Privileged Account Manager

Administration Guide

December 2019

Legal Notice

© Copyright 2019. Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see http://www.microfocus.com/about/legal/.

Contents

About This Book and the Library **11**

1 Overview **13**

How Privileged Account Manager Solves the Business Challenges 13
Protecting Privileged Account Credentials 14
Main Features of Privileged Account Manager 15

2 Welcome to the Framework **17**

Introduction to the Framework 17
Primary Components 17
Framework Manager 18
Framework Manager Console 18
Framework Agent 19
The Workspace Layout 19
Navigation Bar 19
Navigation Pane 19
Viewing the Version and the License Details 20
License Summary 20

3 Getting Started **23**

Managing Privileges in Various Endpoints 23
Windows 24
UNIX/Linux 24
Database and Applications 24
Shared Keys 24

4 Managing Framework Hosts **25**

Managing Domains 25
Creating a Domain 26
Modifying a Domain 26
Deleting a Domain 27
Managing and Monitoring Hosts 27
Adding a Host 27
Viewing Host Details 28
Modifying a Host 29
Registering Hosts 30
Deleting a Host 30
Moving a Host 31
Finding a Host 31
Monitoring Hosts 31
Managing System Alerts 34
Modifying Alert Settings 35
Enabling Crash Dump Capture 36

Managing Host Packages . . . 36
Finding Packages on Hosts . . . 37
Updating Packages for a Host . . . 37
Rolling Back Packages . . . 38
Committing Packages . . . 38
Registering and Unregistering Packages for a Host . . . 39
Installing Packages on a Host . . . 39
Uninstalling Packages from a Host . . . 40
Modifying Audit Settings for the Audit Manager Package . . . 40
Configuring SMTP Settings for the Messaging Component Package . . . 41
Configuring Settings for the dbaudit Package . . . 41
Managing Audit Zones . . . 41
Understanding Tunneling . . . 42
Installing Tunnel Agent and Tunnel Manager Packages . . . 43
Enabling and Disabling Tunneling . . . 44
Reregistering the Tunnel Agent Package . . . 44
Listing Tunnels . . . 45
Securing Access to the Framework Manager Console . . . 45
Requesting a Certificate for the Framework Manager Console . . . 45
Modifying the Connector . . . 46
SSL Renegotiation DOS Attack Protection . . . 46
Using Privileged Account Manager Service . . . 47
Integrating with NetIQ Access Manager . . . 47
Troubleshooting . . . 47
Promoting Managers When the Primary Manager Fails . . . 48
Viewing Store and Forward Messages . . . 48
Managing Low Disk Space . . . 49
Restarting the Agent . . . 50
Managing the Registry Cache . . . 50
Time Synchronization . . . 52

5 Policy Templates 53

Understanding Sample Policy template . . . 53
Importing Sample Policy Templates . . . 54
Adding a Policy Template . . . 54

6 Managing Framework Users and Groups 57

Managing Users . . . 57
Configuring Account Settings . . . 58
Adding a Framework User . . . 59
Modifying a Framework User . . . 60
Removing a Framework User Group from a User . . . 69
Deleting a Framework User . . . 70
Managing Groups . . . 70
Adding a Framework User Group . . . 70
Modifying a Framework User Group . . . 70
Configuring a Help Desk Group . . . 71
Configuring Roles . . . 72
Deleting a Framework User Group . . . 77
Deploying the Access Control Module . . . 78
Changing a Framework User's Password . . . 79

Assigning Framework Roles for LDAP Users . . . 79
Multi-Factor Authentication. . . . 79
Advanced Authentication . . . 80
RADIUS Server . . . 80

7 Managing Audit Reports 83

Audit Settings . . . 83
Encryption Settings . . . 84
Syslog Settings . . . 84
Command Control Reports. . . . 86
Adding a Report . . . 86
Viewing Report Data . . . 87
Filtering the Viewable Records . . . 87
Modifying General Report Information . . . 89
Selecting Log Files . . . 89
Replaying Keystrokes . . . 90
Removing a Report . . . 90
Generating an Activity Report . . . 91
Viewing a Report in a Comma-separated Values (CSV) Format . . . 91
Video Capture . . . 91
Configuring Video Capture . . . 92
Viewing the Videos . . . 95
Video Off-Load . . . 96
Change Management . . . 99
Viewing Report Data . . . 99
Password Management . . . 100
Enabling Password Management . . . 100
Viewing Report Data . . . 100
Shared Key Management . . . 101
Enabling Shared Key Management. . . . 101
Viewing Report Data . . . 101

8 Command Control 103

How Does Command Control Work?. . . . 103
Installing and Deploying Command Control . . . 104
Command Control Modules . . . 104
Auditing Modules . . . 104
Compliance Auditor Modules . . . 104
Installing Command Control . . . 104
Command Control User Interface . . . 105
Configuring Command Control . . . 106
Rules . . . 107
Command Control Groups . . . 115
Commands . . . 121
Finding a Reference . . . 128
Defining Custom Attributes. . . . 128
Functions . . . 129
Adding a Category . . . 130
Deleting a Category . . . 131
Blocked Users . . . 131
Scripts . . . 131

Access Times 136
Command Control Reports 138
Command Control Options. 140
Importing and Exporting Command Control Configuration Data 140
Command Control Transactions 142
Defining Audit Settings 144
Backing Up and Restoring 145
Test Suites. 146
Creating Default Objects 150
Disconnecting a Privileged Session 151
Prerequisites for Disconnecting a Session 151
Disconnecting the Session Manually 151
Disconnecting the Session Automatically 152
Viewing the Disconnect fields in the Reporting Console 152

9 Compliance Auditor 155

Controlling Access to the Compliance Auditor 156
Compliance Audit Rules 156
Adding or Modifying an Audit Rule 157
Compliance Audit Reports 158
Adding, Copying and Modifying an Audit Report 158
Sample Command Control Report Template 160
Deleting a Report 164
Compliance Auditor Records 164
Viewing a Compliance Audit Record 165
Viewing and Editing a Command Control Keystroke Report 165
Viewing a Change Management Audit Record 166
Viewing a Report Audit Record 167
Editing an Audit Record 167
Archiving Records 168
Managing Archived Records 168
Access Control Levels 169
Adding or Modifying a User ACL 169
Deleting a User ACL 169
Deploying the Compliance Auditor 170

10 High Availability 171

Configuring High Availability 172

11 Load Balancing 175

12 Command Line Options 177

The unifi Options. 177
Command Control Options. 178
Importing and Exporting Command Control Settings. 178
Backing Up and Restoring a Command Control Configuration 179
Running Test Suites 181
Package Distribution Options. 181
Package Manager Options 182
Install and Uninstall Packages. 182

Upgrade and Rollback Packages . . . 183
Registry Agent Options . . . 184
Registering an Agent . . . 184
Finding a Primary Manager Package . . . 184
Agent Status . . . 185
Adding Hosts and Domains . . . 185
Registry Manager Options . . . 186
Compliance Auditor Options . . . 186
Exporting and Importing Compliance Auditor Settings . . . 186
Managing Compliance Auditor Records . . . 187
sreplay Command Line Options . . . 189

13 Managing Shared Keys 193

Types of Shared Key . . . 193
Enabling the Key Checkout for Shared Key . . . 194
Managing Credentials for Shared Key . . . 195

14 Privileged Access to Windows 197

Workflow to Configure Privileged Access for Windows . . . 198
Session Management . . . 199
Remote Desktop Protocol Relay . . . 199
Credential Provider . . . 201
Direct Remote Desktop Protocol . . . 202
Application Management . . . 203
Application SSO . . . 203
Run as Privileged User . . . 203
LDAP Group Lookup . . . 204
Creating the LDAP Account in the Credential Vault . . . 205
Defining the User Group . . . 205
Creating a Rule for the LDAP Group . . . 205
Modifying a Rule for the LDAP Group . . . 205

15 Privileged Access to UNIX and Linux 207

Workflow to Configure UNIX and Linux Privileged Sessions . . . 208
Session Management . . . 209
pcksh . . . 209
cpcksh . . . 213
Secure Shell Relay . . . 215
Command Management . . . 220
`usrun` . . . 220
Enhanced Access Control . . . 223
Configuring a Command Control Policy . . . 223
Configuring a Path Policy . . . 223

16 Privileged Access to Databases 227

Database Access Through Credential Checkout . . . 228
Configuring Credential Checkout for Oracle Database . . . 228
Configuring Credential Checkout for Other Databases . . . 229
Checking Out Database Credentials . . . 231

Database Access Through PAM Proxy 231
Prerequisite 232
Adding Database Connectors 233
Adding Rules for Database 237
Managing Database Connectors 237
Viewing Database Activity 239

17 Privileged Access to Applications and Cloud Services 241

Credential Checkout 242
Configuring Credential Checkout for Applications 242
Configuring Credential Checkout for Cloud Services 245
Configuring Credential Checkout Settings 247
Checking Out Credentials 247
Password Reset Scripts 248

18 Privileged Single Sign-On 267

Application SSO 267
RemoteApp Mode 268
Direct Access Mode 271

19 Application to Application Password Management 277

Configuring AAPM 278
Enabling Users to Generate API Tokens 278
Viewing Activities Performed Using API Tokens 279

20 Password Management 281

Understanding Password Management 281
Password Management for Windows, Active Directory, Linux, and Network Devices 283
Prerequisites 284
Configuring Password Management 285
Configuring Password Management in an Upgraded Setup 285
Disabling Password Management 286
Password Management for Database and Applications 286

21 Integration with Ticketing Systems 287

Configuration for Normal Access 287
Configuration for Elevated Access 288

22 Managing Emergency Access Requests 291

Configuring Emergency Access Settings 291

23 Deployment Dashboard 293

Deployment View 293
Live Risk View 294
Customize Deployment Dashboard 294

24 Integrating Privileged Account Manager with Advanced Authentication 295

Benefits of Integration with Advanced Authentication 295
Advanced Authentication Terminologies and Their Usage 296
Checklist to Follow Before Enabling Secondary Authentication 297
Configuring Advanced Authentication Server. 298
Supported Authentication Methods 299
Configuring the Advanced Authentication Server Details in Privileged Account Manager. 299
Enabling Advanced Authentication for Privileged Access 300
Bypassing Secondary Authentication 300
Enabling Advanced Authentication for Administration Console 301
Enabling Advanced Authentication for Privileged Access to End-Points. 301
Troubleshooting 302
Advanced Authentication Server is Down and Users Cannot Log In to Privileged Account Manager End-Points 302

25 Integrating Privileged Account Manager with Identity Manager 303

Benefits of Integration with Identity Manager 303

26 Virtualization Implementation 305

27 Discovering Privileged Accounts 307

Types of Accounts Discovered 307
Administrative Accounts 307
Service Accounts 308
Launching Privileged Account Sniffer 308
Configuring Privileged Account Sniffer 309
Discovering Accounts 309
Discovery Reports 310
Filtering Report Data 310
Importing and Exporting Configuration 310

28 Upgrading Privileged Account Manager 311

Privileged Account Manager Upgrade Checklist. 311
Configuring the Package Manager. 312
Publishing Packages on the Package Manager 313
Publishing Packages from the Downloads Website 313
Publishing Packages from Novell Update Server or another PAM Server. 314
Upgrading Privileged Account Manager 315
Upgrading Through Command Line 315
Upgrading Through Console 315
Upgrading Using the Privileged Account Manager Installer. 317
Troubleshooting 317
AIX Agent Upgrade Through UI Fails With An Error Message 317

29 Troubleshooting 319

The Agent is in an Offline State 319
The Audit Events are Not Displayed in the Reporting Console Even When the Events are Generated . . 319

On an AIX Platform, When the Audit Data Gets Generated in Large Amount, The Privileged Account Manager Service Restarts and an Error is Displayed in the unifid.log file. 319
The RDP Relay Session Does Not Start From the User Console 320
The RDP Relay to a Windows Server 2012 Server Fails 320
The Privileged Session is Not Established Through the Backup Manager 321
The Changes to the Syslog Settings Do Not Get Applied 321
The Manual Disconnect for a Windows session Does Not Work 321
The Run as privileged user Option is not displayed on a Windows 2012 Server 321
Agent Registration Fails on a Windows Platform 321
Direct RDP Sessions are Enabled for all Users By Default 321
Issues When Updating or Downloading the License Summary. 322
Failed to connect to module 322
The system cannot process the details because one or more agents that have the DB Audit module is in Offline state 322
The system cannot process the details because it cannot contact any of the Credential Vault modules 322
SSL Connection to Microsoft SQL Sever Fails with a Timeout Error 323
RDP Relay to Windows 10 or Windows 2016 Fails with a Network Authentication Error 323
SSO to Application Does Not Happen When There are Multiple Concurrent Sessions to the Application SSO Host 323

About This Book and the Library

This guide explains how to use the Framework Manager to control and audit superuser access to Linux, UNIX, Windows, database and application servers.

Intended Audience

This guide is intended for users who manage the Privileged Account Manager product.

Other Information in the Library

Privileged Account Manager Installation Guide

1 Overview

NetIQ Privileged Account Manager (PAM) helps IT administrators to control and monitor the administrative access to servers, network devices and databases. The administrators are allowed controlled delegated access to the systems without exposing the administrative credentials to these systems. It also provides a centralized activity log across multiple platforms. The introduction of NetIQ Privileged Account Manager enriches the NetIQ Identity and Access Management by providing comprehensive Privileged Identity Management as well as auditing and tracking of privileged user activities in the organization. PAM provides Shared Account Password Management (SAPM) and Super User Privilege Management (SUPM) to secure the privileged accounts in the organization.

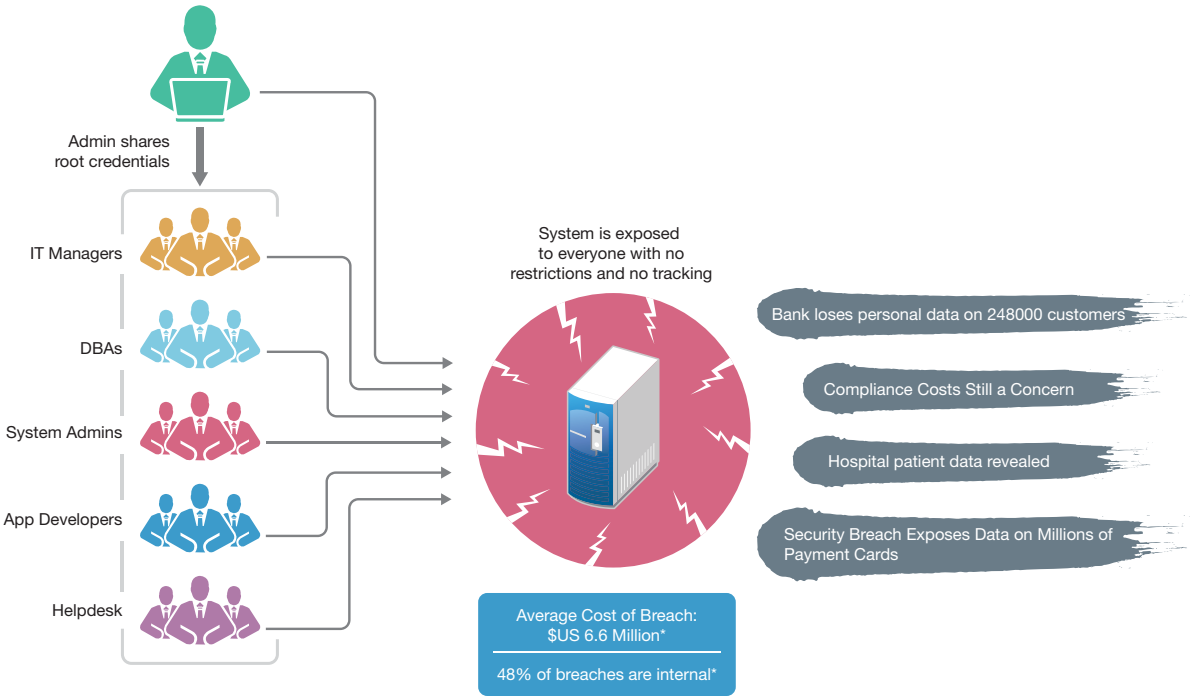
How Privileged Account Manager Solves the Business Challenges

Certain situations open potential back doors into systems and increase the likelihood of a security breach in an enterprise network. For example, when running some commands that require elevated privileges, users sometimes get exposed to the super user or root account credentials. Similarly, passwords are often not changed when a user is no more performing the administrative role.

Privileged Account Manager provides the capability to monitor, audit, and secure the actions of the users by using a centralized and automated management of privileged account. Privileged Account manager helps in overcoming the following challenges:

- The superuser credentials are exposed.
- The confidential data is exposed.
- There is unrestricted access rights provided to the user.
- The identity of the user who accessed a particular system remains unidentified.

Figure 1-1 Challenges of Using a Privileged Account in an Enterprise



The following sections provide details on how PAM provides solution to these challenges:

Protecting Privileged Account Credentials

Privileged Account Manager provides the capability to elevate specific user group as root, or super user without exposing the actual credential of the privileged account. This secures the credentials of the privileged account.

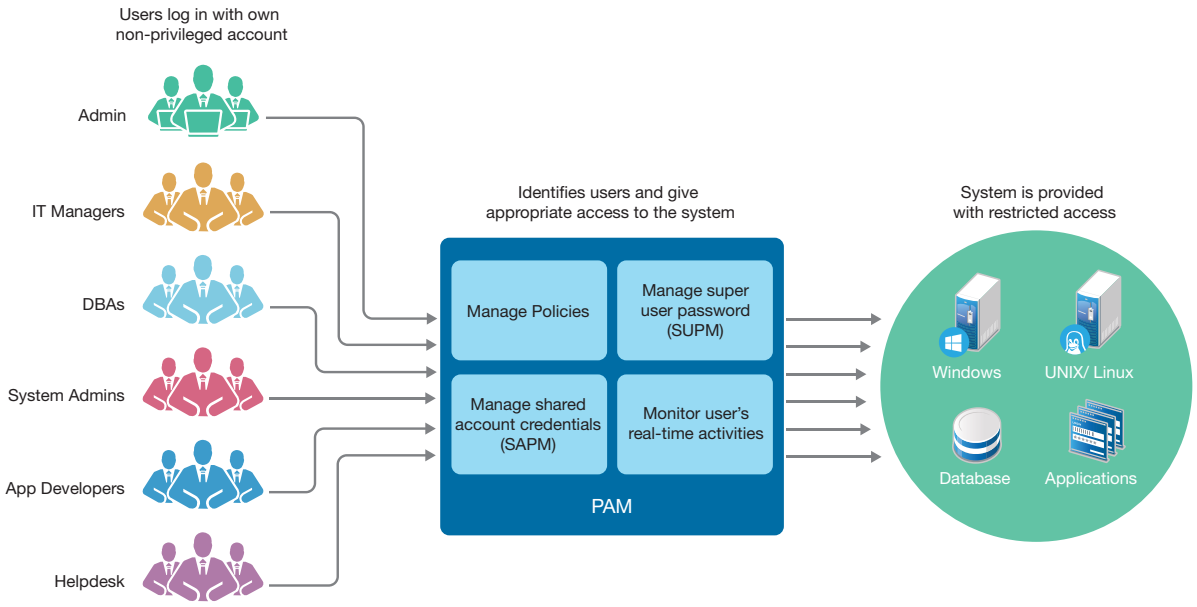
Privileged Account Manager saves the administrator's credentials for any Windows, Linux, application, database, or hypervisors in a privileged credential vault. So, when users wants to perform some activity on a particular server, they log in with their user credentials, PAM verifies the policy defined for accessing that particular session, then based on the policy enters the credentials of the super user or root allowing the user to log in with administrator or root credentials.

This capability is helpful when the privileged account credentials are shared with more than one user. For example, outsourcing an IT operation, where the contractors, or external vendors are given extended and uninterrupted access to sensitive information and corporate assets. This may lead to data loss, or exposing sensitive data to security threat. Privileged Account Manager facilitates the following to protect the account credentials:

- It limits corporate susceptibility to unauthorized transactions and information access by helping organizations rapidly deploy Superuser Privilege Management (SUPM) and tracking across all Windows, UNIX (AIX, Solaris, HPUX), and Linux environments. For more information, see "Managing Privileges in Various Endpoints" on page 23.
- It can manage passwords and control access to the shared accounts, that is, Shared Account Password Management (SAPM). For more information, see Chapter 17, "Privileged Access to Applications and Cloud Services," on page 241.

- It provides facility to monitor in real time and record the session, that is, Privileged Session Management (PSM). For more information, see Chapter 7, “Managing Audit Reports,” on page 83.
- It can securely generate and return random password for any application by using REST API calls, eliminating the use of hard coded password. Hence, facilitating Application-to-Application Password Management (AAPM). For more information about the REST API calls for password management, see the REST API documentation in the user console.
- It provides facility to integrate with Security Information and Event Management (SIEM) system to analyze detailed usage data. For more information, see Chapter 17, “Privileged Access to Applications and Cloud Services,” on page 241.
- It reduces management overhead and infrastructure costs, controls and records which privileged users have access to what, and reduces costs and errors through demonstrable compliance audits.
- It works by delegating privileged access, which is authorized via a centralized database. The end result is that a user is authorized to run the privileged command and all activity is logged.
- It can be deployed quickly, provides faster response time, better logging and auditing and improved administration. The centralized database provides easier administration.
- It provides a more secure system and a fast return on investment.

Figure 1-2 *Privileged Account Manager Provides Solution to the Challenges*



Main Features of Privileged Account Manager

Privileged Account Manager has several features that makes Privileged Account Management simple and robust. Following are the main features of PAM:

- Managing the Privileged accounts
- Controlling administrator access to the Linux, UNIX, Windows, database and application servers
- Managing policies based on roles

- Monitoring the Real-time activities of a user using a privileged account
- Terminating a suspicious remote session and if required, blocking users from further initiating the session
- Video recording, or Keystroke replay
- Active Directory Bridging - User authentication and access control based on user identity and group membership in the Microsoft Active Directory
- Secure Credential Vault which holds the credentials of all the critical servers and applications
- Multi-Factor Authentication and access control using:
  - Advanced Authentication
  - Third-party RADIUS supported Multi-Factor Authentication products
- Easy policy definition using policy templates
- Management of SSH key and other types of keys
- Syslog collector which can send critical data from various events to the SIEM system
- Multi-tenancy support with the integration of NetIQ Cloud Manager
- AAPM support using REST APIs
- Geographical control of the audit data using Audit zones
- Color coding for the risks based on the specified risk level
- Audit Zone for restricting and reducing network traffic
- Restricted access to user’s details based on the type of Administrator
- Compliance auditing and reporting
- Integration with Identity Manager
- Integration with Access Manager
- Integration with Advanced Authentication

2 Welcome to the Framework

NetIQ Privileged Account Manager keeps your organization secure and compliant by controlling and monitoring administrative access to your critical servers, network devices and databases.

NetIQ Privileged Account Manager manages the delegated administration through a centralized policy mechanism. This allows you to define rules for allowing or denying user activity based on a combination of user name, typed command, host name, and time (who, what, where and when). By managing privileges this way, you can control the commands users are authorized to run, along with the time and the location. User activity is recorded in an audit reporting and management tool, which enables you can take action right when suspicious activity occurs.

Privileged account management (PAM) manages the account credentials for database

Privileged Account Manager includes separate web consoles for administrator and users. Administrator console is the framework console and user console is called the My access page.

- "Introduction to the Framework" on page 17
- "Primary Components" on page 17
- "The Workspace Layout" on page 19
- "Viewing the Version and the License Details" on page 20

Introduction to the Framework

NetIQ Privileged Account Manager uses a Framework as the base layer to provide an easy-to-use enterprise architecture into which Privileged Account Manager modules are added to create the necessary problem-solving functionality. The Framework has several key features:

- Provides the core functionality needed to implement secure, enterprise-wide services.
- Provides services such as secure and authenticated communication among components.
- Provides integrated databases and logging.
- Allows the deployment of Privileged Account Manager modules to Framework hosts to implement new functionality.
- With each module that is installed, an additional console is added to the main Framework Manager console to allow access to new administration functionality.

Primary Components

The Framework is made up of three primary components:

- "Framework Manager" on page 18
- "Framework Manager Console" on page 18
- "Framework Agent" on page 19

Framework Manager

The Framework Manager is the server component of the Framework. It provides a centralized registry, enabling services and administration of the entire Framework from any single point on the enterprise network. The Framework Manager is administered through the Framework Manager console.

The manager modules are installed on the Framework Manager by default. The modules can also be distributed to other Framework hosts to provide load balancing and failover for the Framework. If there are multiple occurrences of the same type of manager installed on the Framework, they operate in primary and backup roles. Updates to the data controlled by each group of like managers are only updated at the primary manager.

The default manager modules are:

- **Administration Manager (admin):** Provides the functionality for the Web-based user interface. Framework consoles can be installed on the Administration Manager and are used to control product features.
- **Access Manager (auth):** Maintains a list of Framework user accounts and provides authentication services for the Framework. It needs to be installed with a local Registry Manager in order to create a secure user authentication token.
- **Audit Manager (audit):** Maintains the repository for all auditing information collected by the Framework.

  NOTE: NetIQ recommends to deploy only two Audit Managers, even in large environments.

- **Command Control Manager (cmdctrl):** Maintains the rule configurations and is responsible for validating user command requests.
- **Compliance Auditor (secaudit):** Collects, filters, and generates reports of audit data for analysis and signoff by authorized personnel
- **Messaging Component (msgagnt):** Provides the transport mechanism and interacts with e-mail servers to provide reporting functionality.
- **Package Manager (pkgman):** Manages a repository for Framework packages.
- **Registry Manager (registry):** Maintains a database of all Framework hosts and modules. Provides certificate-based registration features for the hosts.
- **Syslog Emitter (syslogemit):** Provides logging of audit information to a syslog server.

Framework Manager Console

The Framework Manager console is the default user interface for the Framework. It allows configuration and management of the Framework through a graphical user interface.

For a description of this console, see "The Workspace Layout" on page 19.

Framework Agent

The Framework Agent is the client component of the Framework. It is responsible for receiving and carrying out instructions from the Framework Manager on all hosts. The following Framework Agent packages are installed on all Framework hosts:

- **Registry Agent (regclnt):** Provides a local cached lookup for module locations. The Registry Agent queries the Registry Manager when local cached information is not available or isn't fresh.
- **Distribution Agent (distrib):** Provides the interface to control the installation and removal of packages in the Framework. It has methods to install, remove, and list the available and updatable packages. The Distribution Agent retrieves packages from the local Package Managers.
- **Store and Forward Agent (strfwd):** Provides a store and forward mechanism for guaranteed delivery of messages. It is used for various core features such as replication of the manager databases.
- **Command Control Agent (rexec):** Enables the Framework to control and audit user commands.

The Workspace Layout

The Framework Manager console consists of two areas: a navigation bar and a navigation pane.

- "Navigation Bar" on page 19
- "Navigation Pane" on page 19

Navigation Bar

The navigation bar on the top of the page has four options: Home, Consoles, admin, and Help.

Click an item on the navigation path for quick access to a given navigation pane. For example, to return to the home page, click **Home**.

Navigation Pane

In the navigation pane, you have access to the following administrative consoles:

- **Hosts:** Centrally manages Privileged Account Manager installation and updates, load-balancing, redundancy of resources, and host alerts. For more information, see Chapter 4, "Managing Framework Hosts," on page 25.
- **Framework User Manager:** Manages users who log in to the Framework Manager through role-based grouping. For more information, see Chapter 6, "Managing Framework Users and Groups," on page 57.
- **Package Manager:** Allows you to easily update any Privileged Account Manager hosts. For more information, see "Publishing Packages on the Package Manager" on page 313.
- **Command Control:** Uses an intuitive graphical interface to create and manage security policies for privilege management. For more information, see "Command Control" on page 103.

- **Reporting:** Provides easy access and search capability for event logs and allows you review and color-code user keystroke activity through the Command Risk Analysis Engine. For more information, see Chapter 7, "Managing Audit Reports," on page 83.
- **Compliance Auditor:** Proactive auditing tool that pulls events from the Audit database for analysis, according to predefined rules. It can be configured to pull filtered audit events at hourly, daily, weekly or monthly intervals. This enables auditors to view prefiltered security transactions, play back recordings of user activity, and record notes for compliance purposes. In an era of increasing regulatory compliance, the ability to supply demonstrable audit compliance at any time provides a more secure system and reduces audit risk. For more information, see Chapter 9, "Compliance Auditor," on page 155.
- **Access Dashboard:** Allows you to manage the requests for emergency access, and view the details of credential checkout. If required you can check in the checked out password. For more information, see Chapter 22, "Managing Emergency Access Requests," on page 291.
- **Credential Vault formerly known as Enterprise Credential Vault:** Allows you to manage the domains and its credentials. For information about **Credential Vault**, see Contextual Help.

Viewing the Version and the License Details

A framework user who has access to Administration console can verify the version and the license details of the installed Privileged Account Manager from the Administration console. To view the version and license details, the framework user must perform the following on the Administration console:

1. On the Navigation bar, Click ***admin*** > **About Framework**.

   Here, *admin* is the user name of the framework user who is part of default admin group or who has the **admin** role on the unifi module in the Framework User manager console. For more information about the framework user role, see "Configuring Roles" on page 72.
2. For License registration, click **Register Framework** > specify the license > **Finish**.
3. Click **Show License Summary** to view the number of each managed system that are being used through PAM, and the total license count.

   For more information about viewing the license summary and generating detailed report see, "License Summary" on page 20.

License Summary

The License Summary page includes the following information:

- The count for each managed end-points
- Total count of the managed end-points
- Time and date when the summary was last updated
- Option to download the detailed license report
- Option to update the license summary to view the latest license summary

For more information about the Privileged Account Manager license, see the Privileged Account Manager EULA in the Privileged Account Manager documentation website.

Managed End Point Type

The license count is based on the following type of managed end-points:

- **Agents:** This displays the number of all the Host servers that are added in the Hosts console and the agents that are registered in the framework.
- **Databases:** This displays the number of databases that are managed or accessed through PAM. This count is inclusive of all the database connectors that are configured for database monitoring and all the resources of type **Database** in **Credential Vault** for credential checkout/ checkin.
- **Applications:** This displays the number of applications that are managed or accessed through PAM for the password checkin/ checkout feature. This count includes all the resources of type **Applications** that are configured in **Credential Vault**.
- **SSH hosts:** This displays the number of SSH servers that are managed though for SSH relay. This count includes the resources of type **SSH** that are configured in **Credential Vault**.

Update License Summary

When you click **Update License Summary**, PAM deletes the previous license summary and updates the latest license summary. If you want to back up the previous license summary, you can download the license report by clicking **Download Detailed Report** before updating the summary.

The date and time when the existing license summary was generated is displayed at the bottom left corner of the License Summary page.

Download Detailed Report

To view and save the detailed report of the managed end-points that are displayed in the license summary page, click **Download Detailed Report**. The detailed report includes the following:

- Type of managed end-points.
- DNS or IP address of the managed end-points.
- Sub-type of the managed end-points.

  The sub-types can be as following:

  - Agent for all Agents
  - Local for SSH
  - The name of the application for Application
  - The name of the database for Database
- Name of hosts or servers associated with each managed end-point.

  The name can be as following:

  - Configured name for Agent
  - The configured resource name for SSH and Application
  - <*hostname*>:<*port*> for Database

3 Getting Started

PAM allows administrators to grant and manage the user access to the required server through remote desktop, or SSH. To manage privileged account on a Linux, UNIX, application, or a database server you must define rules in PAM manager. A typical workflow of PAM is as following:

1. Install Privileged Account Manager and required packages for your enterprise environment. For more information about installing Privileged Account Manager, refer Privileged Account Manager Installation Guide.
2. Assign proper rights to Administrators by using the Framework Manager console. For information about Framework users and assigning rights to them, refer Chapter 6, “Managing Framework Users and Groups,” on page 57.
3. Register the host machines by using the Hosts console. For more information about registering hosts, refer Chapter 4, “Managing Framework Hosts,” on page 25
4. Create a rule/ policy for a role that is defined in the LDAP directory. For more information about different entities that create rule, refer Chapter 8, “Command Control,” on page 103.
5. Configure the reporting event settings by using the Reporting console. For information about configuring report, refer Chapter 7, “Managing Audit Reports,” on page 83.
6. Configure the audit settings by using the Compliance Auditor console. For information about configuring audit settings for compliance purpose, refer Chapter 9, “Compliance Auditor,” on page 155.

Managing Privileges in Various Endpoints

Privileged Account Manager provides the capability to connect to a remote host using SSH (UNIX/ Linux), RDP Relay (Windows), direct RDP and credential provider (Windows) without knowing the privileged account credentials such as passwords or identity certificate of the user. You can also configure Privileged Account Manager to connect to any database, or application server with secure and controlled access. The use of shared keys allows Privileged Account Manager to provide any type of shared credentials to privileged users. You can capture users’ activity in different formats, such as keystroke, screenshots, session, and video. For endpoints specific details, see the following sections:

- “Windows” on page 24
- “UNIX/Linux” on page 24
- “Database and Applications” on page 24
- “Shared Keys” on page 24

Before trying to connect to remote hosts, you must configure Rules and Policies in Privileged Account Manager. You must create rules in the component called Command Control as an Administrator. For more information about Command Control, see Chapter 8, “Command Control,” on page 103.

Windows

A Windows Server user can get privileged access on the target Windows machine (server and desktop), using RDP Relay, direct RDP, and credential provider. For information about privileged access to Windows machines, see Section 14, “Privileged Access to Windows,” on page 197.

UNIX/Linux

A UNIX/Linux Server user can get privileged access on the target UNIX/Linux machine, using SSH Relay, usrun command, pcksh, and cpcksh. For information about privileged access to UNIX/Linux machines, see Section 15, “Privileged Access to UNIX and Linux,” on page 207.

Database and Applications

A Privileged Account Manager user can access databases such as, Oracle, and any application server such as, LDAP. All the actions that the user performs on the database or any application can be monitored by configuring the settings on the Manager for Privileged Account Manager. The shared credentials are also managed by using **Credential Vault**. For more information about shared account credentials refer Chapter 17, “Privileged Access to Applications and Cloud Services,” on page 241.

A user who has an account in the database server can also be monitored through Privileged Account Manager. For more information about database monitoring, see Chapter 16, “Privileged Access to Databases,” on page 227

Shared Keys

Privileged Account Manager provides shared key functionality to share any type of value or key with privileged users. For more information about shared keys refer, Chapter 13, “Managing Shared Keys,” on page 193.

4 Managing Framework Hosts

The Hosts console provides a hierarchical view of all the defined hosts. Each host machine on which you have installed managers and agents must be added to the Framework Manager console through the Hosts console. Hosts are identified to the Framework Manager console by a unique agent name that is used during the registration process after installation.

Hosts are added to domains, which allow you to organize your hosts into a tree structure.The hierarchical structure allows easy access to a particular host regardless of the number of Privileged Account Manager hosts you have.

The Hosts console includes the following:

- **Task pane (left pane):** This pane includes the tasks or the actions that can be performed on the host servers.
- **Navigation pane (middle pane):** The navigation pane displays hierarchical view of all currently defined hosts and domains.
- **Details pane (right pane):** The details pane displays the details of the selected hosts.

This section lists the tasks that you can perform to manage host servers.

- "Managing Domains" on page 25
- "Managing and Monitoring Hosts" on page 27
- "Managing System Alerts" on page 34
- "Enabling Crash Dump Capture" on page 36
- "Managing Host Packages" on page 36
- "Managing Audit Zones" on page 41
- "Understanding Tunneling" on page 42
- "Securing Access to the Framework Manager Console" on page 45
- "SSL Renegotiation DOS Attack Protection" on page 46
- "Using Privileged Account Manager Service" on page 47
- "Integrating with NetIQ Access Manager" on page 47
- "Troubleshooting" on page 47

Managing Domains

Privileged Account Manager provides load balancing and failover capabilities based on the hierarchical structure of the hosts. Before organizing your hosts into domains and subdomains, refer to High Availability and Load Balancing sections for information about these features.

