Installation and Configuration Guide

NetIQ® Secure Configuration Manager UNIX Agent

March 2014

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Contents

About this Book and the Library

This book provides conceptual and installation information about the agent that provide support for UNIX and Linux computers running the NetIQ Secure Configuration Manager product. This book defines terminology and includes implementation scenarios.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Other Information in the Library

The Secure Configuration Manager library provides the following information resources:

Installation Guide

Provides detailed planning and installation information about Secure Configuration Manager.

User Guide

Provides conceptual information about Secure Configuration Manager. This book also provides an overview of the user interfaces and step-by-step guidance for many administration tasks.

UNIX Agent Manager Help

Provides information for all products that integrate with UNIX Agent Manager.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Introduction

The NetIQ Security UNIX Agent enables UNIX and Linux operating system support for the following NetIQ products:

- NetIQ Change Guardian
- NetIQ Secure Configuration Manager
- NetIQ Security Manager
- NetIQ Sentinel

The NetIQ UNIX Agent includes the following components:

- NetIQ UNIX Agent Manager: A user interface that you can use to manage all you Security UNIX Agent components and your AppManager UNIX Agent components across your enterprise. UNIX Agent Manager runs on Windows, Solaris, and Linux operating systems. You can store information about your agent computers in one UNIX Agent Manager server, then access the information through one or numerous UNIX Agent Manager consoles.
- The NetIQ Security Agent for UNIX: A component of the NetIQ UNIX Agent that enables support for Change Guardian, Secure Configuration Manager, Security Manager, and Sentinel.
- Common components: Components that are shared by the AppManager UNIX Agent and the Security Agent for UNIX.

1.1 Overview of Features

Securing and monitoring the performance of your UNIX and Linux environment can be expensive and time-consuming, especially when you and your staff face tight budgets and escalating security threats. Consider the following issues most enterprise performance and security managers face:

- Deficits in staff knowledge concerning UNIX and Linux security and system expertise
- Managing various operating systems including Red Hat, AIX, HP-UX, Solaris, and SUSE Linux
- Controlling access to privileged commands and sensitive resources
- Lacking intrusion detection and response systems to handle both real and potential security breaches

The NetIQ Security Agent for UNIX (UNIX agent) helps you effectively address these challenges, enabling Secure Configuration Manager to monitor the configuration and risk compliance of your UNIX and Linux environment.

1.2 What is the UNIX Agent?

The **NetIQ UNIX Agent** (UNIX agent) validates the configuration of UNIX and Linux endpoints to ensure compliance with corporate security policies and pinpoint potential vulnerabilities. An endpoint represents an agent-monitored operating system, application, web server, or database instance. You can install and configure your UNIX agent manually, or you can use UNIX Agent Manager.

1.3 What is UNIX Agent Manager?

UNIX Agent Manager allows you to install and configure all your UNIX agent components across your enterprise instead of interacting with the agents individually. UNIX Agent Manager also allows you to see any UNIX computers that NetIQ Security Manager, NetIQ AppManager, NetIQ Sentinel, and NetIQ Change Guardian products monitor. UNIX Agent Manager includes a console and a server that stores information and communicates with the agents. You can install numerous consoles that can connect to a single server. UNIX Agent Manager runs on Windows, Solaris, and Linux computers.

1.4 How Does the UNIX Agent Work?

The UNIX agent can collect security compliance information from one or more endpoints in one or many domains. The UNIX agent receives requests from Secure Configuration Manager Core Services and runs commands or responds by returning data, status, or results. The UNIX agent runs locally on computers throughout your enterprise.

When you install a UNIX agent, you can add the computer on which the agent resides to the Secure Configuration Manager asset map. Secure Configuration Manager registers the new UNIX agent and assigns an endpoint to the agent representing the operating system of the agent computer. As you add more systems and endpoints to the asset map, you can designate the endpoint type. A single UNIX agent can monitor multiple types of endpoints. For more information about discovering and adding endpoints to your managed systems in the asset map, see the *User Guide for NetIQ Secure Configuration Manager*.

Each UNIX agent sends regular communication, called a **heartbeat**, to Secure Configuration Manager to verify operation. When the agent receives a heartbeat request, the agent polls its monitored endpoints to verify their statuses and then responds to Secure Configuration Manager. The UNIX agent also responds to requests for data sent from Core Services in the form of security checks and policy templates. Policy templates are groups of security checks that audit a specific series of IT controls that match a security policy standard. The agent translates the security checks into queries that it forwards to its monitored endpoints. Upon receiving responses to the queries, the agent reports the results to Secure Configuration Manager. For more information about Secure Configuration Manager, see the *User Guide for NetIQ Secure Configuration Manager*.

