b. Click Add Filter.
 - c. For the column entry agent_address, type as the value the IP address of the server where you installed the agent.
 - d. Click Save.
6. Examine the self-monitoring event for System Status:

Current Reporting ELM Server set to <IP address specified as host server>
7. Examine the self-monitoring events for System Startup. Example events follow:

Registered with ELMServers successfully.
Agent's HTTP Listener started on port 25275.
Agent started successfully.

After the Agent started successfully message appears, view the agent status details.
8. If the "Agent started successfully" message does not appear, start the agent service manually as described in "Troubleshooting the Installation."

View the Agent Status Details

The Agent Explorer lists new agents as they are installed. The Agent Status Details for a selected agent displays whether the agent service is Running.

To view the agent status details

1. Log on to the CA Enterprise Log Manager interface with Administrator credentials.
2. Click the Administration tab.

The Log Collection subtab displays the Agent Explorer.

3. Expand Agent Explorer and then expand the Default Agent Group.

The name of the computer on which you installed the agent appears.

4. Click the agent name and verify on Agent Status Details that the Status is displayed as Running.

Note: The status of Not Responding indicates that the agent, watchdog, or dispatcher process is not running. Take remedial action specific to the operating environment.

Preparing Files and Testing Silent Installation

The most efficient way to deploy agents on additional hosts for a given operating environment is to configure sample connectors on the first agent, and then leverage this effort. After you create and test connectors on the first agent, you export those definitions. Then, you deploy a test agent by creating a response file that references Connectors.xml and performing a silent installation. If all goes well with this test deployment, you can confidently deploy all other planned agents with this same response file and same Connectors.xml.

The recommended process follows:

1. From the first agent, create and export connectors as Connectors.xml.
2. From a second test host, do the following:
 - a. Load the Connectors.xml.
 - b. Load the tar file and extract the contents, which includes the installation file.
 - c. Create a response file.
 - d. Perform a silent install.
 - e. Verify that the results are what you want for widespread deployment. If they are not, refine the files as needed.

Create and Export Connectors

Create connectors for a given operating environment on the first agent you install is a good practice. You can then export these connector configurations for use in all subsequent agent installations. Connectors are exported as a Connectors.xml file. When you specify Connectors.xml in the response file for silent installations, the agents are deployed with all connectors in place. After the silent installation with connectors, you configure the event sources that each agent targets.

Alternatively, you can skip this step and deploy each connector in bulk after installing all agents for this operating environment. With the bulk connector deployment wizard, you can create a connector for a specific integration and deploy that connector to multiple agents. With this method, you would use bulk deployment for each desired integration.

The process of creating connectors to use as templates involves the following procedures:

1. Identify the subscription integrations for this operating environment.
2. For each desired integration:
 - a. Configure event sources.
 - b. Configure one connector.
 - c. Examine results of event collection.
3. Refine the connectors
4. Export the connectors as Connectors.xml.

Note: For details on each procedure, see the *Connector Guides* for your operating environment and the *Administration Guide*.

Prepare a Host for Testing Silent Installation

Before running the script to create the response file for silent installation, perform the following tasks:

1. Download the agent binaries, copy the tar file to this host and extract the file.
2. Create a low-privileged user with the planned name.
3. Copy the exported Connectors.xml to this host. Copy it to the directory with the installation file you extracted.

Create the Response File

On the Solaris host you are using for testing, create a response file. A response file provides the specifications for all agents installed silently with this file.

To create a response file for silent agent installation

1. Log on to the host you are using for testing.
2. Navigate to the <install directory> where the ca-elmagent.pkg and Connectors.xml files reside.
3. Begin creating the response file, ca-elmagent.rsp.

```
sh install_ca-elmagent.sh -g ca-elmagent.rsp
```

4. Respond to the prompts exactly as if you were installing the agent locally.

Select package(s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]:

Do you agree to the above license terms? [Yes or No] (No):

Enter the hostname/IP of the ELM server :

Enter ELM server authentication code :

Enter the ELM Agent username (root):

Enter the full path to the ca-elmagent root directory (/opt/CA/ELMAgent):

Do you want to configure default connectors?[Yes or No] (Yes):

Enter default connectors configuration file path :

A confirmation message appears.

5. (Optional) View the response file contents. An example follows:

```
EULA=Y
```

```
ELM_SERVER=172.24.36.107
```

```
AGENT_AUTHKEY=my_authentication_key
```

```
AGENT_USER=elmagentusr
```

```
FIPSMODE=OFF
```

```
INSTALL_DIR=/opt/CA/ELMAgent
```

```
DEFAULT_CONNECTORS=/usr/mydir/connectors.xml
```

Install an Agent Silently

You can invoke a silent installation of an agent on a Solaris server. Use the response file composed of values for this agent installation. You must be logged in as a root user to run a silent installation. The <install directory> must contain the ca-elmagent.pkg and the ca-elmagent.rsp files.

Before you invoke a silent install, review the response file settings. If the response file contains a value other than root for AGENT_USER, verify that a low privileged user with this name has been defined on this host. If the response file includes a path for DEFAULT_CONNECTORS, verify the Connectors.xml resides in that path.

To invoke a silent install

1. Navigate to the directory where you saved the binary (ca-elmagent.pkg) and response file (ca-elmagent.rsp).
2. Run the following command to install an agent silently, where ca-elmagent.rsp is the name of the response file.

```
pkgadd -d ca-elmagent.pkg -n -a admin -r ca-elmagent.rsp ca-elmagent
```

The agent is installed using the settings you provided when you recorded in the response file.

3. Verify that the following message appears:

```
Installation of <ca-elmagent> was successful.
```

Validate Results of the Silent Installation

Before widespread deployment to multiple hosts through silent installation, validate the results of the initial silent installation of the test host.

Deploying All Other Planned Agents

Deploying the first agent and testing a response file that includes connector configurations comprises most of the work in agent deployment. By leveraging that work, you can roll out the remaining agents with much less effort.

Preparing additional hosts and installing the agents requires that you repeat some of the procedures you performed when installing the first two agents. Consider these tasks when deploying each remaining agent that is based on the first agent.

1. Create a directory for loading the agent installation file, response file, and connectors file. This directory is the <install directory>.
2. Copy the tar file to target host, and extract the contents into the <install directory>.
3. Copy the response file to the <install directory>.
4. Copy the Connectors.xml file to the <install directory>.
5. (Optional) Edit the response file.
This step is not needed if you elected to use common elements where possible.
6. Create the planned group and low privileged user.
7. Invoke the silent installation.
8. Verify successful installation.
 - a. Monitor self-monitoring events for agent startup
 - b. View the agent status details.

Edit the Response File

When you install an agent or create a response file on a Solaris system, you specify values for the five parameters listed on the following table. If you copy this file for reuse on other systems, you can edit the original values as needed, or if appropriate, use the original values.

To edit the response file

1. Log on to the host where you plan to invoke the silent installation.
2. Navigate to the <install directory> where the ca-elmagent.rsp resides.
3. Use an editor of your choice to modify any of the values shown on the following table, then save the ca-elmagent.rsp file.

Field	Description
ELM_SERVER	The Host name or IP address of the CA Enterprise Log Manager server. Enter the host name if the CA Enterprise Log Manager server gets its IP address dynamically through DHCP.
BASEDIR	The full path to the agent root directory. Default: /opt/CA/ELMAgent.
AUTH_CODE	The Agent Authentication Key. Select the Agent Authentication Key button in the Agent Explorer under Administration to view or set this key. Note: If the key value you enter during installation does not match the entry in the UI, the agent service will not start after installation.
FIPSMODE	Indicates if the Agent runs in FIPS mode. Default: OFF
AGENT_USER	The user name for running the CA Enterprise Log Manager agent. We recommend that you create a lower-privilege user account to run the agent before starting the agent installation. Default: root
DEFAULT_CONNECTORS	The exported file containing connector configurations, including the path. Leave this field blank if the Connectors.xml file is not available. Default: <blank>

Preparing New Agents for Use

Use the following procedures to prepare each agent for use:

1. Apply subscription updates to new agents and connectors.
2. Complete connector configurations, including configuring the event sources.
Note: The Connectors.xml file derived from the first installed agent provides templates you can use as a basis for event-source specific connectors.
3. Examine query results and reports to determine whether the data is being collected and refined as expected.
4. Tailor the connector configurations to meet local requirements.
5. (Optional) Create agent groups and move the agent to the desired agent group.