- "Creating a Domain" on page 26
- "Modifying a Domain" on page 26
- "Deleting a Domain" on page 27

Creating a Domain

When you install Privileged Account Manager, a top-level domain **Hosts** is automatically created. To rename this domain, see "Modifying a Domain" on page 26. You can create subdomains under the top-level domain.

1. On the home page of the console, click **Hosts**.
2. Select an existing domain to add a subdomain to the existing domain.
3. Click **Add Domain** in the task pane and on the Add Domain page specify the subdomain name.
4. Click **Add**.
5. Select to perform any of the following tasks:
   - To configure the domain, continue with "Modifying a Domain" on page 26.
   - To add hosts to the domain, continue with "Adding a Host" on page 27.
   - To move existing hosts to this domain, continue with "Moving a Host" on page 31.

Modifying a Domain

Use this page to modify the domain name and encryption settings. The encryption settings apply to all hosts within the domain, unless you modify the host encryption settings. Host settings overwrite domain settings.

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, select the domain you want to modify.
3. In the task pane, click **Modify Domain**.
4. Configure the following options:

   Domain Name: Name of the domain is displayed in this field. You can change the name by specifying a new domain name.

   Audit Zone: Specify an audit zone for this domain. For example, DOMAZ1. For more information about audit zones, see "Managing Audit Zones" on page 41.

   NOTE: By default, the domain is associated with audit zone 0.

   Location: Select the country and the province where the domain is located. Based on the selected value, the domains are mapped to the corresponding coordinates in the Deployment Dashboard.

   Key Configuration: Select this option to enable configuration of the encryption key and encryption of the databases stored on the hosts in this domain.

   Host Key Rollover(days): Specify how many days the host key can be used before generating a new key for the hosts in this domain.

   Db Key Rollover(days): Specify how many days the database key can be used before generating a new key for the hosts in this domain.

   Encrypt: Select the databases you want to encrypt for the hosts in this domain.

   Ensure that you select the appropriate database for encryption. When you encrypt some database, it may cause performance issues. NetIQ recommends to encrypt the following:

   - `auth.db`: it contains usernames

- `registry.db`: it contains the hosts.
- `cmdctrl.db`: it contains command control rules with usernames and hosts.
- `PrvCrdVlt.db`: It secures the account and key credentials in the Credential Vault.

NOTE: The encryption of auditing data (/audit/cmdctrl.db) can be enabled from the Reporting console. See "Audit Settings" on page 83.

---

5 Click **Finish**.

Deleting a Domain

You cannot delete a domain if it contains any host. So, you must delete or move the hosts before attempting to delete a domain. For information about moving a host, refer "Moving a Host" on page 31.

1 On the home page of the console, click **Hosts**.

   The navigation pane displays the current hierarchy of the Framework.

2 In the navigation pane, select the domain you want to delete.

3 In the task pane, click **Delete Domain**.

4 Click **Finish**.

Managing and Monitoring Hosts

A host is created for each machine that you want to manage with Privileged Account Manager. You can register the agents and view the list of those as hosts in the Hosts console. Also, you can register the agents after adding the hosts in the Hosts console.

- "Adding a Host" on page 27
- "Viewing Host Details" on page 28
- "Modifying a Host" on page 29
- "Registering Hosts" on page 30
- "Deleting a Host" on page 30
- "Moving a Host" on page 31
- "Finding a Host" on page 31
- "Monitoring Hosts" on page 31

Adding a Host

1 On the home page of the console, click **Hosts**.

2 Select the domain for the new host.

3 Click **Add Hosts** from the task pane.

4 In the text box, specify the agent names for the hosts.

You can type the names one at a time, using one name per line, or you can paste a list of names. When you add a host to the Framework Manager, the name does not need to relate to the existing DNS name that is used in locating the host on your network, however it may be helpful to keep the DNS name and Privileged Account manager host name the same for simplicity.

5 Click **Add**.

A list of agents names is displayed.

6 Click **Finish**.

The status of the host is unregistered until the agent is installed and registered on the host machine. For instructions on this process, see "Installing and Registering a Framework Agent " in the *Privileged Account Manager Installation Guide*.

Viewing Host Details

1 On the home page of the console, click **Hosts**.

2 In the navigation pane, select the domain containing the hosts whose details you want to view.

3 Click the arrow ▸ next to the domain name to display the list of hosts.

4 Click the required host to display the host details and status in the details pane.

Field	Description
Agent name	The agent name configured for this host.
DNS name/ IP address	The name of the host. This is either a resolvable DNS name or the IP address.
Port	The port the host is using for Privileged Account Manager communication.
Platform	The operating system on the host.
Processor	The type of processor on the host.
OS Version	The version of the kernel running on the host.
Agent version	The version of the agent software that the host is running.
System time	The current date and time that the host is configured for, displayed in UTC. Use this time to verify that the agent's time is synchronized with the other hosts.
Service uptime	The number of days, hours, minutes, and seconds the agent has been running since the last start up.
Active sessions	The number of connections currently open between the agent and any other agent, including itself.
Active tasks	The number of internal tasks that the agent is running at any one time.
Installation path	The directory location of the installed agent software.
Disk space	The total amount of available disk space, the amount of free disk space, and the percentage of disk space in use.

Field	Description
Memory (approx)	The amount of memory (heap) currently being used by the agent to store its data. This is the virtual data segment size minus the thread stack and the statically initialized data (because this is a constant value) as returned by the `sbrk` system call.
Registration	The licensing state of the software, either licensed or unlicensed.
Status	The status of the host: online, offline, unregistered.

5 In the navigation pane, select the host to display the **Packages** option on the right pane.

6 Click **Packages** to view details of the packages installed on the selected host.

Modifying a Host

1 On the home page of the console, click **Hosts**.

2 In the navigation pane, select the host to modify.

3 In the task pane, click **Modify Host**.

4 Modify the general details:

Agent Name: Specify a display name for this agent.

Description: Add a description. This description is displayed next to the agent name in the navigation pane.

DNS Name/ IP Address: Specify the DNS name or IP address of the host that is used in locating the host on your network.

Port: Displays the port that was specified when the agent was registered.

Audit Zone: Displays the audit zone of the host. The audit zone of the host will be same as the audit zone of the sub-domain or domain it belongs to. For more information about audit zones, see "Managing Audit Zones" on page 41.

5 Configure the encryption settings. When these settings are modified for an individual host, the host settings overwrite the settings specified for the domain.

Key Configuration: Select this option to enable configuration of the encryption key.

Host Key Rollover (days): Specify how many days the host key can be used before generating a new key.

DB Key Rollover (days): Specify how many days the database key can be used before generating a new key.

Encrypt: Select the databases you want to encrypt.

Encrypting the database can affect the performance. The following databases can be considered for enabling encryption:

- auth.db - Contain usernames
- registry.db - Contains the hostnames.
- cmdctrl.db - Contains command control rules with usernames and hostnames.

NOTE: The encryption of auditing data (/audit/cmdctrl.db) can be enabled from the Reporting console. See "Audit Settings" on page 83.

6 Click **Finish**.

Registering Hosts

You can register the agents before performing any action on the host through the console. When you register the agent, the host is added in the host console. You can also register the agent after adding the host. Perform the following steps to register the agents after adding the host in the console.

1 On the home page of the console, click **Hosts**.

2 In the navigation pane click the root domain, **Hosts**.

3 In the task pane, click **List Unregistered Hosts**.

Unregistered hosts that are in the subnet are listed.

NOTE: If you have registered an agent, then this agent is automatically updated as host in the **Hosts** console.

4 Select the hosts to be registered and provide the following details:

- **PAM Admin Username:** User name for the Framework Manager.
- **PAM Admin Password:** Password for the Framework Manager.
- **Agent Admin Password:** The root password of the Linux or the Unix hosts on Linux platform or the administrator password on Windows platform.

5 Click **Register** to auto register the selected hosts.

NOTE: By default all the registered hosts are registered to the root of the domain. To move the hosts, see "Moving a Host" on page 31.

Deleting a Host

1 On the home page of the console, click **Hosts**.

2 In the navigation pane, select the hosts to delete and click **Delete Host**.

Or

In the details pane, select the hosts to delete.

To select all hosts in a domain, select **Name**.

3 In the task pane, click **Delete Host**.

The selected hosts are listed.

4 Click **Finish**.

WARNING: Deleting the audit manager host might result in losing audit data that is received from the domain or audit zone.

Moving a Host

You can move hosts among the domains.

1. On the home page of the console, click **Hosts**.

   The navigation pane displays the current hierarchy for your Framework.
2. In the navigation pane, click the arrow next to the domain that contains the hosts you want to move.
3. Select the hosts to move.
4. Drag and drop the hosts to the new domain.

   If the list is large, perform the following:

   4a In the middle pane, click the domain that has the required host.

   All the hosts in the domain are listed in the right pane.

   4b In the middle pane, scroll till you can view the destination domain.

   4c Drag the host from the right pane and drop it to the destination domain in the middle pane.

NOTE: When you move a host from one domain to another, the audit zone of the host changes to the audit zone of the domain to which it has been moved.

Finding a Host

1. On the home page of the console, click **Hosts**.
2. On the navigation pane, click the root domain, **Hosts**.
3. In the task pane, click **Find Host**.
4. In the **Agent Name** field, specify the name of the host you are looking for.

   You can use the wildcard characters * and ?. This field is case sensitive.
5. Click **Find**.
6. To go to a host's details, double-click the agent name.

Monitoring Hosts

Privileged Account Manager maintains a log file for each host. Each host can be configured to send alerts to the Framework Manager console when errors occur. It allows you to monitor the status of each host:

- "Viewing the Host Status" on page 32
- "Viewing the Host Log" on page 32
- "Modifying Log Settings" on page 33
- "Example Rollover Script" on page 34

Viewing the Host Status

The **Host Status** option allows you to view the current status of all your hosts, or all the hosts in a domain, on one page.

1. On the home page of the console, click **Hosts**.
2. Select a domain.
3. Click **Host Status** in the task pane.

   The status for each host is displayed, as shown in the following table, with a summary at the bottom of the screen.

	The host is online.
	There is a status problem with the host; for example, the host's time offset exceeds the defined level (see Step 7). Click the arrow to the left of the green box to display status messages.
	The host is offline.
	The host is unregistered.

4. Use the **Online**, **Offline** and **Unregistered** check boxes to select the hosts you want to view.

   If you have a long list of hosts, deselect the **Auto scroll** check box to stop the automatic scrolling.
5. (Conditional) If you want to enable FIPS in all agents and manager component, click **Enable**. Before enabling FIPS, review prerequisites in section Enabling FIPS Mode in the Privileged Account Manager Installation Guide.
6. (Conditional) If you want to disable CBC mode in all agents and manager component, click **Disable**.
7. (Optional) Change the filter settings from the default values and select **Restart** to check the status again. The available filters are:

   Maximum Timeoffset (minutes): The difference in system time between the host and the Primary Registry Manager. If the time offset exceeds the value in this field, a warning indicator is displayed.

   Minimum Disk Space (MB): If the available disk space on the host machine goes below the value in this field, a warning indicator is displayed.

   Maximum Memory (MB): If the memory used by the host exceeds the value in this field, a warning indicator is displayed.
8. To view a host's details, double-click the host or click **Close** to return to the hierarchical view.

To use a command line option to view the status, see "Agent Status" on page 185.

Viewing the Host Log

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, select the required host.
3. In the task pane, click **View Host Log**.

4 Specify the values for the following based on the required log information:

Log Level: Set the level of information you want to see on the screen.

- **Error** displays only Error messages.
- **Warning** displays Warning and Error messages.
- **Information** displays Information, Warning, and Error messages.

Refresh (secs): Set the interval between screen refreshes. You can select intervals from 1 to 60 seconds

Maximum Cached log Messages: Set the maximum number of log messages to display on the screen. You can view from 10 to 1000 messages.

5 Click the **Pause** check box to pause the screen display.

6 Click the **Clear** button to clear the screen display.

7 Click **Close** to return to the Framework hierarchy view.

Modifying Log Settings

You can modify log settings for hosts, hosts in a domain, or an individual host by using the **Domain Log Settings** or **Host Log Settings** options.

1 On the home page of the console, click **Hosts**.

2 To modify the log settings for all hosts in a domain, select the domain. To modify the log settings for an individual host, select the host in the navigation pane.

3 Click **Domain Log Settings** or **Host Log Settings** in the task pane, then modify the following settings:

File Name: Specify the filename and location of the log file. All the details are by default logged in `logs/unifid.log`.

Level: Set the level of information you need. The default level is `Info`.

- **Error** for Error messages.
- **Warning** for Warning and Error messages.
- **Info** for Information, Warning, and Error messages.
- **Debug** for Debug, Information, Warning, and Error messages.
- **Trace** for Trace, Debug, Information, Warning, and Error messages.

NOTE: The **Debug** and **Trace** settings generate a lot of data and are primarily for the use of NetIQ Support.

Show all tasks: Click **Show all tasks** to include all tasks in the log. The **Show all tasks** option is primarily for the use of NetIQ Support.

Roll Over: Select the rollover point from the drop-down list to specify when the log file is overwritten with new information. If the maximum size set for the log file is reached, the log file is overwritten regardless of this setting.

Max Size (MB): Select the maximum size of the log file from the drop-down list. This specifies when the log is overwritten with new information.

Roll Over Script: Enter a Perl script to be executed at the rollover point. For a sample script, see "Example Rollover Script" on page 34.

4 Click **Next** to apply the changes.

If the changes are applied successfully, a green box is displayed next to the agent name.

If the changes are not applied successfully (for example, if the host is not online), a red box is displayed next to the agent name.

5 Click **Close**.

Example Rollover Script

This is an example of a Perl script that can be called at the rollover point for the host log file. The script compresses the old `unifid.log` and then removes any log files that are more than 30 days old.

```
use File::Basename;
# Zip up rolled over logfile
system("/usr/bin/gzip $LOG_FILE");
my $log_root = dirname($LOG_FILE);
$ctx->log_info("Log file directory  - $log_root");
opendir(LOGDIR, $log_root);
$ctx->log_info("Zipping up $LOG_FILE");
# Find all the compressed log files
my @log_files = map { $_->[1] }
map { [ $_, "$log_root/$_" ] }
grep { /\.gz$/ }
readdir(LOGDIR);
closedir(LOGDIR);
# Delete all log files older than 30 days
my $time = time();
foreach my $log (@log_files) {
my ($mtime) = (stat($log))[9];
my $age = int((($time - $mtime) / 3600) / 24);
$ctx->log_info("Checking $log ($age days old)");
next unless $age > 30;
$ctx->log_info("Deleting $log ($age days old)");
unlink $log;
}
```

Managing System Alerts

The System Alerts page shows system status alert messages from all hosts in the Framework. The page shows the time of the alert, the host that originated the alert, the type of alert, and information about the alert.

You can define the level of system alerts by using the **Domain Alert Settings** or **Host Alert Settings** options.

System alerts is indicated by a flashing Framework icon at the bottom right corner of the screen.

1 Click the icon to display the System Alerts page.

2 To clear specific alerts, select the **Resolved** checkbox next to the desired alerts, then click **Finish**.

To clear all alerts, select **Mark all alerts resolved**, then click **Finish**.

3 To close the System Alerts page without clearing the existing alerts, click **Cancel**.

The Framework icon continues to flash.

Modifying Alert Settings

You can configure your Framework hosts to generate system status alert messages when specific events occur, such as when the agent exceeds a specified memory usage. If a system alert is triggered, the Framework icon in the bottom right corner of the screen flashes. To view the system alerts, click the icon (see "Managing System Alerts" on page 34 for details).

You can modify alert settings for all hosts, all hosts in a domain, or an individual host by using the **Domain Alert Settings** or **Host Alert Settings** options.

To modify alert settings:

1 On the home page of the console, click **Hosts**.

2 To modify alert settings for all hosts in a domain, select **Hosts** or the name of a domain. To modify alert settings for an individual host, select the host in the navigation pane.

3 In the task pane, click **Domain Alert Settings** or **Host Alert Settings**.

Changes made to a domain's alert settings override the current settings for individual hosts in that domain. However, subsequent changes made to an individual host's alert settings override the current domain alert settings on that host.

4 Configure the following options:

Alert on Log level: Select the level of log information needed to trigger an alert. For example, if you want alerts to be triggered when error messages occur in the log, select **Error**. The **Warning** option includes **Warning** and **Error** messages. The **Info** option includes **Info**, **Warning,** and **Error** messages. Select **Never** to switch this setting off.

Alert Log Filter: Define a specific message you want to trigger alerts, or part of a message with wildcard symbols *. You can use regular expressions in this field by selecting the **Regular expression** check box and specifying your regular expression.

This setting is independent of the setting in **Alert on log level**.

Time Offset (mins): Specify the time offset in minutes when you want to trigger an alert. An alert is triggered if a host's time setting differs from the time setting of the Primary Registry Manager by this number of minutes. Time offsets can cause problems because certificates are time-based. The UTC (Universal Time Coordinated) value is used.

Pending Messages (mins): Specify the interval for when you want to trigger an alert. An alert is triggered if an event has been in the queue of store and forward messages for this number of minutes.

Maximum Memory (MB): Specify the amount of memory in MB that you want as the threshold for an alert. An alert is triggered if a host is using more than this amount of memory.

Minimum Disk Space (MB): Specify the minimum amount in MB of disk space that you want as the threshold of an alert. An alert is triggered if a host has less than this amount of disk space remaining in the default installation location.

Expired Certificate: Select this option to cause an alert to be triggered when an agent's certificate expires.

5 Click **Next** to apply the settings to the hosts.

If the settings are applied successfully, the indicator next to the hostname is green .

If the settings are not applied successfully (for example, if the host is offline), the indicator is red .

6 Click **Close**.

If any of your settings cause an alert to be triggered, the Framework icon flashes.

Enabling Crash Dump Capture

If you want to enable crash dump capture, add a configuration parameter to the `unifi.xml` file, as follows:

```
<Dump log='1'/>
```

By default, crash dump capture is disabled and there is no XML node for this. You must manually add this node in xml to enable crash dump capture.

When the Privileged Account Manager service starts, it creates an empty dump file and keeps it open. If Privileged Account Manager crashes, dump is logged to the file that is created during Privileged Account Manager service startup. If there is no crash when Privileged Account Manager service is restarted, this file is deleted and a new empty dump file is created.

The format of dump file name is `unifid_child_<pid>_<random_number>`.

NOTE: Crash dump capture is supported only on Windows.

Managing Host Packages

- "Finding Packages on Hosts" on page 37
- "Updating Packages for a Host" on page 37
- "Rolling Back Packages" on page 38
- "Committing Packages" on page 38
- "Registering and Unregistering Packages for a Host" on page 39
- "Installing Packages on a Host" on page 39
- "Uninstalling Packages from a Host" on page 40
- "Modifying Audit Settings for the Audit Manager Package" on page 40
- "Configuring SMTP Settings for the Messaging Component Package" on page 41
- "Configuring Settings for the dbaudit Package" on page 41

Finding Packages on Hosts

You can search through all the hosts to find where a specific package is installed, or find whether the package is installed at all.

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, click **Hosts**.
3. In the task pane, click **Find Package**.
4. From the **Package** drop-down list, select or enter the package you are looking for.

   For example: If you are searching for Audit Manager package, enter `secaudit` in the search field and then click **Find**.
5. If you want to find out which hosts do not have this package installed, select the **package not installed** check box. If you want to find out where the package is installed, deselect the **package not installed** check box.
6. Click **Find**. A list of hosts where the package is installed or not installed is displayed.
7. Double-click the host name to view its details or click **Close** to return to the Hosts page.

Updating Packages for a Host

When updated packages are available on your local Package Manager, you can update the packages installed on individual hosts or for all hosts in a domain. The distribution agent performs a number of checks to ensure that the host has enough disk space to extract and install the package. If there is insufficient space, the package is not updated.

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, select either the host or the domain where you want to update the packages.
3. Click **Update Domain Packages** or **Update Packages** in the task pane.

   The console checks for updates on your Package Manager and displays any updated packages available for download.
4. Select the packages from the list of available packages.

   To select multiple packages, press the Ctrl key and select the packages one at a time, or press the Shift key to select a consecutive list of packages. To select all packages, use Ctrl+A.

   NOTE: The **Create Backup** option which creates a backup of the currently installed packages is selected by default. Only the last backup is stored. Creating backups requires additional space.

   If necessary, you can use the Rollback Packages option to roll back to the previously backed-up packages.

   ---
5. Click **Next** to start downloading the selected packages.
6. Click **Finish**.

Rolling Back Packages

If you chose to create a backup when updating packages for an individual host or for a domain, you can roll back to the last backup.

Prerequisite

Before you rollback packages from 3.5 to any lower version, you must uninstall the Application SSO Manager (`appsso`) and Video Processing Module (`videoprocessor`) packages.

NOTE: When you rollback packages from 3.5 to any lower version, first rollback all the packages except distrib and framework (`spf`) and lastly rollback distrib and framework (`spf`) package.

---

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, select the domain or the host where you want to roll back the packages.
3. In the task pane, click **Rollback Domain Packages** or **Rollback Packages**.
4. Select the packages from the list of available backed-up packages.

   To select multiple packages, press the Ctrl key and select the packages one at a time, or press the Shift key to select a consecutive list of packages. To select all packages, use Ctrl+A.
5. Click **Next** to start rolling back to the previously backed-up packages.
6. Click **Finish**.

Committing Packages

When packages are updated and the **Create backup** option is enabled, a backup of the current package is created and stored in a backup directory in the working package directory. This allows you to roll back to the previous level if the current package does not perform correctly in your environment. (See "Rolling Back Packages" on page 38.)

If the current package does perform correctly in your environment, you can commit the package, which frees up disk space by deleting the files in the backup directory. If your hosts have limited disk space, NetIQ recommends that you commit the packages on all hosts before performing the next update.

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, select the domain or the host where you want to commit packages.
3. Click **Commit Domain Packages** or **Commit Packages** in the task pane.
4. Select the packages from the list of available packages.

   To select multiple packages, press the Ctrl key and select the packages one at a time, or press the Shift key to select a consecutive list of packages. To select all packages, click the Select all checkbox.
5. Click **Next** to start the commit process.
6. Click **Finish**.

Registering and Unregistering Packages for a Host

If you want to stop a package from functioning without removing it completely, you can unregister it. You can then register it again later if necessary. Packages are automatically registered when you add them, so you only need to register them if you have previously unregistered them.

Registered packages are shown with a green check mark: .

Unregistered packages are shown with a red exclamation mark: .

To register or unregister a package for a host:

1. On the home page of the console, click **Hosts**.

   The navigation pane displays the current hierarchy for your Framework.
2. In the navigation pane, select the domain where you want to register or unregister packages.
3. Select the host.
4. With the host's packages displayed, select the packages you want to register or unregister.

   To select multiple packages, press the Ctrl key and select the packages one at a time, or press the Shift key to select a consecutive list of packages. To select all packages, use Ctrl+A.
5. Click **Register Package** or **Unregister Package** in the task pane.

   WARNING: Ensure that you are not unregistering an audit manager package or any other package that might cause loss of audit data.

NOTE: The Framework Manager console does not refresh automatically. To check whether your packages have been successfully registered or unregistered, go to another screen and then return to the list of packages.

Installing Packages on a Host

Ensure that the packages have been downloaded to the Framework Package Manager by viewing packages available to deploy. See section "Publishing Packages on the Package Manager" on page 313.

The distribution agent performs a number of checks to ensure that the host has enough disk space to extract and install the package. If there is insufficient space, the package is not installed.

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, click the arrow next to the domain where you want to install the packages.
3. Select the required host.
4. In the details pane, click **Packages**.
5. In the task pane, click **Install Packages**.
6. Select the packages from the list of available packages.

   To select multiple packages, press the Ctrl key and select the packages one at a time, or press the Shift key to select a consecutive list of packages. To select all packages, use Ctrl+A.

7 Click **Next** to start installing the selected packages.

8 Click **Finish**.

To use a command line option to install packages on hosts, see "Package Manager Options" on page 182.

Uninstalling Packages from a Host

You do not need to uninstall a package to disable it. You can disable it by unregistering the package. See "Registering and Unregistering Packages for a Host" on page 39.

To uninstall a package:

1 On the home page of the console, click **Hosts**.

2 In the navigation pane, click the arrow next to the domain where you want to uninstall packages.

3 Select the required host.

4 In the details pane, click **Packages**. and then select the packages from the list of installed packages.

   To select multiple packages, press the Ctrl key and select the packages one at a time, or press the Shift key to select a consecutive list of packages. To select all packages, click the **Select All** checkbox.

5 Click **Uninstall Packages** in the task pane.

6 Click **Next** to start uninstalling the selected packages.

7 Click **Finish**.

WARNING: Ensure that you are not uninstalling an audit manager package or any other package that might cause loss of audit data.

To use a command line option to install packages on hosts, see "Package Manager Options" on page 182.

Modifying Audit Settings for the Audit Manager Package

The databases containing audited data from command control (`cmndctrl.db`) can be placed in an alternative location. The administration audit files (`audit.db` and `audit.ldb`) and `log.msqs` are still stored in the default location `/opt/netiq/service/local/audit` or `C:\Program Files\Netiq\npum\service\local\audit`, but these files are relatively small.

To define an alternative location for the audit databases:

1 On the home page of the console, click **Hosts**.

2 In the navigation pane, select the host with the Audit Manager installed.

3 With the host's packages displayed, select the **Audit Manager (audit)** package.

4 Click **Audit Settings** in the task pane.

5 In the **Audit Path** field, specify the location for the audit databases.

6 Click **Finish**.

Configuring SMTP Settings for the Messaging Component Package

The **SMTP Settings** option allows you to provide details of your e-mail server so reports such as the Compliance Auditor reports and custom command control reports can be automatically e-mailed to the necessary personnel.

To configure the SMTP settings:

1. On the home page of the console, click **Hosts**.
2. Select the host where the Compliance Auditor and Messaging Component are installed.
3. Click **Packages** to view details of the packages installed on this host.
4. Select the **Messaging Component (msgagnt)**.
5. Click **SMTP Settings** in the task pane.
6. Configure the following fields:

   SMTP Host: Specify the IP address of your e-mail server.

   SMTP Port: Specify the port of your e-mail server.

   SMTP Domain: If you are using a Lotus Notes server, specify the name of your SMTP domain.
7. Click **Finish**.

Configuring Settings for the dbaudit Package

The **Settings** option is only displayed when you select the dbaudit package from the **Packages** page of any host. This is used to configure the credential checkout feature for Oracle and Microsoft SQL Server databases.

For Oracle database, you need to mention the path where Oracle client is installed. For Microsoft SQL Server database, you need to mention the path where the symbolic links are created.

For more information, refer to "Configuring Credential Checkout for Oracle Database" on page 228 and "Configuring Credential Checkout for Other Databases" on page 229.

Managing Audit Zones

Audit zones are logical groups of audit managers, agents for Privileged Account Manager, and managers for Privileged Account Manager. You can configure audit zone for your domains. Audit zones consist of audit managers, to which audit data is sent by hosts. For example, if you configure audit zone as 'AZDOM1' for domain1, all the hosts in domain1 will send their audit data to audit managers of AZDOM1. Advantage of configuring audit zone for your domain is audit data can be sent only to the audit managers of your domain. This helps in restricting who can receive audit data of your domain, in terms of geographical and organizational demographics. It also helps avoid huge amount of data being sent to all the audit managers.

By default, audit zone of all the domains, agents for Privileged Account Manager, and managers is audit zone 0. This means that audit data is sent to all the audit managers. You can configure audit zones for domains, with one or more audit managers. If you have not configured audit zone for your domain, audit data of your domain will be sent to audit managers of audit zone 0.

IMPORTANT: There should be at least one audit manger in audit zone 0 at all times. This is necessary because, if there are no audit managers in the audit zone of any domain, then audit data of that domain is sent to audit zone 0. This prevents the loss of audit data.

If you move a host or a sub-domain from a domain to another, the audit zone of that host or sub-domain automatically changes to the audit zone of the domain to which it is moved.

If the audit managers of your audit zone are down, audit data is not sent to audit managers of audit zone 0. Instead, audit data is accumulated in the agent for Privileged Account Manager and sent to the audit managers of your audit zone when they are up.

If you move an agent host, that is an audit manager, from a domain to another during a session, the session audit data is still sent to that audit manager. This is to avoid loss of audit data. Any new session data will be sent to audit managers as per the new settings.

Here are few recommendations for configuring audit zones:

- Each audit zone should have more than one audit managers.
- If you have enabled video off-loading, ensure that each audit zone has one video off-loading agent.
- Start using Audit Zones feature only after you have upgraded all your agents for Privileged Account Manager and managers to version 3.0.

To view the audit zone configuration information:

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, select **Hosts**.
3. Click **Audit Zones Configurations** in the task pane.
4. Audit zone information is displayed, as shown in the following table.

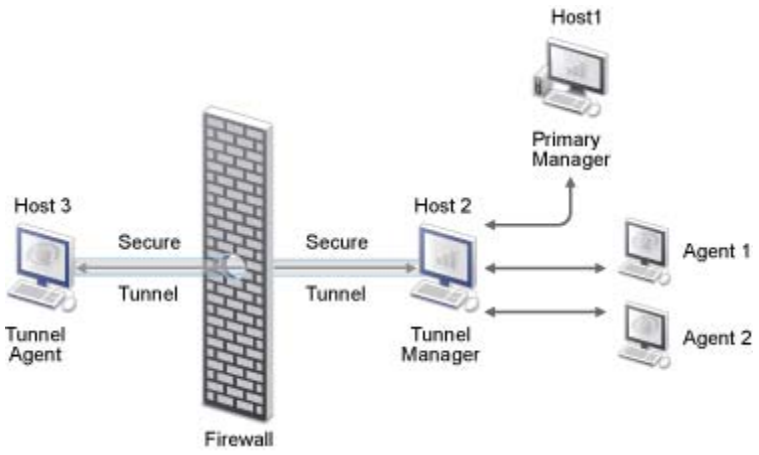
Audit Zones	Name of the audit zone.
Audit Managers	Audit managers that belong to the audit zone.
Domains	Sub-domains that are in the domain.

5. Click **Close** to go back to the **Hosts** home page.

Understanding Tunneling

Tunneling improves the usage of Privileged Account Manager in firewall enabled deployments. It reduces the security risks and enables the exchange of data within the firewall friendly architecture. The communication between the agents/managers in a firewall deployment is established through a secure channel called a tunnel and is an effective way to deploy client server applications on either side of the firewall infrastructure.

Figure 4-1 Tunneling Feature



For Example: In Figure 4-1, Host 3, Host 2, and the Agents are registered with the Primary Manager (Host 1). Tunnel Agent package and the Tunnel Manager package are installed on Host 3 (Tunnel Agent) and Host 2 (Tunnel Manager) respectively. Tunnel Manager behaves as an interface between the Tunnel Agent and the Primary Manager and the communication between the Tunnel Agent and the Tunnel Manager will be through the established tunnel. If the Tunnel Agent has to communicate with Agent 2, all Privileged Account Manager specific communication is channeled through the Tunnel Manager based on the policies configured in the Primary Manager.

NOTE: Tunneling is not supported on Windows. For the list of supported platforms, see the System Requirements in PAM Documentation website.

- "Installing Tunnel Agent and Tunnel Manager Packages" on page 43
- "Enabling and Disabling Tunneling" on page 44
- "Reregistering the Tunnel Agent Package" on page 44
- "Listing Tunnels" on page 45

Installing Tunnel Agent and Tunnel Manager Packages

Before installing the packages, temporarily allow access from Host 3 to the 29120 port of the Primary Manager and Host 2.

NOTE: ◆Ensure that the hosts or agents are registered with the primary manager before installing the packages.

- Ensure that the primary manager, tunnel manager, and tunnel agent are on separate systems.

---

1. Publish the tunnel agent and the tunnel manager packages in the console.

   For more information to publish the **Firewall Tunnel Agent** and **Firewall Tunnel Manager**, see "Publishing Packages of Major Releases" on page 314.

2. Install the **Firewall Tunnel Agent** package (**tnlagnt**). For more information, see "Installing Packages on a Host" on page 39.

   You can install more than one tunnel agents outside the firewall.

NOTE: You can also install tunnel agent directly from the installers and then register it with the primary manager. The tunnel agent rpm is in the `tunnel` folder of the ISO.

3 Install the **Firewall Tunnel Manager** package (**tnlmgr**). For more information, see "Installing Packages on a Host" on page 39.

Enabling and Disabling Tunneling

To establish a secure channel of communication between the tunnel agent and tunnel manager:

1 In the home page of the console, click **Hosts**.

2 In the navigation pane select the tunnel agent host, click **Packages**, then click **tnlagnt**.

3 In the task menu, select **Enable Tunneling**, then click **OK**.

To disable tunnel, select **Disable Tunneling**, then click **OK**.

Reregistering the Tunnel Agent Package

Before reregistering the tunnel agent package, ensure that you complete the following tasks:

1 Remove the access from the tunnel agent to the 29120 port of the primary manager and the tunnel manager.

2 Restart the tunnel agent.

To reregister the tunnel agent package, run the following command in the tunnel agent:

```
bash# /opt/netiq/npum/sbin/unifi regclnt register 127.0.0.1 29121
Please provide the DNS name or IP address of the framework manager :
(127.0.0.1)
Please provide the port number of the framework manager: (29121)
Please provide the DNS name or IP address of this agent: <agent DNS name>
Please provide the registered agent name for this agent: <agent DNS name>

Framework manager: 127.0.0.1:29121
Agent DNS name or IP address : <agent DNS name>
Agent name : <agent name>

Is this correct: (y)
Please enter the name and password of an account
with permission to register this host.
User name: <username>
Password: <password>
Confirm password: <password>
```

NOTE: To verify the re-registration process, check for the following line in the unifid.log:

```
Info, Registration successful for <agent DNS name> to 127.0.0.1:29121
```

Listing Tunnels

To list the agents to which a tunnel is established with the tunnel manager:

1. Click **Hosts** in the home page of the console.
2. In the navigation pane, select the tunnel manager host, click **Packages**, then click **tnlmngr**.
3. In the task menu, select **List Tunnels**.

   A list of agents to which the tunnel is established with the tunnel manager is displayed.

Securing Access to the Framework Manager Console

The following options increase the security of the communication between the browsers and the Framework Manager console. These configuration options do not affect the communications between the Framework managers and the Framework agents.

- "Requesting a Certificate for the Framework Manager Console" on page 45
- "Modifying the Connector" on page 46

Requesting a Certificate for the Framework Manager Console

For added security, you can install a certificate to use when accessing the Framework Manager console. To access this option, you need to select the **Administration Manager (admin)** package on the host that you want to protect. You must then complete a certificate request form, send it to your chosen certification authority, and then install the certificate that you receive.

NOTE: By default OpenSSL accepts DNS, email, URI, RID, IP, dirName as a Subject Alternative Name (SAN). PAM uses OpenSSL to generate a Certificate Signing Request (CSR). When requesting a certificate in PAM use the **Alternative Names** in the console as the "DNS" attribute.

Syntax for **Alternative Names** is:

- `DNS:example.com, DNS:www.example.com`
- `DNS:example.com, DNS:www.example.com, IP:127.0.0.1`

---

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, select the host that you want to protect with a certificate.
3. In the details pane, click **Packages** and select the **Administration Manager (admin)** for the Framework Manager console.
4. Click **Request Certificate** in the task pane.
5. Specify the necessary details as described in your chosen certification authority documentation.
6. Click **Finish**.

   The text for your certificate request is displayed in the text area.
7. Copy the certificate request into an e-mail and send it to your chosen certification authority.
8. When you receive the certificate from your certification authority, install it as described in "Installing a Certificate" on page 46.

Installing a Certificate

When you have received the requested certificate from your certification authority:

1. Copy the certificate to the machine you use to access the Framework Manager console.
2. On the home page of the console, click **Hosts**.
3. In the navigation pane, select the host where you want to install the certificate.
4. In the details pane, click **Packages** and select the **Administration Manager (admin)** package for which you have requested the certificate.
5. Click **Install Certificate** in the task pane.
6. Paste the certificate into the text area.
7. Click **Finish**.