The two key processes used by the UNIX agent are:

- **VigilEntAgent**: The process that the UNIX agent uses to run security checks and perform baselining.
- **uvserv**: The process that the Secure Configuration Manager Core Services database and the Log Management database use to connect to the UNIX agent. Each connection spawns a uvservd process that either performs the operation or sends a request to the VigilEntAgent process to perform the operation. The connection stays open until the requesting database receives the data.

2 Installing and Licensing

This chapter provides information about installing, licensing, upgrading, and uninstalling the UNIX agent on computers you want to monitor. This chapter also provides an overview of starting and stopping the UNIX agent.

This chapter assumes you have an Secure Configuration Manager installed. For more information about installing Secure Configuration Manager or about Secure Configuration Manager system requirements, see the *Installation Guide for Secure Configuration Manager*, which is available on the Secure Configuration Manager Documentation page.

To install UNIX agent, complete the following checklist:

❑	Ensure you have the necessary environment. For more information, see Section 2.1, "System Requirements," on page 12.
❑	Install or upgrade UNIX Agent Manager. If you are upgrading, ensure you export your existing information before upgrading. If you are upgrading from UNIX agent version 7.1, you must use UNIX Agent Manager 7.2 or higher, but you can manage both 7.1, 7.2, and 7.3 UNIX agents from the same console. See Section 2.2, "Installing or Upgrading UNIX Agent Manager," on page 13.
❑	Install or upgrade the agent on the computer you want to manage. ◆ For information about how to install on a local computer, see Section 2.3.1, "Installing or Upgrading the Agent on the Local Computer," on page 14. ◆ For information about how to install using an answer file, see Section 2.3.4, "Silently Installing on the Agent Computer," on page 16. ◆ For information about how to install, or deploy, to one or more computers from the console, see Section 2.3.2, "Deploying the UNIX Agent Using UNIX Agent Manager," on page 15.
❑	Install any agent hotfixes applicable to your environment. For information about how to install patches to the console and the UNIX agent, see Section 2.4, "Applying Patches," on page 17. For a list of available hotfixes, see the Secure Configuration Manager Hotfixes for UNIX and Linux Operating Systems page.
❑	Register your agents in Secure Configuration Manager.
❑	Begin monitoring your UNIX and Linux computers.

2.1 System Requirements

For the latest information about specific supported software versions and the availability of module updates, visit the Secure Configuration Manager Supported Products page.

The UNIX agent, when used with Secure Configuration Manager, has the following system requirements.

Item	Requirement
NetIQ Secure Configuration Manager	5.9 or later
Operating system on agent computers	One of the following: ◆ CentOS ◆ HP-UX ◆ IBM AIX ◆ Oracle Linux ◆ Oracle Solaris ◆ Red Hat Enterprise Linux ◆ SUSE Linux Enterprise Server
Operating system on UNIX Agent Manager computers	One of the following: ◆ Red Hat Enterprise Linux ◆ SUSE Linux Enterprise Server ◆ Windows 7 (32-bit and 64-bit) ◆ Windows 8 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32-bit and 64-bit) ◆ Windows Server 2012
Memory on agent computers	512 MB
Memory on UNIX Agent Manager	UNIX agents require the following: ◆ 128 MB minimum RAM ◆ 512 MB swap file (virtual memory)
Hard disk space on agent computers	350 MB plus 400 Bytes per inode used by local file systems
Hard disk space on UNIX Agent Manager computers	1.2 GB
Accounts	The UNIX Deployment wizard uses the `su` command to access the root account on the computer on which you want to install UNIX agents. The root password is used by the wizard only at installation and is not stored. If you cannot use the root account, you can deploy using an account with sudo privileges.

Item	Requirement
Default port assignments	UNIX agent uses the following default ports: ◆ 2620: The UNIX agent listens for communication from UNIX Agent Manager. ◆ 1622: The UNIX agent listens for communication from Secure Configuration Manager. ◆ 1627: Secure Configuration Manager listens for communication from the UNIX agent when using standard communication algorithms. ◆ 1621: Secure Configuration Manager listens for communication from the UNIX agent when using FIPS-certified encryption algorithms. You can use the *Configure* option in UNIX Agent Manager to change the port assignments.