Note: For details on each procedure, see the *Connector Guides* for your operating environment and the *Administration Guide*.

Maintaining Agents

Maintenance tasks for CA Enterprise Log Manager agents include the following:

- Changing the agent user, if corporate policy mandates a change.
- Troubleshooting when agent installation is successful but the agent service is not started successfully
- Uninstalling an agent, where the procedures can differ depending on whether installation was interactive or silent

Note: For maintenance tasks such as applying subscription updates to agents and connectors, creating agent groups, and starting or stopping agents, see online help.

Troubleshooting Agent Installation

Occasionally, process binding does not take place as expected. Use the following procedure to diagnose this error and take corrective action.

To diagnose and correct a bind failure

1. Log on to the Solaris host as root.
2. Change directories to the agent root directory, /opt/CA/ELMAgent.
3. Type the following command:

```
ps - eaf|grep caelm
```

4. Examine the displayed results.

- A successful bind results in a display similar to the following example. Here, the caelmwatchdog process ID 27773 successfully binds with the caelmagent process ID 27771. A successful bind starts the agent service.

```
root 27773 27771 0 18:11:12 ? 0:00 ./caelmwatchdog
root 27771 1 0 18:11:07 ? 0:02 ./caelmagent -b
root 27793 26155 0 18:14:22 pts/1 0:00 grep caelm
root 27772 27771 0 18:11:07 ? 0:00 ./caelmdispatcher
```

- An unsuccessful bind results in a display similar to the following example. Here, the caelmwatchdog and caelmagent process IDs are not displayed and the agent service is not started.

```
root 28386 26155 0 18:56:18 pts/1 0:00 grep caelm
root 28300 1 0 18:51:39 ? 0:01 ./caelmdispatcher
```

Note: If the caelmwatchdog binding to the caelmagent did not take place, kill the caelmdispatcher and start the agent service manually.

5. If you determine that the agent start was unsuccessful, do the following:

- a. To kill the caelmdispatcher, enter `kill -9 <caelmdispatcher process ID>`, for example:

```
kill -9 28300
```

- b. Change directories to `/opt/CA/ELMAgent/bin`.
- c. Start the CA Enterprise Log Manager agent service.

```
./S99elmagent start
```

The message "CA ELM Agent Started Successfully" appears.

Note: View the agent status details again and verify that the agent is Running.

Change the Low Privileged User for an Agent

You can change `<original_username>` to `<replacement_username>` for the low privileged user on the agent host. When you change the user name under which the agent runs, update the CA Enterprise Log Manager UI with the new user name.

To change the low privileged user for an agent that is running as a low privileged user

1. Make the replacement user part of the primary group.
2. Set a password for the replacement user and confirm the new password.
3. (Optional) Remove the `<original_username>` from the group.
4. (Optional) Delete the `<original_username>` from the host.

5. Update the CA Enterprise Log Manager UI with the <replacement_username> for the agent:
 - a. Click the Administration tab.
 - b. Expand the Agent Explorer.
 - c. Expand the Default Agent Group or the user-defined agent group to which the agent belongs, and select the agent.
 - d. Click Edit Agent Details.
 - e. Enter the new user name.
 - f. Click Save.

Uninstall an Interactively Installed Agent

You can uninstall an agent on a Solaris computer using this procedure.

To uninstall an agent that was interactively installed on a Solaris system

1. Access the target Solaris system locally or remotely.
2. Log in as a root user.
3. Access a Unix shell.
4. Change directories to /opt/CA/ELMAgent.
5. Type the following commands to initiate the uninstall process.

```
pkgrm ca-elmagent
```
6. When the following prompts appear, type y for yes:

```
Do you want to remove this package [y, n, ?, q]
Do you want to continue with the removal of this package [y, n, ?, q]
```

The uninstall process runs. Detailed information is saved in /tmp/uninstall_ca-elmagent.<timestamp>.log.
7. Verify that the following confirmation message appears:

```
Removal of <ca-elmagent> was successful.
The agent is uninstalled.
```

Important! Log on to the CA Enterprise Log Manager server that managed the agent you uninstalled. If the agent is still displayed in an agent group under the Log Collection, Agent Explorer folder, delete the agent. Click Select in the Agent Status Details, click Delete, and respond Yes to the confirmation prompt.

Uninstall a Silently Installed Agent

The command to uninstall a silently installed agent is different from the command to uninstall a manually installed agent. The difference is due to the existence of the admin file that is used only for silent installations.

To uninstall an agent that was silently installed on a Solaris host

1. Log on as root to the Solaris host where the agent is installed.
2. Access a command prompt.
3. Change directories to the <install directory>.
4. Type the following command:

```
pkgm -a admin -n ca-elmagent
```

5. Verify that the final message indicates removal of the agent. For example:

```
Removal of <ca-elmagent> was successful.
```

Chapter 5: Installing an Agent on HP-UX Systems

This section contains the following topics:

- [Prerequisite](#) (see page 63)
- [Least-Privileged User Requirements](#) (see page 63)
- [Agent Deployment Flowchart for UNIX Platforms](#) (see page 64)
- [Planning Agent Deployment](#) (see page 65)
- [Deploying the First Agent](#) (see page 66)
- [Preparing Files and Testing Silent Installation](#) (see page 72)
- [Deploying All Other Planned Agents](#) (see page 75)
- [Preparing New Agents for Use](#) (see page 77)
- [Maintaining Agents](#) (see page 77)

Prerequisite

Before you install the CA Enterprise Log Manager agent on an HP-UX system, you must install the patches PHNE_41060 and PHNE_41004 on the HP-UX system. For more information about these patches, see www.hp.com www.hp.com.

Least-Privileged User Requirements

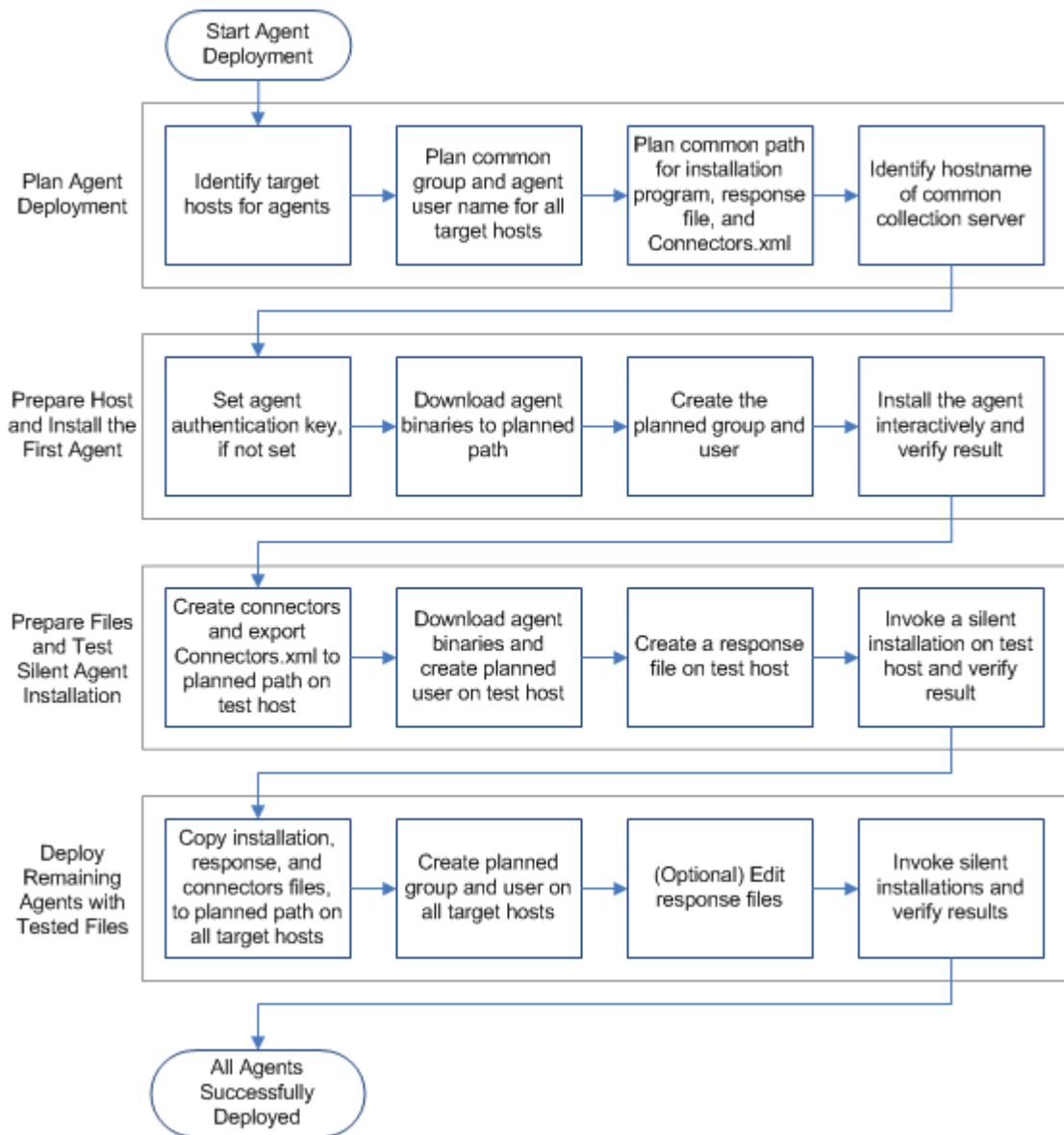
The agent installation for CA Enterprise Log Manager agents does not offer automatic user or user group creation. Use a root account to install the agent.