Modifying the Connector

You can modify the way you connect to the Framework Manager console. You can define which interface card and port to use, and increase the security of the connection by using SSL.

To access this option, you need to select the **Administration Manager (admin)** package on the host you want to modify.

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, select the host where you want to modify the connector.
3. In the details pane, click **Packages** and select the **Administration Manager (admin)** for the Framework Manager console.
4. Click **Modify Connector** in the task pane.
5. Make the changes you want:
   - Define the address of a specific interface card
   - Define which port to use
   - Select the **SSL** check box if you want to use SSL.
6. Click **Finish**.

SSL Renegotiation DOS Attack Protection

Clients can attack the SSL server by sending many renegotiation (SSL handshake) requests to it. This can overwhelm the server and it might go down. To prevent such attacks, you can enable DOS attack protection.

To enable SSL renegotiation DOS attack protection:

1. In the `<Installation Path>/config/unifi.xml` file, edit the following line:

   ```
   <SSL reneg_dos_protection="0"/>
   ```

   reneg_dos_protection: Set the value to 1 to enable DOS attack protection. The default value is 0.
2. Save the file.

Using Privileged Account Manager Service

The Privileged Account Manager Service (PaaS) is a is part of the *Identity as a Service Powered by NetIQ* solution. Service providers host the Privileged Account Manager Service for their tenants. For more information, see the *Privileged Administrator Manager Service Installation and Configuration* Guide.

Integrating with NetIQ Access Manager

You can configure Privileged Account Manager as an protected resource in NetIQ Access Manager (NAM). This helps the NAM administrator to use the single sign-on feature of NetIQ Access Manager.

Prerequisites for Privileged Account Manager and NAM integration:

1. Install and configure NAM on a supported platform. For the list of supported platforms, see the *NetIQ Access Manager 4.1 Installation Guide*.
2. Install and configure Privileged Account Manager on a supported platform. For the list of supported platforms, see the *Privileged Account Manager Installation Guide*.
3. Ensure that you have administrator privileges in NAM.

To integrate Privileged Account Manager with NAM:

1. Create a protected resource in Access Manager for Privileged Account Manager (for example, www.pam.com) and a policy for injecting headers `X_PUM_ADMIN` and `X_PUM_PASSWD`. For more information, see the *NetIQ Access Manager 4.0 Administration Console Guide*.
2. Specify the following values in the policy:
   - Specify any PAM user for `X_PUM_ADMIN`.
   - Specify the PAM user password for `X_PUM_PASSWD`.

After you have integrated PAM with NAM, type the following URL in a browser to access PAM:

```
https://<NAM IP address:port>/pam/?sso=1
```

Troubleshooting

- "Promoting Managers When the Primary Manager Fails" on page 48
- "Viewing Store and Forward Messages" on page 48
- "Managing Low Disk Space" on page 49
- "Restarting the Agent" on page 50
- "Managing the Registry Cache" on page 50
- "Time Synchronization" on page 52

Promoting Managers When the Primary Manager Fails

If you have multiple Framework Managers deployed, the first manager installed is defined as the primary manager by default, and its packages are defined as primary. Manager packages on all other manager hosts act as backups. If your primary manager becomes unavailable, you can select single or multiple manager packages on a host to be promoted to primary status.

The Framework continues to function when the primary manager is unavailable, but no changes can be made to the Framework. Changes can only be written to the databases on the primary manager, which are then replicated to the backup managers. The only exception to this is the audit database. Each audit agent is responsible for sending its audit messages to each audit manager. This ensures that audit data is not lost.

NetIQ recommends having one host designated as a complete mirror of your primary manager. In event of a total failure of the primary manager, you can log into the backup console and promote it to primary status with no disruption of Privileged Account Manager services.

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, select the host where you want to promote a manager.
3. Click **Packages** and then select the manager packages you want to promote.

   To select multiple manager packages, press the Ctrl key and select the packages one at a time, or press the Shift key to select a consecutive list of manager packages.

   When you are promoting backup manager to primary, you must first promote the Registry module and then promote all the other modules.
4. Click **Promote Manager** in the task pane.
5. Review the list of manager packages you have selected.
6. Click **Finish**.
7. View the host's packages again and verify that the **Status** of the promoted manager packages has changed to Primary.

To use a command line option to promote backup host to primary status, see "Registry Manager Options" on page 186.

Viewing Store and Forward Messages

Messages from one host to another are stored if the sending host cannot communicate with the receiving host, and forwarded when the communication link is restored. You can view these messages and delete them if you do not need them.

You can use this feature to analyze a host and to discover whether it is having problems contacting a particular host. This problem usually occurs when a host is down or when a DNS name for a host name cannot be resolved.

1. On the home page of the console, click **Hosts**.

   The navigation pane displays the current hierarchy for your Framework.
2. Select the host for which you want to view store and forward messages.
3. In the details pane, click **Packages.** .
4. In the task pane, Select **View Messages**.

If any stored messages exist, they are displayed. Information about the message is displayed such as, the time the message was sent, the host on which the message was sent, the module that sent the message, the type of the message (method), the number of failed attempts when sending the message, and the next scheduled attempt to send the message, if any.

5 To attempt to send one or more messages again, select the messages and select **Retry**.

6 To delete one or more messages, select the messages and click **Delete**.

7 To refresh the screen, click **Refresh**.

8 Click **Close**.

Managing Low Disk Space

In Privileged Account Manager, the usrun sessions are terminated with an auditing error when the server ran out of disk space. For long term running processes, this is not the ideal solution. You can use Command Control scripts to slow down or freeze input/output for the following conditions:

- In usrun sessions when disk space is low.
- When the store and forward process cannot contact an audit manager and its queue size is increasing.

You can control what happens under these conditions by configuring the following attributes:

disk_min_free (default: 1MB): Minimum free disk space. When free disk space goes below this level, the action defined in backoff_action is applied.

- If the backoff_action is block, the audit message is paused until disk space becomes available.
- If the backoff_action is fail, the request to store the audit message fails with an error, and the user session is terminated.
- If the backoff_action is allow, the session is unaffected.

disk_wm_free (default: 2MB): Free disk space watermark. When the free disk space goes below this level, the delay defined in backoff_delay is applied between each audited message.

queue_max_size (default: 250MB): Maximum queue size. When the queue size goes above this level, the action defined in backoff_action is applied.

- If the backoff_action is block, the audit message is paused until the queue size reduces below this level.
- If backoff_action is fail, the request to store the audit message fails with an error, and the user session is terminated.
- If backoff_action is allow, the session is unaffected.

queue_wm_size (default: 100MB): Queue size watermark. When the queue size goes above this level, the delay defined in backoff_delay is applied between each audited message.

backoff_divisor (default: 1): Provides the ability to increase the delay as the disk space reduces or the queue size increases. The delay is calculated by dividing the range between the disk_wm_free and disk_min_free (or queue_max_size and queue_wm_size) by the backoff_divisor and then applying the delay for each increment.

backoff_delay (default: 500ms): Time in milliseconds to delay the audit request.

backoff_action (default: block): Either block, fail, or allow.

The following Command Control script illustrates how to change these settings:

```
my $t=$meta->child("Audit");
$t=$meta->add_node("Audit") if(! $t);
$t->arg("disk_min_free","10");
$t->arg("disk_wm_free","20");
return 1;
```

This script sets the disk_min_free attribute to 10MB and the disk_wm_free attribute to 20 MB. You can assign this script to any rule or you can assign it to a rule at the top of the tree that all commands pass through.

You should create an emergency policy that allows administrators to access the machine when disk space is low or the store-and-forward queue size is large. Such a script would look similar to the following:

```
my $t=$meta->child("Audit");
$t=$meta->add_node("Audit") if(! $t);
$t->arg("disk_min_free","0");
$t->arg("disk_wm_free","0");
$t->arg("queue_max_size","0");
$t->arg("queue_wm_size","0");
$t->arg("backoff_action","allow");
return 1;
```

You can assign this script to any rule or you can assign it to a rule at the top of the tree that all commands pass through

Restarting the Agent

If you are having problems, NetIQ Support might ask you to restart an agent.

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, select the host on which you want to restart the agent.

   To select multiple hosts in a domain, select the domain, then press the Ctrl key and select the hosts one at a time, or press the Shift key to select a consecutive list of hosts. To select all hosts in a domain, click **Select All**.
3. Click **Restart Agent** in the task pane.
4. Select the type of restart you want to perform, as advised by NetIQ Support.

   Soft restart: Reloads the module libraries and resets the service uptime.

   Hard restart: Restarts the daemon, reloads all modules, and resets the service uptime.
5. Click **Finish.**

Managing the Registry Cache

The registry cache is held by the Registry Agent on each host, and it contains a list of the packages deployed on each host in your Framework. This list is a copy of part of the information held by the Registry Manager, and it enables Framework components to locate and communicate with each

other, according to their position in the hierarchy created when you add domains and hosts to your Framework. Agents send requests to managers in the immediate subdomain, and if a request is unsuccessful, they try a manager higher up in the hierarchy.

- You can view the registry cache to check hosts in your Framework to see if a specific manager or agent module is installed, and check the order in the Framework hierarchy according to the hosts the modules are installed on. See "Viewing the Registry Cache" on page 51.
- If the registry cache becomes out-of-date, communication problems can occur. To fix this, try clearing the registry cache on the Registry Agent to allow it to be updated by the Registry Manager. See "Clearing the Registry Cache" on page 51.

Viewing the Registry Cache

When viewing the registry cache, you can use the stale cache (the default option). The cache is considered stale if it has not been updated by the Registry Manager for 2 hours, and this is usually adequate. If you deselect the **Use Stale Cache** check box, the information is provided by the Registry Manager.

1. On the home page of the console, click **Hosts**.

   The navigation pane displays the current hierarchy for your Framework.
2. Select the host for which you want to view the registry cache.
3. Click the **Packages**.
4. Click **View Cache** in the task pane.
5. From the drop-down list, select the package you want to look up in the registry cache.
6. If you want to view the latest information from the Registry Manager, deselect the **Use stale cache** check box, then click **Lookup**.

   Details of the hosts where the module is installed are displayed in order according to their position in the Framework hierarchy. Information shown includes the Framework agent name, IP address, port number, and whether the host has the primary manager component installed (indicated by 1 in the **Primary** column) or not (indicated by 0).
7. (Optional) To clear the registry cache, click **Clear Cache.**

   This marks the cache as stale, and it is automatically updated by the Registry Manager. You can also clear the cache by using the **Clear Cache** option in the task pane.
8. Click **Close**.

Clearing the Registry Cache

NetIQ Support might advise you to try clearing the registry cache if you have communication problems among Privileged Account Manager components. The registry cache is held by the Registry Agent and contains a list of manager and agents in your Framework, copied from the Registry Manager. See "Managing the Registry Cache" on page 50 for more details.

1. On the home page of the console, click **Hosts**.

   The navigation pane displays the current hierarchy for your Framework.
2. Select the host for which you want to clear the registry cache.
3. Click the host's **Packages** icon (click the arrow next to the host's name to display it).

4 Click **Clear Cache** in the task pane.

The registry cache is marked as stale and is updated by the Registry Manager. You can also clear the registry cache by using the **View Cache** option (see "Viewing the Registry Cache" on page 51).

Time Synchronization

All agents should be configured to use a Network Time Protocol (NTP) server. Agents must have their time synchronized with the primary registry manager so that the time difference is less than two hours.

If the time difference is greater than two hours, the agent can appear offline and Command Control requests can fail.

5 Policy Templates

Privileged Account manager includes templates to import policies in the Command Control console. These templates help in better accessibility and better understanding of the policies. You can customize the policy with minimal changes and start using the policies without any hassle. You can import sample policies by using the **Import Sample Policy** template in the **Getting Started** page and add individual policies by using the Add Policy Template in the Command Control console. The sample template includes some of the commonly used policies, which an administrator can modify as per the requirement. For more information about Sample template, refer "Understanding Sample Policy template" on page 53. You can add additional sample policy after importing the sample policy template. If you already have policies created and do not want those policies to be overwritten by importing the sample policies, then you can add the additional policy individually from **Add Policy Template**. The additional sample policy creates a specific policy based on your requirement and it can be added to the existing hierarchy of policies. For more information about adding a sample policy, refer "Adding a Policy Template" on page 54.

NOTE: You can create a backup for the transaction settings by using the **Backup and Restore** option in the Command Control console. Before importing the policy template you can start the transaction so that if you require reverting back to the earlier Command Control settings you can cancel the transaction and if you require the changes after the import, you can commit the transaction.

Understanding Sample Policy template

The sample policy template is a template that imports various sample policies with required conditions. These policies include all the configuration settings for all the entities that are required to create sample policies in the Command Control console. This template helps in providing some of the sample policies that an administrator can use and it helps the administrators to understand how they can create policies with any required condition. The administrators can either use the same policy or modify it according to their requirements.

You can import the Sample Policy templates from the "**Getting Started page**" of the console. The Getting Started page is displayed initially when you install Privileged Account Manager. You can also open the Getting Started page from the home page of the console. When you import the template, all the sample policies are listed in the command control console.

IMPORTANT: If you have already defined some policies in the Command Control console, then importing these policies will overwrite those policies. The import of the sample template is helpful for the administrators who are creating policies for the first time.

To open the **Getting Started** page, perform the following:

1. (Conditional), If you are accessing the Manager for Privileged Account Manager for the first time, the first screen that gets displayed is the **Getting Started** page.
2. On the navigation path of the administration console, click ***User Name*** > **Getting started**.
   Here, User Name is the name that you use to login to the administration console of Privileged Account Manager.

Importing Sample Policy Templates

When you import Sample Policy template, the sample policies are added in the Command Control console. These policies are created with some specific conditions. The entities such as Account Group, Commands, and so on are also created with the policies. These entities are required to create the sample policies.

To import sample Policies, perform the following:

1. On the Getting started page, click **Import Sample Policy**.
2. Click **Import**.

   The Command Control console launches with all the sample policies in the Command Control pane.

Adding a Policy Template

The policy templates are available in the Command Control console and importing any of these templates, will display the policy in the Command Control pane. You can add specific policies by selecting the required Policy template from the Command Control console. These templates help in defining the policies for a specific action that can be performed on a Host server. The policies are displayed in a hierarchical structure. To add a policy at a specific location, select the location, then select the required Policy template. You can also change the order of the policy. For more information about changing the order refer, "Moving a Rule" on page 114. By default the policies are disabled. The administrator can customize the policy as per the requirement and enable the policy when it is placed in the correct order in the hierarchy.

To add a specific policy template, perform the following:

1. On the home page of the console, click **Command Control**.
2. On the Command Control pane click **Rules**.

   If you want to add a rule under a parent rule then, select that specific rule.
3. In the details pane, click **Add Policy Template** then, select the required policy from the drop-down list. For example, SSH Relay, RDP Relay, Oracle DB Session and so on.

   When adding a policy template, you can get the details of that policy in the description field when you import the policy.
4. Click **Import**.

   A policy is created with the specified template. The status and the information about the policy is displayed under **Status** in the details pane.

NOTE: ◆By default the new policy is dimmed. In the details pane, after you modify the policy with the required changes, you can enable this policy by deselecting the **Disable** checkbox and then clicking **Apply**.

- Single sample policy can be imported multiple times at any level in the hierarchy.

6 Managing Framework Users and Groups

Privileged Account Manager provides comprehensive user management facilities to control access to the Framework consoles. The admin user created when the Framework is initially installed belongs to the admin group, which has full access to all installed consoles and can perform all tasks. You can use this user account to create additional user accounts and groups through the Framework User Manager console, which is part of the Access Control module. Role-based authorization is used to determine which user groups can access specific consoles and perform specific tasks.

This section describes the following Framework User Manager tasks:

- "Managing Users" on page 57
- "Managing Groups" on page 70
- "Deploying the Access Control Module" on page 78
- "Changing a Framework User's Password" on page 79
- "Assigning Framework Roles for LDAP Users" on page 79
- "Multi-Factor Authentication" on page 79

Managing Users

When you add a new user, the user cannot access any of the Framework consoles until the user is added to a group that contains a role allowing the appropriate access. For example, if you want a user to be able to access only the Compliance Auditor console, you must create a group and configure the appropriate Compliance Auditor roles, then create the user and add the user to the group.

You can create additional users with the same access as the admin user by adding them to the admin group, or create your own group with access to all modules and roles. You can also configure these additional users to be superusers. Only users who belong to a group with the "super" role can view and administer superusers.

- "Configuring Account Settings" on page 58
- "Adding a Framework User" on page 59
- "Modifying a Framework User" on page 60
- "Removing a Framework User Group from a User" on page 69
- "Deleting a Framework User" on page 70

Configuring Account Settings

The **Account Settings** option allows you to set the default values for user settings such as minimum password length. When you add a new user, these default settings apply, but they can be overridden for individual users by modifying the individual account settings.

1. Click **Framework User Manager** on the home page of the console.
2. Select **Options**, and then click **Account Settings** in the **Users** task pane.
3. Configure the following account options:

   Inactivity Timeout (Minutes): Specify the number of minutes that users can be inactive before logging them out of the Framework Manager console.

   Account Lockout: Specify the number of times a user can enter the wrong password before being locked out. You can re-enable the user's account by using the **Edit User** option and clearing the **Disabled** check box. You can reset the user's password by using the **Edit User** option.

   Inactive Days (Disable): Specify the number of days that a user's account can be inactive before it is disabled. You can reactivate the user's account by using the **Edit User** option and using the **Reactivate** account check box in the **Account** section.

   Inactive Days (Delete): Specify the number of days a user's account can be inactive before it is deleted.

   Display Last Logon: Specify when the **Last Logon** box is displayed during a Framework login. The options are **After Failure**, **Never**, or **Always**.

   Authentication Domain: Specify a configured privileged resource. Privileged resources are configured through **Credential Vault**. Valid authentication domains can be configured to validate against NetIQ eDirectory or Microsoft Active Directory. Authentication Domains are used for External Groups within Command Control, or for authentication to the RDP Relay Console.

   Password Lifetime (Days): Specify the number of days a user's password can be used before it expires and the user is prompted to change the password.

   Minimum Password Length: Specify the minimum number of characters that must be used in a user's password.

   Password History: Specify the number of unique passwords that a user must use before being allowed to reuse an old password.

   Minimum Alpha: Specify the minimum number of alphabetic characters that must be used in a user's password.

   Minimum Numerics: Specify the minimum number of numeric characters that must be used in a user's password.

   Cache Native Passwords: Enable this option if you want the Framework Manager passwords updated with LDAP passwords. When you set up a mapping for users with an LDAP server, the Framework Manager password is updated to match the LDAP password with each successful login. (For information on setting up an LDAP mapping, see "Modify User: Native Maps" on page 64.)

   If a user never successfully logs into the LDAP server, the local password is never updated, and the user can use the local Framework Manager password to log in.

   If this option is disabled, the local Framework Manager passwords are never updated with the LDAP passwords. Users can attempt an LDAP login, and if that fails, they can log in locally with their Framework Manager passwords.

4 Configure the following help desk attributes.These attributes control the functionality of the Help Desk role and determine the actions that can be performed by a help desk user. For information about creating a group to use these attributes, see "Configuring a Help Desk Group" on page 71.

   Disabled: Allows the help desk user to enable and disable user accounts.

   Password: Allows the help desk user to change an existing password.

   Change at Next Login: Allows the help desk user to determine whether the user is forced to change the password on the next login.

   Last Changed: Displays the last time the password was changed and allows the help desk user to reset it to the current date and time.

   Bad Logons: Displays the number of bad logins and allows the help desk user to reset the count.

   Last Bad Logon: Displays the time and date of the last bad login and allows the help desk user to reset it to the current date and time.

   Last Logon: Displays the last successful login of the user and allows the help desk user to reactivate the account.

   Group Membership: Allows the help desk user to assign the user to non-administrative accounts.

5 Click **Finish**.

Adding a Framework User

When you add a new Framework user:

- The user's account is set up according to the default values defined in the **Account Settings** option. You can change these settings for individual users by using the **Edit User** option.
- The user's password is set to expire immediately so he or she is prompted to change it on the first login to the Framework Manager console. You can change this setting for individual users by using the **Edit User** option.
- The user cannot access any of the Framework consoles until you have added the user to a group with the required roles defined. For more information, see "Modifying a Framework User" on page 60 and "Configuring Roles" on page 72.

To add a new Framework user:

1 Click **Framework User Manager** on the home page of the console.

2 Click **Create** in the **Users** task pane.

3 In the **Add New User** pane, specify a name for the user in the **Username** field and a password for the user in the **Password** field.

   The password must comply with the default account settings for the Framework.

4 Click **Add <user name>**.

5 To configure additional settings for the user's account, continue with "Modifying a Framework User" on page 60.

Modifying a Framework User

The **Edit User** option allows you to override the default account settings for an individual user, and also provides a number of additional configuration settings and tasks, including resetting a user's password and assigning a user to a group.

To modify a Framework user account:

1. Click **Framework User Manager** on the home page of the console.
2. In the **Users** pane, select the user you want to modify.
3. Click **Edit** in the **User Information** task pane.
4. Change the settings as required:

   Disable Account: Select this option to disable the user's account.

   Comment: Specify a short comment in the text box.

   Description: Specify a detailed description in the text box.
5. To configure additional options, click **Edit** and select the section in the **Edit User: <user name>** pane:

   Password: Allows you to reset the user's password and configure other password settings. For specific instructions and additional options, see "Modify User: Password" on page 61.

   Password Validation: Allows you to define the minimum number of alphabetic and numeric characters required in the user's password. For specific instructions and additional options, see "Modify User: Password Validation" on page 61.

   Account: Allows you to configure the user as a superuser, provides information about the user's account, and provides other account configuration options. For specific instructions and additional options, see "Modify User: Account" on page 62.

   Account Details: Allows you to enter personal information for the user, including Staff ID and contact details. For specific instructions and additional options, see "Modify User: Account Details" on page 63.

   Host Access Control: Allows you to control where the user can access the console from. For specific instructions and additional options, see "Modify User: Host Access Control" on page 63.

   Native Maps: Allows you to map the Framework user account to a user account on a UNIX platform or on an LDAP server. For specific instructions and additional options, see "Modify User: Native Maps" on page 64.

   Sign in Script: Allows you to define a Perl sign in script for the user. For specific instructions and additional options, see "Modify User: Signin Script" on page 66.

   Authentication Script: Allows you to enable additional authentication apart from the default password authentication. For specific instructions and additional options, see "Modify User: Authentication Script" on page 66.

   Groups: Allows you to add the user to one or more groups. For specific instructions and additional options, see "Modify User: Groups" on page 69.
6. When you have completed your changes, click **Update**.

Modify User: Password

To set password options for a Framework user:

1. Click **Framework User Manager** on the home page of the console.
2. Select the user account you want to modify, and click **Edit** in the **User Information** pane.
3. Click **Password**.
4. Change the options as desired:

   Password: To reset the user's password, type the new password and retype it in the **Confirm Password** field.

   NOTE: The password must comply with the default account settings for the Framework, and comply with individual user settings defined by using this option and the **Password Validation** option.

   Change at Next Signin: Select the **Change at Next Signin** check box to expire the user's current password immediately, forcing the user to change it on the next login.

   Last Changed: Indicates when the password was last changed by the user, or, if the password has not yet been changed by the user, indicates when the user and password were created.

   Reset Password Age: Select the **Reset password age** check box to reset the age of the password to zero. The user can use the password for the full number of days defined in **Password lifetime (days)** (see "Configuring Account Settings" on page 58), or in the **Maximum age** field if it has been configured.

   Minimum Length: Override the default account settings by specifying the minimum number of characters you require in a user's password.

   Maximum Age: Override the default account settings by specifying the number of days before a user's password expires, prompting the user to change the password.

   History: Override the default account settings by specifying the number of unique passwords that a user must use before being allowed to reuse an old password.
5. Click **Update** or select another option.

Modify User: Password Validation

To set password validation options for a Framework user:

1. Click **Framework User Manager** on the home page of the console.
2. Select the user account you want to modify, and click **Edit** in the **User Information** pane.
3. Click **Password Validation**.
4. To override the default account settings for this user, select the appropriate check box and set the required values as follows:

   Min Alpha Characters: Specify the minimum number of alphabetic characters you require in the user's password.

   Min Numeric Characters: Specify the minimum number of numeric characters you require in the user's password.
5. Click **Update** or select another option.

Modify User: Account

To set account options for a Framework user:

1. Click **Framework User Manager** on the home page of the console.
2. Select the user account you want to modify, and click **Edit** in the **User Information** pane.
3. Click **Account**.
4. Change the options as required:

   Super user: Select this check box to make this user a superuser.

   Disable account: Select this check box to disable this user account.

   NOTE: The **Super user** and **Disable account** options are available only if you are logged in as a superuser. Superusers can be viewed and administered only by users belonging to a group with the super role defined for the auth module.

   Comment: Add comment about the user account.

   Last Bad Logon: The last time the user failed to log on successfully.

   Last Logon: Indicates when the user last logged in to the Framework Manager console.

   Reactivate Account: Select the **Reactivate account** check box to re-enable a user's account that has been locked through bad logons.

   Disable Inactive Days: Override the default account settings by specifying the number of days the user's account can be inactive before it is disabled. You can reactivate the user's account by using the **Reactivate** account option described above.

   Delete Inactive Days: Override the default account settings by specifying the number of days the user's account can be inactive before it is deleted.

   Inactivity Logout Mins: Override the default account settings by specifying the number of minutes the user can be inactive before the user is logged out of the Framework Manager console.

   Bad Logons: The number of times the user has failed to log on successfully since the last successful logon.

   Reset Bad Logon Count: Resets the number of unsuccessful logons to zero.

   Lockout: Override the default account settings by specifying the number of times the user can enter the wrong password before being locked out. You can re-enable the user's account by clearing the **Disabled** check box in the main **Modify User** section. You can reset the user's password in the **Password** section.

   Message of the day: Override the default account settings by specifying a message to be displayed to the user after a successful logon.

   Description: add a description about the user account.
5. Click **Update** or select another option.

Modify User: Account Details

To set personal account details for a Framework user:

1. Click **Framework User Manager** on the home page of the console.
2. Select the user account you want to modify, and click **Edit** in the **User Information** pane.
3. Click **Account Details**.
4. To set the following options, select the appropriate check box and specify the text:

   Staff ID: Specify the user's staff ID, for example, the user's unique company identifier.

   Display Name: Specify a display name for the user, for example, the user's full name. If a name is defined here it can be automatically entered as the **Manager Name** in Account Group and User Group definitions for Command Control by selecting the manager's Framework user name (see "Modifying an Account Group" on page 120 and "Modifying a User Group" on page 117). It can also be used in Compliance Auditor reports (see "Adding, Copying and Modifying an Audit Report" on page 158).

   Email Address: Specify the user's e-mail address. If an e-mail address is defined here, it can also be used in Command Control (see "Modifying an Account Group" on page 120 and "Modifying a User Group" on page 117) and in the Compliance Auditor (see "Adding, Copying and Modifying an Audit Report" on page 158).

   Telephone Number: Specify the user's telephone number. If a telephone number is defined here, it can also be used in Command Control (see "Modifying an Account Group" on page 120 and "Modifying a User Group" on page 117) and in the Compliance Auditor (see "Adding, Copying and Modifying an Audit Report" on page 158).
5. Click **Update** or select another option.

Modify User: Host Access Control

You can control where the user can access a Framework Manager console from by defining a list of ports and hosts to which access is allowed, or a list of ports and hosts to which access is denied.

If you make no entries for this option, access is allowed from any location.

To control where the user can access the Framework Manager console from:

1. Click **Framework User Manager** on the home page of the console.
2. Select the user account you want to modify, and click **Edit** in the **User Information** pane.
3. Click **Host Access Control**.
4. (Optional) Define a list of locations from where the user is allowed to access the console, and deny access from all other locations:

   4a If auditing is required, select the **Auditing** check box and use the drop-down list to select the events you want to be audited.

   4b Select the **Host Access** check box.

   4c Click the **Add** button below the **Host Access** list.

   4d In the **Port Range** column, specify the required port number or range of port numbers. The following entries are allowed:

*	All ports
port	A single port, such as 80
port-port	A range of ports, such as 20-30
svcname	Resolves a service name to its port, such as HTTP

4e In the **Host/IP Subnet** column, specify the required host definition. The following entries are allowed:

*	All hosts
ip address	A full IP address, such as 192.168.1.1
ip address-ip address	A range of IP addresses, such as 192.168.1.1-192.168.1.12
part ip address	Part of an IP address, such as 192.168.1
network/netmask	A network/netmask pair, such as 192.168.1.0/255.255.255.0
network/nnn CIDR	A network/nnn CIDR, such as 192.168.11.0/24
hostname	A hostname, such as dellsrv1.netiq.com
domain	A domain name, such as *.netiq.com

4f In the **Allow** column, click the check box.

4g Repeat Step 4c through Step 4e for any other required location definitions.

5 (Optional) Define a list of locations from which the user is denied access to the console, and allow access from all other locations:

5a If auditing is required, select the **Auditing** check box and use the drop-down list to select the events you want to be audited.

5b Select the **Host Access** check box.

5c Click the **Add** button below the Host Access list.

5d Specify the desired locations as described in Step 4d and Step 4e above.

5e To make this a deny entry, make sure the check box is not selected in the **Allow** column.

5f Repeat steps Step 5c and Step 5e for any other required location definitions.

6 Click **Update** or select another option.

Modify User: Native Maps

The **Native Maps** option allows you to map Framework User accounts to UNIX or Linux accounts and to LDAP accounts.

- "UNIX or Linux Account Mapping" on page 65
- "LDAP Account Mapping" on page 65

UNIX or Linux Account Mapping

The Privileged Account Manager Framework provides the ability to perform a number of functions from the command line. When using the command line, you are required to authenticate to the Framework. For example, the following command returns the status of all agents:

```
/opt/netiq/npum/sbin/unifi -u admin regclnt status -a
```

The command contains a switch for the username (`-u admin`). When the command is executed, the user is prompted for a password.

You can use the **Native Maps** option to map a platform system user to a Privileged Account Manager account.If you use an additional switch in the command line call, you are no longer required to provide authentication. A user with a native map can enter the following command:

```
/opt/netiq/npum/sbin/unifi -n regclnt status -a
```

The native map plus the `-n` switch allows the command to be executed without prompting the user for a name or a password.

To add a native map for a UNIX or Linux user:

1. Click **Framework User Manager** on the home page of the console.
2. Select the user account you want to modify, and click **Edit** in the **User Information** pane.
3. Click **Native Maps**.
4. Click **Add**.
5. In the **User** column, specify the user's name for the UNIX or Linux platform.
6. In the **Host** column, select the hostname for the UNIX or Linux platform.
7. Repeat Step 4 through Step 6 for any additional maps you require.
8. To edit a native map, select it and make the required changes.
9. To remove a native map, select it and click **Remove**.
10. Click **Update** or select another option.

LDAP Account Mapping

Native maps can be used to allow Framework Manager users to obtain their authentication credentials from an LDAP server. This allows the LDAP server to remain the authoritative source for user credentials and active accounts. If you want LDAP mapped users to be able to log in when the LDAP server is not available, see the **Cache native passwords** option in "Configuring Account Settings" on page 58.

To configure an LDAP mapping:

1. Click **Framework User Manager** on the home page of the console.
2. Select the user account you want to modify, and click **Edit** in the **User Information** pane.
3. Click **Native Maps**.
4. Click **Add**.
5. In the **User** column, specify the user's fully qualified distinguished name. For example:

   ```
   cn=plou,ou=development,o=netiq
   ```

6 In the **Host** column, specify the scheme (`ldap` or `ldaps`) and IP address of the LDAP server. Specify a port only if the LDAP server is not using the standard port for the scheme. For example:

```
ldaps://10.10.16.165
ldaps://10.10.16.166:736
```

7 Click **Update** or select another option.

Modify User: Signin Script

You can assign a Perl script to a user to be run when the user logs on to the Framework Manager console. For example, you could assign a script that causes an e-mail to be sent to a manager when the user logs on.

1 Click **Framework User Manager** on the home page of the console.

2 Select the user account you want to modify, and click **Edit** in the **User Information** pane.

3 Click **Signin Script**.

4 Specify the logon script you require for this user. You can type the script or paste it from another document.

5 Click **Update** or select another option.

Modify User: Authentication Script

Two factor authentication is required to enhance the security and to ensure the identity of the user is valid. Any framework user has to enter the secondary password to log in to the Privileged Account Manager Administration Console. To enable two factor authentication:

1 Click **Framework User Manager** on the home page of the console.

2 Select the user account you want to modify, and click **Edit** in the **User Information** pane.

3 Click **Authentication Script**.

4 Add the following script based on your requirement:

Script to Prompt the Secondary Password in the Hidden Mode

```
my $module = $args->child("Args")->child("Module");
my $http_req = $args->child("Args")->child("http_req");

#RDPRelay Checks
if($http_req && ($http_req->child()->arg("HTTP_REFERER") =~ m/rdprelay/
) )  {
  return 0;
}

#myaccess Checks
if($http_req && ($http_req->child()->arg("HTTP_REFERER") =~ m/myaccess/
) )  {
  return 0;
}

#Non Admin Module Checks
if($$module && ($module->arg("name") ne "admin")) {
```

```
  return 0;
}

my $exauth = get_msgs($args);
if($exauth) {
    my $pwd=$exauth->arg("imsg");
    if($pwd && $pwd eq "letmein") {
        return 0;
    } else {
        return -1;
    }
} else {
    add_conv($args,"Enter your Secondary Password in the below Text Box
and Press on 'Finish' Button", 1);
    return 1;
}
```

Script to Prompt the Secondary Password and Display It

```
my $module = $args->child("Args")->child("Module");
my $http_req = $args->child("Args")->child("http_req");

#RDPRelay Checks
if($http_req && ($http_req->child()->arg("HTTP_REFERER") =~ m/rdprelay/
) )  {
  return 0;
}

#myaccess Checks
if($http_req && ($http_req->child()->arg("HTTP_REFERER") =~ m/myaccess/
) )  {
  return 0;
}

#Non Admin Module Checks
if($$module && ($module->arg("name") ne "admin")) {
  return 0;
}

my $exauth = get_msgs($args);
if($exauth) {
    my $pwd=$exauth->arg("imsg");
    if($pwd && $pwd eq "letmein") {
        return 0;
    } else {
        return -1;
    }
} else {
    add_conv($args,"Enter your Secondary Password in the below Text Box
and Press on 'Finish' Button", 0);
    return 1;
}
```

Show the Configured Message After Primary Login

```
my $module = $args->child("Args")->child("Module");
my $http_req = $args->child("Args")->child("http_req");

#RDPRelay Checks
if($http_req && ($http_req->child()->arg("HTTP_REFERER") =~ m/rdprelay/
) )  {
  return 0;
}

#myaccess Checks
if($http_req && ($http_req->child()->arg("HTTP_REFERER") =~ m/myaccess/
) )  {
  return 0;
}

#Non Admin Module Checks
if($$module && ($module->arg("name") ne "admin")) {
  return 0;
}

my $exauth = get_msgs($args);
if($exauth) {
        return 0;
} else {
    add_msg($args, "Message from Administrator : Click on OK to Login");
    return 1;
}
```

Combination of all the Previous Scripts

```
my $module = $args->child("Args")->child("Module");
my $http_req = $args->child("Args")->child("http_req");

#RDPRelay Checks
if($http_req && ($http_req->child()->arg("HTTP_REFERER") =~ m/rdprelay/
) )  {
  return 0;
}

#myaccess Checks
if($http_req && ($http_req->child()->arg("HTTP_REFERER") =~ m/myaccess/
) )  {
  return 0;
}


#Non Admin Module Checks
if($$module && ($module->arg("name") ne "admin")) {
  return 0;
}

my @exauth = get_msgs($args);
if($#exauth > 0) {
    my $pwd=$exauth[0]->arg("imsg");
    my $inp=$exauth[2]->arg("imsg");
```

```
        # Second Password is - letmein
        # Third Password is - 123

        if($pwd && $pwd eq "letmein" && $inp && $inp eq "123") {
             return 0;
         } else {
             #(Show the message if any or both the passwords are wrong)
             $eval_rsp->arg('message', "Admin Message : Wrong Password!!!");

             return -1;
         }
    } else {
        #(Ask for input as password)
        add_conv($args, "Enter your Secondary Password", 1);

        #(Show the message with 'OK')
        add_msg($args, "Click on OK");

        #(Ask for input as clear text)
        add_conv($args, "Enter your Third Password", 0);

        return 1;
    }
```

5 Click **Update** or select another option.

Modify User: Groups

To assign a Framework user to one or more groups:

1 Click **Framework User Manager** on the home page of the console.

2 Select the user account you want to modify, and click **Edit** in the **User Information** pane.

3 Click **Groups**.

4 Select the check boxes for the groups you want this user to belong to.

5 Click **Finish**.

You can also assign a user to a group by using the **Modify Group** option, by dragging and dropping the user to the group, or by dragging and dropping the group onto the user.