2.2 Installing or Upgrading UNIX Agent Manager

NetIQ UNIX Agent Manager is a console that you can use to manage all your UNIX agent components across your enterprise. UNIX Agent Manager runs on Windows and Linux. You can use UNIX Agent Manager to install to several computers at the same time. UNIX Agent Manager also allows you to see any UNIX computers that other NetIQ products monitor.

UNIX Agent Manager version 7.2 and higher includes a server component and a console. If you use UNIX agent version 7.3, you must use UNIX Agent Manager version 7.2 or higher. However, you can also use older versions of the agent with UNIX Agent Manager version 7.2 or higher. The following procedure guides you through installing or upgrading UNIX Agent Manager components.

2.2.1 Installing UNIX Agent Manager on a Microsoft Windows Computer

Complete the following steps to install the either the UNIX Agent Manager server, the UNIX Agent Manager console, or both on a Windows computer.

To install UNIX Agent Manager on a Windows computer:

1. Log on to the Windows computer using a local administrator account.
2. (Conditional) If you are upgrading from UNIX Agent Manager 7.1, save the information for your existing agents to a file using the **Export/Import Host Lists** menu option in UNIX Agent Manager. When the export completes, remove the program using the Remove Programs utility in the Windows operating system or the Uninstall UNIX Agent Manager utility from the NetIQ program group.
3. Run `UAMInstaller.MSI` in the root folder of the installation kit, and begin responding to the questions in the wizard.
4. When you are given the option of communication security settings, do not restrict communication to only Federal Information Processing Standard (FIPS) encrypted algorithms unless you are certain that your environment requires that restriction. If you select that option, UNIX Agent Manager cannot communicate with agents that do not have the same restriction. For more information about this option, see Section 3.3, “Understanding FIPS Communication,” on page 22.

5. Complete the automatic installer wizard. The wizard guides you through the Trial Software License Agreement and installs the UNIX Agent Manager to the folder that you specify.
6. Type and confirm a password that the UNIX Agent Manager server will use for the admin user account.
7. (Conditional) If you are upgrading from UNIX Agent Manager version 7.1, import your agent information using the **Import 7.1 Host List** under the **File** menu.

2.2.2 Installing UNIX Agent Manager on a Linux Computer

Complete the following steps to install the either the UNIX Agent Manager server, the UNIX Agent Manager console, or both on a Linux computer.

To install the UNIX Agent Manager on a Linux computer:

1. Change directories to where you copied the installation package for UNIX Agent Manager. In the installation package, change directories to where the installation files are located.
2. Extract the appropriate `.tar.gz` file for your platform.
3. In the new `UAM` folder, start the installation by running `./installserver.sh install`.
4. Type and confirm a password that the UNIX Agent Manager server will use for the admin user account.
5. Start the UNIX Agent Manager console by running the `run.sh` script.

2.3 Installing and Upgrading the Agent

You can install the agent locally on the computer you will monitor, by deploying from UNIX Agent Manager, or without user interaction by using an answer file.

If you are upgrading the agent, you can choose to create a custom configuration file that contains one or more configuration parameters instead of entering each parameter manually. For any configuration parameter in the file, the UNIX agent upgrade program uses that parameter instead of using the fields in the upgrade screen. You set the parameters in the file using the same format as the silent installation file. For more information about the silent installation file parameters, see Section 2.3.4, “Silently Installing on the Agent Computer,” on page 16

2.3.1 Installing or Upgrading the Agent on the Local Computer

The following procedure guides you through logging on to an agent computer and locally installing all required components on the agent computer. If you are upgrading and have used UNIX Agent Manager, make sure to export your host list.

To install or upgrade an agent on the local computer:

1. (Conditional) If you are upgrading and use UNIX Agent Manager, ensure you have upgraded UNIX Agent Manager to version 7.2 or higher. For information about upgrading UNIX Agent Manager, see Section 2.2, “Installing or Upgrading UNIX Agent Manager,” on page 13.
2. Log on to an agent computer using an account with super user privileges.
3. Change directories to the product installation package, and then enter the following command to start the install script:

   ```
   /bin/sh ./install.sh
   ```

4. Proceed through the prompts.

5. When you are given the option to configure the agent for use with other products, select the option only if you run NetIQ Sentinel, NetIQ Change Guardian, or NetIQ Security Manager to monitor the computer. If you will not use those products, type n instead of accepting the default response of y for those questions.
6. When you are given the option to specify the restart method, NetIQ recommends that you accept the default, rclink. For more information about restart methods, see Section 3.4, “Restart Methods for the UNIX Agent,” on page 22.
7. (Conditional) If you receive a warning message stating that you do not have a required operating system patch installed, install the patch. If you have a later patch that supersedes the required patch, download a new patch version checker from www.netiq.com/support.