While you can run the agent as a root user, it is a better security practice to create a least-privileged account for the agent to use. You can give this user any account name you like, such as *elmagentsr*.

The agent installation adjusts the permissions on the existing user account you specify during installation. The folder permissions include the following:

- Permission 775 (rwxrwxr-x) over the CA Enterprise Log Manager Agent installation folder, its sub-directories, and files.
- As owner, the account has full permissions for all of the files and directories in the agent install directory.
- Other accounts have read and execute permissions.
- The caelmupdatehandler executable has the setuid bit set.

Agent Deployment Flowchart for UNIX Platforms



This section is based on the following agent deployment workflow. See online help for tasks related to monitoring and maintaining agents.

Planning Agent Deployment

Before you begin agent deployments, it is a good practice to identify elements that all agent installations can share and elements unique to each installation. The more elements that agents have in common, the easier agent installations become. Elements unique to each installation are the computers on which agents are installed and computers from which the agents collect events. Elements all agents can share include the collection server that manages the agents, the credentials of the low-privileged user under which the agent service runs, and the authentication key.

Common planning tasks include the following:

- Identify event sources from which to collect events.
- Identify computers that meet system requirements for agent installation.
Note: See the CA Enterprise Log Manager [Agent Hardware and Software Certification Matrix](#).
- Determine the IP addresses and host names of the computers that require agents.
- Identify the CA Enterprise Log Manager collection server that each agent is to register with.
- Decide on a common name and group for the low privileged user for agents.
- Set the authentication key to use for all agent installations. If already set, record the current setting for use during installation.
- Identify the host to target for the first agent installation. This agent can be used for creating connectors and exporting Connectors.xml to be referenced in the response file.
- Identify a second host to target for creating a response file and testing silent installation.
- Plan a common path for saving the exported Connectors.xml, the response file, and the installation program. You specify the path for the Connectors.xml file when you create a response file. It is convenient to copy all three files to the same location when preparing for mass deployment.
- Accept the default directory for agent installation, /opt/CA/ELMAgent, or determine another directory to use for all agent installations.

Deploying the First Agent

Efficient agent deployment takes planning. After determining common and unique elements for planned agents, you are ready to deploy the first agent. The recommended process follows:

1. Get the authentication key and installation software from the collection server.
 - a. View and remember the agent authentication key or set a new value.
 - b. Download agent binaries.
2. Prepare to install the first agent on a new operating environment.
 - a. Copy the binaries to the target host.
 - b. Create an <install directory> and extract binaries.
 - c. Create a low privileged user for the agent.
3. Install the first agent interactively.
4. Verify successful installation or troubleshoot and then verify successful installation.
 - a. Monitor agent installation self-monitoring events.
 - b. Examine agent status detail.
 - c. Troubleshoot the installation.

View or Set the Agent Authentication Key

If you are a CA Enterprise Log Manager Administrator, you can set the agent authentication key or view the current setting.

To view or set the agent authentication key

1. Click the Administration tab and then click the Log Collection subtab.


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

A toolbar appears in the main pane.
 3. Click Agent Authentication Key.
 4. Take one of the following actions:
 - Record the configured name so you have it ready to enter during agent installation.
 - Set or reset it by entering and confirming the agent authentication key to be used for the agent installation.
- Note:** The default value is: `This_is_default_authentication_key`.
5. Click Save.

Download Agent Binaries

Download agent binaries from the collection server that is to manage the agent. Download the binaries to the computer from which you browsed to the CA Enterprise Log Manager.

To download the agent binaries

1. Log on to CA Enterprise Log Manager as an Administrator.
2. Click the Administration tab.
The Log Collection subtab displays the Log Collection Explorer in the left pane.
3. Select the Agent Explorer folder.
A toolbar displays in the main pane.
4. Click Download Agent binaries. 
Links for the available agent binaries appear in the main pane.
5. Click the link for the desired operating environment and version.
6. Select a directory to download the installation file and click Save.
The CA Enterprise Log Manager server downloads the file. A message showing the download progress of the selected agent binary appears, followed by a confirmation message.
7. Click OK.

Note: Unless you downloaded the agent binaries to the target host, export the downloaded tar file to the target host. Then, log on to this host and extract the tar file. The directory containing the installation file is referred to in this guide as the <install directory>.

Create a Low Privileged User for a Planned Agent

While you can run the agent as a root user, it is a better security practice to create a low privileged account for the agent to use. We recommend that you create a low privileged user and group before installing the agent. Assign required permissions to the group and user.

Determine whether your site policies permit identical account on all agent hosts with passwords that never expire. If so, you can create a response file where the same agent user name can be used for all silent installations.

Note: The following procedures assume that the directory, `/usr/sbin` is in the system path.

To add a group and a user account for use by an agent that is not yet installed

1. Log into the target agent host as root and access a command prompt.
2. Create a group in `/etc/group`.
3. Give the primary group full permissions to support subsequent changes to this low privileged user.
4. Add the name of the planned low privileged user to the group you created.
Consider an easily recognized username, such as *elmagentusr*.
5. Set a password for the new user and re-enter to confirm it.

Installing an Agent Interactively

The prerequisites for installing a CA Enterprise Log Manager agent interactively are the same on any UNIX system.

Prerequisites include:

- The following information for entry during the installation process
 - Host name or IP address of the CA Enterprise Log Manager server to which the agent is to return events.
 - Agent authentication key configured in the CA Enterprise Log Manager server.
 - Name of the low-privileged user defined on the target host.
- The target host location of the agent installation tar file.

When you download the agent binaries from CA Enterprise Log Manager, you save the tar file to the host from which you opened the browser to access CA Enterprise Log Manager. Copy this file to the host where you plan to install the agent. Consider creating a directory on the target host under `/usr` and copying the tar file to `/usr/<mydirectory>`.

Important! In this guide, we refer to the directory containing the file you invoke to install the agent as the *<install directory>*.

The installation program installs the agent and creates the *agent root directory*, `/opt/CA/ELMAgent`. The installation program refers to `/opt/CA/ELMAgent` as the install path.

Install the Agent on an HP-UX Host

Installing a CA Enterprise Log Manager agent on an HP-UX system is done from the command line.

To install a CA Enterprise Log Manager agent on an HP-UX host

1. Log on to the target host as root.
2. From the command prompt, navigate to the directory with the agent tar file.
3. Extract the contents of the HP-caelmagent.tar file.

```
tar -xvf HP-caelmagent.tar
```

The tar command creates a subdirectory named hpux_parisc_32 under the current directory.