You can remove a user from a group by deselecting the check box for the required group. See "Removing a Framework User Group from a User" on page 69 for other methods.

Removing a Framework User Group from a User

There are several ways of removing a Framework user group from a Framework user's account. You can modify the user, modify the group, or use the objects in the navigation pane.

1 Click **Framework User Manager** on the home page of the console.

2 Select the group you want to remove from the user's account.

3 In the right pane, select the user.

4 Click **Remove User** in the task pane. The user is removed.

Deleting a Framework User

1. Click **Framework User Manager** on the home page of the console.
2. In the **Users** task pane, select the user you want to delete.
3. Click **Delete** in the **User Information** task pane.
4. Click **Finish** to confirm the deletion.

Managing Groups

Framework users must be assigned to one or more groups with the appropriate roles defined before they can access any Framework consoles or perform any tasks.

- "Adding a Framework User Group" on page 70
- "Modifying a Framework User Group" on page 70
- "Configuring a Help Desk Group" on page 71
- "Configuring Roles" on page 72
- "Deleting a Framework User Group" on page 77

Adding a Framework User Group

1. Click **Framework User Manager** on the home page of the console.
2. Click **Create** in the **Groups** task pane.
3. Specify a name for the group in the **Add New Group** task pane.
4. Click **Create <group name>**.
5. To configure the group, continue with "Modifying a Framework User Group" on page 70.

Modifying a Framework User Group

Modifying a user group allows you to:

- Add a comment describing the group
- Add users and subgroups to the group
- Define administrative roles for the group
- Specify an audit manager for the group.

To modify a Framework user group :

1. Click **Framework User Manager** on the home page of the console.
2. In the **Groups** pane, select the group you want to modify.
3. Click **Edit** in the **Group Information** task pane.
4. (Optional) In the **Comment** field, enter a comment.
5. In the **Members** section, select the users you want to be members of this group.

   You can also add a user to groups in the **Groups** section of the **Edit User** option, by dragging and dropping the user onto the group, or by dragging and dropping the group onto the user.

You can remove users from the group by deselecting them here. See "Removing a Framework User Group from a User" on page 69 for other methods.

6 In the **Sub Groups** section, select the groups you want to be subgroups of this group.

   You can also add subgroups to groups by dragging and dropping the group onto the main group.

7 In the **Roles** section, configure the roles you require for this group of users according to the consoles you want them to be able to access and the tasks you want them to be able to perform. You must assign at least one role. See "Configuring Roles" on page 72 for more details.

8 In the **Audit Manager** section, specify the details of the group's manager.

9 In the **Secondary Authentication** section, select **Bypass Secondary Authentication** option if you have enabled secondary authentication for the Administration Console and want to bypass it. See "Enabling Advanced Authentication for Administration Console" on page 301 for more details.

10 In the **LDAP Group Maps** section, add the Microsoft Active Directory, NetIQ eDirectory, and OpenLDAP groups.

   NOTE: To configure **LDAP Group Maps**, first, go to **Account Settings** and select the **Authentication Domain**.

   See "Assigning Framework Roles for LDAP Users" on page 79 for more details.

11 Click **Update**.

Configuring a Help Desk Group

The help desk role allows a predefined set of attributes to be set on the Account Settings page so that users assigned to the help desk group can only manage the subset of user attributes.

To set up a help desk group:

1 Configure the attributes:

   1a Click **Framework User Manager** on the home page of the console.

   1b Click **Account Settings** in the **Users** task pane.

   1c Configure the **Helpdesk Attributes**.

      For information about these attributes, see "Configuring Account Settings" on page 58.

   1d Click **Finish**.

2 Create the group:

   2a Click **Create** in the **Groups** task pane.

   2b Specify a name for the group, then click **Create <group name>**.

   2c Select the group you just created, then click **Edit**.

   2d In the **Members** option, select the users that you want to belong to the help desk group.

2e In the **Roles** option, click **Add**, then add the following roles:

Module	Role
auth	console
auth	read
auth	helpdesk

3 Click **Update**.

Configuring Roles

When you create a new Framework user group, you must assign at least one role to the group to allow the users in the group to access one or more Framework modules and perform tasks.

To allow access to all modules and tasks, you can define a role with Module set to * and Role set to *. This is how the default admin group containing the default admin user is initially configured.

To allow access only to specific modules and tasks, use the **Modify Group** option (see "Modifying a Framework User Group" on page 70) and define one or more roles according to the tables below:

- "Access Dashboard Roles" on page 72
- "Reporting Roles" on page 73
- "Command Control Roles" on page 74
- "Compliance Auditor Roles" on page 75
- "Credential Vault Roles" on page 75
- "Framework User Manager Roles" on page 76
- "Hosts Roles" on page 76
- "Package Manager Roles" on page 77

Access Dashboard Roles

The following roles can be assigned to control access to the Access Dashboard console. Select from the following roles when you are creating a group to manage the Access Dashboard.

Module	Role	Allows users to
userreqdashboard	console	View the Access Dashboard console.
	admin	View and update emergency access and credential checkout requests.
	*	Perform all roles.

Reporting Roles

The following roles can be assigned to the auditing module in order to control access to the Reporting console. Select from these roles when you are setting up a group to manage the command control reports.

Module	Role	Allows users to
audit	console	View the Reporting console.
	read	Read the audit database.
		You must use `console` along with `read` role to view the Reporting console and its content.
	admin	Modify reporting settings.
	command	View Command Control reports.
	logon	View Account Logon reports.
	*	Perform all roles.
	write	Create new audit reports and adjust filter settings.
	report	Access reports with the report defined roles.
	<report defined>	Read and update the reports defined in the **General** tab of the Reporting console.
		This role is only useful when used in conjunction with the report role.

You can use these Audit Report roles to create the following types of audit managers:

- **Administrator:** To allow the group to update all aspects of the auditing module, including encryption and rollover, the group needs to be assigned the following roles for the audit module:

  admin
  write
  read
  command
  console

- **Manager:** To allow the group to update all aspects of the auditing module, except encryption and rollover, the group needs to be assigned the following roles for the audit module:

  write
  read
  command
  console

- **User:** To allow the group to read and update a specific report, the group needs to be assigned the following roles for the audit module:

  command

console

report

<report defined read>

<report defined update>

If you want the group to have read-only privileges to the report, do no assign the <report defined update> role. Users with read-only rights to a report can view the report from the console, view the keystroke sessions within the report, and select which audit databases to view (see the **LogFiles** tab). Users who also have the update right can update the report's filter, its name, and its description.

Each report allows you to specify a read role and an update role. You need to remember those names and manually enter them here. The console does not provide any error checking, so you need to make sure to enter the correct name. For information on how to enable a report for a role, see "Modifying General Report Information" on page 89.

Command Control Roles

The following roles can be assigned to the command control module in order to control access to the Command Control console. Select from the following roles when you are creating a group that you want to manage and test the rules in the command control database.

Module	Role	Allows users to
cmdctrl	console	View the Command Control console.
	read	View the Command Control console content and run test suites. You must use `console` role along with `read` role to view the Command Control console and its content.
	write	Modify the command control database. Users with this role cannot cancel other users' transactions or modify audit or transaction settings. Must be used in conjunction with the cmdctrl read role.
	admin	Modify the Command Control database, including canceling other users' transactions and modifying audit and transaction settings.
	*	Perform all roles.
auth	read	Extract user credentials, including name and e-mail address, from the auth database into the account and user group definitions. Used in conjunction with the cmdctrl write (with read) and admin roles.
prvcrdvlt	read	Configure the resources and credentials in the command control rules.

Compliance Auditor Roles

The following roles can be assigned to the compliance auditing module in order to control access to the Compliance Auditor console. For a group to manage compliance auditing, the group also needs read roles to the auditing and authentication modules.

Module	Role	Allows users to
secaudit	console	View the Compliance Auditor console.
	audit	View and edit records.
	admin	Add and modify audit rules.
	*	Perform the console, audit, and admin roles.
	<audit role name >	Access the records collected by audit rules with this role defined in the **Audit Role** field on the Modify Audit Rule page. You can choose your own name for the role. See "Adding or Modifying an Audit Rule" on page 157 for details about configuring audit rules.
audit	read	View a keystroke replay.
auth	read	Extract user credentials, including name and e-mail address, from the auth database for use with reports.

Credential Vault Roles

The following roles can be assigned to the credential vault module in order to control access to the Credential Vault console. Select from the following roles when you are creating a group to manage the Credential Vault.

Module	Role	Allows users to
prvcrdvlt	console	View the Credential Vault console.
	read	View the resources and credentials in Credential Vault. You must use `console` role along with `read` role to view the Credential Vault console and its content.
	write	Add and modify the resources and credentials in Credential Vault. Must be used in conjunction with the prvcrdvlt read role.
	admin	View, add, and modify the domains and credentials in Credential Vault.
	*	Perform all roles.

Framework User Manager Roles

The following roles can be assigned to the authentication module in order to control access to the Framework User Manager console. Select from these roles when you are setting up a group to manage Framework Manager users and groups.

Module	Role	Allows users to
auth	console	View the Framework User Manager console.
	act_settings	Modify account settings.
	admin	Add or delete users and groups, and assign users to groups.
	helpdesk	Modify the user account settings. To change which attributes are available for modification, see "Configuring Account Settings" on page 58. For information on how to use this role to create a Help Desk group that can manage user passwords, see "Configuring a Help Desk Group" on page 71.
	read	Read the auth database. You must use `console` role along with `read` role to view the Framework User Manager and its content. This role must be used with all other auth roles.
	role_admin	Add or remove roles.
	super	View and modify superusers, and view and modify groups with the super role defined.
	api_token	Generate API tokens.
	*	Perform all roles.

Hosts Roles

The following roles can be assigned to the host module in order to control access to the Hosts console. Select from the following roles when creating a group to manage the hosts.

Module	Role	Allows users to
unifi	console	View the Hosts console.
	info	Run the host status check by using the command line interface. You must type the word `info` because it is not available in the drop-down list.
	admin	View the Hosts console and perform administrative actions.

Package Manager Roles

The following role can be assigned to the package manager module in order to control access to the Package Manager console. When you are creating a group that you want to manage the distribution of updates to Privileged Account Manager, select the following:

Module	Role	Allows users to
pkgman	console	View the Package Manager console.
	admin	View, add, update, or remove packages.

Distribution Roles

The following roles can be assigned to the distribution module in order to restrict the installation and deployment of certain packages.

Module	Role	Allows users to
distrib	acl	Restricts deployment of packages to specified modules.
	Module:rexec	Install or patch the Command Control Agent (rexec).
	Module:distrib	Install or patch the Distribution Agent (distrib).
	Module:regclnt	Install or patch the Registry Agent (reglcnt).
	Module:strfwd	Install or patch the Store and Forward Agent (strfwd).
	Module:sysinfo	Install or patch the System Information Agent (sysinfo).

All modules can be allowed by following the above configuration of Module:<desired-package-name>.

Deleting a Framework User Group

1. Click **Framework User Manager** on the home page of the console.
2. In the **Groups** pane, select the group you want to delete.
3. Click **Delete** in the **Group Information** task pane.
4. Click **Finish** to confirm the deletion.

Deploying the Access Control Module

When you install Privileged Account Manager, the Framework User Manager console is installed with the other required modules. If you want to manage Framework users from other hosts, you need to deploy the Access Control modules on these hosts. You should always have at least one host that contains a backup of this console.

The Access Control module consists of the following packages:

- **Access Manager (auth):** Holds the Framework user account information and controls access to the Framework modules.
- **Access Control Console:** Required for configuring Framework users and groups. It is installed into the Framework Manager console as the **Framework User Manager** console.

The Access Control module has the following dependencies:

- The Access Manager package is shown as an available package only on hosts that have the Registry Manager (registry) package installed.
- The Access Control Console can only be deployed on hosts that have the Administration Manager (admin) package installed.

To deploy the Access Control modules on another host:

1. Download the following packages to your local Package Manager:
   - Access Manager
   - Access Control Console
   - Registry Manager
   - Administration Manager

   See "Publishing Packages on the Package Manager" on page 313 for details.
2. Install the Registry Manager on the host you want to be the Access Manager, then install the Access Manager on the same host.

   This can be on any operating system, including Windows*. See "Installing Packages on a Host" on page 39 for details. The packages can be deployed to as many hosts as you need in order to build an environment with load balancing and failover.
3. Install the Administration Manager on the same host or a different host.

   It can be deployed to as many hosts as you need in order to build an environment with load balancing and failover.

The Access Control module is now deployed and ready to use.

Changing a Framework User's Password

Framework users can change their own passwords by using the **Change Password** option, which is always available in the task pane. If a Framework user belongs to a group with the appropriate auth role defined (see "Configuring Roles" on page 72), they can also change other users' passwords by using the **Modify User** option.

To change your own password:

1. Click **admin**>**Change Password** in the navigation bar.
   Here, admin is the user name that is used to log in to the administration console of the Privileged Account Manager. This name will change depending on the user name that you define.
2. In the **Old Password** field, specify your current password.
3. In the **New Password** field, specify your new password and confirm it in the **Confirm Password** field.

   Your password must comply with the default **Account Settings** for the Framework, and comply with individual user settings defined by using the **Edit User** option.
4. Click **Ok**.

Assigning Framework Roles for LDAP Users

LDAP users (Microsoft Active Directory, NetIQ eDirectory, or OpenLDAP) can get administration privileges on PAM framework through their LDAP group membership. To achieve this, map the LDAP groups of the LDAP users to the Framework groups in the PAM Administration Console. Assign the roles configured in the Framework group to the logged-in LDAP users, based on their group membership in the LDAP server.

Configure an Identity Manager Active Directory or LDAP driver with the LDAP group membership entitlements to provision the roles for LDAP users by mapping those LDAP groups in the PAM framework.

For more information on mapping, refer to Step 10 on page 71 in "Modifying a Framework User Group" on page 70.

NOTE: This feature is not supported for Advanced Authentication users.

Multi-Factor Authentication

This section describes the following Multi-Factor Authentication (MFA) options:

- "Advanced Authentication" on page 80
- "RADIUS Server" on page 80

Advanced Authentication

Privileged Account Manager integrates with the Advanced Authentication application to secure and control the access to privileged endpoints using the multi-factor authentication methods.

For more information, see Chapter 24, “Integrating Privileged Account Manager with Advanced Authentication,” on page 295.

RADIUS Server

You must specify the details of the Remote Authentication Dial-In User Service (RADIUS) server in Privileged Account Manager to authenticate users with a third-party RADIUS server.

Prerequisite

- On Linux, publish and install the `radiusagnt` package to enable the RADIUS Server configuration.

  NOTE: The `radiusagnt` package cannot be installed on a Windows manager. If you have a Windows only PAM manager environment, you will need to add a backup PAM Linux manager to your deployment.

- If Advanced Authentication is configured and you want to configure PAM for RADIUS, ensure that you delete Advanced Authentication configuration from **Options** page.

Configuring a RADIUS Server

To configure the RADIUS server details, perform the following:

1. On the Home page of the Administration Console, click **Framework User Manager**.
2. Select **Options**, and then click **RADIUS Server Configuration**.
3. In the right pane, specify the RADIUS server configuration details:
   - **Host**: Specify the hostname or IP address of the RADIUS server.
   - **Port**: Specify the port where the RADIUS authentication request is sent. The default port is 1812.
   - **Secret**: Specify the shared secret between the RADIUS server and Privileged Account Manager where RADIUS Agent is installed.
   - **Timeout**: Specify the duration (in seconds) for which the RADIUS client should wait for the RADIUS server to reply. The default value is 15 seconds.
   - **Retry count**: Specify the number of times the RADIUS client should try to connect to the RADIUS server. The default value is set to 3. If set to 0, the RADIUS client does not try to connect after the first unsuccessful attempt.
4. Add the **RADIUS Dictionary Attributes**.

   For example, "NAS ID" attribute is named "NAS-Identifier" in the RADIUS Dictionary.

   For more information, see the FreeRADIUS 'man' pages and the FreeRADIUS dictionary.

NOTE: ◆You can modify the **RADIUS Dictionary Attributes** using the **Manage Attributes** option.

- RADIUS authentication functionality is available for logins but not for command control policy based authorization.

7 Managing Audit Reports

Privileged Account Manager enables auditing of events at several levels, such as keystroke logging, command authorization, and login success or failure. The Reporting console allows you to view these records and manage them.

- "Audit Settings" on page 83
- "Encryption Settings" on page 84
- "Syslog Settings" on page 84
- "Command Control Reports" on page 86
- "Video Capture" on page 91
- "Change Management" on page 99
- "Password Management" on page 100
- "Shared Key Management" on page 101

Audit Settings

Use this page to control the rollover of the audit database files. The default configuration does not encrypt or roll over the audit databases. If your security model requires you to keep audit records available for years, you need to configure the rollover options and move the rolled-over files to an archive location.

1. Click **Reporting** on the home page of the console.
2. Click **Audit Settings** in the task pane.
3. For each audit database file, set the rollover parameters. Rolled-over databases are kept as SQLite databases.

   Time (hours): Specify the time interval for rolling over the audit file. If the time interval is always reached before the maximum size is reached, the time interval is used for rollover and the size restriction is ignored.

   Size (MB): Specify the maximum size the file can reach before the audit file is rolled over. If the file always reaches the maximum size before the time interval is reached, the size restriction is used for rollover and the time interval is ignored.

   Protection: Select **None** to allow the rollover file to be an unencrypted file or select **Encrypted** to encrypt the audit database.

   When you select **Encrypted** to encrypt any database, ensure that the **NULL Cipher (clear text)** key is disabled at **Reporting > Encryption Settings**.

   Encrypting the file can impact performance of your audit managers. Also, the encrypted file can be decrypted by the Framework Console, but it cannot be displayed on new systems that do not know the encryption keys.

   To configure the encryption keys, click **Reporting** > **Encryption settings**.

4 If you want to zip the rollover files or move them to another location, use the **Rollover Script** option to specify a Perl script that can perform these tasks. The script is called whenever an audit database is rolled over.

   For example, the following script uses gzip to compress the rolled-over file and enters an error message in the `unifid.log` file.

```
if ($DBGRP eq 'cmdctrl') {
system("gzip $AUDIT_FILE");
$ctx->log_error("Audit rollover $DBGRP $AUDIT_FILE");
}
```

5 Click **Finish**.

Encryption Settings

Use this page to configure when the randomly generated encryption key is changed.

1 Click **Reporting** on the home page of the console.
2 Click **Encryption Settings** in the task pane.
3 To specify how frequently the key is changed, specify a **Key Rollover** interval, then select the type of interval (years, months, weeks, or days).
4 (Optional) In the **Key** list, disable or enable keys.

   Each time a new key is generated, it is added to the list.

   If you disable a previous key, Privileged Account Manager re-encrypts all database with the old key to the latest key. This can be very time-intensive and can affect performance until it is completed.

   If you disable the null cipher key, Privileged Account Manager encrypts all the databases, which has the **Protection** set to **Encrypted** in **Reporting > Audit Settings**, with the latest key. This can be very time-intensive and can affect performance until it is completed.

5 Click **Finish**.

Syslog Settings

Use this page to configure Privileged Account Manager so that it can send syslog messages to a syslog server. This server can be a Sentinel server, a Sentinel Log Manager, or a syslog server that supports TCP with optional TLS or SSL support. Older syslog servers require UDP for the transport protocol.

To configure communication with a syslog server:

1 Click **Reporting** on the home page of the console.
2 Click **Syslog Settings** in the task pane.
3 Configure the following fields:

   Syslog host: Specify the DNS name or IP address of the syslog server.

   Port: Specify the port the syslog server is listening on for syslog events. The default port is 514. The default port for a Sentinel server or a Sentinel Log Manager is 1468.

SSL: Select the check box to enable SSL communication with a Sentinel server. For a syslog server, do not select this box.

Allow Persistent Connections: Select the check box to enable a connection in which, a single connection provides multiple responses instead of opening a new connection for every single request and response.

Use Audit Zones: Select the check box to enable the audit manager in a audit zone to send the audit data to syslog emitter.

NOTE: To apply the changes made to the persistent connection, you must restart Privileged Account Manager.

---

4 In the Event table, select the events and the format. All possible events are select:

Session Failure: Sends an event when a Privileged Account Manager session fails.

Start Session: Sends an event when a user starts a Privileged Account Manager session on a host.

Session Terminate: Sends an event when a user logs out of the Privileged Account Manager session.

Command Audit: If you have enabled auditing on the user's session or on commands, this option sends all audited events as syslog events.

- For information on configuring commands for auditing, see "Configuring Auditing with the Rewrite Functionality" on page 126.
- For information on using a .profile file to enable session auditing, see "Complete Session Control Using pcksh" on page 211.

Privilege Escalation: Sends an event when a user starts a privileged session.

4a To delete an event, highlight it, then click **Remove**.

4b To configure the format, click the format text box and specify a format string.

The ${}$ string logs the complete string of the audit record in JSON format. For a Sentinel server, format string must be set to ${}$.

If you are sending the events to a syslog server, you can specify strings from the Privileged Account Manager templates. For example, the format of the Start Session event could use the following string:

```
User ${StartSession.user}$ initiated a Command Control session from
${StartSession.host}$
```

This format string would produce output similar to the following:

```
Jan 1 01:20:45 localhost npum: User ctaylor initiated a Command
Control session from citlaptop
```

5 Click **Finish**.

Sentinel Notes

For Privilege Account Manager to communicate with a Sentinel server, you need to add a Syslog Connector to the Sentinel console. You can download the Syslog Connector from the Sentinel Plug-ins website. This connector must be configured to listen on port TCP 514 using SSL and the SSL type must be Open. Configure it to listen specifically for the host that has the Syslog Emitter installed. This is usually the Framework Manager console.

Command Control Reports

After you have installed the Framework Manager, all command control requests have records automatically created in the audit database. The default Sample Report displays all of the collected audit records and any associated keystroke captures. In the Command Control Reporting console, you add reports that can be customized by using the **Filters** tab to display records according to your preferences. You can also assign custom roles to the report, which allows you to restrict the read and write access your Framework Manager users have to these reports.

- "Adding a Report" on page 86
- "Viewing Report Data" on page 87
- "Filtering the Viewable Records" on page 87
- "Modifying General Report Information" on page 89
- "Selecting Log Files" on page 89
- "Replaying Keystrokes" on page 90
- "Removing a Report" on page 90
- "Generating an Activity Report" on page 91
- "Viewing a Report in a Comma-separated Values (CSV) Format" on page 91

Adding a Report

1. Click **Reporting** on the home page of the console.
2. Click **Command Control Reports** in the navigation pane.
3. Click **Add Report** in the task pane.
4. Configure the following fields in the General tab:

   Report Name: Specify a name for the report.

   Description: (Optional) Describe the purpose of the report.

   Roles: Specify values if you want to allow users read access to this report and the ability to update specific information such as its name, description, and filters.

   - **Read:** To enable read access, specify a unique name for the read role for this report.
   - **Update:** To enable update rights, specify a unique name for the update role for this report.
5. Click **Filter** tab in the navigation pane.

   For understanding fields in the **Filter** tab, please refer to "Filtering the Viewable Records" on page 87
6. Click **Logfiles** tab in the navigation pane.

For understanding fields in the Logfiles tab, please refer to "Selecting Log Files" on page 89

7 Click **Finish**.

Viewing Report Data

1 Click **Reporting** on the home page of the console.

2 Click **Command Control Reports** in the navigation pane.

3 Select the report in the navigation pane.

The navigation pane displays the following information about each instance of the report.

Column	Description
Start Time	Displays the date and time when the report started. **NOTE:** It displays the session start time as set in the Manager.
End Time	Displays the date and time when the report ended.
User	Displays the name of the Framework user who issued the command.
Host	Displays the name of the host from which the command was issued.
RunAs	Displays the name of the user who ran the command.
RunHost	Displays the name of the host that the command was run on.
Command	Displays the command that was executed.
Authorized	Displays whether the rule for this command authorized the command.
Capture	Displays whether the rule for this command captured the keystrokes. If a keystroke is present, the **Keystroke Replay** option is available in the task pane.
Audit Status	If the record has been referenced in the Compliance Auditor, displays the name of the compliance rule and the status.
Audit ID	Displays the unique ID of the audit record.

Filtering the Viewable Records

Use the **Filter** tab to build a list of matching conditions that allows you to customize the records that are displayed in the **Report Data** tab. This allows you to build reports that show only the information that your users require.

1 Click **Reporting** on the home page of the console.

2 Click **Command Control Reports** in the navigation pane.

3 Select the report in the navigation pane.

4 Click the **Filter** tab in the navigation pane.

5 Select from the following conditions. You can combine conditions with AND logic, which requires the report to match all conditions that have been joined with an AND. You can also combine conditions with OR logic, which requires the report to match either the conditions before the OR or the conditions after the OR.

Authorized: Select this option to use session authorization by the Command Control as a matching criteria. Use the Yes/No drop-down list to specify whether the session matches when the session was authorized or not.

Session Capture: Select this option to use session capture as a matching criteria. Use the Yes/No drop-down list to specify whether the report matches when the session capture was authorized or not.

User: Select whether you want to match on the submitting user or the run user. For the matching type, select one of the following:

- Select **Matches** or **Doesn't Match**, then specify an exact value or a value with an asterisk (*) wildcard such as jo*.
- Select **Regexp** or **Doesn't Regexp**, then specify a regular expression.

User Domain: Select whether you want to match the domain on the native mapped user or the second factor authenticated user. For the matching type, select one of the following:

- Select **Matches** or **Doesn't Match**, then specify an exact value or a value with an asterisk (*) wildcard such as jo*.
- Select **Regexp** or **Doesn't Regexp**, then specify a regular expression.

Host: Select whether you want to match on the submitted host or the run host. For the matching type, select one of the following:

- Select **Matches** or **Doesn't Match**, then specify an exact value or a value with an asterisk (*) wildcard such as jo*.
- Select **Regexp** or **Doesn't Regexp**, then specify a regular expression.

Command: Select whether you want to match on the submitted command or the audited command. An audited command is a command that has been audited within a session capture. Audited commands are collected when the session used the pcksh shell with the audit option. For the matching type, select one of the following:

- Select **Matches** or **Doesn't Match**, then specify an exact value or a value with an asterisk (*) wildcard such as jo*.
- Select **Regexp** or **Doesn't Regexp**, then specify a regular expression.

Audit ID: Select to match the session on the audit ID assigned to the session. For the matching type, select one of the following:

- Select **Matches** or **Doesn't Match**, then specify an exact value or a value with an asterisk (*) wildcard such as 4bd*.
- Select **Regexp** or **Doesn't Regexp**, then specify a regular expression.

Time: Select to match the session on when it started or when it ended. Select either **Session Start** or **Session End**, select **After** or **Before** for the matching operator, then use the calendar to specify a date and use the time fields to specify the hour and minute.

Disconnect Type: Select to match based on the Disconnect Type of the session. For the matching type, select one of the following:

- Select **Matches** or **Doesn't Match**, then specify an exact value or a value with an asterisk (*) wildcard such as 4bd*.
- Select **Regexp** or **Doesn't Regexp**, then specify a regular expression.

(): Select to group conditions so that the record is displayed if it matches the conditions defined by one group in the filter.

6 Click **Apply**.

7 To view the results, click the **Report Data** tab.

Modifying General Report Information

Use the **General** tab to keep the report's name and description in sync with the configured filter and to restrict access to the report by assigning read and update roles.

1 Click **Reporting** on the home page of the console.

2 Click **Command Control Reports** in the navigation pane.

3 Select the report in the navigation pane.

4 Click the **General** tab in the navigation pane.

5 Modify the values of the following fields:

Report name: Specify a new name for the report.

Description: Describe the type of records that the report displays.

Roles: Specify values if you want to allow users read access to this report and the ability to update specific information such as its name, description, and filters.

- **Read:** To enable read access, specify a unique name for the read role for this report.
- **Update:** To enable update rights, specify a unique name for the update role for this report.

If you use the same name for a role on multiple reports, the role grants rights to multiple reports. If you use the same name for both the read role and the update role, the role grants both read and update rights.

To assign these roles to a group, see "Reporting Roles" on page 73.

6 To save your changes, click **Apply**, or to discard your changes, click **Reset**.

Selecting Log Files

Any rolled-over audit database is indexed by the Audit Manager. You use the **Log Files** tab to select which of these rolled-over databases is used to display information in the **Report Data** tab. This allows you to review archived data or current activity.

Only the audit databases currently in the audit directory view are displayed. If an audit database has been taken offline (zipped or moved), it does not appear in the list.

1 Click **Reporting** on the home page of the console.

2 Click **Command Control Reports** in the navigation pane.

3 Select the report in the navigation pane.

4 Click the **Log Files** tab in the navigation pane.

5 Select the log files that are required for the report.

   To include all available log files, select the **All log files** box.

6 Click **Apply**.

Replaying Keystrokes

Where a rule has been configured to capture session information, you can review the entire session in the report.

1 Click **Reporting** on the home page of the console.

2 Click **Command Control Reports** in the navigation pane.

3 Select the report in the navigation pane.

4 In the navigation pane, select the session that you want to review

   Commands for the session data that has been captured are indicated by a Yes in the **Capture** column.

5 Click **Keystroke Replay** in the task pane.

6 Edit the following fields:

   Terminal Type: Change the terminal type if it is set incorrectly.

   Find: To find a specify command or string in the report, specify the text in the text box, then click **Find**. If the report contains hundreds of lines, this allows you to find the command you are interested in.

   Show control characters: Use this option to show or hide control characters on the screen.

   Show audited commands: Use this option to show or hide the full list of audited commands. If this option is enabled, the screen shows the actual commands that are being run when a user types a command. You can also view each input command individually by mousing over the command.

   Show profile commands: Use this option to show or hide the commands run in the user's login profile when the user's pcksh login shell has auditing configured to level 2.

7 From the list of input commands, select a command, then click **Output**.

8 Use the **Play**, **Rewind**, and **Pause** buttons to review the data.

9 Click **Cancel** to return to the list of reports.

Removing a Report

IMPORTANT: This action can not be undone.

---

1 Click **Reporting** on the home page of the console.

2 Click **Command Control Reports** in the navigation pane.

3 Select the report you want to delete.

4 Click **Delete Report** in the task pane.

5 Click **Finish**.

Generating an Activity Report

The Activity Report option allows you to generate a graphical snapshot of all the audit records currently being displayed in the report. The activity report can then be printed, providing a visual record for managers to see the number of commands each host is processing, the names of users requesting sessions, and the number of session accepted or rejected.

1. Click **Reporting** on the home page of the console.
2. Click **Command Control Reports** in the navigation pane.
3. Select the report you want generate an activity report for.
4. Click **Activity Report** in the task pane.

   The navigation pane displays the selected activity report.
5. To print the report, click **Print**.
6. To return to the list of reports, click **Cancel.**

Viewing a Report in a Comma-separated Values (CSV) Format

You can view an audit report in a CSV format when PAM is installed on a Linux or a UNIX server. Run the `sreplay -c <host>` command to view the report. For more information about the sreplay command refer, "sreplay Command Line Options" on page 189.

Video Capture

- "Configuring Video Capture" on page 92
- "Viewing the Videos" on page 95
- "Video Off-Load" on page 96

Video Capture monitors the user activity by capturing videos of every task performed by the user.

- You can schedule compression and archiving of video files to external storage.
- You can turn the Video Capture feature ON or OFF for a particular user based on your requirement. This way you can manage your system's storage capacity.
- You can off-load the session screen to video conversion operation to a dedicated video off-load agent. This way you can improve the agent performance.
- For Windows session, you can browse the text log of a user and select a particular task and watch the video. This way you do not have to go through the entire video but watch the video of the specific user activity that you require.
- For Windows session, you can search for a particular event in a video based on the keyword search option. For example, if an important file is deleted, then you can search for all the user activities where a deletion task is performed just by the keyword search, and then select the video of your interest.

Configuring Video Capture

- "Configuring the Video Path (Optional)" on page 92
- "Configuring the Video Report Filter Settings (Optional)" on page 93
- "Configuring Video Archival (Optional)" on page 93
- "Configuring the Video Conversion Settings" on page 94
- "Enabling Video Capture" on page 95
- "Converting the FLV Videos to WebM" on page 95

Configuring the Video Path (Optional)

The video path is where all the recorded videos are stored. This feature creates the path by default.

NOTE: This video path configuration and audit settings are specific to respective hosts. To maintain consistency ensure that all the hosts with the Audit Manager package contains appropriate video configuration.

For example, if the Framework Manager has 2 hosts with Audit Manager package and one has the **Video Subfolder Configuration** enabled and other has the option disabled results in the videos being stored in different folder structure. To avoid this ensure that the video configuration is consistent across all the hosts.

To modify the video storage path:

1. Click **Hosts** in the home page of the console.
2. Select the host for which you want to configure the video path.
3. Click **Packages** > **Audit** > **Audit Settings**.
4. Specify the following:

   Video Path: Specify the path where the videos must be stored. Ensure that you have created the new folders before you change the path. If you want to store the video in a shared folder, you must specify the video path in the format:

   ```
   \\<ip address>\<sharedfolder>
   ```

   Video Subfolder Configuration: Select **Enable** to store the videos in the sub folders created under the Video Path, that is, `<Video Path>/<Host Name>/<Year>/<Month>/<Session ID>`.

   Select **Disable** to store the videos directly in the path specified in **Video Path**.

   Shared Folder Access Domain: If you want to store the video in a shared folder, select the domain on which the shared folder is located.

   Shared Folder Access Credentials: If you want to store the video in a shared folder, select the credentials to access the shared folder.

   If Audit Manager is in a non Windows environment, change the path accordingly.

NOTE: ◆ Access credential drop down will contain only those credentials which are created in the Command Control under Privileged Accounts.

◆ The access credential for the Windows shared folder must have write permission.

5 Click **Finish**.

Configuring the Video Report Filter Settings (Optional)

To simplify the search of a particular video, Video Capture for Windows has a set of preconfigured filters for any task performed by you, like type, click and so forth.

NOTE: The Video Report filter is supported only for Windows sessions.

To edit the filter settings:

1 Click **Reporting** in the home page of the console.

2 Click **Video Report Setting**.

3 Edit the **Video Report Filter Settings**.

By default, **Video Report Filter Settings** has the following filters:

`Type|click|Checked|Close window|Terminate|msc|user|group|start|stop|Log Off`

4 Click Finish.

NOTE: After editing the filter configuration if you want the initial filter configuration then click **Reset** > **Finish**.

Configuring Video Archival (Optional)

To archive the videos:

1 Click **Reporting** in the home page of the console.

2 Click **Audit Settings**.

3 Add the following sample script under **Rollover Script**:

```
\nuse warnings;\nuse File::Copy; \n  $ctx-
>log_info(\"============================================================
=========================\");\nif ($DBGRP eq \'cmdctrl\') {\n    my
$srcdir = ($^O eq \'MSWin32\') ? \"C:/Program Files/Netiq/npum/service/
local/audit/video/capture/\" :  \"/opt/netiq/npum/service/local/audit/
video/capture/\"; \n\n    my $dest = ($^O eq \'MSWin32\') ? \"C:/Program
Files/Netiq/npum/service/local/audit/videobck/\" : \"/opt/netiq/npum/
service/local/audit/videobck/\";\n\n    my $fileage = 1;     #Age in
days \n\n    opendir(DIR, $srcdir) or die $ctx->log_error(\"Can\'t open
$srcdir: $!\");\n    my @files = grep {!/^\\. $/ } readdir(DIR);\n
foreach my $file (@files) {\n       my $old = \"$srcdir/$file\";\n
if( (-f $ol
 d) && ($fileage< -M $old) ) {\n            move($old, $dest) or die
$ctx->log_error(\"Move $old -> $dest failed: $!\");\n
\n        }\n    }  \n    close(DIR);\n    $ctx->log_info(\"Backup
Complete\");\n}
```

4 Click **Finish**.

Configuring the Video Conversion Settings

Using this video conversion settings, you can optimize the videos conversion process based on quality, size and CPU utilization.