When you finish the installation process, the UNIX agent starts the daemons.

2.3.2 Deploying the UNIX Agent Using UNIX Agent Manager

Remote deployment provides a convenient and uniform method for installing one or more UNIX agents. You can use the Deployment wizard provided in the UNIX Agent Manager for remote deployment, unless one of the following conditions exists:

- You installed UNIX Agent Manager using the options to restrict all communication to FIPS certified encryption algorithms.
- Your site standards prohibit your access to root passwords.
- Your site standards require a specific software distribution mechanism.
- Your site standards prohibit software distribution mechanisms.

For information about installing UNIX Agent Manager, see Section 2.2, “Installing or Upgrading UNIX Agent Manager,” on page 13.

To remotely deploy UNIX agent components:

1. In the **File** menu of UNIX Agent Manager, select **Remote Deployment**.
2. Click the **Add Host** button and fill in the fields as prompted.
3. When you are given the option of communication security settings, do not restrict communication to only Federal Information Processing Standard (FIPS) encrypted algorithms unless you are certain that your environment requires that restriction. If you select that option, UNIX Agent Manager cannot fully communicate with agents that do not have the same restriction. For more information, see Section 3.3, “Understanding FIPS Communication,” on page 22
4. When you are given the option to specify the restart method, NetIQ recommends that you accept the default, rclink. For more information about restart methods, see Section 3.4, “Restart Methods for the UNIX Agent,” on page 22.
5. Proceed through the wizard to complete installation.
6. (Conditional) If you receive a warning message stating that you do not have a required operating system patch installed, install the patch. If you have a later patch that supersedes the required patch, download a new patch version checker from www.netiq.com/support.

2.3.3 Upgrading UNIX Agent version 7.1 Using UNIX Agent Manager

UNIX Agent Manager provides a utility to upgrade existing agents. You cannot use this feature if your UNIX Agent Manager restricts communication to FIPS certified encryption algorithms.

To upgrade version 7.1 UNIX agents using UNIX Agent Manager version 7.2 or higher:

1. Ensure the computer that you want to upgrade is registered in UNIX Agent Manager. You can do this by either importing an existing list that contains the computer using **Manage Hosts** > **Import/Export Host Lists**, or by adding the computer using **Manage Hosts** > **Add Host**.
2. Highlight the computer you want to upgrade, and select **Manage 7.1 Hosts** > **Upgrade Hosts**. The left pane will display any options you need to select for your agent.
3. Scroll to the bottom of the panel and click the **Start Upgrade** button.

2.3.4 Silently Installing on the Agent Computer

Performing a silent installation allows you to install the UNIX agent without interactively running the installation script. Instead, silent installation uses an installation file that records the information required for completing the installation. Each line in the file is a *name=value* pair that provides the required information, for example, `HOME=/usr/netiq`.

If you use the deployment wizard to perform a local installation on one computer, the wizard offers you an opportunity to create a silent installation file based on your choices. A sample installation file, `SampleSilentInstallation.cfg`, is located on your UNIX agent download package. The following parameters are available for silent installation for the NetIQ UNIX Agent working with Secure Configuration Manager:

Parameter	Description
`CREATE_TARGET_DIR`	Specifies whether you want the install program to create the target installation directory if it does not already exist. Valid entries are `y` and `n`. The default is `y`.
`CONTINUE_WITHOUT_PATCHES`	Specifies whether the install program stops or continues when the operating system is not a supported version. Valid entries are `y` and `n`. The default is `n`.
`IQCONNECT_PORT`	Specifies the port that the UNIX agent uses to listen for communications from UNIX Agent Manager. The default is `2620`.
`IQ_STARTUP`	Specifies restart method for the uagent process. For information about the options, see Section 3.4, "Restart Methods for the UNIX Agent," on page 22. Valid entries are `rclink` and `inittab`. The default is `rclink`.
`USE_FIPS_COMMON`	Specifies whether the UNIX agent communicates with UNIX Agent Manager using only FIPS certified encryption algorithms. Only use this option if your environment requires this restriction. For more information about this option, see Section 3.3, "Understanding FIPS Communication," on page 22. Valid entries are `0`, meaning that communication is not restricted, and `1`, meaning that communication is restricted. The default is `0`.