4. Navigate to the hpux_parisc_32 directory.
5. Run the script file, install_ca-elmagent.sh, to begin the agent installation process.

```
sh install_ca-elmagent.sh
```

The license agreement appears.

6. Read the end-user license agreement.
A message asking if you agree to the license terms appears.
7. To accept the license terms, type Yes.
8. Enter the IP address or host name for the CA Enterprise Log Manager to which this agent forwards the logs it collects.

Important! Enter the host name if the CA Enterprise Log Manager is assigned its IP address dynamically.

9. Enter the authentication key defined in the CA Enterprise Log Manager server.
10. Enter the agent username or, if root, press Enter.
11. Do *one* of the following:
 - If you want to run the Agent in FIPS mode, type YES and press Enter.
 - If you want to run the Agent in non-FIPS mode, type NO and press Enter.
12. Enter the full path to the ca-elmagent root directory, or press Enter to accept the default, /opt/CA/ELMAgent.

13. Do *one* of the following:

- If you did not export the connector configuration file to this host, type No.
- If you did export Connector.xml, type Yes.

A prompt that requests the default connectors configuration file path appears.

a. Type the path.

A message designed to determine the availability of the Connectors.xml file appears.

The following message appears: Installation of <ca-elmagent> was successful.

If you specified a low privileged user as the agent username, the installation process assigns required permissions to this user.

Agent installation on HP-UX systems creates subdirectories under the agent root directory, /opt/CA/ELMAgent. The /opt/CA/ELMAgent/install directory contains the script for uninstalling the agent.

Verify Locally that the Agent is Running

Successful agent installation typically starts the agent service. Technically, the agent service starts when the caelmwatchdog process successfully binds with the caelmagent process.

You can determine whether the agent you installed is running while still logged on to the HP-UX host.

To verify locally that the agent service is running

1. Change directories to the agent root directory, /opt/CA/ELMAgent.
2. Enter the following:

```
ps -ef|grep caelm
```

3. Verify that the agent, caelmagent, is running. If two lines similar to the following example appear in the command results, the agent is running.

```
root 16843 16809 0 17:58:11 ?    0:00 ./caelmwatchdog
root 16809  1 0 17:57:57 ?    0:57 ./caelmagent -b
```

4. If the agent service is not running, see Troubleshooting Agent Installation for remedial action.

More information:

[Troubleshooting Agent Installation](#) (see page 77)

Examine Self-Monitoring Events for Agent Startup

Examine self-monitoring events to determine whether the agent service of the installed agent started successfully. You can monitor the agent installation process, whether installing manually or silently.

To monitor agent registration and startup processing

1. Browse to the CA Enterprise Log Manager server that is managing the agent that you installed.
2. Click the Queries and Reports tab.
3. Type self in the Search field under Query List.
4. Select the query, System Self Monitoring Events Detail.
5. Create a filter that displays only events from the server where you installed the agent:
 - a. Click Show/Edit Local Filters
 - b. Click Add Filter.
 - c. For the column entry agent_address, type as the value the IP address of the server where you installed the agent.
 - d. Click Save.
6. Examine the self-monitoring event for System Status:

Current Reporting ELM Server set to <IP address specified as host server>
7. Examine the self-monitoring events for System Startup. Example events follow:

Registered with ELMServers successfully.
Agent's HTTP Listener started on port 6789.
Agent started successfully.

After the Agent started successfully message appears, view the agent status details.
8. If the "Agent started successfully" message does not appear, start the agent service manually as described in "Troubleshooting the Installation."

View the Agent Status Details

The Agent Explorer lists new agents as they are installed. The Agent Status Details for a selected agent displays whether the agent service is Running.

To view the agent status details

1. Log on to the CA Enterprise Log Manager interface with Administrator credentials.
2. Click the Administration tab.

The Log Collection subtab displays the Agent Explorer.

3. Expand Agent Explorer and then expand the Default Agent Group.

The name of the computer on which you installed the agent appears.

4. Click the agent name and verify on Agent Status Details that the Status is displayed as Running.

Note: The status of Not Responding indicates that the agent, watchdog, or dispatcher process is not running. Take remedial action specific to the operating environment.

Preparing Files and Testing Silent Installation

The most efficient way to deploy agents on additional hosts for a given operating environment is to configure sample connectors on the first agent, and then leverage this effort. After you create and test connectors on the first agent, you export those definitions. Then, you deploy a test agent by creating a response file that references Connectors.xml and performing a silent installation. If all goes well with this test deployment, you can confidently deploy all other planned agents with this same response file and same Connectors.xml.

The recommended process follows:

1. From the first agent, create and export connectors as Connectors.xml.
2. From a second test host, do the following:
 - a. Load the Connectors.xml.
 - b. Load the tar file and extract the contents, which includes the installation file.
 - c. Create a response file.
 - d. Perform a silent install.
 - e. Verify that the results are what you want for widespread deployment. If they are not, refine the files as needed.

Create and Export Connectors

Create connectors for a given operating environment on the first agent you install is a good practice. You can then export these connector configurations for use in all subsequent agent installations. Connectors are exported as a Connectors.xml file. When you specify Connectors.xml in the response file for silent installations, the agents are deployed with all connectors in place. After the silent installation with connectors, you configure the event sources that each agent targets.

Alternatively, you can skip this step and deploy each connector in bulk after installing all agents for this operating environment. With the bulk connector deployment wizard, you can create a connector for a specific integration and deploy that connector to multiple agents. With this method, you would use bulk deployment for each desired integration.

The process of creating connectors to use as templates involves the following procedures:

1. Identify the subscription integrations for this operating environment.
2. For each desired integration:
 - a. Configure event sources.
 - b. Configure one connector.
 - c. Examine results of event collection.
3. Refine the connectors
4. Export the connectors as Connectors.xml.

Note: For details on each procedure, see the *Connector Guides* for your operating environment and the *Administration Guide*.

Prepare a Host for Testing Silent Installation

Before running the script to create the response file for silent installation, perform the following tasks:

1. Download the agent binaries, copy the tar file to this host and extract the file.
2. Create a low-privileged user with the planned name.
3. Copy the exported Connectors.xml to this host. Copy it to the directory with the installation file you extracted.

Create the Response File

On HP-UX systems, you can create a response file for installing an agent silently. This response file provides the specifications for all agents installed silently with this file.

To create a response file for silent agent installation

1. Log on to the host you are using for testing.
2. Navigate to the <install directory> where install_ca-elmagent.sh resides. For example, navigate to /usr/mydir/hpux_parisc_32.
3. If referencing connector configurations in the response file, verify the location of Connectors.xml.

The <install directory> is the preferred location.

4. Begin creating the response file, where <response_file> is the name of your choosing.

```
sh install_ca-elmagent.sh -g <response_file>
```

5. Respond to the following prompts exactly as if you were installing the agent locally.

Do you agree to the above license terms? [Yes or No] (No):

Enter the hostname/IP of the ELM server :

Enter ELM server authentication code :

Enter the ELM Agent username (root):

Enter the full path to the ca-elmagent root directory (/opt/CA/ELMAgent):

Do you want to configure default connectors? (Yes):

Enter default connectors configuration file path :

A confirmation message appears.

6. (Optional) View the response file contents.

```
cat <response_file>
```

An example response file follows:

```
EULA=Y
```

```
ELM_SERVER=172.24.36.107
```

```
AGENT_AUTHKEY=my_authentication_key
```

```
AGENT_USER=elmagentusr
```

```
INSTALL_DIR=/opt/CA/ELMAgent
```

```
DEFAULT_CONNECTORS=/usr/mydir/hpux
```

Install an Agent Silently

You can install a CA Enterprise Log Manager agent on an HP-UX host silently with the responses stored in the specified response file.

To install a CA Enterprise Log Manager agent silently on an HP-UX host

1. Log on as root to the HP-UX host where you want to install the agent.
2. Navigate to the <install directory>, for example, /usr/<mydirectory>/hpux.
3. Verify that the following files reside in this directory:
 - install_ca-elmagent.sh
 - <response_file>
 - Connectors.xml.