The video conversion settings is a global settings that will be applied to all the policies which have the **Video Capture** option enabled. Based on this configuration, the images are captured for the sessions and converted to videos.

To edit the Video Conversion Settings:

1 On the home page of the console, click **Command Control**.

2 In the left pane, click **Command Control**.

3 In the right pane, click **Video Settings**.

4 In the right pane, edit the following fields for Windows and SSH:

Settings: Select **Default** or **Low Priority** to use the predefined settings, you cannot modify the predefined settings.

Select **Customize** to customize the video settings.

Video fps: This option determines the quality of the video. The Video fps value that is set is the maximum video fps that can be achieved. Based on the factors such as type of Processor, RAM capacity, CPU availability, and so on, the video fps may vary.

If video fps value is high, the video quality is good and consumes more storage.

Video Duration: Select the Video duration as 1 min or 2 min based on the requirement.

If video duration is more, number of video files are less.

Video Conversion Priority: This option determines the video conversion process priority in CPU. By setting the priority, you can ensure that other operations of the CPU are uninterrupted.

Set this option to **Low** when video conversion is not of high priority.

Set this option to **Normal** when video conversion process is of moderate or high priority.

5 Click **Save**.

Enabling Video Capture

To enable video capture:

1. Add an resource. For more information, see Contextual Help.
2. Click **Command Control** on the home page of the console, then click **Create a rule**.
3. Select the account that you created from the **Credentials** drop-down list.
4. Select the following options:

   For Windows:

   Session Capture: Set this option to **ON** to enable session capture

   Video Capture: Set this option to **ON** to enable video capture

   For SSH:

   Session Capture: Set this option to **ON** to enable session capture.

   X11 Enable: Set this option to **Yes** to enable X11 application access.

   Video Capture: Set this option to **ON** to enable video capture.
5. Click **Finish**.

Converting the FLV Videos to WebM

Privileged Account Manager supports videos only in WebM format. If you have videos in FLV format, you need to convert the videos to WebM format to enable playback of the recorded videos.

Convert the FLV Videos to WebM in Windows

To convert the videos to WebM format, download the FFmpeg executable from the download site and execute the following command:

```
ffmpeg.exe -i <input_file_name>.flv -c:v libvpx-vp9 -speed 8 -deadline
realtime <output_file_name>.webm
```

Convert the FLV Videos to WebM in Linux/Unix

To convert the videos to WebM format, download the FFmpeg executable from the download site and execute the following command:

```
./ffmpeg -i <input_file_name>.flv -c:v libvpx-vp9 -speed 8 -deadline
realtime <output_file_name>.webm
```

Viewing the Videos

To view the videos:

1. Click **Reporting** on the home page of the console.
2. Click **Command Control** > **Sample Report**.
3. Select the session report you want to view, then click **Keystroke Replay**.
4. In the Command Control Keystroke Report page, click **Playback**.

   The Playback button is displayed only if video capture is enabled for that session.

NOTE: ◆If the recorded videos with `.flv` extension are not displayed, ensure that you have converted those videos to `.webm` format. For more information, refer to "Converting the FLV Videos to WebM" on page 95.

- Video playback is not supported in Edge Browser as Edge browser does not support WebM format. Instead use Google Chrome or Mozilla Firefox to play the videos.

5 In the Video playback screen, click the button to play the video.

Time: The time when the event occurred.

Standard Input: Action performed by the user.

All events: Displays all the events.

Filtered events: You can filter the events based on the predefined filter option. For more information, see "Configuring the Video Report Filter Settings (Optional)" on page 93.

Find: Searches the events based on the options provided by you.

Video Off-Load

Privileged Account Manager audits all the privileged session operations in the form of keystrokes and videos based on the command control rule configuration. If you have enabled video capture in the rule, the video is generated in the agent where the session is running. In an agentless environment, such as SSH relay with X11 enabled, the video is generated in the SSH relay manager. After the video is generated, it is sent to audit manager in the audit zone.

The video generation operation consumes more CPU if there are multiple concurrent sessions to the agent or SSH relay manager. Hence, PAM provides an option to configure a server (video off-load agent) exclusively for video generation operation. You can use a video off-load agent, when you are using SSH Relay, Application SSO or when the agent has limited resource. When the video off-load agent is down, the conversion operation is performed on the PAM agent where the session is running.

Figure 7-1 *The following illustrations explains the flow of the video generation process in a multi-agent environment:*

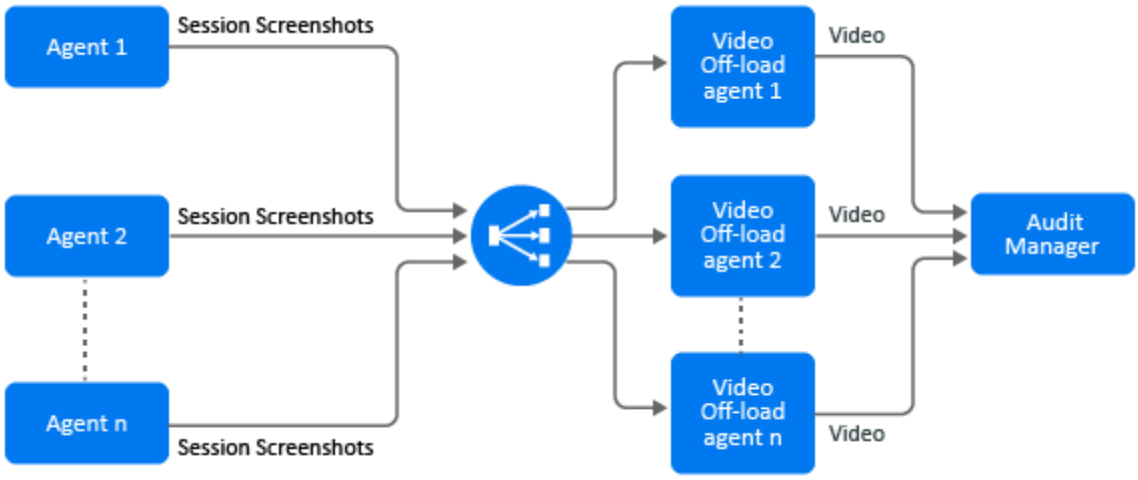
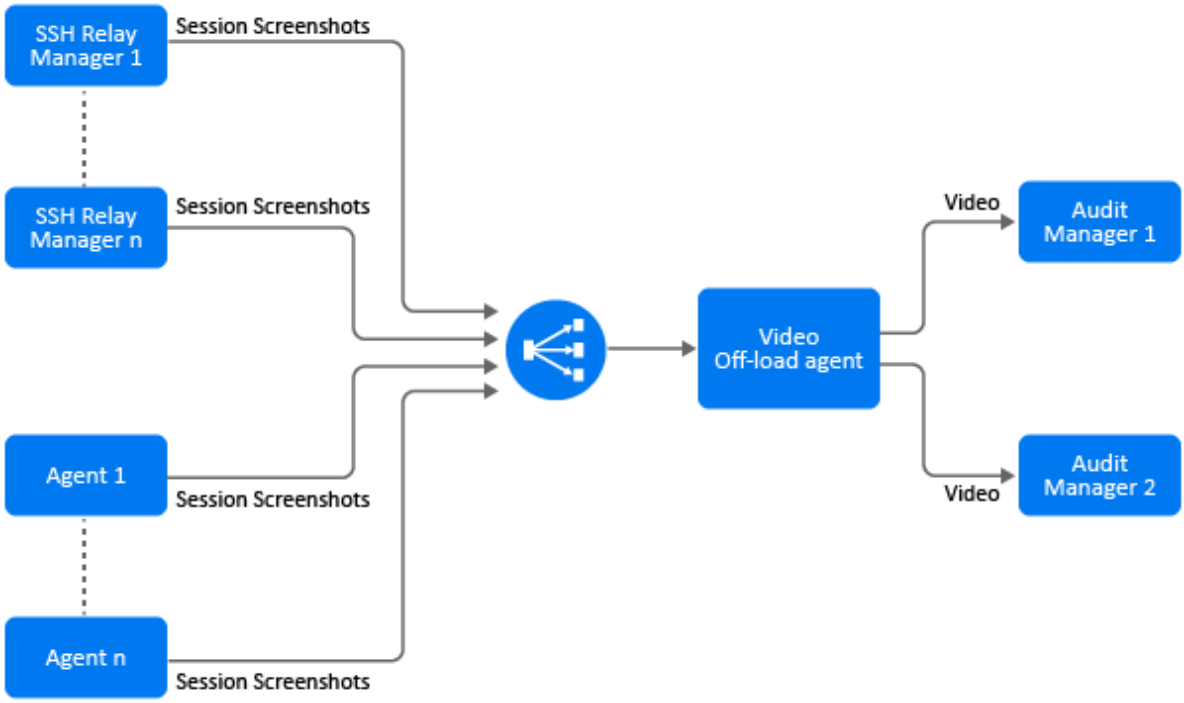


Figure 7-2 The following illustrations explains the flow of the video generation process with multiple audit manager:



- Setting Up Video Off-Load Agent
- Video Off-Load Settings
- Enabling Video Off-Load

Setting Up Video Off-Load Agent

The video off-load server is a PAM agent, where the session images are converted to videos. For the system requirements of the video off-load server, see the System Requirements in PAM Documentation website.

To setup and configure a video off-load agent:

1 Install and register the PAM agent on every video off-load server.

NOTE: You can use only Linux server as a video off-load server.

For more information about installing and registering a PAM agent, see Installing and Registering a Framework Agent in the Privileged Account Manager Installation Guide.

2 Install the `videoprocessor` package on every video off-load server:

2a Click **Hosts**.

2b Select the host which is a video off-load server, then click **Packages**.

2c Click **Install Packages**.

2d Select the `videoprocessor` package.

2e Click **Next** to start installing the selected package.

2f Click **Finish**.

For more information about installing a package on the agent, see Installing Packages on a Host.

3 Configure a location on every video off-load server to store session images and videos:

   3a Click **Hosts**.

   3b Select the host which is a video off-load server, then click **Packages**.

   3c Select the `videoprocessor` package.

   3d Click **Video Settings**.

   3e Specify the **Video Processor Path**, then click **Next**.

   Video Processor Path is the location in the video off-load server where:

   - The temporary video capture data that is used for video generation is stored.
   - The generated videos are stored before sending them to the audit manager.

Video Off-Load Settings

Video off-load settings help in tuning the performance of the video off-load agent to optimize the video generation operation based on the resources available on the video-offload agent.

The video off-load setting is a global setting that is applied to all the video off-load agents.

To edit video off-load settings:

1 Click **Command Control > Video Settings.**

2 Click **Video Processor** and specify the following:

   Apply Settings: Select **Default** to use the predefined settings, you cannot modify the predefined settings. When you select **Default**, **Conversion Priority** is set to **Normal** and **Auto Manage Resources** is set to **Yes**.

   Select **Customize** to customize the following settings:

   Auto Manage Resources: If you set this option to **Yes**, then based on the CPU and memory usage at any given time, PAM determines the number of video conversion instances that can be executed simultaneously. For better throughput and optimized CPU and RAM usage, you must set this option to **Yes**.

   If you set this option to **NO**, you must define **Number of Simultaneous Instances**.

   Number of Simultaneous Instances: Specify the maximum number of video conversion instances that can run simultaneously at a time in the video off-load agent.

   Conversion Priority: This option determines the video conversion process priority in CPU. By setting the priority, you can ensure that other operations of the CPU are uninterrupted.

   Set this option to **Low** when video conversion is not of high priority. If you set the priority to **Low** the video generation operation would be slow and would consume more temporary storage to accumulated the video generation data.

   Set this option to **Normal** when video conversion process is of moderate or high priority.

3 Click **Finish**.

Enabling Video Off-Load

You must enable **Video Off-load** in the appropriate PAM rule to transfer the session image to video conversion activity to the video off-load agent.

Before enabling video off-load, ensure that you have setup the video-offload agent. For more information about setting up the video-offload agent, see Setting Up Video Off-Load Agent.

To enable video off-load:

1. Click **Command Control** on the home page of the console, then click **Create a rule**.
2. (Conditional) If you are creating a new rule, then click **Create a rule**.
3. (Conditional) If you are updating an existing rule to support video off-load, then click the appropriate rule.
4. Select the following options:

   For Windows:

   - **Session Capture:** Set this option to **ON** to enable session capture.
   - **Video Capture:** Set this option to **ON** to enable video capture.
   - **Video Offload:** Set this option to **ON** to enable video offload.

   For SSH:

   - **Session Capture:** Set this option to **ON** to enable session capture.
   - **X11 Enable:** Set this option to **Yes** to enable X11 application access.
   - **Video Capture:** Set this option to **ON** to enable video capture.
   - **Video Offload:** Set this option to **ON** to enable video offload.

   For more information about the rule configuration fields, see the "Modifying a Rule" on page 109.
5. Click **Finish**.

For emergency access requests, you can off-load the video generation operation by selecting **Video Capture** and **Video Offload** when approving the request.

Change Management

Any GUI specific operation performed by you is audited by the Change Management feature. Each operation is tracked and the log is maintained in the Change Management report. The default Sample Report displays all of the collected audit records and any associated keystroke capture.

Viewing Report Data

1. Click **Reporting** on the home page of the console.
2. Click **Change Management** in the navigation pane.
3. Select the report in the navigation pane.

The navigation pane displays the following information about each instance of the report.

Column	Description
Change Time	Displays the date and time when the GUI operation was performed.
User	Displays the name of the Framework user who performed the GUI operation.
Module	Displays the module where the GUI operation was made.
Source	Displays the name of the particular functionality within the module where the GUI operation was performed.
Action	Displays the specific operation performed by the user. For example, registering a host to the PAM Framework.
Host	Displays the name of the host on which the GUI operation was performed.
Audit ID	Displays the unique ID of the audit record.

Password Management

When a user performs any password check out operation, the password management feature audits the records. Any password specific operation performed by the user is audited by the Password Management feature. Each operation is tracked and the log is maintained in the Password Management report. The default Sample Report displays all of the collected audit records. For information about accounts refer, Chapter 17, “Privileged Access to Applications and Cloud Services,” on page 241.

Enabling Password Management

A console package named `report_pwdcheckout` needs to be installed to enable the Password Management feature.

Viewing Report Data

1. Click **Reporting** on the home page of the console.
2. Click **Password Management** in the navigation pane.
3. Select the report in the navigation pane.

   The navigation pane displays the following information about each instance of the report.

Column	Description
Password Checkout Time	Displays the date and time when the password was checked-out.
User	Displays the name of the user who checked-out the password.
Run As	Displays the name of the user who checked-out the password.
Run Host	Displays the name of the host from which the password was issued
Password Checked-in By	Displays the user who checked-in the password

Column	Description
Password Check-in Time	Displays the check-in time of the password
Target	Displays the target for which password was checked-out
Request ID	Displays the request ID of the password checkout

Shared Key Management

Any key specific operations performed by a user is audited by the Shared Key Management feature. Each operation is tracked and the log is maintained in the Shared Key Management report. The default **Sample Report** displays all of the collected audit records. For more information about using shared accounts refer, Chapter 13, "Managing Shared Keys," on page 193.

Enabling Shared Key Management

A console package named `report_sharedkeycheckout` needs to be installed to enable the Shared Key Management feature.

Viewing Report Data

1. On the home page of the console, click **Reporting**.
2. In the navigation pane, click **Shared Key Management**.
3. In the navigation pane, select the report.

   The navigation pane displays the following information about each instance of the report.

Column	Description
Shared Key Checkout Time	Displays the date and time when the key was checked-out.
User	Displays the name of the user who checked-out the key.
Key	Displays the name of the checked out key under the shared key domain
Key Domain	Displays the shared key domain from which the key was checked-out
Shared Key Checked-in By	Displays the users who checked-in the shared key
Shared Key Check-in Time	Displays the check-in time of the shared key
Shared Key Target	Displays the type of the checked-out key
Request ID	Displays the request ID of the key checkout
Usage Count	Displays the number of keys which have been used
Total Allowed	Displays the total number of keys available under the shared key domain

8 Command Control

The Command Control feature provides users controlled access to privileged commands in a secure manner across the enterprise. Command Control enables the complete lockdown of user privilege by providing rules to determine the commands that are authorized to run, and a powerful account delegation feature that removes the need for common access to the `root` account.

Using Command Control you can enable centralized logging of activity across all platforms, and the selective capture of session activity for any user, to the keystroke level, which can be viewed through the Compliance Auditor and reporting features.

Additional features include external scripting that provides the ability to authenticate via third-party security databases or applications, and comprehensive test suite tools that allow the administrator to model and test new rule combinations before committing them to production use.

This section lists the tasks that you can perform to manage the policies.

- "How Does Command Control Work?" on page 103
- "Installing and Deploying Command Control" on page 104
- "Command Control User Interface" on page 105
- "Configuring Command Control" on page 106
- "Command Control Options" on page 140
- "Disconnecting a Privileged Session" on page 151

How Does Command Control Work?

The commands are passed to the Command Control through scripts, commands, or replacement shells.

When a command is received, the Command Control uses the following to evaluate the command:

- The command is validated against configured rule criteria such as submit user, submit host, run host requested, date/time, and the command name itself.
- Any Perl script associated with the rules are executed, such as setting environment variables.

If the evaluation authorizes the command to run:

- The command is executed on the requested run host unless a matching rule specifies a run host. When a rule specifies a run host, the command is executed on that host. Rule values always overwrite values in the command request.
- The command is executed as the requested run user unless a matching rule specifies a run user. When a rule specifies a run user, the command is executed as that user. Rule values always overwrite values in the command request.

If the evaluation returns unauthorized, the command is not executed and the reason for the failure is returned.

Installing and Deploying Command Control

To deploy Command Control, you must download several modules to your local Package Manager, then install them:

- "Command Control Modules" on page 104
- "Auditing Modules" on page 104
- "Compliance Auditor Modules" on page 104
- "Installing Command Control" on page 104

Command Control Modules

The Command Control feature is made up of the following packages:

- **Command Control Manager:** Holds the rule configuration and is responsible for validating user command requests.
- **Command Control Agents:** Installed on machines where user commands are to be controlled or audited.
- **Command Control Console:** Installed into the Framework Manager console. Required for configuring Command Control rules.

Auditing Modules

The auditing modules are made up of the following packages:

- **Audit Manager:** Acts as the repository for auditing information collected by the Framework.
- **Reporting Console:** Installed into the Framework Manager console. Required for viewing audit information.
- **Command Reporting Console:** Installed into the main Reporting Console. Required for viewing Command Control audit information.

Compliance Auditor Modules

The Compliance Auditor modules are made up of the following packages:

- **Compliance Auditor:** Holds the compliance auditor rules and audit information.
- **Compliance Auditor Console:** Installed into the Framework Manager console. Required for configuring compliance auditor rules and for viewing audit information.

Installing Command Control

To install Command Control, perform the following:

1. Download the required packages to your local Package Manager. See "Installing and Deploying Command Control" on page 104 for details.
2. Install the Command Control Manager package on the host you want to be the Command Control Manager. This can be on any operating system, including Windows.

See "Installing Packages on a Host" on page 39 for details. Command Control Managers can be deployed to as many hosts as you need in order to build an environment with load balancing and failover.

3. Install the Command Control Agent package on all UNIX hosts on which you want to implement Command Control.
4. Install the Audit Manager package on the host you want to be the Audit Manager, then install the Compliance Auditor package on the same host.

   This can be on any operating system, including Windows, and can be a different host from your Command Control Manager. The auditing packages can be deployed to as many hosts as you need in order to build an environment with load balancing and failover.

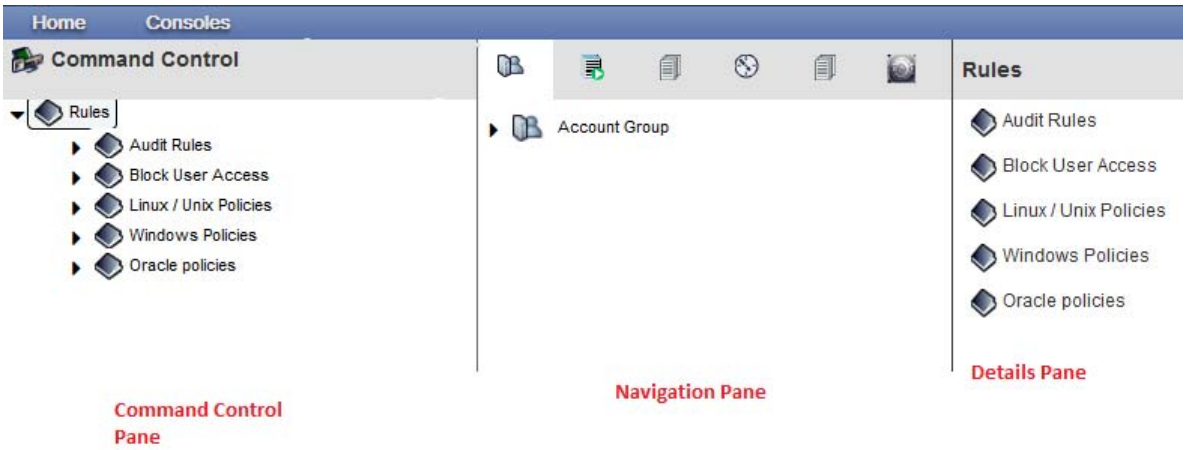
Command control is now deployed and ready to use.

Command Control User Interface

The Command Control console includes the following:

- **Command Control pane (left pane):** This pane includes the rules and policies. You can create policies and manage those by using this pane.
- **Navigation pane (middle pane):** The navigation pane displays the icons for the following entities:
  - Account Group
  - Commands
  - Scripts
  - Access Time
  - Reports

  When you select any of the icons the hierarchy of that group is displayed.
- **Details pane (right pane):** The details pane displays the details of whatever you select in the Command Control pane, and the navigation pane. All the required tasks such as, adding, modifying, deleting and so on are performed through the details pane.



Configuring Command Control

Command Control uses rules to protect and control user commands. When configuring a rule, you must set conditions for the rules to determine which rule or rules are processed, for example, on the command submitted or the user who submitted it. You also need to define what processing to do if the rule conditions are matched.

The components that you can define and configure for a rule are as following:

- The rule. For configuration information, see "Rules" on page 107.
- Account groups, user groups, and host groups, which determine who matches the rule. For configuration information, see "Command Control Groups" on page 115.
- Commands. For configuration information, see "Commands" on page 121.
- Credential Vault. For configuration information, see Contextual Help.
- Scripts for additional functionality. For configuration information, see "Scripts" on page 131.
- Access time to define specific time interval during which access is denied or granted. For configuration information, see "Access Times" on page 136.

NOTE: To enable access to the Command Control console for a Framework user and to control the level of access available, you must add the user to a group with the appropriate roles defined. See "Configuring Roles" on page 72 for details.

The following additional features are provided to assist you with Command Control configuration and management:

- "Rules" on page 107
- "Command Control Groups" on page 115
- "Commands" on page 121

- “Finding a Reference” on page 128
- “Defining Custom Attributes” on page 128
- “Functions” on page 129
- “Adding a Category” on page 130
- “Deleting a Category” on page 131
- “Blocked Users” on page 131
- “Scripts” on page 131
- “Access Times” on page 136
- “Command Control Reports” on page 138

Rules

Rules provide the means by which you can control commands. Commands can be authorized to run, or not authorized to run, by setting rule conditions based on different criteria:

- The command being submitted
- The user and host submitting the command
- The user and host assigned to run the command
- The time the command is submitted
- The contents of Perl scripts you have defined.

See “Setting Conditions for a Rule” on page 111 for details.

If a rule’s conditions are met, there are a number of options you can set to determine how the rule processes the command. You can configure a rule to:

- Display a message to the user submitting the command
- Capture the user session for reporting and auditing purposes
- Authorize or not authorize the command to be run
- Specify what further rule processing to do. The rule can specify that the processing of additional rules ends by using the stop conditions (**Stop**, **Stop if authorized**, **Stop if unauthorized**).

  When the Framework Manager receives a command request, the evaluation starts at the top of the rule tree. Even when a request matches a rule, the evaluation continues until a rule has a stop condition or the rule tree has been processed.

You can also:

- Specify the user and host to run the command
- Set a risk level for use with keystroke reports
- Assign an audit group to the rule for use with the Compliance Auditor.

See “Modifying a Rule” on page 109 for details.

You can also create and assign Perl scripts to the rule to provide additional functionality. See “Adding a Script” on page 132 and “Assigning a Script to a Rule” on page 112 for details.

NOTE: If you are using a different user (run user) to run an authorized command than the user who submitted the command (submit user), by default the submit user's environment variables are used for the run user. If you want to use the environment variables associated with the run user, you can add a script to a rule containing the following text:

```
$meta->get_params("Job")->arg("job_default_env",0);
return 1;
```


- "Adding a Rule" on page 108
- "Modifying a Rule" on page 109
- "Viewing Conditions for a Rule" on page 110
- "Setting Conditions for a Rule" on page 111
- "Removing Conditions for a Rule" on page 112
- "Configuring Script Arguments and Entities for a Rule" on page 112
- "Assigning a Script to a Rule" on page 112
- "Removing Script Arguments and Entities" on page 113
- "Removing a Script from a Rule" on page 113
- "Finding a Rule" on page 113
- "Moving a Rule" on page 114
- "Copying a Rule" on page 114
- "Linking a Rule" on page 114
- "Deleting a Rule" on page 115
- "Viewing Pseudocode" on page 115

Adding a Rule

1. On the home page of the console, click **Command Control**.
2. In the command control pane, click **Rules**.
3. In the task pane, click **Add** to add a rule at the top level.

   To add a rule as a child of another rule, select the rule and click **Add** in the task pane.
4. Specify a name for the rule.
5. Click **Finish** to add a new rule.
6. Select the rule, then click **Modify Rule** in the task pane.

   For configuration information, see "Modifying a Rule" on page 109.
7. Move the rule by using the Alt key and drag and drop it to the correct position according to the order in which you want to process the rules. This moves the rule in the same hierarchy.

   When a user specifies a command under Command Control, the following rule processing takes place:

   - The conditions set for the first rule in the hierarchy are checked.

- If there is a match, the rule is processed. Depending on how the rule is configured, processing of additional rules takes place or stops. If rule processing is not stopped, the next rule for which conditions are checked is the child of this rule. Rule checking and processing continues until it is stopped by a rule, or until all appropriate rules have been processed.
- If there is no match, the conditions for the next rule at the same hierarchical level as the first rule are checked, and this continues until a match is found. Rule processing then takes place as described above.

You can change the default order of rule processing on the **Modify Rule** screen, or by using scripts. See "Modifying a Script" on page 132.

Modifying a Rule

1. On the home page of the console, click **Command Control**.
2. In the command control pane, click **Rules**.
3. Select the rule you want to modify.
4. In the details pane, click the edit icon.
5. Modify the following as per your requirement:

   Name: Change the name of the rule.

   Disabled: To disable the rule, select the **Disabled** box. A disabled rule is dimmed.

   Description: Specify a description of the rule.

   User Message: Specify a user message to be displayed to the user when this rule is processed, before any commands are run.

   Session Capture: Select either **On** or **Off**. Setting **Session Capture** to **On** allows the Audit Manager to perform keystroke logging for the rule.

   To view a captured session from a Command Control report, an Auditing Manager and the Reporting Console must be installed.

   X11 Enable: Select either **Yes** or **No** to enable the X11 application access over SSH Relay.

   When you enable X11 application access, you can choose to enable the video recording of the session. Select **Video Capture On** to enable video capture of the session.

   Authorize: Select either **Yes** or **No**, depending on whether you want the command protected by the rule to be authorized or not authorized if the rule conditions are met.

   Define what happens next by using the drop-down list as follows:

   - **Blank:** The next rule in the hierarchy is checked.
   - **Stop:** No more rules are checked for the command.
   - **Return:** The next rule to be checked is up one level in the hierarchy from the current rule.
   - **Stop if authorized:** If **Authorize** is set to **Yes**, no more rules are checked for the command.
   - **Stop if unauthorized:** If **Authorize** is set to **No**, no more rules are checked for the command.

   Secondary Authentication: If **Secondary Authentication** is set to **Yes**, then Multi-Factor Authentication is applied during authorization. This is supported for Advanced Authentication only.

Run User: Define a run user by selecting the name of the user you want to run this command (this overrides any username defined through a set command).

Account Domain: Select the appropriate LDAP or SSH resource from the drop down list.

Credentials: The credential for the selected resource gets populated. You can also select the required credential from the drop-down list.

Run User: The Run User gets automatically populated with the domain user provided in the resource.

Run Host: Define a run host by selecting the name of the host on which you want to run this command (this overrides any hostname defined through a set command).

NOTE: When modifying a rule for Run as Privileged User method, ensure to modify the **Run Host** as `Submit Host`.

Risk Level: Set a **Risk Level** of 0 to 99. This option allows you to set a value representing the relative risk of a rule with the session auditing option (see "cpcksh" on page 213). When viewing a Command Control Keystroke Report, you see commands controlled by rules with different risk values represented in different colors.

Audit Group: Define an **Audit Group**. This setting is for use in Compliance Auditor reports.

NOTE: To configure video capturing refer section "Video Capture" on page 91

---

6 Click **Modify**.

7 Drag-and-drop **Account Groups**, **User Groups**, **Host Groups**, **Commands**, **Scripts**, or **Access Times** to add them to **Rules**. In the pop-up window that appears, select **Yes** to add them or **No** to discard your changes.

Viewing Conditions for a Rule

You can view all the conditions that create a rule. These conditions are created with the help of the entities such as host group, user group and so on. You can view the entity that includes the condition and also modify it if required.

To view the condition perform the following steps:

1 In the Command Control pane, click the required rule.

2 In the details pane, click **View Condition**.

This displays the list of entities that are part of the condition.

3 (Conditional) Click **Locate** to locate the required entity.

This locates and selects the required entity in the middle pane.

4 (Conditional) In the details pane, click the edit icon o modify the fields of the entity.

Setting Conditions for a Rule

You can set a number of conditions for a rule to determine whether the rule is processed or not. For example, you can set a particular command as a condition, and only process the rule if a user enters that command.

There are two ways of setting conditions for a rule:

- Dragging and dropping an entity onto the rule.
- Using the **Edit Condition** option, as described in the steps below.

NOTE: When you drag and drop an entity onto a rule, you might need to edit the condition to ensure that the condition logic is what you want. If you want to use a script in rule conditions, you must set it to Conditional first (see "Modifying a Script" on page 132).

To set conditions by using the **Edit Condition** option:

1. On the home page of the console, click **Command Control**.
2. In the Command Control pane, click **Rules**.
3. Select the rule for which you want to set conditions.
4. In the details pane, select the currently defined condition then click **Edit Condition**.

   If you have not yet defined a condition, select **Match All**
5. In the **Add Condition** drop-down list, select the type of condition you want.
6. Set the condition to the value and logic you want. For example, if you set a condition to match a run user to a user group:

   6a Change **user** (submit user) to **run user**.

   6b Leave the logic setting as **IN**.

   6c Select the user group you require from the user group drop-down list.
7. Repeat Step 5 and Step 6 for any other conditions you want. Set the condition logic as necessary.

   You can use parentheses to group conditions according to the necessary logic by selecting the parentheses ( ) entry from the **Add Condition** drop-down list. The opening and closing parentheses are displayed.

   7a Select the opening parenthesis.

   7b Select the condition type you want to place inside the parentheses and set it as necessary.

   7c Select the opening parenthesis again.

   7d Select another condition type to place inside the parentheses and set it as necessary.

   7e If necessary, change OR to AND.

   7f Repeat Step 7d through Step 7f for any other conditions you require inside this set of parentheses. You can also place parentheses within parentheses.
8. Click **Finish**.

Removing Conditions for a Rule

You can remove all the conditions for a rule, or you can remove individual conditions.

1. On the home page of the console, click **Command Control**.
2. In the Command Control pane, click **Rules**.
3. Use the arrow to display all the rules and select the rule for which you want to remove conditions.
4. In the task pane, select the currently defined condition.
5. To remove all conditions, click **Remove Condition** in the task pane, then click **OK** to remove the condition.

   The rule condition is displayed as **Match All.**
6. To remove individual conditions, click **Edit Condition** in the task pane, click the delete icon against the condition to remove the condition, then click **Finish**.

Configuring Script Arguments and Entities for a Rule

You can configure script arguments and entities for the scripts assigned to a rule before or after assigning the scripts. You can define only one set of arguments and entities, which applies to all scripts assigned to a rule.

1. On the home page of the console, click **Command Control**.
2. In the Command Control pane, click **Rules**.
3. Select the rule for which you want to add script arguments.
4. In the task pane, click **Script Arguments**.
5. Click **Add**.
6. In the **Name** field, specify a name for the argument.
7. In the **Value** field, specify a value for the argument.
8. To add more arguments, repeat Step 5 through Step 7.
9. When you finish adding arguments, click **Finish**, or continue with Step 10 to add script entities.
10. Click the arrow under **Add Script Entity** to display the list of available entities, then select the type of entity you want.

    A drop-down list of entities is displayed in the **Script Entities** table.
11. Select the entity you want from the drop-down list.
12. To add more entities, repeat Step 10 and Step 11.
13. Click **Finish**.

Assigning a Script to a Rule

You can use Perl scripts to provide additional, customized functionality to the rules (see "Adding a Script" on page 132). To assign a script to a rule, use drag and drop as described in the following procedure.

NOTE: If you drag and drop a script that has been set to Conditional, the script is added to the rule conditions.

1. On the home page of the console, click **Command Control**.
2. In the Command control pane, click **Rules**.
3. Click the arrow to display the list of rules.
4. In the navigation pane, click the **Scripts** icon.
5. Select the script you want to assign to the rule.
6. Drag and drop the selected script to the rule.
7. Configure script arguments and entities for the scripts if necessary. For more information, see "Configuring Script Arguments and Entities for a Rule" on page 112.

Removing Script Arguments and Entities

1. To remove a script argument, select the argument, then click **Remove**.
2. To remove a script entity, select the icon next to the name of the entity, then click **Remove**.

Removing a Script from a Rule

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Rules**.
3. Use the arrow to display the list of rules, then select the rule from which you want to remove a script.
4. In the details pane, select the required script.
5. Click **Remove Script**.
6. Click **OK** to confirm the removal. The scripts are removed from the rule.

Finding a Rule

1. On the home page of the console, click **Command Control**.
2. In the Command Control pane, click **Rules**.
3. In the details pane, click the Find Rule icon to find a rule from the entire list of rules.

   or

   Select the parent rule, then in the details pane click the Find Rule icon.
4. In the **Rule Filter** field, specify the name of the rule you are looking for, then click **Find**.

   You can use wildcard characters "*" and "?". This field is case sensitive.

NOTE: Some special characters, such as "[" and "]", might not work in this field. For example, if you search for *first rule [linked rule]*, you might get an error message. In such case, replace "[" and "]" with "*" or "?".

5 When the name of the rule is displayed, you can modify the rule by using **Modify Rule** and if you want to view the rule in the Command Control pane, click **Goto Rule**. Click **Close** to return to the Command Control pane without a rule selected.

Moving a Rule

1 On the home page of the console, click **Command Control**.

2 In the Command Control pane, click **Rules**.

3 Select the rule you want to move.

4 Press the Alt key then drag and drop the selected rule to the location in the same hierarchy. If you require to move a rule to a child hierarchy then drag and drop the rule to the required location.

Copying a Rule

You can create a copy of an existing rule in the rule hierarchy, so you can use the same rule in more than one place in the hierarchy, or so you can create a new rule based on the existing rule.