Parameter	Description
`INSTALL_SCM`	Specifies whether the UNIX agent works with Secure Configuration Manager. Valid entries are `y` and `n`.
`SCM_CORE_ADDR`	Specifies the IP address of the computer where you installed Secure Configuration Manager Core Services.
`SCM_CORE_PORT`	Specifies the port that the UNIX agent will use to communicate with Secure Configuration Manager Core Services.
`SCM_UVSERV_PORT`	Specifies the port that the UNIX agent will use to communicate with Secure Configuration Manager.
`SCM_UVSERV_STARTUP`	Specifies the restart method for the uvserv process. For information about the options, see Section 3.4, "Restart Methods for the UNIX Agent," on page 22. Valid entries are `rclink`, `inetd`, and `inittab`. The default is `rclink`.
`USE_FIPS_SCM`	Specifies whether the UNIX agent communicates with Secure Configuration Manager using only FIPS certified encryption algorithms. Only use this option if your environment requires this restriction. For more information, see Section 3.3, "Understanding FIPS Communication," on page 22. Valid entries are `0`, meaning that communication is not restricted, and `1`, meaning that communication is restricted. The default is `0`.

Once you have created the installation file, you can run the silent installation from the command line. For example:

```
./install.sh <Target_Directory> -s <SilentConfigurationFile>.cfg
```

Where <Target_Directory> is the directory you want to install to and <SilentConfigurationFile> is the file name you used to specify the installation options. You can also use the default configuration file, `SampleSilentInstallation.cfg`.

The script will then extract information from the installation file and install the agent according to the values you have specified.

NOTE: The installation filename must be specified as an absolute path. By default, SampleSilentInstallation.cfg is located in the UNIX agent install directory.

2.4 Applying Patches

NetIQ provides patches in a zipped file known as a **p-ball** for agent components.

Patches to UNIX Agent Manager are applied to the UNIX Agent Manager server, which automatically applies any required changes to the consoles using that server. To update UNIX Agent Manager on Windows, click **Update UAM** on the Start menu. To update UNIX Agent Manager on Linux, run the `update.sh` command.

To upgrade the agent computer using the UNIX Agent Manager:

1 Click **Patch > Patch Manager**.

2 Click **Load Patch** to add the patch you want to apply to the list of available patches.

3. Select the computers where you want to apply the patch.
4. Select the patch or patches that you want to apply.
5. Click **Start Install**. The time necessary to update your agents depends on the number of agents to update, distance from the UNIX Agent Manager server, network connectivity, and bandwidth, among other factors. This process can take up to 20 minutes per agent.
6. Click **Back** to close the Patch Manager.

2.5 Uninstalling UNIX Agents and UNIX Agent Manager

You can uninstall the UNIX agent components manually or using UNIX Agent Manager.

2.5.1 Uninstalling the UNIX Agent

You can use UNIX Agent Manager to uninstall agents from remote computers, or you can uninstall them locally. When you uninstall the agent, you can choose to uninstall all components, or only one the are for specific products.

NOTE: You do not need to uninstall agents with a lower version number before upgrading agents. Use this procedure only if you want to completely remove agents from remote computers. For more information about upgrading agents, see Section 3.5, “Saving UNIX Agent Information to a File,” on page 22.

To uninstall the agent locally, change to the installation directory, then run the following command:

```
./uninstall.sh
```

You can also uninstall using the console. This option allows you to uninstall from many computers at once. To uninstall an agent in UNIX Agent Manager, select the computers where you want to uninstall the agent, click **Manage Hosts > Uninstall Agent**.

2.5.2 Uninstalling UNIX Agent Manager

To uninstall the UNIX Agent Manager on Windows computers, use the **Add/Remove Programs** Control Panel to remove the **UNIX Agent Manager** program.

To uninstall the UNIX Agent Manager on a Linux computer, change directories to the UNIX Agent Manager installation directory and run `installserver.sh`. When you have completed the uninstall program, you can remove the UAM directory by running `rm -rf UAM`.