4. Run the agent installation script.

```
sh install_ca-elmagent.sh -s <response_file>
```

The following messages appear:

```
Running Silent installation process !
Source Depot location: /usr/<mydir>/hpux/ca-elmagent.depot
Software depot registration is done successfully
Proceeding with the Depot Installation...
Installation of 'ca-elmagent' product succeeds!
Check the Installation Log File - /tmp/install_ca-elmagent.031310.0115.log for more information about the
progress of 'ca-elmagent' Installation!
```

Validate Results of the Silent Installation

Before widespread deployment to multiple hosts through silent installation, validate the results of the initial silent installation of the test host.

Deploying All Other Planned Agents

Deploying the first agent and testing a response file that includes connector configurations comprises most of the work in agent deployment. By leveraging that work, you can roll out the remaining agents with much less effort.

Preparing additional hosts and installing the agents requires that you repeat some of the procedures you performed when installing the first two agents. Consider these tasks when deploying each remaining agent that is based on the first agent.

1. Create a directory for loading the agent installation file, response file, and connectors file. This directory is the <install directory>.
2. Copy the tar file to target host, and extract the contents into the <install directory>.
3. Copy the response file to the <install directory>.
4. Copy the Connectors.xml file to the <install directory>.
5. (Optional) Edit the response file.
This step is not needed if you elected to use common elements where possible.
6. Create the planned group and low privileged user.
7. Invoke the silent installation.
8. Verify successful installation.
 - a. Monitor self-monitoring events for agent startup
 - b. View the agent status details.

Edit the Response File

When you install an agent or create a response file on an HP-UX host, you specify values for the five parameters listed on the following table. If you copy this file for reuse on other systems, you can edit the original values as needed, or if appropriate, use the original values.

To edit the response file

1. Log on to the host where you plan to invoke the silent installation.
2. Navigate to the <install directory> where `install_ca-elmagent.sh` and the response file reside.
3. Use an editor of your choice to modify any of the values shown on the following table, then save the response file to the original name.

Field	Description
ELM_SERVER	The Host name or IP address of the CA Enterprise Log Manager server. Enter the host name if the CA Enterprise Log Manager server gets its IP address dynamically through DHCP.
INSTALL_DIR	The full path to the agent root directory. Default: /opt/CA/ELMAgent.
AGENT_AUTHKEY	The Agent Authentication Key. Select the Agent Authentication Key button in the Agent Explorer under Administration to view or set this key. Note: If the key value you enter during installation does not match the entry in the UI, the agent service will not start after installation.
AGENT_USER	The user name for running the CA Enterprise Log Manager agent. We recommend that you create a lower-privilege user account to run the agent before starting the agent installation. Default: root
FIPSMODE	Indicates if the Agent runs in FIPS mode. Default: OFF
DEFAULT_CONNECTORS	The exported file containing connector configurations, including the path. Leave this field blank if the Connectors.xml file is not available. Default: <blank>

Preparing New Agents for Use

Use the following procedures to prepare each agent for use:

1. Apply subscription updates to new agents and connectors.
2. Complete connector configurations, including configuring the event sources.
Note: The Connectors.xml file derived from the first installed agent provides templates you can use as a basis for event-source specific connectors.
3. Examine query results and reports to determine whether the data is being collected and refined as expected.
4. Tailor the connector configurations to meet local requirements.
5. (Optional) Create agent groups and move the agent to the desired agent group.

Note: For details on each procedure, see the *Connector Guides* for your operating environment and the *Administration Guide*.

Maintaining Agents

Maintenance tasks for CA Enterprise Log Manager agents include the following:

- Changing the agent user, if corporate policy mandates a change.
- Troubleshooting when agent installation is successful but the agent service is not started successfully
- Uninstalling an agent, where the procedures can differ depending on whether installation was interactive or silent

Note: For maintenance tasks such as applying subscription updates to agents and connectors, creating agent groups, and starting or stopping agents, see online help.

Troubleshooting Agent Installation

Occasionally, process binding does not take place as expected. Use the following procedure to diagnose this error and take corrective action.

To diagnose whether the agent has started on HP-UX and start it manually if needed

1. Log on to the HP-UX host as root.
2. Change directories to the <install directory>, for example, /usr/<mydirectory>/hpux.
3. Display details of caelm processes.

```
ps -ef|grep caelm
```

4. Examine the displayed results.

- A successful agent start has results similar to the following:

```
root 16843 16809 0 17:58:11 ?    0:00 ./caelmwatcdog
root 16809   1 0 17:57:57 ?    0:57 ./caelmagent -b
root 16811 16809 0 17:57:58 ?    0:20 ./caelmdispatcher
```

- An unsuccessful agent start has results similar to the following:

```
root 25285   1 0 01:15:32 ?    0:01 ./caelmagent -b
```

5. If you determine that the agent start was unsuccessful, do the following:

- a. Change directories to the location of the stopped agent, `/opt/CA/ELMAGENT/bin`.
- b. Start the agent manually

```
./S99elmagent start
```

Determine Whether an Agent Exists on a Specified Host

You can determine whether an agent is installed on a given HP-UX host.

To determine whether an agent is installed and if so what version

1. Log on to the host where you want to determine agent status.
2. Run the following command:

```
swlist -l product ca-elmagent
```

3. Review the last line of the system response.

- If the CA Enterprise Log Manager agent is installed, the following message is displayed, where details include the package name, version number, and description:

```
ca-elmagent 12.1.70.1 CA ELM AGENT Software Distributor
```

- If the agent is not installed on the local host, the following message is displayed.

```
Software "ca-elmagent" was not found on host <HOST>:/"
```

Change the Low Privileged User for an Agent

You can change <original_username> to <replacement_username> for the low privileged user on the agent host. When you change the user name under which the agent runs, update the CA Enterprise Log Manager UI with the new user name.

To change the low privileged user for an agent that is running as a low privileged user

1. Make the replacement user part of the primary group.
2. Set a password for the replacement user and confirm the new password.
3. (Optional) Remove the <original_username> from the group.
4. (Optional) Delete the <original_username> from the host.
5. Update the CA Enterprise Log Manager UI with the <replacement_username> for the agent:
 - a. Click the Administration tab.
 - b. Expand the Agent Explorer.
 - c. Expand the Default Agent Group or the user-defined agent group to which the agent belongs, and select the agent.
 - d. Click Edit Agent Details.
 - e. Enter the new user name.
 - f. Click Save.

Uninstall an Agent

You can uninstall a CA Enterprise Log Manager agent on an HP-UX host.

To uninstall an agent on HP-UX

1. Log on to the target HP-UX system.
2. Navigate to /opt/CA/ELMAgent/install.
This directory contains the script to uninstall the agent.
3. Run the unininstall_ca-elmagent.sh script.

```
sh unininstall_ca-elmagent.sh
```

The following message appears, followed by the location of the resulting log file:

```
Uninstallation of 'ca-elmagent' is completed!
```


Chapter 6: Installing an Agent on AIX Systems

This section contains the following topics:

[Least-Privileged User Requirements](#) (see page 81)

[Agent Deployment Flowchart for UNIX Platforms](#) (see page 82)

[Planning Agent Deployment](#) (see page 83)

[Deploying the First Agent](#) (see page 84)

[Preparing Files and Testing Silent Installation](#) (see page 90)

[Deploying All Other Planned Agents](#) (see page 93)

[Preparing New Agents for Use](#) (see page 95)

[Maintaining Agents](#) (see page 95)