NOTE: If you want to use the same rule in more than one place and you want any changes you make to the rule to be reflected in the other copy or copies, you should link the rule instead. See "Linking a Rule" on page 114 for details.

1 On the home page of the console, click **Command Control**.

2 In the Command Control pane, click **Rules**.

3 Select the rule you want to copy.

4 To create the copy, press the Ctrl key and drag and drop the selected rule to the desired location

5 (Optional) Use the **Modify Rule** option to rename or modify the copy.

6 Move the rule to the correct position according to the order in which you want to process the rules. See "Adding a Rule" on page 108 for details.

Linking a Rule

If you want a specific rule to be used in different places in the hierarchy of rules, you can create a linked rule. Any changes you make to the linked rule are reflected in all the instances of the rule in the hierarchy. If you simply copy the rule, any changes made to the original rule or to one of its copies are not reflected in the other copies.

Changes to sub-rules of a linked rule are not linked. For example if you add or modify a rule under a linked rule, the change is not reflected in other instances of the linked rule.

1 On the home page of the console, click **Command Control**.

2 In the Command Control pane, click **Rules**.

3 Select the rule to link.

4 To create the links, press the Ctrl key and the Shift key at the same time, then drag and drop the selected rule to the location you want.

   A linked rule is displayed with an arrow .

Deleting a Rule

1 On the home page of the console, click **Command Control**.

2 In the Command Console pane, click **Rules**.

3 Select the rule you want to delete.

4 In the details pane, click **Delete**.

5 Click **Delete** to delete the rule and all rule children.

Viewing Pseudocode

The pseudocode for a rule provides a simplified representation of the actual code that is processed when the rule is activated. For complex rules, this can assist you with understanding what happens in different situations.

To view the pseudocode for a rule:

1 On the home page of the console, click **Command Control**.

2 In the Command Control pane, click **Rules**.

3 Select the rule for which you want to view the pseudocode.

4 In the details pane, click **Pseudocode**.

   You can copy the pseudocode by using Ctrl+A or Ctrl+C, then paste it into a document for printing.

5 Click **Close**.

Command Control Groups

Command Control has three types of groups:

User Groups: Contain users with similar responsibilities. This allows you to use the group as a condition for a rule, which either allows or denies the users the rights to run commands.

Host Groups: Contains hosts with similar content. This allows you to use the group as a condition for a rule that either allows or denies the rights to run the command on a host.

Account Groups: Combine host groups and user groups to be used together in setting rule conditions. Account groups can also contain other account groups. You can also use account groups as script entities.

For example, you could create a Web Account Group, and to this group you could add a user group that contains all the Web server managers and a host group that contains all the host that are Web servers. You could then use the Web Account Group as a condition when creating rules for Web server management.

The following sections explain how to manage these groups:

- "User Groups" on page 116
- "Host Groups" on page 118
- "Adding an Account Group" on page 120
- "Modifying an Account Group" on page 120
- "Deleting an Account Group" on page 120
- "Copying a Group" on page 121
- "Moving a Group" on page 121
- "Finding a Group" on page 121

User Groups

User groups contain users who are allowed, or not allowed, to submit or run commands controlled by the rules that you specify. You can add user groups to the specified rule conditions to control whether the rule is processed, depending on the user who is submitting a command or the user who is specified to run a command. You can also use user groups as script entities.

Command Control has the default user groups, **Everyone** and **Submit User**. Do not modify these groups.

Everyone: Use this group to match against any user who has a local account on the hosts where Privileged Account Manager is installed.

Submit User: Use this group to match against the user that submitted the privileged request. This is useful if you want to ensure that a rule only authorizes access to the account that submitted the request. For example when adding a cpcksh login shell, you should add a clause to the rule that ensures that the run user is in the Submit User group. This ensures that a user cannot use the `-u` option in `usrun` to gain access to other accounts.

You can search for a specific user in a user group by using suitable regular expressions, strings, or wild cards in the command. For example, the wildcards that you can use in the command could be `vi *` or `/usr/bin/vi *`.

To add a regular expression term to the list, prefix the regular expression with =~. For example,

```
=~/^vi .*$/
```

```
=~/^user*/
```

Command Control also includes a user group that is used for adding or deleting the users in the blocked list.

IMPORTANT: The User Name for Windows user must be provided in capital letters.

Managing the User Groups

The following sections explain how to manage user groups:

- "Adding a User Group" on page 117
- "Modifying a User Group" on page 117
- "Deleting a User Group" on page 118

Adding a User Group

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click the **Account Groups** icon.
3. Click **User Groups**.
4. In the details pane, click **Add** to add a user group to root level. To add the user group for a category, select the category then click **Add**.
5. Specify a name for the user group.
6. Click **Add**.

   User groups are represented by the group icon.
7. To configure the user group, continue with "Modifying a User Group" on page 117.

Modifying a User Group

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Account Groups**, then click **User Groups**.
3. In the details pane, select the user group you want to modify, then click the edit icon next to the user group name.
4. Configure the following fields:

   Name: Specify a name for the group.

   Disabled: Select this check box to disable the group. A disabled user group is dimmed.

   Description: Describe the purpose of this user group.

   Manager Name, Manager Tel., Manager Email: Specify the name, telephone number, and e-mail address of the manager of this user group. The manager details can be used in the Compliance Auditor.

   If these details have been entered in the manager's Framework user account details (see "Modify User: Account Details" on page 63), they can be entered automatically by selecting the manager's username from the drop-down list. This option is only available if you belong to a Framework user group with the read role defined for the auth module (see "Configuring Roles" on page 72).

   Users: Add or change the users you want to include in this group. You can type the user names, one on each line, or paste them from elsewhere. You can use the **Sort** button to sort the list of users into alphabetical order. For Windows users, specify the user name in capital letters.

   NOTE: The user names must be provided in capital letters for the LDAP users who are part of the authentication domain.

User Groups: From the list of groups you have already defined, select the user groups you want to include as subgroups of this user group. You can also add subgroups to a user group by dragging and dropping the groups to the target user group in the navigation pane.

5 Click **Modify**.

You can now use this user group in rule conditions or as a script entity.

Deleting a User Group

1 On the home page of the console, click **Command Control**.

2 In the navigation pane, click **Account Groups**, then click **User Groups**.

3 In the details pane, select the required user group and click the delete icon next to the user group name.

To delete multiple user groups, click **Delete Multiple** then select the user groups from the list to delete.

4 Click **Delete** to delete the selected user groups.

Host Groups

Host groups contain hosts that are allowed, or not allowed, to submit or run commands that the rules control. You can add host groups to the rule conditions to control whether the rule is processed, depending on the host that is submitting a command or the host specified to run a command. You can also use host groups as script entities.

Command Control has two default host groups. Do not modify these groups.

All Hosts: Use this group to match against any host that have been registered with the Framework. Use the Hosts console to view the hosts that are included has matches for this group.

Submit Host: Use this group to match against the host from which the privileged request was made. This is useful if you want to ensure that a rule only authorizes access to the host from which the privileged request was made. This ensures that a user cannot use the `-h` option in `usrun` to gain access to other hosts.

You can search for a specific host in a host group by using suitable regular expressions, strings, or wild cards in the command. For example, the wildcards that you can use in the command could be `vi *` or `/usr/bin/vi *`.

To add a regular expression term to the list, prefix the regular expression with =~. For example,

```
=~/^vi .*$/
```

```
=~\w+\.netiq\.com
```

The following sections explain how to manage host groups:

- "Adding a Host Group" on page 119
- "Modifying a Host Group" on page 119
- "Deleting a Host Group" on page 119

Adding a Host Group

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Account Groups**, then click **Host Groups**.
3. In the details pane, click **Add**. To add a host group to a category, select the category and click **Add**.
4. Specify a name for the host group.
5. Click **Add**.

   Host groups are represented by the icon.
6. To configure the host group, refer "Modifying a Host Group" on page 119.

Modifying a Host Group

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Account Groups**, then click **Host Groups**.
3. In the details pane, select the host group you want to modify, then click the edit icon next to the host group name.
4. Configure the following fields:

   Name: Specify a name for the group.

   Disabled: Select this check box to disable the group. A disabled host group is dimmed.

   Description: Describe the purpose of this host group.

   Hosts: Add or change the hosts you want to include in this group. You can type the host names, one on each line, or paste them from elsewhere. You can use the **Sort** button to sort the list of hosts into alphabetical order.

   Host Groups: From the list of groups you have already defined, select the host groups you want to include as subgroups of this host group. You can also add subgroups to a host group by dragging and dropping the groups to the host group in the navigation pane.
5. Click **Modify**. You can use this host group in rule conditions or as a script entity.

Deleting a Host Group

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Account Groups**, then click **Host Groups**.
3. In the details pane, select the host group you want to delete, then click the delete icon next to the host group name.

   To select multiple host groups, click **Delete Multiple** and select the host groups from the list.
4. Click **Delete.** The selected host groups are deleted and are also removed from any account group, rule conditions, and script entities in which they have been defined.

Adding an Account Group

To add a new account group:

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Account Groups**.
3. In the details pane, click **Add**. To add an account group to a category, select the category, then click **Add**.

   For information about categories, refer "Adding a Category" on page 130.
4. Specify a name for the account group.
5. Click **Add**.

   Account groups are represented by the icon.
6. To configure the group, continue with "Modifying an Account Group" on page 120.

Modifying an Account Group

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Account Groups**.
3. In the details pane, select the account group you want to modify and click the edit icon next to the account group name.
4. Modify the following fields:

   Name: Change the name of the group.

   Disabled: To disable the account group, click **Disabled**. A disabled account group is dimmed.

   Description: Add or change the description.

   Manager Name, Manager Tel., Manager Email: Specify the name, phone number, and e-mail address of the manager of the users in this account group.

   If these details have been entered in the manager's Framework user account details (see "Modify User: Account Details" on page 63), they can be entered automatically by selecting the manager's username from the drop-down list. This option is only available if you belong to a Framework user group with the read role defined for the auth module (see "Configuring Roles" on page 72).

   The manager details can be used in the Compliance Auditor.

   User Groups, Host Groups, Account Groups: From the lists of groups you have already defined, select or remove the user groups, host groups, and account groups. You can also add groups to an account group by dragging and dropping the groups to the target account group in the navigation pane.
5. Click **Modify**. You can now use this account group in rule conditions or as a script entity.

Deleting an Account Group

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Account Groups**.

3 In the details pane, select the account group that you want to delete and click the delete icon next to the account group name.

   To select multiple account groups, click the top level account group and click **Delete Multiple**.

4 Click **Delete**. The selected account groups are deleted and are also removed from any other account groups, rule conditions, and script entities where they have been defined.

Copying a Group

1 On the home page of the console, click **Command Control**.

2 Click the category of the group that you are copying such as **Account Groups**, **Host Groups**, or **User Groups**.

3 Select the group you want to copy.

4 To create the copy, press the Ctrl key and drag and drop the selected group to the desired location.

Moving a Group

1 On the home page of the console, click **Command Control**.

2 Click the category of the group you are copying such as **Account Groups**, **Host Groups**, or **User Groups**.

3 Select the group you want to move.

4 Drag and drop the selected group to the desired location.

You can also drag and drop account groups, user groups, and host groups into an account group. This does not delete the groups from their original location.

Finding a Group

1 On the home page of the console, click Accounts Group icon and select **Account Groups** in the middle pane.

2 In the details pane click **Find**.

3 In the **Account Group Filter** field type the required group name.

   For finding user groups or host groups, click **User Groups** or **Host Groups** in the middle pane, then click **Find** in the details pane.

Commands

Command definitions contain the commands you want to control. A command definition can contain a single command, or several commands that you want to control in the same way. You can also specify a command that you want to run in place of a submitted command.

- "Finding a Command" on page 122
- "Adding a Command" on page 122
- "Modifying a Command" on page 122
- "Setting the Command Risk" on page 126

- “Removing a Command Risk” on page 127
- “Copying a Command” on page 127
- “Moving a Command” on page 127
- “Deleting a Command” on page 127
- “Importing Sample Commands” on page 127

Finding a Command

1. On the home page of the console click **Command Control**.
2. In the navigation pane, select Commands icon and select **Command**.
3. In the details pane, select **Find**.
4. In the find filter, type the required name.

   As you type, the search displays the results. When you click on the required name, that command gets selected in the middle pane. If you require to modify that command you can modify it from the details pane.

Adding a Command

You can add command definitions to your rule conditions to control whether the rule is processed, depending on the command that is submitted by the user. You can also use commands as script entities.

To add a new command:

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Commands**.
3. In the details pane, click **Add** in the task pane. To add a command to a category, select the category and click **Add**.
4. Specify a name for the command. This can be different from the name of the actual command you want to control.
5. Click **Add**.
6. To configure the command, continue with “Modifying a Command” on page 122.

Modifying a Command

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Commands**.
3. In the details pane, select the command you want to modify and click on the edit icon next to it.
4. Configure the following fields:

   Name: Specify a different name for the command.

   Disabled: Select this check box to disable the command. A disabled command is dimmed.

   Description: Describe the purpose of this command.

Rewrite: In the **Rewrite** field, define a command to be used in place of the commands listed in the **Command** field. You can also enter command arguments. Positional parameters can be used, as described in "Using the Command Rewrite Functionality for Command Arguments" on page 125. To use the **Rewrite** field to enable auditing of the command, see "Configuring Auditing with the Rewrite Functionality" on page 126

Commands: Define one or more commands, one on each line. You can also enter command arguments. For example:

```
vi *
/usr/bin/vi *
```

To add a regular expression term to the list, prefix the regular expression with =~. For example,

```
=~/^vi .*$/
```

```
=~#/usr/bin/vi .*#
```

You can copy and paste a list of commands from elsewhere. You can use the **Sort** button to sort the commands into alphabetical order.

Sub Commands: From the list of command definitions you have already created, select the subcommands you want to include in this command definition. You can also add subcommands to a command definition by dragging and dropping them to the command definition in the navigation pane.

Refer the following table to modify the command fields based on the endpoint access methods:

Methods	Command fields
Unix/Linux	
pcksh	Specify values for the fields **Rewrite** and **Commands**. For example: **Rewrite:** /usr/bin/pcksh -o audit 1 **Commands:** (Specify the commands in separate line) pcksh shell
cpcksh	Specify values for the fields **Rewrite** and **Commands**. For example: **Rewrite:** /usr/bin/pcksh -o audit 1 **Commands:** `-cpcksh`
usrun	Specify the commands that require privileged access in the **Commands** field. For example: **Commands:** `*passwd`
Windows	
RDP Relay	Specify `<rdp>*` in the **Command** field.
Credential Provider	Specify <NPAMCP>* in the **Command** field.
Direct RDP	Specify `<rdpDirect>*` in the **Command** field.
Run as privileged user	Specify the process or files that require privileged access in the **Command** field. For example, if you want to give privileged access to notepad, you can specify the value in following ways: **Command:***notepad.exe* **Command:***note*d.e*e* **Command:***n.....ex.* You can also provide the absolute path of the application. For example, `C:\Windows\System32\notepad.exe`. If the absolute path contains space, include the absolute path between quotes. For example, `"C:\Program Files (x86)\WinSCP\WinSCP.exe"`.

5 Click **Finish**.

- “Using the Command Rewrite Functionality for Command Arguments” on page 125
- “Configuring Auditing with the Rewrite Functionality” on page 126

Using the Command Rewrite Functionality for Command Arguments

The following table provides examples showing how the command rewrite functionality provided on the Modify Command page can be used with positional parameters to replace the submitted command and parameters. The examples use the echo command as the rewritten command to display the selected parameters on the screen.

Table 8-1 *Command Rewrite Examples*

Function	Rewrite	Submitted Command	Executed Command
Insert all arguments ($0 is not displayed)	`echo $*`	`ls passwd shadow fstab`	`echo passwd shadow fstab`
Insert argument ’r;n’	`echo $3`	`ls passwd shadow fstab`	`echo fstab`
Insert all but argument 'n' ($0 is not displayed)	`echo ${^2}`	`ls passwd shadow fstab`	`echo passwd fstab`
Insert arguments from 'n' to end	`echo ${2-}`	`ls passwd shadow fstab`	`echo shadow fstab`
Insert arguments from 0 to 'n'	`echo ${-2}`	`ls passwd shadow fstab`	`echo ls passwd shadow`
Insert arguments from 'm' to 'n'	`echo ${1-2}`	`ls passwd shadow fstab`	`echo passwd shadow`
Insert the total number of arguments	`echo $#`	`ls passwd shadow fstab`	`echo 3`
Insert contents of argument $#	`echo ${$#}`	`ls passwd shadow fstab`	`echo fstab`

Rewrite Example Using ufsdump

In this example, the administrator usually does a backup of the system by using the following command:

```
ufsdump -0f /dev/rmt/0 /usr
```

Assume that new tape drive is installed on the host, and it must be used for the backup. In addition, the administrator must make sure that it is working correctly by using the -v flag to verify the tape.

You can ensure that the administrator doesn’t need to remember the changes by using the **Rewrite** field to create a command definition for the original command:

```
$0 -v $1 /dev/rmt/1 ${$#}
```

When the administrator enters the original command, the following command runs instead:

```
ufsdump -v -0f /dev/rmt/1 /usr
```

Configuring Auditing with the Rewrite Functionality

To enable auditing of the command, add the following to the **Rewrite** field:

```
-o audit <n>
```

Replace *<n>* with one of the following values:

- **0:** Disables auditing. It has the same effect as removing the audit setting from the **Rewrite** field.
- **1:** Enables auditing of all commands that are not built into the user's shell.
- **2:** Enables auditing of all commands, including commands that are built into the user's shell. This level of auditing can affect login times.

Setting the Command Risk

This option allows you to set a value representing the relative risk of a command when using the pcksh or cpcksh clients, the RDP sessions, and DB monitoring sessions with the session auditing option (see "cpcksh" on page 213). When you view a Command Control Keystroke Report, the commands with different risk values are represented in different colors.

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click the **Commands** icon.
3. In the details pane, click **Command Risk**.
4. Click **Add**.
5. Set a value for the command risk. You can specify any value between 0 to 9 where:
   - 0 indicates no risk
   - 1 – 3 indicate low risk
   - 4 – 6 indicate medium risk
   - 7 – 9 indicate high risk
6. Specify the command you want to set a risk value for, or the regular expression. You can use wildcard symbols.
7. If you want to base the risk level on the directory in which the command is running, define a working directory.
8. If you want to base the risk level on who is running the command, define a user.
9. If you want to base the risk level on the host where the command is running, define a host.
10. If you want to disconnect any particular user using a particular command, specify the user in the **Submit User** field.

    Ensure that the user name is typed in capital letters for the following users:
    - Windows users for Direct RDP
    - LDAP users who are part of the authentication domain
11. If you want to disconnect the user when the specified command is executed, specify 1 in the **Auto Disconnect** field.

    If you want to refrain the user from starting the session again after it was disconnected, specify 1 in the **Auto Block** field.

12 If you want to change the order in which the commands are listed, use the arrow buttons.

13 Click **Finish**.

Removing a Command Risk

1 On the home page of the console, click **Command Control**.

2 In the navigation pane, click the **Commands icon**.

3 In the details pane, click **Command Risk**.

4 Select the entry, then click **Remove**.

Copying a Command

1 On the home page of the console, click **Command Control** on the home page of the console.

2 In the navigation pane, click the **Commands** icon.

3 Select the command you want to copy.

To select multiple commands in the same category, press the Ctrl key and select the required commands one at a time, or press the Shift key to select a consecutive list of commands.

4 To create the copy, press the Ctrl key and drag and drop the selected command to the desired location

Moving a Command

1 On the home page of the console, click **Command Control**.

2 In the navigation pane, click **Commands**.

3 Select the command you want to move.

4 Drag and drop the selected command to the desired location.

Deleting a Command

1 On the home page of the console, click **Command Control**.

2 In the navigation pane, click **Commands**.

3 In the details pane, select the command you want to delete and click the delete icon next to it.

To select multiple commands in the same category, click **Delete Multiple** and select the required commands.

4 Click **Delete**. The selected commands are deleted and are also removed from any rule conditions and script entities in which they are defined.

Importing Sample Commands

Privileged Account Manager ships with the following types of sample commands that you can import and use or import and modify to fit your needs:

- Shell commands (`ksh`, `sh`, `csh`, `bash`)
- vi commands

- System commands (`kill, mount, passwd, date, mkdir, useradd, chgrp, chown`)
- User commands (`env, ls, id, cat uname`)

To import these sample commands, click `Command Control` > `Import Samples` > `Sample commands`.

Finding a Reference

The **Find References** option allows you to find where a specific account group, user group, host group, command, script, or access time is referenced in the database. For example, you could use this option to find out which account group or groups a specific user group belongs to.

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, select the required icon and select the entity for which you want to find references.
3. In the task pane, click the **Find References** icon. The groups or rules in which the entity is referenced are displayed.
4. To go to one of the listed groups or rules, click on **Goto Rule** or **Goto *<entity>***.

   To modify the rule or groups from the task pane, click **Modify Rule** or **Modify *<entity>***

Defining Custom Attributes

Custom attributes can be defined for account groups, user groups, host groups, commands, and access times to provide additional parameters for use in scripts. For example, you could set an expiration date as a custom attribute for a user group, check for this date in the script, then expire the user group when the date is reached.

To define custom attributes:

1. On the home page of the console, click **Command Control**.
2. Select the entity you want to add custom attributes to.
3. In the task pane, click the **Define Custom Attributes** icon.
4. Click **Add**.
5. In the **Name** field, specify the name of the custom attribute. For example, `Expiration date`.
6. In the **Value** field, specify the value for the attribute. For example, the date you want the entity to expire.
7. Repeat Step 4 through Step 6 for any other custom attributes you want to add.
8. Click **Finish**.

Functions

The udsh command invokes commands on a set of hosts. It concurrently issues a Command Control request for each host that is specified and returns the output from all the hosts, formatted so that command results from all hosts can be managed.

- "Syntax" on page 129
- "Options" on page 129
- "Keywords" on page 130

Syntax

```
udsh [-bcdqv] [-t <timeout>] [-l <user>] [-f <num>] [-w <host>, <host
wildcard>] [-g <hostgrp>, <hostgrp wildcard>] [cmd ...]
```

Options

The following options can be specified only on the command line:

Table 8-2 *udsh Options*

Option	Description
-b	Do not break lines to column width when displaying output.
-c	Do not remove the host from the list if the command fails.
-d	Add a time stamp to the displayed output.
-f *<num>*	Specify the maximum number of concurrent processes to run.
-g *<hostgrp>*, *<hostgrp wildcard>*	Specify the Command Control host groups to retrieve the list of agents to run the command on. Wildcards must be properly escaped. For example to run udsh against all host groups that begin with ho, enter the following: `-g ho\*`
-l *<user>*	Specify the user to run the command as.
-q	Quiet. Do not display output.
-t *<timeout>*	Specify the timeout in seconds for the command to complete on each host.
-v	Verbose output.
-w *<host>*, *<host wildcard>*	Specify the agents to run the command on. Wildcards must be properly escaped. For example, to run udsh against all hosts that begin with host1, enter the following: `-w host1\*`

If a command is not specified, the user is placed at a command prompt. Each entry run from this prompt is run separately on each host. If readline(3) is available, command line editing and history are provided.

Keywords

There are various macros that can be specified in the command to substitute keywords when the command is run on the remote host. For example, the following command uses the `${rhost}$` keyword. It performs a `usrun echo` command of the remote host name on all agents that have a command control agent deployed:

```
udsh -w \* /bin/echo '${rhost}$'
```

Table 8-3 *udsh Keywords*

Keyword	Description
${uid}$	Calling user's UID
${gid}$	Calling user's primary group ID
${gecos}$	Calling user's gecos
${home}$	Calling user's home directory
${shell}$	Calling user's shell
${cwd}$	Calling user's current working directory
${lhost}$	Local hostname
${rhost}$	Remote hostname
${pid}$	PID of the individual `udsh` call
${ppid}$	PID of the `udsh`

Adding a Category

You can use the appropriate **Add Category** option for account groups, user groups, host groups, commands, scripts, and access times into categories for ease of use and maintenance.

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click the required icon and select the section to which you want to add a category.

   You can also add subcategories to the existing categories.
3. In the task pane, click **Add Category**.
4. Specify a name for the category.
5. Click **Finish**.

Deleting a Category

Before deleting a category, you must delete or move the items and subcategories that it contains.

1 On the home page of the console, click **Command Control**.

2 In the navigation pane, select the category that you want to delete.

3 In the task pane, click **Delete Category**.

Blocked Users

The Blocked Users list displays all the users who are blocked from accessing any privileged account session. This group includes the list of users who are blocked from accessing any server. The users are either added automatically when you block the session during a manual/ automatic disconnect, or added manually when you block a user by adding the user to the **Blocked Users** list.

To add a user to the blocked user group refer, "Adding Users in Blocked Users Group" on page 131. If you do not want a particular user in the blocked list then you can delete the user from the list. To delete a user from the group refer, "Deleting Users in Blocked User Group" on page 131.

Adding Users in Blocked Users Group

1 In the navigation pane of the Command control console click the User Groups icon > **Blocked Users**.

2 In the details pane, click **Add** then specify the user.

IMPORTANT: The User Name must be provided in capital letters for the following type of users:

- Windows users for direct RDP
- LDAP users who are part of the authentication domain.

---

3 Click **Finish**.

Deleting Users in Blocked User Group

1 In the navigation pane of the Command control console click the User Groups icon > **Blocked Users**.

2 In the details pane, select the user that you require to remove from the blocked user list, then click the delete icon.

Scripts

You can use Perl scripts to provide additional, customized functionality to your rules. You can also use scripts in rule conditions. Privileged Account Manager contains the embedded Perl interpreter version 5.8.9. You can use any of the core Perl modules for your script. It is not recommended that you install any CPAN Perl modules into the embedded Perl interpreter. If you create a script, be aware that any time consuming tasks within the script affect response times.

- "Finding a Script" on page 132
- "Adding a Script" on page 132

- “Modifying a Script” on page 132
- “Copying a Script” on page 133
- “Moving a Script” on page 133
- “Deleting a Script” on page 133
- “Sample Scripts” on page 133

Finding a Script

1. On the home page of the console click Command Control
2. In the navigation pane, select Scripts icon and in the details pane select Scripts.
3. In the details pane, select Find.
4. In the filter type the required name.

   As you type, the search displays the results. When you click on the required name, that script gets selected in the middle pane. If you require to modify that script you can modify it from the details pane.

Adding a Script

You can add your own custom attributes for account groups, user groups, host groups, commands, and access times to provide additional parameters for use in your scripts. See “Defining Custom Attributes” on page 128 for details.

To add a new script:

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click the **Scripts** icon.
3. In the details pane, click **Add**. To add a script to a category, select the category and click **Add**.
4. Specify a name for the script.
5. Click **Add**.
6. To configure the script, continue with “Modifying a Script” on page 132.

Modifying a Script

1. On the home page of the console, click **Command Control** on the home page of the console.
2. In the navigation pane, click the **Scripts** icon.
3. Select the script you want to modify.
4. In the details pane, click the edit icon next to the script.
5. Configure the following fields:

   Name: Specify a different name for the script.

   Conditional script: Select the check box to set the script to be conditional. Scripts defined as conditional can be used in rule conditions. The return codes are limited to 1 for true and 0 for false.

   Disabled: Select the check box to disable the script. A disabled script is dimmed.

Description: Describe the purpose of the script.

Script: Specify the text of your script in the text box by typing it or by pasting it from elsewhere. The possible return codes you can use in your script for processing by the Command Control software are shown below this field.

For some sample scripts, see "Sample Scripts" on page 133.

6 Click **Modify**.

You can assign the script to a rule, or you can specify it in rule conditions if you have set the script to be conditional.

Copying a Script

1 On the home page of the console, click **Command Control**.

2 In the navigation pane, click **Scripts**.

3 Select the script you want to copy.

4 To create the copy, press the Ctrl key and drag and drop the selected script to the desired location.

5 If necessary, use the **Modify Script** option to rename or modify the copy. For details, see "Modifying a Script" on page 132.

Moving a Script

1 On the home page of the console, click **Command Control**.

2 In the navigation pane, click **Scripts**.

3 Select the script you want to move.

4 Drag and drop the selected script to the desired location.

Deleting a Script

1 On the home page of the console, click **Command Control**.

2 In the navigation pane, click.

3 Select the script you want to delete.

To delete multiple scripts click **Delete Multiple** and select the scripts from the list.

4 Click **Delete.**

Sample Scripts

Privileged Account Manager ships with the following sample scripts that you can import and use:

- Display message scripts
- Password validation scripts
- Alternate validation scripts
- Email scripts
- Modify environment script

- Emulate `su` script
- Secure `vi` script

Before creating your own Perl script, check out the sample scripts to see if one is available that meets your needs or one that can be modified to meet your needs. To understand what is available, see the sample scripts in the following sections.

- "Modify Environment Script" on page 134
- "pcksh Illegal Commands Script" on page 135

To import a sample script, click `Command Control` > `Import Samples` > `Sample Perl Script`.

Modify Environment Script

This script is used to process environment variables. It has a number of script arguments that can add, delete, clear, and keep environment variables.

Argument	Description
`clearenv=1:`	Clears all environment variables (unless specifically kept using keepenv)
`keepenv=VAR:`	Specifically keeps environment variables. As soon as this is set, all other environment variables are deleted.
`setenv=VAR=val:`	Sets up a specific environment variable.
`unsetenv=VAR:`	Deletes a specific environment variable.
`defaultenv=#:`	Sets the default environment: **0:** Sets up no default environment variables. **1:** Sets up all default environment variables. **2:** Sets up default environment variables that do not already exist in the environment.

Sample Environment Script

```
my $e=$meta->child("Environment");
return(1) if(! $e);

my $n=$e->node_args();
my %env=();

while($n) {
    $env{$1}=$2 if($n->key() ne "items" && $n->value() =~ /^(.*)=(.*)$/);
    $n=$n->next();
}

my %keepenv=();
my $clearenv=0;

for(my $a=$args->node_args();$a;$a=$a->next()) {
    if($a->key() eq "clearenv" && $a->value() > 0) {
        $clearenv=1;
```

```
    } elsif($a->key() eq "keepenv" && $a->value() ne "") {
        $keepenv{$a->value()}=1;
    } elsif($a->key() eq "defaultenv" && $a->value >= 0) {
        $meta->child("Job")->arg_int("job_default_env",$a->value());
    }
}

if(scalar %keepenv || $clearenv) {
    while(my ($key,$val) = each %env) {
        delete $env{$key} if(! $keepenv{$key});
    }
}

for(my $a=$args->node_args();$a;$a=$a->next()) {
    if($a->key() eq "unsetenv" && $a->value() ne "") {
        delete $env{$a->value()};
    } elsif($a->key() eq "setenv" && $a->value() =~ /^(.*)\s*=\s*(.*)$/) {
        $env{$1}=$2;
    }
}

$meta->del($e);
$e=$meta->add_node("Environment");

my $items=0;

while(my ($key,$val) = each(%env)) {
    $e->arg("arg-$items","$key=$val");
    $items++;
}

$e->arg_int("items","$items");

return(1);
```

pcksh Illegal Commands Script

When using the pcksh shell, Command Control has the ability to restrict the commands being run (even as root). This sample script is named illegalcmd, and it restricts the use of the `passwd` command.

This script does not restrict a user that initiates another shell from within a session. When a user does this, Command Control cannot continue a full audit or control the illegal commands, although the session is still captured

```
#to set script argument - name=illegalcmd value= kill *
my $t=$meta->get_params('Ticket');
if(! $t) {
$t=$meta->add_param('Ticket');
}

my $i=$t->get_params('IllegalCmds');
if(! $i) {
$i=$t->add_param('IllegalCmds');
}

my @illegal = $args->arg_values('illegalcmd');

#my @illegal=("echo","ls -l","passwd","/usr/bin/ls -l","ksh","echo date");
foreach my $b (@illegal) {
my $c=$i->add_param('Command');
$c->arg("cmd",$b);
}
return 1;
```

Access Times

You can restrict the times when a rule is valid by defining an access time and adding it to the rule conditions. You can also use access times as script entities.

- "Finding an Access Time" on page 136
- "Adding an Access Time" on page 136
- "Modifying an Access Time" on page 137
- "Copying an Access Time" on page 137
- "Moving an Access Time" on page 137
- "Deleting an Access Time" on page 138

Finding an Access Time

1. On the home page of the console click Command Control
2. In the navigation pane, select Access Times icon and in the details pane select Access Time.
3. In the details pane, select Find.
4. In the filter type the required name.

   As you type, the search displays the results. When you click on the required access time, that gets selected in the middle pane. In the details pane, click modify to modify the access time.

Adding an Access Time

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click the **Access Times** icon.
3. In the details pane, click **Add**. To add an access time to a category, select the category and click **Add**.

4 Specify a name for the access time, for example, `Office hours`.

5 Click **Add**.

6 To configure the access time, continue with "Modifying an Access Time" on page 137.

Modifying an Access Time

1 On the home page of the console, click **Command Control**.

2 In the navigation pane, click **Access Times**.

3 In the details pane, select the access time you want to modify and click the edit icon next to it.

4 Modify the access time as required:

- Change the name of the access time.
- Specify a description of the access time.
- Click **Disabled** to disable the access time. A disabled access time is dimmed.
- Set the access time as described in Step 5.

5 Set the access time in multiples of half-hourly intervals. The default access time is set to **Deny Access** for the whole week, shown in the calendar as blue.

- To allow access at specific times, drag and drop across the days and times until the hours when you want to grant access are shown in green,
- To allow access for the majority of times and deny access for specific times, click the **Grant Access** box below the table to grant access for the whole week, then click and drag across the days and times until the hours when you want to deny access are shown in blue.

For example, to allow access only during the hours from 9:00 to 18:00 from Monday to Friday:

5a Ensure that the whole week is set to Deny Access (blue).

5b Click in the calendar on 9 on Monday morning, then drag and drop to 18 and down to Friday. This creates a green block representing the times when access is allowed.

6 Click **Finish**. You can now use this access time in rule conditions or as a script entity.

Copying an Access Time

1 On the home page of the console, click **Command Control**.

2 In the navigation pane, click **Access Times**.

3 Select the access time you want to copy.

4 To create the copy, press the Ctrl key and drag the selected access time and drop it to the desired location.

5 If necessary, rename or modify the copy by using the **Modify Access Time** option, as described in "Modifying an Access Time" on page 137.

Moving an Access Time

1 On the home page of the console, click **Command Control**.

2 In the navigation pane, click **Access Times** in the navigation pane.

3 Select the access time you want to move.

4 Drag and drop the selected access time to the desired location.

Deleting an Access Time

1 On the home page of the console, click **Command Control**.

2 In the navigation pane, click **Access Times**.

3 In the details pane, select the access time you want to delete and click the delete icon next to the access time.

To delete multiple access times in the same category, click **Delete Multiple** and select the access times.

4 Click **Delete**.

The access time is deleted, and is also removed from any rule conditions and script entities in which it is defined.

Command Control Reports

You can configure customized reports of the contents of the Command Control configuration database, which are dynamically created and e-mailed to the specified person at defined intervals. You can use Perl template scripting to extract the required information and format it into an e-mail for the target person. An option is available for sending your reports to the Compliance Auditor for escalation management.

To use this feature, you must provide details of your e-mail server to the Messaging Component (msgagnt) so that reports can be e-mailed. See "Configuring SMTP Settings for the Messaging Component Package" on page 41 for details.

- "Finding a Report" on page 138
- "Adding a Command Control Report" on page 139
- "Modifying a Command Control Report" on page 139
- "Copying a Command Control Report" on page 140
- "Moving a Command Control Report" on page 140
- "Deleting a Command Control Report" on page 140

Finding a Report

1 On the home page of the console click Command Control

2 In the navigation pane, select Reports icon and in the details pane select Reports.

3 In the details pane, select Find.

4 In the filter type the required name.

As you type, the search displays the results. When you click on the required name, that report gets selected in the middle pane. If you require to modify that report you can modify it from the details pane.

Adding a Command Control Report

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Reports**.
3. In the details pane, click **Add**.