2.6 Licensing

The UNIX agent requires the use of a license key file. The Secure Configuration Manager console requires a valid license. Ensure your licenses provide the appropriate coverage for your needs.

Your trial license allows you to experience the convenience and security of deployed NetIQ Security agents for up to one month. When you decide to move your trial into production, contact your NetIQ sales representative for a production license.

3 Working with the UNIX Agent and UNIX Agent Manager

This chapter describes features of the UNIX agent and UNIX Agent Manager beyond installation. This chapter also presents internal product concepts, such as communication between the components and restart options.

UNIX Agent Manager provides some features that this guide does not describe. The console provides these features for backward compatibility purposes or for products other than Secure Configuration Manager.

3.1 Configuring Secure Configuration Manager Support for Oracle

Secure Configuration Manager handles agents monitoring UNIX computers as it does any other kind of agent, with no special configuration necessary. However, if you are monitoring Oracle, you must ensure that the endpoints are properly configured. To configure Secure Configuration Manager to monitor Oracle, you must first install an UNIX agent on the computer running Oracle, then you can add one or more Oracle endpoints to the new UNIX agent.

To add Oracle endpoints to a UNIX agent:

1. Ensure you have a UNIX agent installed on the computer running Oracle.
2. In the tree pane, expand **NetIQ Secure Configuration Manager > IT Assets > Agents > OS > Unix**.
3. In the content pane, select the UNIX agent to which you want to add the endpoint.
4. On the Actions menu, click **Add Endpoint**.
5. Select the UNIX agent you want the endpoint to monitor and click **Next**.
6. In the **Name** field, type a name for the endpoint.
7. In the **Endpoint Type** field, select **Oracle**.
8. Complete the required information in the following fields.

   Oracle Instance ID

   Name of the Oracle instance

   User Name

   User account used to access the Oracle database. If your Oracle environment requires `name@sid` format, use that format here. This account must have access to read tables and views. The specific requirements for access depend on which checks you run. You must assign adequate permission for the checks you use to access the information you need.

   Password:

   Password for the user account used to access the Oracle database.

9 (Conditional) If you want to add more information about the endpoint, complete the following optional fields.

Contact Email

Email address of the contact person.

Contact Name

Name of the designated contact person.

Importance

Criticality level of the endpoint.

Location

Location of the computer hardware.

Major Version

Version of Oracle the endpoint is running.

10 (Conditional) If you want to add the endpoint to a group, complete the following steps:

10a Click **Add Endpoint to a Group**.

10b Select an existing group to which you want to add the endpoint, or click **Create** to create a new group.

10c Click **Finish** to return to the Define Endpoint window.

11 (Conditional) If you are adding more than one endpoint, click **Add Endpoint**. Repeat Step 5 through Step 9 for each endpoint that you want to add.

12 Click *Finish*.

3.2 Managing Users in UNIX Agent Manager

UNIX Agent Manager allows administrators to control user access to features and computers. To log into any UNIX Agent Manager server, an administrator on that server must create the user account in the UNIX Agent Manager Administrator Console, which is part of the UNIX Agent Manager console.

You can grant different permissions to each user account that allows access to only the features required by that user’s role. Permission sets allow you to simplify this process. Permission sets define product, computer, and feature access. Once you create a permission set, you can assign it to multiple user accounts with the same role.

For example, you can create a permission set that grants access to all AppManager functionality separate from Secure Configuration Manager functionality. You can then assign this permission set to all computers running AppManager. When you grant a new AppManager user access to a console, simply assign the user to the AppManager permission set to grant them access to the applicable features and computers.

To assign permissions, log into a UNIX Agent Manager console as an administrator and click **Access Control** > **Admin Console**. From there, add the users that need access to that UNIX Agent Manager server, then assign the appropriate permissions.

3.2.1 Using LDAP or Microsoft Active Directory Credentials

UNIX Agent Manager can access the information you have already set up in your LDAP or Microsoft Active Directory server to allow users to log into the UNIX Agent Manager server. This functionality is not available if you restricted UNIX Agent Manager to only use Federal Information Processing Standard (FIPS) encrypted algorithms.