Least-Privileged User Requirements

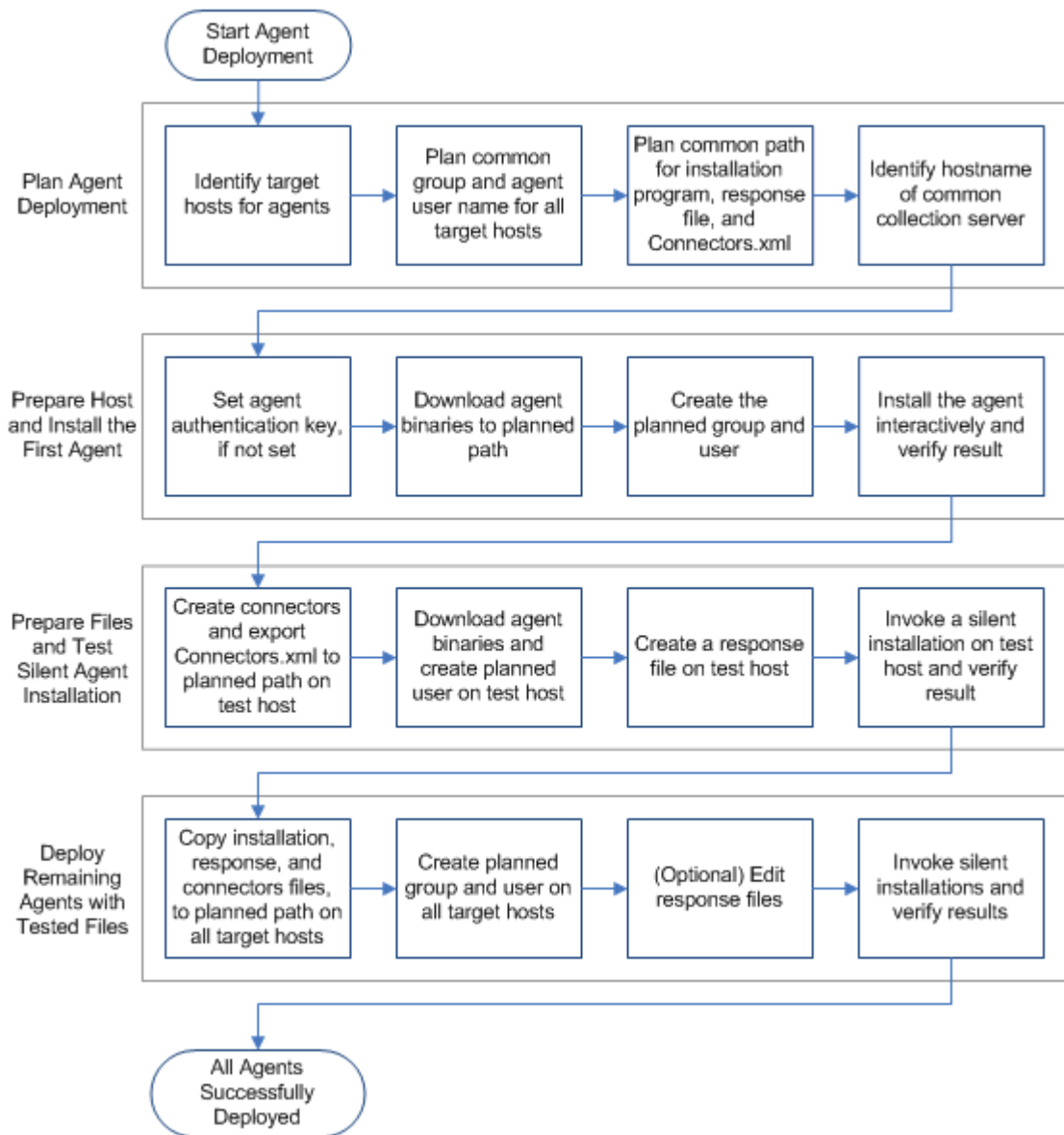
The agent installation for CA Enterprise Log Manager agents does not offer automatic user or user group creation. Use a root account to install the agent.

While you can run the agent as a root user, it is a better security practice to create a least-privileged account for the agent to use. You can give this user any account name you like, such as *elmagentsr*.

The agent installation adjusts the permissions on the existing user account you specify during installation. The folder permissions include the following:

- Permission 775 (rwxrwxr-x) over the CA Enterprise Log Manager Agent installation folder, its sub-directories, and files.
- As owner, the account has full permissions for all of the files and directories in the agent install directory.
- Other accounts have read and execute permissions.
- The caelmupdatehandler executable has the setuid bit set.

Agent Deployment Flowchart for UNIX Platforms



This section is based on the following agent deployment workflow. See online help for tasks related to monitoring and maintaining agents.

Planning Agent Deployment

Before you begin agent deployments, it is a good practice to identify elements that all agent installations can share and elements unique to each installation. The more elements that agents have in common, the easier agent installations become. Elements unique to each installation are the computers on which agents are installed and computers from which the agents collect events. Elements all agents can share include the collection server that manages the agents, the credentials of the low-privileged user under which the agent service runs, and the authentication key.

Common planning tasks include the following:

- Identify event sources from which to collect events.
- Identify computers that meet system requirements for agent installation.
Note: See the CA Enterprise Log Manager [Agent Hardware and Software Certification Matrix](#).
- Determine the IP addresses and host names of the computers that require agents.
- Identify the CA Enterprise Log Manager collection server that each agent is to register with.
- Decide on a common name and group for the low privileged user for agents.
- Set the authentication key to use for all agent installations. If already set, record the current setting for use during installation.
- Identify the host to target for the first agent installation. This agent can be used for creating connectors and exporting Connectors.xml to be referenced in the response file.
- Identify a second host to target for creating a response file and testing silent installation.
- Plan a common path for saving the exported Connectors.xml, the response file, and the installation program. You specify the path for the Connectors.xml file when you create a response file. It is convenient to copy all three files to the same location when preparing for mass deployment.
- Accept the default directory for agent installation, /opt/CA/ELMAgent, or determine another directory to use for all agent installations.

Deploying the First Agent

Efficient agent deployment takes planning. After determining common and unique elements for planned agents, you are ready to deploy the first agent. The recommended process follows:

1. Get the authentication key and installation software from the collection server.
 - a. View and remember the agent authentication key or set a new value.
 - b. Download agent binaries.
2. Prepare to install the first agent on a new operating environment.
 - a. Copy the binaries to the target host.
 - b. Create an <install directory> and extract binaries.
 - c. Create a low privileged user for the agent.
3. Install the first agent interactively.
4. Verify successful installation or troubleshoot and then verify successful installation.
 - a. Monitor agent installation self-monitoring events.
 - b. Examine agent status detail.
 - c. Troubleshoot the installation.

View or Set the Agent Authentication Key

If you are a CA Enterprise Log Manager Administrator, you can set the agent authentication key or view the current setting.

To view or set the agent authentication key

1. Click the Administration tab and then click the Log Collection subtab.


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

A toolbar appears in the main pane.
 3. Click Agent Authentication Key.
 4. Take one of the following actions:
 - Record the configured name so you have it ready to enter during agent installation.
 - Set or reset it by entering and confirming the agent authentication key to be used for the agent installation.
- Note:** The default value is: `This_is_default_authentication_key`.
5. Click Save.

Download Agent Binaries

Download agent binaries from the collection server that is to manage the agent. Download the binaries to the computer from which you browsed to the CA Enterprise Log Manager.

To download the agent binaries

1. Log on to CA Enterprise Log Manager as an Administrator.
2. Click the Administration tab.
The Log Collection subtab displays the Log Collection Explorer in the left pane.
3. Select the Agent Explorer folder.
A toolbar displays in the main pane.
4. Click Download Agent binaries. 
Links for the available agent binaries appear in the main pane.
5. Click the link for the desired operating environment and version.
6. Select a directory to download the installation file and click Save.
The CA Enterprise Log Manager server downloads the file. A message showing the download progress of the selected agent binary appears, followed by a confirmation message.
7. Click OK.

Note: Unless you downloaded the agent binaries to the target host, export the downloaded tar file to the target host. Then, log on to this host and extract the tar file. The directory containing the installation file is referred to in this guide as the <install directory>.

Create a Low Privileged User for a Planned Agent

While you can run the agent as a root user, it is a better security practice to create a low privileged account for the agent to use. We recommend that you create a low privileged user and group before installing the agent. Assign required permissions to the group and user.

Determine whether your site policies permit identical account on all agent hosts with passwords that never expire. If so, you can create a response file where the same agent user name can be used for all silent installations.

Note: The following procedures assume that the directory, `/usr/sbin` is in the system path.

To add a group and a user account for use by an agent that is not yet installed

1. Log into the target agent host as root and access a command prompt.
2. Create a group in `/etc/group`.
3. Give the primary group full permissions to support subsequent changes to this low privileged user.
4. Add the name of the planned low privileged user to the group you created.
Consider an easily recognized username, such as *elmagentusr*.
5. Set a password for the new user and re-enter to confirm it.