   To add a report to a category, select the category and click **Add**.
4. Specify a name for the report.
5. Click **Add**.
6. To configure the report, continue with "Modifying a Command Control Report" on page 139.

Modifying a Command Control Report

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click the **Reports** icon and click **Report**.
3. In the details pane, select the report you want to modify and click the edit icon next to it.
4. Modify the report as required:
   - Change the name of the report.
   - Click **Disabled** to disable the report. A disabled report is dimmed.
   - Set the **Run Report** settings to determine the time of the first report and subsequent frequency of each report. You can set the initial date by using the calendar and type in the time, then set the frequency as required.
5. Select the e-mail options you want:

   5a In the **Email To** field, specify the e-mail address of the person you want to send the report to.

   5b In the **Email From** field, specify the e-mail address of the person you want to send the report from.

   5c In the **Email Subject** field, specify a subject for the e-mail.

   5d If you want the e-mail to be displayed in HTML, select the **HTML** check box.

   5e If you require a receipt, select the **Receipt** check box.

   5f Enter a Perl script in the **Report Template** field to control how the e-mail will be formatted and what it will contain.

   5g If you want the report to be available for auditing through Compliance Auditor, select the **Audit** check box.
6. If you want to send an e-mail while testing this report, select the **Send email** check box.
7. (Optional) Click **Test Report** to view the report that will be sent to the defined e-mail address. If there are errors in the Report Template, those are displayed.
8. Click **Back** to return to the report configuration page.
9. Click **Finish**.

Copying a Command Control Report

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Reports**.
3. Select the report you want to copy.
4. To create the copy, press the Ctrl key and drag and drop the selected report to the desired location.
5. If necessary, use the **Modify Report** option to rename or modify the copy, as explained in "Modifying a Command Control Report" on page 139.

Moving a Command Control Report

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click **Reports**.
3. Select the report you want to move.
4. Drag and drop the selected report to the desired location.

Deleting a Command Control Report

1. On the home page of the console, click **Command Control** on the home page of the console.
2. In the navigation pane, click the Reports icon and click **Report**.
3. In the details pane, select the report you want to delete and click the delete icon next to the report.

   To select multiple reports in the same category, click **Delete Multiple** and select the reports.
4. Click **Delete.**

Command Control Options

Importing and Exporting Command Control Configuration Data

You can import a complete command control configuration database, including test suites, using the Import Settings option, or you can import test suites only, using the Import Test Suites option under Test Suites.

If you import a complete command control configuration database, all existing data is overwritten, including test suites. If you import test suites only, they are added to the existing configuration and do not overwrite the existing test suites.

- "Exporting Command Control Settings" on page 141
- "Importing Command Control Settings" on page 141
- "Importing Command Control Samples" on page 142

Exporting Command Control Settings

You can export the Command Control configuration settings to a text file for backup purposes, or for use in another Framework. You use the **Import Settings** option to restore the backed-up configuration settings, or to import the settings into another Framework.

NOTE: NetIQ recommends that you take frequent backups of the Command Control configuration settings.

---

1. On the home page of the console, click **Command Control**.
2. In the command control pane, click **Command Control**.
3. In the details pane, click **Export Settings**.
4. Use Ctrl+A to select all the Command Control configuration settings, or right-click in the text window and click **Select All**.
5. Use Ctrl+C to copy the settings, or right-click in the text window and click **Copy**.
6. Paste the text into a text document and save it.
7. Click **Close**.

To use a command line option to export Command Control settings, see "Importing and Exporting Command Control Settings" on page 178.

Importing Command Control Settings

You can use the **Import Settings** option to restore a previously backed-up version of the Command Control configuration settings, or to import Command Control configuration settings from another Framework. You then use the **Export Settings** option to obtain configuration settings so you can paste them into a text document for backup or for use on another Framework.

IMPORTANT: This process overwrites the existing configuration settings.

---

1. Access the Command Control configuration settings you need and copy the whole configuration.
2. On the home page of the console, click **Command Control**.
3. In the Command Control pane, click **Command control**.
4. In the details pane, click **Import Settings**.
5. Click in the text area, then use Ctrl+V to paste the copied settings, or right-click in the text area and click **Paste**.
6. Click **Finish**.

To use a command line option to import Command Control settings, see "Importing and Exporting Command Control Settings" on page 178.

Importing Command Control Samples

NetIQ Privileged Account Manager provides a set of sample commands and Perl scripts to assist you with configuring the Command Control rules.

To add these samples to the configuration:

1. On the home page of the console, click **Command Control**.
2. In the command control pane, click **Command Control**.
3. In the details pane, click **Import Samples**.
4. Select the samples you want.

   To select multiple samples in a folder, display the samples, then press the Ctrl key and select the required samples one at a time, or press the Shift key and select a consecutive list of samples. You cannot import samples by selecting a folder.
5. Click **Finish**. The samples are added to the appropriate section of the configuration.

Command Control Transactions

The Command Control database can be protected through the use of the Transactions feature, which automatically locks the database when you start making changes and prevents other Framework users from making any changes. You must then commit the transaction to save the changes and release the lock, and you are prompted by customized questions to provide information that can be viewed in the Compliance Auditor. You can cancel the transaction at any time.

To use this feature, you must first enable it and create a customized Commit Transactions page, then you can use the feature and commit the changes you have made.

- "Enabling Transactions and Configuring Settings" on page 142
- "Making Command Control Configuration Changes with Transactions Enabled" on page 143
- "Committing a Transaction" on page 143

Enabling Transactions and Configuring Settings

You can configure the Command Control Manager to use the Transactions feature when configuring Command Control rules.

You can also configure the Commit Transaction page that can be used for committing a transaction. The data entered on the Commit Transaction page is displayed in Compliance Auditor.

To configure this feature:

1. On the home page of the console, click **Command Control**.
2. In the command control pane, click **Command Control**.
3. In the details pane, click **Transaction Settings**.
4. Select the **Enable Transaction** check box to enable the use of Command Control transactions.
5. Click **Add**.

6 Specify a name for the field that you want to be displayed when a user commits a transaction. For example, to request the user's name when committing a transaction, specify the value as **Name**.

7 Select **Text** if you want the user to enter one line of text, or select **TextArea** if you want the user to be able to enter several lines of text.

8 Select **required** if you want to force the user to enter text in this field. The **Finish** button on the **Commit Transaction** page does not become available until the user has entered text in this field.

9 Repeat Step 5 through Step 8 for any other fields you want to display when the user commits the transaction.

10 Select **Finish**.

Making Command Control Configuration Changes with Transactions Enabled

1 On the home page of the console, click **Command Control**.

2 Make the configuration changes you want.

   A message appears next to **Command Control** in the navigation pane to indicate that the Command Control database is locked, by whom, and when it was locked.

3 In the command control pane, click **Command Control**, then in the details pane, click **Commit Transaction**.

   Complete the fields as set up on the Transaction Settings page, then click **Finish**.

   Alternatively, if you do not want to keep the changes you have made, select **Cancel Transaction** in the details pane and select **Yes** to confirm. Any changes you have made since the database was locked are removed.

Committing a Transaction

When you have finished changing the Command Control database, you must commit the transaction to save the changes and release the lock on the database. The Commit Transaction page can be customized to request whatever information you require when a transaction is committed (see "Enabling Transactions and Configuring Settings" on page 142 for details).

To commit a transaction:

1 On the home page of the console, click **Command Control**.

2 In the command control pane, click Command Control.

3 In the details pane, click **Commit Transaction**.

4 To create a backup of the Command Control database enable the **Create Backup** checkbox to restore it in future and, then specify a reason for the backup in the text box.

5 Complete the customized fields according to company policies.

6 Click **Finish**.

Defining Audit Settings

All Command Control audit records contain the following information:

- Submit details such as, the submitting username, hostname, and primary group.
- Target details such as, the run username and the run hostname.
- Command details, which include the original command requested and the actual command run.
- Authorization status, either yes or no.
- Session capture status, either yes or no.
- Audit ID, which is the unique ID used to group audit events for the user's session.
- Codeset, which is the character encoding used for localization.
- Terminal details such as tty name, terminal dimensions, and type.

The **Audit Settings** option allows you to modify this default record and add the following:

- Encryption of sensitive password data in keystroke capture reports along with a password that allows authorized Framework administrators to decrypt it.
- Additional options that can be audited for each record.

To define audit settings:

1. On the home page of the console, click **Command Control**.
2. In the command control pane, click **Command Control**.
3. In the details pane, click **Audit Settings**.
4. Configure the Password keystroke settings:
   - **4a** Select the **Password filter** check box.
   - **4b** In the **Password filter** text box, specify the text that is used to prompt users for their passwords.

     For example, if the systems request a user's password by using the word `Password`, specify `Password` in this field. If the systems use `password`, enter `password` in this field. This ensures that the password the user enters in response to this prompt is encrypted in the command control reports.

     You can also use regular expressions as a password filter.

     For example:

     ```
     =~#([Pp]assword:)|(RDN:)#
     ```

     This password filter would match Password, password, or RDN.
   - **4c** Select the **Encryption password** check box.

     NOTE: If a filter is set and the **Encryption Password** is not set, then the filtered data is deleted from audit records.
   - **4d** In the **Encryption password** text box, specify the password that you require to decrypt the sensitive password data in the report.

This password must be entered on the **Command Control Keystroke Report** page under the Reporting console to decrypt the password data.

4e Specify the password again in the **Confirm password** text box.

5 (Optional) Select the required check boxes under **Metadata Audit Settings** to add more information to the audit record:

Command: Complete information about the command being run, including the actual filename and arguments.

Host: Information about the submitting host

Environment: Complete list of the environment variables that are passed to the executed command.

Local time: The time on the machine that submitted the request.

Cwd: Details about the current working directory where the command was executed.

Options: Details about the various process control options for executing the command.

Run Account: Information about the account that is used to execute the command.

Process: Details about the process that submitted the request.

Jobs: The job control setting that were passed to the executed command.

Passwd: Details of the `/etc/passwd` entry for the user submitting the request.

Groups: The group membership details for the executed command.

Logon: The login time and source for the user submitting the request.

6 Click **Finish**.

Backing Up and Restoring

The backup option allows you to create snapshots of the command control database and restore these snapshots at future date. You can back up and restore from the Framework Manager console, but you need to use the command line to remove a backed-up snapshot. For information about the command line options, see "Backing Up and Restoring a Command Control Configuration" on page 179.

1 On the home page of the console, click **Command Control**.

2 In the Command Control pane, click **Command Control**.

3 In the details pane, click **Backup and Restore**.

4 To back up the database, specify a reason for the backup, then click **Backup**.

5 To restore a previous version of the database, select the version, then click **Restore**.

The current version is overwritten by the selected version.

6 Click **Close**.

The following information is recorded for each backed-up version:

Date: The date and time the backup was performed.

Administrator: The user that performed the backup.

Reason: The reason for performing the backup. This is optional information, but recommended.

Test Suites

Command control test suites allow you to test the defined rules by running specified commands, submit users and other input values through your rule configuration, and performs a check to ensure the result is as expected. Each test suite can contain a number of test cases where you specify the expected outcome for one or more input values.

- "Adding a Test Suite" on page 146
- "Adding or Modifying a Test Case" on page 146
- "Running a Test Suite" on page 148
- "Viewing a Test Suite" on page 148
- "Modifying a Test Suite" on page 149
- "Deleting a Test Case" on page 149
- "Deleting a Test Suite" on page 149
- "Importing a Test Suite" on page 149
- "Exporting a Test Suite" on page 150

Adding a Test Suite

1. On the home page of the console, click **Command Control**.
2. In the Command Control pane, click **Command Control**.
3. In the details pane, click **Test Suites**.
4. Click **Add Test Suite** in the task pane.
5. Specify a name for the test suite.
6. Specify a description for the test suite.
7. Click **Finish**.
8. Continue with "Adding or Modifying a Test Case" on page 146 to add test cases to your test suite.

Adding or Modifying a Test Case

A test case allows you to emulate an end user running a command through the Command Control system.

1. On the home page of the console, click **Command Control**.
2. In the details pane, click **Test Suites**.
3. Select the test suite to add a test case, or modify an existing test case.
4. In the details pane, click **View Test Suite**.
5. Perform either of the following:
   - To add a new test case, click **Add Test Case** in the task pane.
   - To modify a test case, select the test case, then click **Modify Test Case**.

6 Specify the values and the expected results that you want to run through the rule configuration. (To review the rule configuration you want to test with this case, see "Modifying a Rule" on page 109.)

Enter a single value in each field. The purpose of the test case is emulate the user performing a `usrun` command from the command line.

- To create a test case that can be used for general testing and could possible match multiple rules, supply only submit information for the test case.
- To create a test case that matches only one rule, use the expected fields to specify values that match a single rule.

Command: (Required) Specify the command the user would run.

For example, if the user would enter the following on the command line:

```
usrun passwd user1
```

Specify the following as the command:

```
passwd user1
```

Submit User: (Required) Specify the name of the user who is entering the privileged command.

Submit Host: (Required) Specify the name of the host that the submit user is logged in to.

Run User: (Optional) When the submit user is requesting to run the command as a specific user with the usrun command, specify the username that is being requested. For example, if the user would enter the following on the command line:

```
usrun -u root ksh
```

Specify the following as the run user:

```
root
```

Run Host: (Optional) When the submit user is requesting to run the command on a specific host, specify the hostname that is being requested. For example, if the user would enter the following on the command line:

```
usrun -h hosta ksh
```

Specify the following as the run host:

```
hosta
```

User Input: (Optional) Use this field to specify the information that a script, associated with the Command Control policy, expects the user to enter.

Expected command: (Optional) Use this field to confirm that the command being executed is the correct command. If the command specified in this field does not match the results, the test case fails.

Expected authorized: (Optional) Use this field to confirm that the request was authorised. If value in this field does not match the results, the test case fails.

Expected capture: (Optional) This field is compared with the result of the authorization request to confirm the capture mode is correct. If this field does not match the results, the test case fails.

Expected run user: (Optional) Use this field to confirm that the user context used to execute the command is correct. If this field does not match the results, the test case fails.

Expected run host: (Optional) Use this field to confirm that the host on which the command is being executed is correct. If this field does not match the results, the test case fails.

Expected risk: (Optional) This field is compared with the result of the authorization request in order to confirm the risk associated with the command being executed is correct. If this field does not match the results, the test case fails.

Submit Time: (Optional) Specify the time that the request should appear to be made. This is useful for testing access time restrictions in the policy.

Custom Input: (Optional) Use this field to add attributes within the request object. These XML definitions are inserted into the privileged request. For example, you could use this field to configure the group memberships for a user in order to test policies that perform tests on the user's group membership:

```
<Groups>
  <Group name='grpa'/>
  <Group name='grpb'/>
</Groups>
```

7 Click **Finish**. The input values are shown in the **Test Cases** table.

8 Repeat Step 5 through Step 7 for any additional test cases you want to include or modify in this test suite.

You can now run the test suite as explained in "Running a Test Suite" on page 148.

Running a Test Suite

1 On the home page of the console, click **Command Control**.

2 In the details pane, click **Test Suites**.

3 Select the required test suite.

To select multiple test suites, press the Ctrl key and select the required test suites one at a time, or press the Shift key to select a consecutive list of test suites. Use Ctrl+A to select all test suites.

4 Click **Run Test Suites** in the task pane. The results are displayed for each test case as Success or as Failure, along with the reason for the failure.

5 Use the buttons on the left and right of the table to find previous successes and failures, and the next successes and failures.

6 To view further details on a specific entry, select the entry and click **Details**.

The configuration for the test case is shown, and a list of rules that have been tested, with configuration settings for each rule. The **Matched** column shows true if the rule conditions were met, and false if the rule conditions were not met.

7 Click **Back** to return to the main Run Test Suite page.

8 Click **Cancel** to return to the list of test suites.

To use a command line option to run a test suite or to run a specific test case, see "Running Test Suites" on page 181.

Viewing a Test Suite

1 On the home page of the console, click **Command Control**.

2 In the details pane, click **Test Suites**.

3 Select the required test suite, then click **View Test Suite**.

From here you can also modify the test suite; add, modify and delete test cases; and run the test suite.

Modifying a Test Suite

1 On the home page of the console, click **Command Control**.
2 In the details pane, click **Test Suites**.
3 Select the test suite you want to modify.
4 In the details pane, click **View Test Suite**.
5 Click **Modify Test Suite**.
6 Modify the test suite as desired:
   - Change the name of the test suite.
   - Add or change the description.
   - Use the **Up** and **Down** buttons to change the order in which the test cases are run.
7 Click **Finish**.

Deleting a Test Case

1 On the home page of the console, click **Command Control**.
2 In the details pane, click **Test Suites**.
3 Select the test suite from which you want to delete a test case.
4 In the details pane, click **View Test Suite**.
5 Select the test case to delete.
6 In the details pane, click **Delete Test Case**.
7 Click **Yes** to confirm the deletion.

Deleting a Test Suite

1 On the home page of the console, click **Command Control**.
2 In the details pane, click **Test Suites**.
3 Select the test suite that you want to delete.

To select multiple test suites, press the Ctrl key and select the required test suites one at a time, or press the Shift key to select a consecutive list of test suites.

4 Click **Delete Test Suite**.
5 Click **Yes** to confirm the deletion.

Importing a Test Suite

You use the **Import Test Suites** option to restores a previously backed-up test suite, or to test suites from another Framework. You then use the **Export Test Suites** option to obtain configuration details so you can then paste them into a text document for backup or for use on another Framework.

NOTE: When you import test suites, they are added to your existing configuration and do not overwrite your existing test suites. However, if you import a Command Control database by using the **Import Settings** option, your existing test suites are overwritten.

1. Access the test suite data you require and copy it.
2. Click **Command Control** on the home page of the console.
3. Click **Test Suites** in the task pane.
4. Click **Import Test Suites** in the task pane.
5. Click in the text area, then paste the copied settings by using Ctrl+V, or right-click in the text area and click **Paste**.
6. Click **Finish**.

Exporting a Test Suite

You can export your Command Control test suites to a text file for backup purposes, or for use in another Framework. You can then use the **Import Test Suites** option to restore the backed-up test suites, or to import the test suites into another Framework.

1. Click **Command Control** on the home page of the console.
2. Click **Test Suites** in the task pane.
3. Select the test suite you want to export.

   To select multiple test suites, press the Ctrl key and select the required test suites one at a time, or press the Shift key to select a consecutive list of test suites. To select all test suites, use Ctrl+A.
4. Click **Export Test Suites** in the task pane.
5. Select the test suite data by using Ctrl+A, or right-click in the text window and click **Select All**.
6. Copy the test suite data by using Ctrl+C, or right-click in the text window and click **Copy**.
7. Paste the text into a text document.
8. Click **Finish**.

Creating Default Objects

When you install Privileged Account Manager, some objects are created by default. These are required for the proper functioning of the policies. If you have upgraded from an earlier release to the latest release, the manager for Privileged Account Manager may not have all the new default objects. You can add those default objects by using the **Create Default Objects** option in the **Command Control** console.

To create default objects, perform the following:

1. On the home page of the administrator console, click **Command Control**.
2. In the left pane click **Command Control**.
3. In the details pane, click **Create Default Objects**.
4. Click **Create**.

Disconnecting a Privileged Session

A privileged user is allowed to start a remote desktop session to a Windows server or desktop by using RDP relay, Direct RDP or Credential Provider, and to a Linux server by using pcksh and SSH relay. But if the user performs an action that is unauthorized, you as an administrator can disconnect that session and if required you can block the user from starting the session again. The administrator can configure the level of risk, enable auto disconnect, and enable auto block. You can either disconnect the session manually or you can configure this feature to disconnect the session automatically.

You can also disconnect a database or an application session.

Prerequisites for Disconnecting a Session

- When defining policies ensure that **Run Host** should be same as the agent name that you have specified in the **Host** console.
- If you want to grant access to any framework user to use the reporting console that includes the disconnect field, then in the **Framework User Manager** console, you need to add the user to a group that has a role with the following specification:
  - **Module:** *
  - **Role:** *

  For information about **Framework User Manager**, refer Chapter 6, "Managing Framework Users and Groups," on page 57.

Disconnecting the Session Manually

When you, as an administrator, are monitoring every activity that is performed on a remote machine for a particular session, and if you find an unexpected command that is run on the remote server, you can disconnect the session manually and send the reason for disconnecting the session to the user. You can also block the user from using the session again.

The administrator can disconnect the session when a high risk level or any suspicious activity is displayed in the Report data of the Reporting console. To disconnect a user from the session on which an unauthorized command is used, perform the following steps in the **Reporting** console:

1. Click **Command Control Reports** then select the report.
2. Open the session that is active.
3. In the **Disconnect Reason** field, specify the reason for disconnecting the session.

   This is required for auditing.
4. (Conditional) If you want to block the user from connecting to the same session, select **Block User**.

   By default this checkbox is deselected. Because you may not want to block the user but warn the user about the unauthorized activity that was performed during the session.

   NOTE: When you block a user from a session, the user gets added to the **Blocked Users** list and the user will be blocked from accessing any of the sessions.

   ---
5. Click **Disconnect**.

Disconnecting the Session Automatically

You can automatically disconnect the session based on the risk of using a command. In case of emergency access, the session is disconnected automatically based on the expiry time that is specified for emergency access.

NOTE: An SSH relay session cannot be disconnected automatically.

Disconnecting a Session Based on Risk Level

An Administrator can configure **Command Risk** to automatically disconnect a remote session when a particular risk level is detected or when a user executes a particular command.

The administrator can add commands to a rule and enable the auto disconnect feature for the required commands that can be performed on the remote Windows server or desktop.

NOTE: For a pcksh session: the disconnect based on the risk can happen either when the command `/usr/bin/pcksh -o audit 1` or /usr/bin/pcksh -o audit 2 is defined in the **Rewrite** field for the **Commands** object, or when the **Enhanced Access Control Policy** script is added.

To configure disconnecting the session automatically, perform the following:

1. In the navigation pane of the command control console, click the command icon then select **Command**.
2. In the details pane, click **Command risk**.
3. Set **Command Risk**.

   For information on setting the command risk refer "Setting the Command Risk" on page 126.

   Specifying 1 in **Auto disconnect** field will automatically disconnect the user when the specified command is executed on the host server. Specifying 1 in **Auto Block** will block the user from further starting the session.

Disconnecting a Session Based on Expiry of an Emergency Access Request

When you have approved a request for emergency access for a specific time frame, the session gets expired after the expiry time that includes the grace period with the specified time. To disconnect a session based on the expiry time you need to configure the administrative settings for emergency access. For information about configuring the settings, refer "Configuring Emergency Access Settings" on page 291.

Viewing the Disconnect fields in the Reporting Console

In the Reporting console, an administrator can view which session was disconnected, the type of disconnect (automatic or manual disconnect), and the reason of disconnecting the session. This can be monitored by using Command Control Reports. To include the fields that display the disconnect information you must perform the following:

1. On the home page of the console, click **Reporting**.
2. Click **Command Control Reports** then, click the required report.

To add a report, refer section "Adding a Report" on page 86.

3 Click the **Filter** tab then, select **Disconnect Details**.

The **Disconnect Type** and the **Disconnect Reason** fields are displayed under **Report Data**.

To view the reports for only the disconnected sessions, select **Disconnect Report** in the **Command Control Reports**.

9 Compliance Auditor

The Compliance Auditor collects, filters, and generates reports of audit data for analysis and sign-off by authorized personnel. The Compliance Auditor can be used in conjunction with Command Control to enable auditors to view security transactions and play back recordings of user activity. Auditors can record notes against each record, creating permanent archives of activity.

Rules can be configured to pull any number of audit events matching a given filter into the Compliance Auditor at specific intervals. Examples of filters include username, host, and command for Command Control. Roles can be assigned to each rule to ensure that an auditor is able to view only extracted records with a matching role defined in his or her user account. In addition, Access Control Levels (ACLs) can be defined to restrict access to individual events, and to prevent users from auditing their own activity.

When an audit event is viewed, auditors can authorize the event, or mark it as unauthorized, escalate it, and assign it to someone else. Each change is recorded in an indelible audit trail within each record, along with any notes made by the auditor. Automatic reports can be generated and e-mailed to the appropriate personnel, and can be used, for example, for daily reporting to managers on audit activity awaiting sign-off, or hourly reporting triggered by an escalation value to notify senior management of activity.

To use the Compliance Auditor:

- Define roles in user groups to control user access to the Compliance Auditor. See "Controlling Access to the Compliance Auditor" on page 156.
- Create one or more rules to pull the required events into the Compliance Auditor. See "Adding or Modifying an Audit Rule" on page 157.
- Define ACLs for individual users. See "Access Control Levels" on page 169.
- View event records and authorize them, or mark them as unauthorized and define further action. See "Compliance Auditor Records" on page 164.
- Configure auditing reports to be automatically e-mailed to the appropriate personnel. See "Adding, Copying and Modifying an Audit Report" on page 158.
- Provide failover and load balancing by installing the Compliance Auditor on multiple hosts. See "Deploying the Compliance Auditor" on page 170.
- Export and import compliance auditing settings. See "Exporting and Importing Compliance Auditor Settings" on page 186.

Controlling Access to the Compliance Auditor

Roles can be used to restrict the Compliance Auditor options available to Framework users. For example, you might want users to be able to audit events, but not administer rules, ACLs, or reports.

To define roles for a user group to control use of the Compliance Auditor:

1. Click **Framework User Manager** on the home page of the console.
2. (Conditional) To add a new group, click **Groups** > **Create**, specify a name, then click **Add**.
3. To modify an existing group or configure the group you just created, select the group, then click **Edit**.
4. Select the users you want to be members of this compliance auditing group.
5. In the **Roles** option, click **Add**, then add the following roles

Module	Role	Description
secaudit	console	View the Compliance Auditor console.
secaudit	audit	View and edit records.
secaudit	*<audit role name>*	(Optional) Custom role. Allows the users to access records retrieved by the Audit Rules configured to use this Audit Role. If you do not add the *<audit role name>* role, the users can only access records generated by rules with no Audit Role defined.
audit	read	View a keystroke replay.

   Users belonging to this group can access the Compliance Auditor console, view and edit records, and review keystroke logs. If you do not add the *<audit role name>* role, the users can access all records. If you add the *<audit role name>* role, the users can access only the records retrieved by the Audit rules configured to use this Audit Role.

   With these roles, the users cannot manage rules, reports, or ACLs. For the roles required for these additional tasks, see "Compliance Auditor Roles" on page 75.

6. Click **Update**.
7. To continue setting up the Compliance Auditor, see "Adding or Modifying an Audit Rule" on page 157.

Compliance Audit Rules

Audit rules specify the events to be pulled in to the Compliance Auditor for viewing and authorization. You can specify:

- The filters to display the type of event
- The number of events
- The time and frequency when the events are pulled in
- An audit role to restrict access to records of events pulled in by a specific rule

To add or modify a rule, see "Adding or Modifying an Audit Rule" on page 157.

Adding or Modifying an Audit Rule

You can add, modify, and disable audit rules, but you cannot delete them.

1. Click **Compliance Auditor** on the home page of the console.
2. Click **Audit Rules** in the task pane.
3. Select one of the following:
   - To add a new rule, click **Add** in the task pane
   - To modify an existing rule, select the rule, then click **Modify**
   - To copy an existing rule and modify it, select the rule, then click **Copy**.
4. Configure the following fields:

   Rule Name: Specify a name for your rule.

   Disabled: Select the check box to disable the rule.

   By default, disabled rules are not shown in the rule list. You cannot delete a rule.

   Records and All Records: To collect all records, enable the **All Records** check box, or deselect the **All Records** option and set the number of records to be collected on each audit run.

   Audit Role: (Optional) Specify the audit role that has been assigned to a group. For configuration information, see Step 5 in "Controlling Access to the Compliance Auditor" on page 156.

   Run Filter: To determine the time and frequency of each audit run, use the calendar to set the initial date, then set the frequency as required.

   Audit Category: Select the category of events to audit.

   Add Filter: (Optional) Select one or more filters from the **Add Filter** drop-down list for the type of event you want this rule to pull in, and configure them as required

   The filters and configuration options depend on the **Audit Category** selected. For example, you can choose to pull in only those Command Control events that have been submitted by a particular user and that include a session capture.

   Filters: Filters section displays all the filters added by you. You can add more than one filter of the same type for filters such as the Command Control Submit User, then select the logic you require from AND or OR. You can also set these filters to be inclusive or exclusive using **matches** or **does not match**.

   You can remove a filter by clicking the button to the right of the filter.
5. Click **Finish**.

Compliance Audit Reports

You can configure customized reports of events that require compliance auditing. The reports are dynamically created and e-mailed to selected users at defined intervals. You can use filtering and Perl template scripting to extract the appropriate event information and format it into an e-mail for each target user.

Audit reporting uses a tokens object that contains all the user information and other information. You can use keyword anchors in your report configuration, which are replaced by the appropriate values from the tokens object. It is also possible for the Perl code in the report template to set values in the tokens object. Sample report templates are supplied to assist you with creating your own.

- "Adding, Copying and Modifying an Audit Report" on page 158
- "Sample Command Control Report Template" on page 160
- "Deleting a Report" on page 164

Adding, Copying and Modifying an Audit Report

To use this feature, you must provide details of your e-mail server to the Messaging Component (msgagnt) so that reports can be e-mailed. See "Configuring SMTP Settings for the Messaging Component Package" on page 41 for details.

To add or modify an audit report:

1. Click **Compliance Auditor** on the home page of the console.
2. Click **Audit Reports** in the task pane.
3. Select one of the following:
   - To add a new report, click **Add** in the task pane.
   - To modify an existing report, select the required report, then click **Modify** in the task pane.
   - To copy an existing report, select the report, then click **Copy** in the task pane.
4. Configure the following fields:

   Report Name: Specify a name for the report.

   Disabled: To disable the report, select the **Disabled** check box.

   By default, disabled reports are not shown on the report list.

   Run Report: To determine the time and frequency of each audit report, use the calendar to set the initial date, then set the frequency as required

   Report Category: To limit the report to one category, select the category, or to include all categories, select **All**.

   Report Target: (Conditional) To send the report to a user or all users in a group, click **User Report** in the **Report Target** section, then select the user or group from the drop-down list.

   Ensure that the users' e-mail addresses are defined in the **Account Details** section in the Framework User Account definitions. You must define a keyword anchor in the **Email To** field.

   Report Filter: Set the **Report Filter** to include the required event records:

   - Select one or more from **New**, **Pending**, **Authorized**, and **Unauthorized**.

- Select the age of events you want to include in the report. Events older than the number of days you specify are included.
- Select the escalation level of events you want to include in the report. Events at this escalation level and above are included.

Age(Days): Enter the **Age** of the report in days.

Escalation Level: Enter the **Escalation Level** of the report.

Email To: Specify the e-mail address of the user who is to receive the report:

- If you want the report to be sent to a user who is not defined as a Framework user, specify the user's e-mail address in the **Email To** field.
- If you want the report to be sent to a user or group defined as the **Report Target** above, specify the following keyword anchor in the **Email To** field:

```
$User.ACT_EMAIL.value$
```

You can view the format in XML of the object tokens passed into the audit report by entering $<>$ in the **Report Template** field, deselecting the HTML check box, then clicking **Test Report** (ensure that you have defined a **Report Target**). To view just the user subtree, use $<User>$.

The tokens that appear are dependent upon what has been configured for the users. If the ACT_EMAIL.value token is not present for the target, an email address has not been defined for the user. For user configuration information, see "Modifying a Framework User" on page 60.

Email From: Specify the email address of the user sending the report.

You can also use a keyword anchor in the **Email From** field.

Receipt: Select if you want to enable notification when the receiver has read the message. The message is sent to the email address specified in the **Email From** field.

Email Subject: Specify a subject for the email message.

This can be a text string or you can use a keyword anchor in the **Email Subject** field. For example, if you wanted to display the target user's name in the e-mail subject, you could enter the following in the **Email Subject** field.

```
Report for $User.ACT_FULL_NAME.value$
```

Report Template: Specify a Perl script in the **Report Template** field to control how the e-mail messages are formatted and what they contain. If you want the messages to be displayed in HTML, select the **HTML** check box.

For an example report template, see "Sample Command Control Report Template" on page 160.

5 Click **Test Report** to view the report that is sent to each e-mail target.

Use the arrow buttons with the mouse to page through the reports. In the test, the reports are not shown in HTML format. If there are errors in the **Report Template**, these are shown.

6 Click **Back** to return to the report configuration screen.

7 Click **Finish**.

Sample Command Control Report Template

If you are using this sample as a base for your own report templates, select **HTML** to correctly display the messages. The sample displays a message to the recipients of the e-mail messages, requesting them to log in to the Compliance Auditor and review activity. It extracts selected events and lists them in tables according to the age of the events, and provides information about the events.

As shown in the sample, you can use the user name keyword anchor $User.ACT_FULL_NAME.value$ to display a user's name in the e-mail, if you are using the Report Target option. You must ensure that a **Display name** is entered for the user in the **Account Details** section in the Framework User Account definitions.

```
<%!
my @lvl0;
my @lvl1;
my @lvl2;
my @lvl3;
my @gt0;
my @gt5;
my @gt10;
my @gt20;
%>
<%
my @audit_records = @{$tokens->{'AuditRecords'}->{'AuditRecord'}} if
(defined($tokens->{'AuditRecords'}) && defined($tokens->{'AuditRecords'}-
>{'AuditRecord'}));
foreach my $ar (@audit_records) {
  my $age = $ar->{'age'};
  my $lvl = $ar->{'level'};

  if ($age > 5 && $age < 10) {
    push(@gt5,$ar);
  } elsif ($age >= 10 && $age < 20) {
    push(@gt10,$ar);
  } elsif ($age >= 20) {
    push(@gt20,$ar);
  } else {
    push(@gt0,$ar);
  }
  if ($lvl == 1) {
    push(@lvl1,$ar);
  } elsif ($lvl == 2) {
    push(@lvl2,$ar);
  } elsif ($lvl >= 3) {
    push(@lvl3,$ar);
  } else {
    push(@lvl0,$ar);
  }
}
%>
<%
my $total = @audit_records;
if ($total > 0) {
%>
<style type="text/css">
```

```
<!--
.style1 {
 color: #000000;
 font-family: Arial, Helvetica, sans-serif;
 font-size: 12px;
}
.style2 {
 color: #000000;
 font-family: Arial, Helvetica, sans-serif;
 font-size: 12px;
 font-weight:bold;
}
.style4 {
 color: #000000
}
-->
</style>
<p class="style1"> Hello $User.ACT_FULL_NAME.value$,<br/>
  <br/>
  This is an automated event notification email from the Compliance
Auditor. <br/>
<br/>

  It is the responsibility of management to log into the Compliance Auditor
each day and review their team's keystroke logs.  <br/> <br/>

  Please log on to the Compliance Auditor at your earliest convenience
using this link: <a href="https://admin.company.com">https://
admin.company.com</a></p>

<%
my $gt0 = @gt0;
%>
<span class="style2">Events &lt; 5 days old (<%= "$gt0" %>)</span>
<table border="1">
  <tr class="style1">
    <td>Time</td>
    <td>User</td>
    <td>Run As</td>
    <td>Host</td>
    <td>Command</td>
  </tr>
  <%
foreach my $ar (@gt0) {
  my $cmd = $ar->{'cmdctrl'}->{'cmd'};
  my $usr = $ar->{'cmdctrl'}->{'user'};
  my $ras = $ar->{'cmdctrl'}->{'runAs'};
  my $hst = $ar->{'cmdctrl'}->{'host'};
  my $tme = $ar->{'cmdctrl'}->{'time'};
 $tme = localtime($tme);
%>
  <tr class="style1">
    <td><%= "$tme" %></td>
    <td><%= "$usr" %></td>
    <td><%= "$ras" %></td>
```

```
    <td><%= "$hst" %></td>
    <td><%= "$cmd" %></td>
  </tr>
<%
}
%>
</table>
<br/>

<%
my $gt5 = @gt5;
%>
<span class="style2">Events &gt; 5 days old (<%= "$gt5" %>)</span>
<table border="1">
  <tr class="style1">
    <td>Time</td>
    <td>User</td>
    <td>Run As</td>
    <td>Host</td>
    <td>Command</td>
  </tr>
<%
foreach my $ar (@gt5) {
  my $cmd = $ar->{'cmdctrl'}->{'cmd'};
  my $usr = $ar->{'cmdctrl'}->{'user'};
  my $ras = $ar->{'cmdctrl'}->{'runAs'};
  my $hst = $ar->{'cmdctrl'}->{'host'};
  my $tme = $ar->{'cmdctrl'}->{'time'};
 $tme = localtime($tme);
%>
  <tr class="style1">
    <td>
    <td><%= "$usr" %></td>
    <td><%= "$ras" %></td>
    <td><%= "$hst" %></td>
    <td><%= "$cmd" %></td>
  </tr>
<%
}
%>
</table>
<br/>

<%
my $gt10 = @gt10;
%>
<span class="style2">Events &gt; 10 days old (<%= "$gt10" %>)</span>
<table border="1">
  <tr class="style1">
    <td>Time</td>
    <td>User</td>
    <td>Run As</td>
    <td>Host</td>
    <td>Command</td>
  </tr>
```

```
<%
foreach my $ar (@gt10) {
  my $cmd = $ar->{'cmdctrl'}->{'cmd'};
  my $usr = $ar->{'cmdctrl'}->{'user'};
  my $ras = $ar->{'cmdctrl'}->{'runAs'};
  my $hst = $ar->{'cmdctrl'}->{'host'};
  my $tme = $ar->{'cmdctrl'}->{'time'};
 $tme = localtime($tme);
%>
  <tr class="style1">
    <td><%= "$tme" %></td>
    <td><%= "$usr" %></td>
    <td><%= "$ras" %></td>
    <td><%= "$hst" %></td>
    <td><%= "$cmd" %></td>
  </tr>
<%
}
%>
</table>
<br/>

<%
my $gt20 = @gt20;
%>
<span class="style2">Events &gt; 20 days old (<%= "$gt20" %>)</span>
<table border="1">
  <tr class="style1">
    <td>Time</td>
    <td>User</td>
    <td>Run As</td>
    <td>Host</td>
    <td>Command</td>
  </tr>
<%
foreach my $ar (@gt20) {
  my $cmd = $ar->{'cmdctrl'}->{'cmd'};
  my $usr = $ar->{'cmdctrl'}->{'user'};
  my $ras = $ar->{'cmdctrl'}->{'runAs'};
  my $hst = $ar->{'cmdctrl'}->{'host'};
  my $tme = $ar->{'cmdctrl'}->{'time'};
 $tme = localtime($tme);
%>
  <tr class="style1">
    <td><%= "$tme" %></td>
    <td><%= "$usr" %></td>
    <td><%= "$ras" %></td>
```

```
    <td><%= "$hst" %></td>
    <td><%= "$cmd" %></td>
  </tr>
<%
}
%>
</table>
<br/>

<p class="style2">Total Events = <%= $total %></p>

<%
}
%>
```

Deleting a Report

1. Click **Compliance Auditor** on the home page of the console.
2. Click **Audit Reports** in the task pane.
3. Select the report you want to delete.
4. Click **Delete** in the task pane.
5. Click **Finish** to confirm the deletion.