To configure UNIX Agent Manager server to use LDAP or Active Directory credentials:

1. Ensure you have the following information:
   - The domain and computer address, such as ldap://houston.itservice.production:389, of the LDAP or Active Directory server
   - The location of the user entries in the structure of the LDAP or Active Directory server
   - The attribute that identifies the login name for each user
   - An account that UNIX Agent Manager server can use to access the LDAP or Active Directory server
2. Log into a UNIX Agent Manager console as an administrator, and open the **Manage Server** window.
3. Click the **LDAP** tab, then the **Add** button.
4. Enter the name of the domain that contains the LDAP or AD server. Users must also enter this domain name when they log into UNIX Agent Manager.
5. Select the domain and provide the information as requested on the window using the following guidelines:
   - In **Server Address**, enter LDAP or Active Directory server computer name and port. For example, `ldap://houston.itservice.production:389`
   - In **User's Parent DN**, enter the path to the node that contains the usernames you want to use. For example, `ou=AMAdmins,dc=netiq,dn=com`
   - In **Username Attribute**, enter the attribute you want UNIX Agent Manager to use to identify the user. This attribute will be used as a consistent identifier even if the user name changes. The default and only attribute supported by UNIX Agent Manager 7.2 is `uid`
   - (Conditional) If you use simple authentication for specific users, in **Username**, enter the path to the user name. For example, `ou=Operator,dc=netiq,dn=com`
6. Click **Save**.

3.2.2 SSL Communication with the LDAP or Active Directory Server

The UNIX Agent Manager server can communicate with the LDAP or Active Directory server using Secure Sockets Layer (SSL). If you choose to have UNIX Agent Manager server communicate with the server using SSL, you must obtain and manage the required certificates. UNIX Agent Manager requires certificates that are base-64 encoded and use the `.cer` extension.

For example, to get a certificate from an OpenLDAP server, run the following command from the `/etc/openldap/certs` directory on the computer that is running the slapd daemon:

```
certutil –L –a –n “OpenLDAP Server” –d `pwd` > servername.pem
```

The command creates a `servername.pem` file that you can import into UNIX Agent Manager using the Manage Server window where you identify your LDAP server.

Ensure you close and restart the UNIX Agent Manager after you import the certificate.

3.3 Understanding FIPS Communication

Use this feature only if you are sure that your environment requires this restriction.

Secure Configuration Manager supports Federal Information Processing Standard (FIPS) 140-2 communication among the product components. You can configure the UNIX agent and UNIX Agent Manager to restrict all communication to FIPS certified encryption algorithms. Be aware that when you configure UNIX Agent Manager to use only these communication algorithms, UNIX Agent Manager cannot communicate with any UNIX agent that does not also use these algorithms. Also, if you configure UNIX Agent Manager to use these algorithms, you cannot deploy a UNIX agent to a remote computer.

NOTE: The Secure Configuration Manager Core Services can communicate with a FIPS-enabled agent. However, if you have not specified FIPS communication for the Core Services Configuration Utility, the communication will not use FIPS-certified algorithms and your environment will not be FIPS compliant. For more information, see the *User Guide for Secure Configuration Manager*.

3.4 Restart Methods for the UNIX Agent

NetIQ recommends that you accept the default, rclink. However, the following start methods are available.

Option	Description
`rclink`	Starts the agent daemons immediately after the deployment process and adds a startup script to the `/etc/rc.d` directory. This startup script starts the agent daemons after each reboot when the master rc script runs. This is the default method, and should be used in nearly all environments.
`inittab`	Starts the agent daemons immediately after the deployment process and adds an entry to the `/etc/inittab` file. This inittab file entry starts the agent daemons at the default run level after each reboot.
`inetd`	Configures the (x)inetd daemon to start the agent daemons when needed and then stop and unload the agent daemons.

3.5 Saving UNIX Agent Information to a File

The UNIX Agent Manager server stores the information about the UNIX agents you monitor. However, storing the information to a separate file can be useful for backups or for copying the server to another computer. You can store your UNIX agent list and configuration information in a file outside the UNIX Agent Manager server by clicking **Manage Hosts > Export/Import Host Lists** in UNIX Agent Manager version 7.2.

If you are upgrading from UNIX Agent Manager 7.1 to 7.2, save your configuration information before you upgrade so you can import it after you upgrade. You can export your UNIX agent information from UNIX Agent Manager version 7.1, then import the information into UNIX Agent Manager 7.2.

To export the host information from UNIX Agent Manager 7.1:

1 In the left pane of UNIX Agent Manager 7.1, click **Agent Manager**.

2 Click **Hosts > Edit Hosts**.

3 Select all of the hosts in the Current Hosts list.

4 Click **Export Selected.**