Installing an Agent Interactively

The prerequisites for installing a CA Enterprise Log Manager agent interactively are the same on any UNIX system.

Prerequisites include:

- The following information for entry during the installation process
 - Host name or IP address of the CA Enterprise Log Manager server to which the agent is to return events.
 - Agent authentication key configured in the CA Enterprise Log Manager server.
 - Name of the low-privileged user defined on the target host.
- The target host location of the agent installation tar file.

When you download the agent binaries from CA Enterprise Log Manager, you save the tar file to the host from which you opened the browser to access CA Enterprise Log Manager. Copy this file to the host where you plan to install the agent. Consider creating a directory on the target host under `/usr` and copying the tar file to `/usr/<mydirectory>`.

Important! In this guide, we refer to the directory containing the file you invoke to install the agent as the *<install directory>*.

The installation program installs the agent and creates the *agent root directory*, `/opt/CA/ELMAgent`. The installation program refers to `/opt/CA/ELMAgent` as the install path.

Install the Agent on an AIX Host

Installing a CA Enterprise Log Manager agent on an AIX system is done from the command line.

To install an AIX agent

1. Log on to the target host as root.
2. From the command prompt, navigate to the directory where you saved the agent tar binary file.
3. Run the following command:

```
tar -xvf <tar_File_Name>
```

The directory `aix_ppc` is created. The `_AIX_install_support_ca-elmagent.tar`, `ca-elmagent-build_number.aix5.3.ppc.rpm`, and `install_ca-elmagent.sh` files are extracted from the agent tar binary file in to `aix_ppc`.

4. Navigate to the `aix_ppc` folder, and run the following command:

```
sh install_ca-elmagent.sh
```

The license agreement appears.

5. Read the end-user license agreement. To accept, type Yes.
6. Enter the IP address or host name for the CA Enterprise Log Manager to which this agent forwards the logs it collects.

Important! Enter the host name if the CA Enterprise Log Manager is assigned its IP address dynamically.

7. Enter the authentication key defined in the CA Enterprise Log Manager server.
8. Enter the agent username or, if root, press Enter.
9. Do *one* of the following:
 - If you want to run the Agent in FIPS mode, type YES and press Enter.
 - If you want to run the Agent in non-FIPS mode, type NO and press Enter.
10. Enter the full path to the `ca-elmagent` root directory, or press Enter to accept the default, `/opt/CA/ELMAgent`.

11. Do *one* of the following:

- If you did not export the connector configuration file to this host, type No.

Note: No is the typical response for the first installation.

- If you did export Connector.xml, type Yes.

A prompt that requests the default connectors configuration file path appears.

- a. Type the path.

A message designed to determine the availability of the Connectors.xml file appears.

The following message appears: Installation of <ca-elmagent> was successful. If you specified a low privileged user as the agent username, the installation process assigned required permissions.

Note: Technically, the agent service starts when the caelmmatchdog process successfully binds with the caelmagent process. To verify that a successful bind occurred or to troubleshoot a bind failure, see Troubleshooting Agent Installation.

More information

[Troubleshooting Agent Installation](#) (see page 95)

Verify Locally that the Agent is Running

Successful agent installation typically starts the agent service. Technically, the agent service starts when the caelmmatchdog process successfully binds with the caelmagent process.

You can determine whether the agent you installed is running while still logged on to the AIX host.

To verify locally that the agent service is running

1. Change directories to the agent root directory, /opt/CA/ELMAgent.
2. Enter the following:

```
ps -eaf|grep caelm
```

3. Verify that the agent, caelmagent, is running. If two lines similar to the following example appear in the command results, the agent is running.

```
root 16843 16809 0 17:58:11 ?    0:00 ./caelmmatchdog
root 16809  1 0 17:57:57 ?    0:57 ./caelmagent -b
```

4. If the agent service is not running, see Troubleshooting Agent Installation for remedial action.

More information

[Troubleshooting Agent Installation](#) (see page 95)

Examine Self-Monitoring Events for Agent Startup

Examine self-monitoring events to determine whether the agent service of the installed agent started successfully. You can monitor the agent installation process, whether installing manually or silently.

To monitor agent registration and startup processing

1. Browse to the CA Enterprise Log Manager server that is managing the agent that you installed.
2. Click the Queries and Reports tab.
3. Type self in the Search field under Query List.
4. Select the query, System Self Monitoring Events Detail.
5. Create a filter that displays only events from the server where you installed the agent:
 - a. Click Show/Edit Local Filters
 - b. Click Add Filter.
 - c. For the column entry agent_address, type as the value the IP address of the server where you installed the agent.
 - d. Click Save.
6. Examine the self-monitoring event for System Status:

Current Reporting ELM Server set to <IP address specified as host server>
7. Examine the self-monitoring events for System Startup. Example events follow:

Registered with ELMServers successfully.
Agent's HTTP Listener started on port 6789.
Agent started successfully.

After the Agent started successfully message appears, view the agent status details.
8. If the "Agent started successfully" message does not appear, start the agent service manually as described in "Troubleshooting the Installation."

View the Agent Status Details

The Agent Explorer lists new agents as they are installed. The Agent Status Details for a selected agent displays whether the agent service is Running.

To view the agent status details

1. Log on to the CA Enterprise Log Manager interface with Administrator credentials.
2. Click the Administration tab.

The Log Collection subtab displays the Agent Explorer.

3. Expand Agent Explorer and then expand the Default Agent Group.

The name of the computer on which you installed the agent appears.

4. Click the agent name and verify on Agent Status Details that the Status is displayed as Running.

Note: The status of Not Responding indicates that the agent, watchdog, or dispatcher process is not running. Take remedial action specific to the operating environment.

Preparing Files and Testing Silent Installation

The most efficient way to deploy agents on additional hosts for a given operating environment is to configure sample connectors on the first agent, and then leverage this effort. After you create and test connectors on the first agent, you export those definitions. Then, you deploy a test agent by creating a response file that references Connectors.xml and performing a silent installation. If all goes well with this test deployment, you can confidently deploy all other planned agents with this same response file and same Connectors.xml.

The recommended process follows:

1. From the first agent, create and export connectors as Connectors.xml.
2. From a second test host, do the following:
 - a. Load the Connectors.xml.
 - b. Load the tar file and extract the contents, which includes the installation file.
 - c. Create a response file.
 - d. Perform a silent install.
 - e. Verify that the results are what you want for widespread deployment. If they are not, refine the files as needed.

Create and Export Connectors

Create connectors for a given operating environment on the first agent you install is a good practice. You can then export these connector configurations for use in all subsequent agent installations. Connectors are exported as a Connectors.xml file. When you specify Connectors.xml in the response file for silent installations, the agents are deployed with all connectors in place. After the silent installation with connectors, you configure the event sources that each agent targets.

Alternatively, you can skip this step and deploy each connector in bulk after installing all agents for this operating environment. With the bulk connector deployment wizard, you can create a connector for a specific integration and deploy that connector to multiple agents. With this method, you would use bulk deployment for each desired integration.

The process of creating connectors to use as templates involves the following procedures:

1. Identify the subscription integrations for this operating environment.
2. For each desired integration:
 - a. Configure event sources.
 - b. Configure one connector.
 - c. Examine results of event collection.
3. Refine the connectors
4. Export the connectors as Connectors.xml.

Note: For details on each procedure, see the *Connector Guides* for your operating environment and the *Administration Guide*.

Prepare a Host for Testing Silent Installation

Before running the script to create the response file for silent installation, perform the following tasks:

1. Download the agent binaries, copy the tar file to this host and extract the file.
2. Create a low-privileged user with the planned name.
3. Copy the exported Connectors.xml to this host. Copy it to the directory with the installation file you extracted.

Create the Response File

On the AIX host you are using for testing, create a response file. A response file provides the specifications for all agents installed silently with this file.

To create a response file for silent agent installation

1. Log on to the host you are using for testing.
2. Navigate to the <install directory> where the ca-elmagent.pkg and Connectors.xml files reside.

3. Begin creating the response file.

```
pkgask -r response_filename.rsp -d ca-elmagent.pkg
```

4. Respond to the prompts exactly as if you were installing the agent locally.

Select package(s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]:

Do you agree to the above license terms? [Yes or No] (No):

Enter the hostname/IP of the ELM server :

Enter ELM server authentication code :

Enter the ELM Agent username (root):

Enter the full path to the ca-elmagent root directory (/opt/CA/ELMAgent):

Do you want to configure default connectors?[Yes or No] (Yes):

Enter default connectors configuration file path :

A confirmation message appears.

5. (Optional) View the response file contents. An example follows:

```
EULA=Y
```

```
ELM_SERVER=172.24.36.107
```

```
BASEDIR=/opt/CA/ELMAgent
```

```
AUTH_CODE=my_authentication_key
```

```
AGENT_USER=elmagentusr
```

```
DEFAULT_CONNECTORS=/usr/mydir
```

```
INST_MSGFILE=/tmp/install_ca-elm.msg.EN
```

```
INST_LOGFILE=/tmp/install_ca-elmagent.030410.1749.log
```

Invoke an Agent Silently

You can invoke a silent installation of an agent on a UNIX server. Use the response file composed of values for this agent installation. You must be logged in as a root user to run a silent installation. The <install directory> must contain the ca-elmagent.pkg and the ca-elmagent.rsp files.

Before you invoke a silent install, review the response file settings. If the response file contains a value other than root for AGENT_USER, verify that a low privileged user with this name has been defined on this host. If the response file includes a path for DEFAULT_CONNECTORS, verify the Connectors.xml resides in that path.

To invoke a silent install

1. Navigate to the directory where you saved the binary (ca-elmagent.pkg) and response file (ca-elmagent.rsp).
2. Run the following command to install an agent silently, where ca-elmagent.rsp is the name of the response file.

```
sh install_ca-elmagent.sh -s ca-elmagent.rsp
```

The agent is installed using the settings you provided when you recorded in the response file.

3. Verify that the following message appears:

```
Installation of <ca-elmagent> was successful.
```

Validate Results of the Silent Installation

Before widespread deployment to multiple hosts through silent installation, validate the results of the initial silent installation of the test host.

Deploying All Other Planned Agents

Deploying the first agent and testing a response file that includes connector configurations comprises most of the work in agent deployment. By leveraging that work, you can roll out the remaining agents with much less effort.

Preparing additional hosts and installing the agents requires that you repeat some of the procedures you performed when installing the first two agents. Consider these tasks when deploying each remaining agent that is based on the first agent.

1. Create a directory for loading the agent installation file, response file, and connectors file. This directory is the <install directory>.
2. Copy the tar file to target host, and extract the contents into the <install directory>.
3. Copy the response file to the <install directory>.
4. Copy the Connectors.xml file to the <install directory>.
5. (Optional) Edit the response file.
This step is not needed if you elected to use common elements where possible.
6. Create the planned group and low privileged user.
7. Invoke the silent installation.
8. Verify successful installation.
 - a. Monitor self-monitoring events for agent startup
 - b. View the agent status details.

Edit the Response File

When you install an agent or create a response file on an AIX system, you specify values for the five parameters listed on the following table. If you copy this file for reuse on other systems, you can edit the original values as needed, or if appropriate, use the original values.

To edit the response file

1. Log on to the host where you plan to invoke the silent installation.
2. Navigate to the <install directory> where the ca-elmagent.rsp resides.
3. Use an editor of your choice to modify any of the values shown on the following table, then save the ca-elmagent.rsp file.

Field	Description
ELM_SERVER	The Host name or IP address of the CA Enterprise Log Manager server. Enter the host name if the CA Enterprise Log Manager server gets its IP address dynamically through DHCP.
INSTALL_DIR	The full path to the agent root directory. Default: /opt/CA/ELMAgent.
AGENT_AUTHKEY	The Agent Authentication Key. Select the Agent Authentication Key button in the Agent Explorer under Administration to view or set this key. Note: If the key value you enter during installation does not match the entry in the UI, the agent service will not start after installation.
AGENT_USER	The user name for running the CA Enterprise Log Manager agent. We recommend that you create a lower-privilege user account to run the agent before starting the agent installation. Default: root
FIPSMODE	Indicates if the Agent runs in FIPS mode. Default: OFF
DEFAULT_CONNECTORS	The exported file containing connector configurations, including the path. Leave this field blank if the Connectors.xml file is not available. Default: <blank>

Preparing New Agents for Use

Use the following procedures to prepare each agent for use:

1. Apply subscription updates to new agents and connectors.
2. Complete connector configurations, including configuring the event sources.
Note: The Connectors.xml file derived from the first installed agent provides templates you can use as a basis for event-source specific connectors.
3. Examine query results and reports to determine whether the data is being collected and refined as expected.
4. Tailor the connector configurations to meet local requirements.
5. (Optional) Create agent groups and move the agent to the desired agent group.

Note: For details on each procedure, see the *Connector Guides* for your operating environment and the *Administration Guide*.

Maintaining Agents

Maintenance tasks for CA Enterprise Log Manager agents include the following:

- Changing the agent user, if corporate policy mandates a change.
- Troubleshooting when agent installation is successful but the agent service is not started successfully
- Uninstalling an agent, where the procedures can differ depending on whether installation was interactive or silent

Note: For maintenance tasks such as applying subscription updates to agents and connectors, creating agent groups, and starting or stopping agents, see online help.

Troubleshooting Agent Installation

Occasionally, process binding does not take place as expected. Use the following procedure to diagnose this error and take corrective action.

To diagnose and correct a bind failure

1. Log on to the AIX host as root.
2. Change directories to the agent root directory, /opt/CA/ELMAgent.
3. Type the following command:

```
ps - eaf|grep caelm
```

4. Examine the displayed results.

- A successful bind results in a display similar to the following example. Here, the caelmwatchdog process ID 27773 successfully binds with the caelmagent process ID 27771. A successful bind starts the agent service.

```
root 27773 27771 0 18:11:12 ? 0:00 ./caelmwatchdog
root 27771 1 0 18:11:07 ? 0:02 ./caelmagent -b
root 27793 26155 0 18:14:22 pts/1 0:00 grep caelm
root 27772 27771 0 18:11:07 ? 0:00 ./caelmdispatcher
```

- An unsuccessful bind results in a display similar to the following example. Here, the caelmwatchdog and caelmagent process IDs are not displayed and the agent service is not started.

```
root 28386 26155 0 18:56:18 pts/1 0:00 grep caelm
root 28300 1 0 18:51:39 ? 0:01 ./caelmdispatcher
```

Note: If the caelmwatchdog binding to the caelmagent did not take place, kill the caelmdispatcher and start the agent service manually.

5. If you determine that the agent start was unsuccessful, do the following:

- To kill the caelmdispatcher, enter `kill -9 <caelmdispatcher process ID>`, for example:

```
kill -9 28300
```

- Change directories to `/opt/CA/ELMAgent/bin`.
- Start the CA Enterprise Log Manager agent service.

```
/S99elmagent start
```

The message "CA ELM Agent Started Successfully" appears.

Note: View the agent status details again and verify that the agent is Running.

Change the Low Privileged User for an Agent

You can change `<original_username>` to `<replacement_username>` for the low privileged user on the agent host. When you change the user name under which the agent runs, update the CA Enterprise Log Manager UI with the new user name.

To change the low privileged user for an agent that is running as a low privileged user

- Make the replacement user part of the primary group.
- Set a password for the replacement user and confirm the new password.
- (Optional) Remove the `<original_username>` from the group.
- (Optional) Delete the `<original_username>` from the host.

5. Update the CA Enterprise Log Manager UI with the <replacement_username> for the agent:
 - a. Click the Administration tab.
 - b. Expand the Agent Explorer.
 - c. Expand the Default Agent Group or the user-defined agent group to which the agent belongs, and select the agent.
 - d. Click Edit Agent Details.
 - e. Enter the new user name.
 - f. Click Save.

Uninstall an Agent

Perform the following procedure to uninstall the agent on an AIX host.

To uninstall an agent

1. Log on as root to the AIX host where the agent is installed.
2. Access the command prompt, and navigate to the following path:
installation_directory/install folder
3. Run the following command:
`sh uninstall_ca-elmagent.sh`
4. Verify that the final message indicates removal of the agent. For example:
Removal of <ca-elmagent> was successful.