Compliance Auditor Records

The Compliance Auditor main page lists the records (events) collected according to defined audit rules.

By default, all new and pending events are displayed, as indicated in the **Status** column. To view authorized and unauthorized events, select the appropriate check boxes and click the refresh icon. Pending events are events that have been viewed and their records edited, but they have not been classified as authorized or unauthorized. You can click any of the column headings to sort by that column.

To view events for a specific time period, select the **From** and **To** check boxes, select the required dates, specify the required times, and click **Refresh**.

The table displays the following information about each event:

Column	Description
Risk	The color-coded indicators for Command Control command risk level and rule risk level, ranging from green (low) to red (high). For more information, see "Setting the Command Risk" on page 126.
Level	The escalation level set by the auditor editing the event record.
Status	The status of the event, indicating whether an auditor has classified the event as authorized or unauthorized. New events have not been viewed. Pending events have been viewed and edited, but have not been marked as authorized or unauthorized.

Column	Description
Time	The date and time the event occurred.
Event	A description of what the record contains.
Note	Any notes made by the auditor when editing the event record.
Assigned	The user the event has been assigned to by the auditor of the event record.
Rule	The audit rule that is pulled in the event.
Type	The type of event.
Size	The size of the keystroke capture with the total time of the session displayed between parentheses.
Event ID	The unique event ID.

From this page, you can perform the following tasks:

- "Viewing a Compliance Audit Record" on page 165
- "Viewing and Editing a Command Control Keystroke Report" on page 165
- "Viewing a Change Management Audit Record" on page 166
- "Viewing a Report Audit Record" on page 167
- "Editing an Audit Record" on page 167
- "Archiving Records" on page 168
- "Managing Archived Records" on page 168

Viewing a Compliance Audit Record

1. Click **Compliance Auditor** on the home page of the console.
2. Select the record you want to view.
3. Click **View Record** in the task pane.

   Record data for this event is shown, including the submit user and host, the run user and host, the command, whether it was authorized by Command Control, and whether the session was captured.

From here you can view a Command Control keystroke report, if it exists, or edit the record. If a keystroke report exists, you must review it before you can edit the record. See "Viewing and Editing a Command Control Keystroke Report" on page 165 for more information.

Viewing and Editing a Command Control Keystroke Report

1. Click **Compliance Auditor** on the home page of the console.
2. Select the record for which you want to view a keystroke report.
3. Click **View Record** in the task pane.
4. Click **View Keystroke Report** in the task pane, or click the **Keystroke** button.

The text that the user entered during the session is shown on the Input page. The first column displays color-coded indicators for command risk level and rule risk level, ranging from green (low) to red (high). For more information, see "Setting the Command Risk" on page 126 and "Modifying a Rule" on page 109.

5 On the Command Control Keystroke Report page, edit the following fields:

Terminal Type: Change the terminal type if it is set incorrectly.

Find: To find a specify command or string in the report, specify the text in the text box, then click **Find**.

Show control characters: Use the **Show control characters** check box to show or hide control characters on the screen.

Show audited commands: Use the check box to show or hide the full list of audited commands. If this option is enabled, the screen shows the actual commands that are being run when a user types a command. You can also view each input command individually by mousing over the command.

Show profile commands: Use the check box to show or hide the commands run in the user's login profile when the user's pcksh login shell has auditing configured to level 2.

6 (Optional) To see the keystroke text being played back with the screen output, click **Output**.

You can start the playback from a specific line in the input by selecting that line before clicking **Output**.

- Click **Play** to play the keystroke entries and view the output.
- Click **Rewind** to go back to the beginning.
- Click **Pause** to pause the playback.
- Click **Forward** to skip any pauses in the playback where the user might have taken a break from typing.
- Set the **Playback Speed** to **Real Time**, **Double Speed**, or **Full Speed**.
- Set the **Scrollback** field to the amount of text you want to be able to scroll back through, in kilobytes.
- Change the **Terminal Type** to the one you want.

7 Click **Cancel** to return to the record list.

Viewing a Change Management Audit Record

1 Click **Compliance Auditor** on the home page of the console.

2 Select the Command Control Change Management record you want to view.

The record type is shown in the **Type** column. You might need to scroll to the right to see this column.

3 Click **View Record** in the task pane.

Information about the Change Management action is displayed, including the name of the user who made changes to the database, and any entries the user made when committing the Command Control transaction.

4 To edit the record, see "Editing an Audit Record" on page 167.

Viewing a Report Audit Record

1 Click **Compliance Auditor** on the home page of the console.

2 Click the record you want to view.

The record type is shown in the **Type** column. You might need to scroll to the right to see this column.

3 Click **View Record** in the task pane.

Record data for this report is shown, including the contents of the report sent.

4 To edit the record, see "Editing an Audit Record" on page 167.

Editing an Audit Record

For each event listed in the Compliance Auditor, you can edit the audit record to authorize the event, or mark it as unauthorized, escalate it, and assign it to another user. You can also add notes for display in the event record, and comments that are permanently recorded in the event history.

NOTE: For Command Control events for which a keystroke report exists, you must view the keystroke report before editing the audit record. See "Viewing and Editing a Command Control Keystroke Report" on page 165 for more information.

To edit an audit record:

1 Click **Compliance Auditor** on the home page of the console.

2 Select the record you want to edit.

3 Click **View Record** in the task pane.

4 Click **Edit Record**.

5 (Optional) Authorize the event:

- **5a** Select the **Authorized** check box.
- **5b** In the **Note** field, specify a note to be displayed on the event list and event record.
- **5c** In the **Comment** field, specify a comment to be permanently displayed in the **History** on the View Record page.

6 (Optional) Mark the event as unauthorized:

- **6a** Select the **Unauthorized** check box.
- **6b** If necessary, set an **Escalation Level** to be displayed on the event list.

  This can be used as a report filter when setting up reports. See "Adding, Copying and Modifying an Audit Report" on page 158.
- **6c** If necessary, use the **Assigned to** field to assign the record to a different user.
- **6d** Specify a **Note** or a **Comment** to explain why the event is unauthorized.

7 Click **Finish**.

Archiving Records

Audit records can be archived from the console or from the command line. For information about the command line options, see "Managing Compliance Auditor Records" on page 187.

To archive records from the console:

1. Click **Compliance Auditor** on the home page of the console.
2. Select the records you want to archive.

   To select multiple records, press the Ctrl key and select the records one at a time, or press the Shift key to select a consecutive list of records.
3. Click **Archive Records** in the task pane.

   A list of the selected records is displayed.
4. Configure the following fields:

   Comment: (Required) Specify the reason for the archive.

   Keep Online: (Optional) Select if you want the archived records to continue to be displayed in the list of records.
5. Configure the types of records to archive.

   By default, authorized and unauthorized records are selected. New and pending records are not displayed. If you want to archive these records, select the **New** and **Pending** options.

   IMPORTANT: After a record is archived, it cannot be modified. If you archive new or pending records, their status can never change.

   ---
6. Click **Finish**.

Managing Archived Records

From the Framework Manager console, you can restore an archive and move archives from an online state (viewable in the console) and to an offline state (not viewable in the console) and from an offline state to an online state. You must use the command line options to purge an archive. See "Managing Compliance Auditor Records" on page 187.

NOTE: When you archive secaudit events, the archived events are only stored on the primary secaudit manager and not on the backup secaudit manager. Back up these files for fault tolerance.

To manage archived records from the console:

1. Click **Compliance Auditor** on the home page of the console.
2. Click **Manage Archives** in the task pane.
3. To restore an archive to an online status, select the archive, then click **Make Online**.
4. To move an archive from an online status to an offline status, select the archive, then click **Make Offline**.
5. Click **Close**.

Access Control Levels

You can define an Access Control Level (ACL) for your auditors that specifies which events they are allowed to view and restricts auditors from authorizing their own activity.

- "Adding or Modifying a User ACL" on page 169
- "Deleting a User ACL" on page 169

Adding or Modifying a User ACL

1. Click **Compliance Auditor** on the home page of the console.
2. Click **Access Control** in the task pane.
3. To add a new ACL, click **Add User ACL** in the task pane. To modify an existing ACL, select the required **User** and click **Modify ACL** in the task pane.

   When creating a new user ACL, select the user from the **Username** drop-down list.
4. At the bottom of the table, select the attribute from the drop-down list that describes the entity to which you want to control access for the selected user.

   For example, if you do not want this user to be able to audit Command Control events involving a particular command, click **Command**.
5. In the **Matches** field, specify the value of the attribute you want to control access to.

   For example, if you do not want this user to be able to audit any Command Control events that involve SSH session, specify command `<ssh>` in this field. You can use wildcard characters in this field.
6. Set the **Action** to allow or deny.
7. Click **Add**.
8. (Optional) Use the arrow buttons to move entries up and down the list.

   You might want to do this if, for example, you are allowing the user to access a restricted list of commands, and using the wildcard * to deny access to all other commands. The `allowed commands` entries must be above the `deny all` entry. By default, all commands are allowed.
9. (Optional) Remove an attribute by selecting it and then clicking the **Remove** button.
10. (Optional) Modify an entry by selecting it, then specifying the changes. Click **Update** to save the changes.
11. Click **Finish**.

Deleting a User ACL

1. Click **Compliance Auditor** on the home page of the console.
2. Click **Access Control** in the task pane.
3. Select the user for whom you want to delete an ACL.
4. Click **Delete User ACL** in the task pane.
5. Click **Finish** to delete the ACL for the user.

Deploying the Compliance Auditor

You can provide failover and load balancing by installing the Compliance Auditor on multiple hosts. The Compliance Auditor consists of the following packages:

- **Compliance Auditor (secaudit):** Holds the compliance auditor rules and audit information.
- **Compliance Auditor Console:** Installed into the Framework Manager console. Required for configuring Compliance Auditor rules and for viewing audit information.

The Compliance Auditor has the following dependencies:

- The Compliance Auditor package is shown as an available package only on hosts that have the Audit Manager (audit) deployed.
- If you want to use the Compliance Auditor reporting facilities, you need to install the Access Manager (auth) on the host with the Compliance Auditor.

To deploy the Compliance Auditor:

1. Download the required packages to your local Package Manager. See "Publishing Packages on the Package Manager" on page 313.
2. Install the Audit Manager package on the host you want to be the Audit Manager, then install the Compliance Auditor package on the same host.

   This can be on any operating system, including Windows. See "Installing Packages on a Host" on page 39 for details. The auditing packages can be deployed to as many hosts as you need in order to build an environment with load balancing and failover.
3. If you need reporting facilities, install the Access Manager package on the same host as the Compliance Auditor package.

The Compliance Auditor is now deployed and ready to use.

10 High Availability

The high availability or failover feature works by using a hierarchical view of the hosts associated with the Framework.

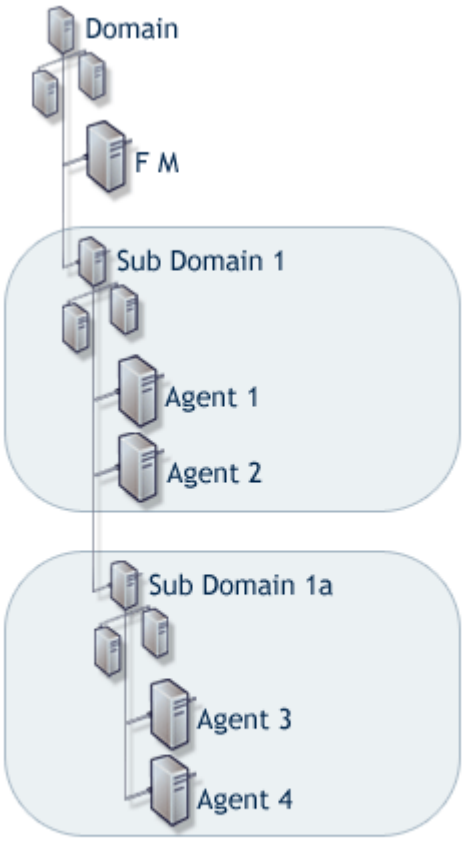
The hierarchy of hosts is created by using the Hosts console to group hosts into domains and subdomains, which are representative of your enterprise network structure. This effectively gives them a chain of command, where they always address requests to managers in their immediate subdomain before moving along a branch to another subdomain or parent domain.

To achieve an effective failover environment, at least two Framework Manager packages must be deployed across the same Framework. The licensing model is not based on how many managers or agents are deployed, but how many hosts the Framework is deployed on. This means that there are no restrictions on how many Framework Manager packages you can deploy.

The Registry Manager controls a database that records the location and status of each package deployed on each of the hosts within the Framework. A copy of this information is held at each host by the Registry Agent package that is included as part of the agent installation. The distributed information is used to calculate the route to the appropriate manager for requests from any agent registered on the Framework. The structure of the registry data enables each host to determine which Framework Manager on the Framework should be the target of requests, and which Framework Manager to use if there is a failure or withdrawal of the initially selected Framework Manager.

The failover feature automatically and transparently redirects requests from a failed or withdrawn Framework Manager to the next available manager of the same type. The agent automatically connects to a manager that is next in line in accordance with your defined hierarchy.

Table 10-1 Creating a Failover Environment



This diagram shows an example of a typical way to create an effective failover environment.

Deployment: Deploy the Command Control Manager package on the Framework Manager, Agent 1, and Agent 3 hosts.

Who authenticates to whom: By default, each agent contacts the following host for Command Control authorization:

Agent 1 and 2 contact Agent 1.

Agent 3 and 4 contact Agent 3.

Examples:

1. Agent 3 is downed for maintenance. Agent 4 seeks authorization from Agent 1.
2. Agent 1 is also downed because of a broken network card. Agents 2, 3, and 4 seek authorization from the Framework Manager.
3. The Command Control Manager package is removed from the Framework Manager and the Agent 1 is still broken. Agents 2, 3, and 4 seek authorization from Agent 3, considering Agent 3 is up and Agent 1 is still broken.

IMPORTANT: If an additional subdomain is added, agents under Subdomain 1 and 1a then seek authorization from the new Subdomain if no other Command Control Manager is available.

If the primary fails, see "Promoting Managers When the Primary Manager Fails" on page 48.

Configuring High Availability

To configure high availability, you must do the following:

- Install and register the agents to the manager.
- Define the domain.
- (Conditional) Promote the backup manager when primary fails. To write configuration changes, you must first try to get the primary up again. If you are unable to get the primary up again, you can promote the backup manager.

To configure high availability:

1 Install and register the PAM managers:

1a Install a PAM manager.

The first manager you install is defined as the primary manager by default, and its packages are defined as primary. Manager packages on all other manager hosts act as backups.

1b Install another PAM manager.

For more information about installing PAM managers, see Installing the Framework Manager in the Privileged Account Manager Installation Guide.

1c Register the second PAM manager you installed to the PAM instance you installed first. After you register, the second PAM manager acts as a backup manager.

2 To define the domain:

2a Login to PAM administrator console.

2b On the home page of the console, click **Hosts** > **Add Domain**.

2c Specify a domain name.

2d Click **Add**.

2e To add managers and agents to the domain, drag and drop the managers and agents from the list to the domain.

You can have multiple domains in PAM. If you have multiple domains, you can add a backup manager in every domain. So, any request from the agent can be processed by the manager in their domain.

3 (Conditional) To promote a backup when the primary fails:

3a Select a host from **Hosts**.

3b Click **Packages**.

The **Status** column indicates whether the status of a module is primary or backup.

3c To promote a backup manager:

3c1 Ensure that the registry manager package is promoted to primary.

3c2 Select the required backup packages and click **Promote Manager**.

11 Load Balancing

The load balancing feature work by using a hierarchical view of the hosts associated with the Framework.

The hierarchy of hosts is created by using the Hosts console to group hosts into domains and subdomains, which are representative of your enterprise network structure. This effectively gives them a chain of command, where they always address requests to managers in their immediate subdomain before moving along a branch to another subdomain or parent domain.

To achieve an effective load balancing environment, at least two Framework Manager packages must be deployed across the same Framework. The licensing model is not based on how many managers or agents are deployed, but how many hosts the Framework is deployed on. This means that there are no restrictions on how many Framework Manager packages you can deploy.

The Registry Manager controls a database that records the location and status of each package deployed on each of the hosts within the Framework. A copy of this information is held at each host by the Registry Agent package that is included as part of the agent installation. The distributed information is used to calculate the route to the appropriate manager for requests from any agent registered on the Framework. The structure of the registry data enables each host to determine which Framework Manager on the Framework should be the target of requests, and which Framework Manager to use if there is a failure or withdrawal of the initially selected Framework Manager.

Load balancing means the ability to evenly distribute processing and communications activity across the Framework so that no single Framework Manager is overwhelmed by agent requests.

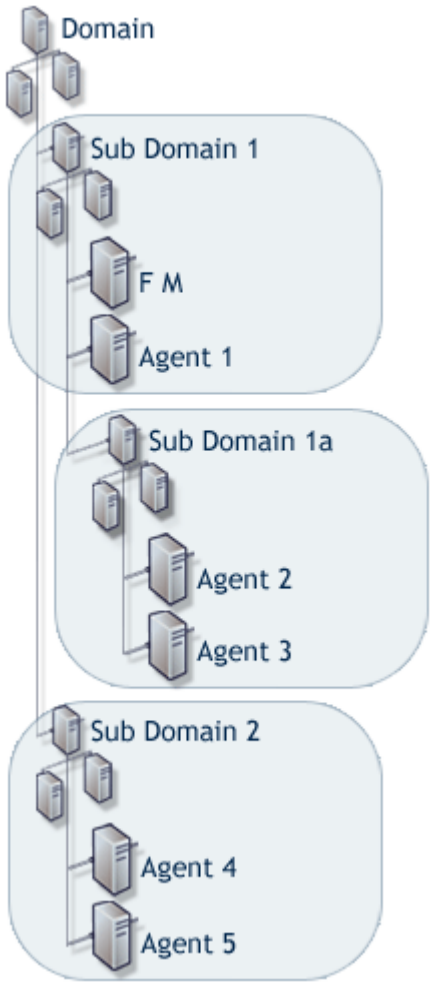
Load balancing is particularly important in situations where it is difficult to predict the number of requests that are directed to a specific category of manager.

The Framework automatically replicates data from the defined primary manager to each additional manager that is deployed in the Framework. Replication takes place automatically when the manager is initially deployed and then again at any stage when the data on the primary manager is modified.

The following packages can be load balanced:

- **Registry Manager:** Maintains a database of all hosts and modules and provides certificate-based registration features for the hosts.
- **Package Manager:** Manages a repository for packages.
- **Administration Agent:** Provides the functionality for the Web-based user interface. Consoles can be installed on the Administration Agent and used to control product features.
- **Access Manager:** Maintains a list of Framework user accounts and provides authentication services for the Framework. This package must be installed with a local Registry Manager in order to create a secure user authentication token.
- **Command Control Manager:** Maintains a database of all defined command control rules, commands, and scripts.

Table 11-1 Creating a Load Balancing Environment



This diagram is an example of a typical way to create an effective load-balanced environment.

Deployment: Deploy the Command Control Manager package on the Framework Manager, Agent 2, and Agent 4.

Who authenticates to whom: By default, each agent contacts the following host for Command Control authorization:

Agent 1 contacts the Framework Manager.

Agents 2 and 3 contact Agent 2.

Agents 4 and 5 contact Agent 4.

Example of load balancing working with failover:

1. Agent 2 is downed for maintenance. Agent 3 seeks authorization from the Framework Manager.
2. Agent 4 is down because of a broken network card. Agents 5 seeks authorization from the Framework Manager.

12 Command Line Options

The command line options can be run from either a Linux/UNIX Framework Manager or a Windows Framework Manager. Some can be run from an agent machine.

To use the command line options, change to the `unifi` directory:

Linux/UNIX: `/opt/netiq/npum/sbin/unifi`

Windows: `<Drive>:\Program Files\Netiq\npum\sbin\unifi`

The following sections assume that you are running the commands from the `unifi` directory. If you are using the new Windows power shell, replace the `./` of the syntax with `.\`. If you are not using this new Windows shell, remove the `./` from the command. For example:

Linux/UNIX: `./unifi -v`

Windows Power Shell: `.\unifi -v`

Windows: `unifi -v`

This command displays version information for the Command Control module.

Privileged Account Manager supports the following command line options:

- "The unifi Options" on page 177
- "Command Control Options" on page 178
- "Package Distribution Options" on page 181
- "Package Manager Options" on page 182
- "Registry Agent Options" on page 184
- "Registry Manager Options" on page 186
- "Compliance Auditor Options" on page 186
- "sreplay Command Line Options" on page 189

The unifi Options

The `unifi` binary is located in the `/opt/netiq/npum/sbin/unifi` directory for Linux and Unix platforms and in the `\Program Files\Netiq\npum\sbin\unifi` directory for the Windows platform. The command has the following syntax:

Syntax: `./unifi [options]`

Replace `[options]` with one or more of the following:

Option	Description
-v	Displays the version of the Framework patch.

Option	Description
-s	Displays the service name if you have changed it by modifying the `unifi.xml` file.
-u *<username>*	Specifies the username of the user requesting the command. This is used to verify that the user has sufficient rights to execute the command. Most, but not all commands, require authorization.
-p *<pwd>*	Specifies the password of the user.
-n	Indicates that the user's native account can be used for credentials. This option replaces the -u *<username>* -p *<pwd>* options. For information on how to set up native maps, see "Modify User: Native Maps" on page 64. Most of the module commands require authentication credentials to verify the user's rights to issue the command. **NOTE:** Native mapping of local account is supported from Privileged Account Manager 3.2.

For example:

```
/opt/netiq/npum/sbin/unifi -v
```

This command displays the version of the Framework patch.

Command Control Options

The command line options for the Command Control module allow you to perform the following tasks:

- "Importing and Exporting Command Control Settings" on page 178
- "Backing Up and Restoring a Command Control Configuration" on page 179
- "Running Test Suites" on page 181

Importing and Exporting Command Control Settings

The following commands allow you to export a current command control configuration and import one. Importing a configuration overwirtes any existing rule set; therefore before importing a configuration, you should back up the current configuration (see "Backing Up and Restoring a Command Control Configuration" on page 179).

The export command has the following syntax:

Syntax: `./unifi -n cmdctrl export [options]`

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u *<username>* -p *<password>* options and specify the name and password of a Framework Manager user who has the rights to perform this task.

Replace [options] with one or more of the following:

Options	Description
-f *<arg>*	Specifies where to export the configuration to. Replace *<arg>* with a filename or a path and filename.
-c	Specifies that the configuration should be exported in clear text. This option cannot be used with the -p option.
-p *<pwd>*	Specifies an encryption password for the file. If a password is specified, the password must be entered when importing the file. This option cannot be used with the -c option.

The import command has the following syntax:

Linux Syntax: `./unifi -n cmdctrl import [options]`

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u *<username>* -p *<password>* options and specify the name and password of a Framework Manager user who has the rights to perform this task.

Replace [options] with one or more of the following:

Options	Description
-f *<arg>*	Specifies the file to import. Replace *<arg>* with a filename or a path and filename.
-p *<pwd>*	Specifies the password that was used to encrypt the configuration when it was exported.

Backing Up and Restoring a Command Control Configuration

The following commands can be executed on the primary console or on backup hosts. When they are executed on a backup host, the commands actually execute on the primary console.

Syntax: `./unifi -n cmdctrl [option]`

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u *<username>* -p *<password>* options and specify the name and password of a Framework Manager user who has the rights to perform this task.

Replace `[option]` with one of the following:

Option	Description
`backup -t <"reason">`	Backs up the current command control database. The -t *<"reason">* parameter allows you to supply a reason for the backup, and is optional but recommended. Enclose the reason text in double quotes.

Option	Description

`listcfg` *<format>*	Lists the backups that are available for restoration. To specify a format, use one of the following:
	
	-x: `For XML output. For example: <a.Item I.version="0" who="admin" reason="Backup 1" I.timestmp="1247146780" I.id="1"/>`
	
	-D *<date>*: For modifying the date format. For example, if you replace *<date>* with %D for the format, the time stamp is displayed as `07/14/09` rather than `2009-07-14_11-52-56`. For possible options, see strftime(3C).
	
	-F *<fmt>*: For specifying what template information is displayed. By default, the following information is displayed.
	
	◆ **id:** The unique ID of the backup.
	◆ **who:** The ID of the user who created the backup.
	◆ **reason:** The reason for the backup, if provided by the user.
	◆ **timestmp:** The date and time when the backup occurred.
	
	Replace *<fmt>* with one or more of these options. Individual options are enclosed with ${ }$ and separated from other options with a comma. The entire string is enclosed in single quotes. For example:
	
	`-F '${id}$,${reason}$'`
	
	This string would print out the following:
	
	`1,Basic test rules for session closure`

`restore -n` *<id>*	Restores the command control database to the select version. Replace *<id>* with the version number you want to restore. The current configuration is overwritten. You cannot restore when transactions are enabled (see "Command Control Transactions" on page 142).
`delcfg -n` *<id>*	Deletes the selected backup from the list. Replace *<id>* with the version number you want to delete. Deleting a backup is permanent and cannot be undone.
`backup --?`	Displays the usage help for the `backup` command.
`listcfg --?`	Displays the usage help for the `list` command.
`restore --?`	Displays the usage help for the `restore` command.
`delcfg --?`	Displays the usage help for the `delete` command.

Sample Commands

To back up the database:

```
./unifi -n cmdctrl backup -t "Added the ls command."
```

To restore the second backup in the list:

```
./unifi -n cmdctrl restore -n 2
```

Running Test Suites

The test suite options allow you to run part or all of the Command Control test suites.

Syntax: `./unifi -n cmdctrl runTest [option]`

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u <*username*> -p <*password*> options and specify the name and password of a Framework Manager user who has the rights to perform this task.

Replace `[option]` with one or more of the following:

Option	Description
`-t <'arg'>`	Specifies a specific test suite to run. Replace <*arg*> with the name of the test suite. This option cannot be used with the -A option
`-A`	Runs all the test suites. This option cannot be used with the -t option.
`-v`	Outputs the full debug information to the screen.
`-V <file>`	Outputs the full debug information to the specified file or the specified path and file.
`-o <file>`	Outputs the test results to the specified file or the specified path and file.

For example:

```
./unifi -u admin cmdctrl runTest -A -o /tmp/test.log
```

This command writes the results of the test suites to the `test.log` file in the `/tmp` directory.

Package Distribution Options

The following command allows you to import packages into the Package Manager

Syntax: `./unifi -n distrib publish [option]`

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u <*username*> -p <*password*> options and specify the name and password of a Framework Manager user who has the rights to perform this task.

Replace `[option]` with one of the following:

Option	Description
`-d <directory>`	Imports the packages from the specified directory, for example: `-d /tmp/framework`
`-f <package>`	Imports the specified package, for example: `-f /tmp/framework/xxx.pak`

Package Manager Options

- "Install and Uninstall Packages" on page 182
- "Upgrade and Rollback Packages" on page 183

Install and Uninstall Packages

You can install and uninstall packages on the agent or the manager by using one of the following approaches:

- "Install and Uninstall Packages From Framework Manager" on page 182
- "Install and Uninstall Packages From Agent Machine" on page 182

Install and Uninstall Packages From Framework Manager

You can install and uninstall packages on the agent or manager from the Framework Manager using the following commands:

Syntax: `./unifi -n pkgman install <agent> <package>`

Syntax: `./unifi -n pkgman uninstall <agent> <package>`

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u *<username>* -p *<password>* options and specify the name and password of a Framework Manager user who has the rights to perform this task.

Replace *<agent>* with the agent name for the host. To view a list of these names, click **Hosts** on the home page of the Framework Console.

Replace *<package>* with the name of the package to install or uninstall. To view a list of package names in the Framework Console, click **Hosts**, select a host, select to display the packages. The name field contains the package name that is used in this command.

NOTE: You cannot use this command to install or uninstall consoles. It can only be used to install and uninstall modules.

Install and Uninstall Packages From Agent Machine

You can install or uninstall multiple package on the agent or the manager from the respective workstation using the following commands:

Prerequisite

- You must have the admin privileges for the `unifi` module to execute this command in the local agent machine.
- The packages that are to be installed must be available in the primary framework manager.

Syntax: `./unifi -n distrib install` *<package1_name> <package2_name>*

Syntax: `./unifi -n distrib uninstall` *<package1_name> <package2_name>*

NOTE: You must not uninstall the packages rexec, strfwd, regclnt, distrib in the agent. Uninstalling any of these packages will affect the functionality.

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u *<username>* -p *<password>* options and specify the name and password of a Framework Manager user who has the rights to perform this task.

Replace *<package1_name> <package2_name>* with the name of the package to install or uninstall. To view a list of package names in the Framework Console, click **Hosts**, select a host, select to display the packages. The name field contains the package name that is used in this command.

You can also install and uninstall console packages. To install or uninstall console packages, use the following syntax:

Syntax: `./unifi -n distrib install` *<module_package_name> Console/ <console_package_name>*

Syntax: `./unifi -n distrib uninstall` *<module_package_name> Console/ <console_package_name>*

Replace *<module_package_name>* with the name of the module package and <console_package_name> with the name of the console package that must be installed or uninstalled.

Upgrade and Rollback Packages

Prerequisite

- You must have the admin privileges for the `unifi` module to execute this command in the local agent machine.
- Before upgrading, ensure that the latest version of the package are available in the primary framework manager. For information about configuring the package manager and downloading the packages, see "Publishing Packages on the Package Manager" on page 313.
- Before you rollback packages from 3.5 to any lower version, you must uninstall the Application SSO Manager (`appsso`) and Video Processing Module (`videoprocessor`) packages. For information about the commands to uninstall the packages, see "Install and Uninstall Packages" on page 182

You can upgrade and rollback packages on the agent or the manager using the following commands:

Syntax: `./unifi -n distrib update`

When you upgrade packages, all the current packages are backed up and Privileged Account Manager stores only one version of the backup file that is the last backup.

To rollback the packages to the previous version, run the following command in the agent or the framework manager.

NOTE: When you rollback packages from 3.5 to any lower version, first rollback all the packages except distrib and framework (`spf`) and lastly rollback distrib and framework (`spf`) package.

Syntax: `./unifi -n distrib rollback`

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u *<username>* -p *<password>* options and specify the name and password of a Framework Manager user who has the rights to perform this task.

Registry Agent Options

The Registry Agent module allows you to perform the following tasks from the command line:

- "Registering an Agent" on page 184
- "Finding a Primary Manager Package" on page 184
- "Agent Status" on page 185
- "Adding Hosts and Domains" on page 185

Registering an Agent

The following command registers an agent with the Framework Manager. It must be run from the agent machine.

To run the command and be prompted to supply information:

```
./unifi regclnt register
```

You are prompted to supply the IP address of the Framework Manager, the registration port (the default port is 29120), the DNS name or IP address of the agent machine, the agent name, then a Framework Manager username and password.

To run the command with all the parameters on the command line:

```
./unifi regclnt register <manager> 29120 <hostname> <agent name> <admin>
<password>
```

Replace *<manager>* with the IP address of the Framework Manager, *<hostname>* with the DNS name or IP address of the agent machine, *<agent name>* with the name of the agent, *<admin>* with a Framework Manager username, and *<password>* with the user's password. For example:

```
./unifi regclnt register manager1 29120 agent1.domain.com agent1 admin
netiq
```

Finding a Primary Manager Package

The following command displays details about primary manager packages. It can be run from any host machine, and displays the primary manager information contained in the local machine's databases.

Syntax: `./unifi -n regclnt getManager <package>`

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u *<username>* -p *<password>* options and specify the name and password of a Framework Manager user who has the rights to perform this task.

Replace *<package>* with one of the following: `admin, audit, auth, cmdctrl, msgagnt, pkgman, registry, secaudit, syslogemit`.

For example, the following command returns details about the primary Command Control Manager:

```
./unifi regclnt getManager cmdctrl
```

Agent Status

The following command displays the status of agents within the framework. It can be run from any host machine.

Syntax: `./unifi -n regclnt status` *[option]*

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u *<username>* -p *<password>* options and specify the name and password of a Framework Manager user who has the rights to perform this task.

Replace *[option]* with one or more of the following:

Option	Description
`-s` *<server>*	Displays status of the specified host. This option can be repeated on the command line for more than one host.
`-o` *<domain>*	Allows you to request status for all agents in a domain. This option can be repeated on the command line for more than one domain.
`-S` *<server>*	Confirms whether the host can communicate with the specified agent.
`-M` *<module>*	Confirms whether the agent can communicate with the specified module.
`-a`	Displays the status for all defined hosts.
`-c`	Provides output in CSV format.
`-h`	Prevents the display of the CVS header.
`-?`	Displays the usage message.

Adding Hosts and Domains

The `unifi` command supports the addition of hosts and domains directly from the command line during the host registration process. The additional roles that must be provided in the Framework User Manager are:

- To allow creation of host records during registration

  Module: unifi Role: register_host

  Module: unifi Role: register

- To allow creation of domain records during registration

  Module: unifi Role: register_domain

  Module: unifi Role: register

For example:

- To create a host record from command line:

Syntax: `/opt/netiq/npum/sbin/unifi regclnt register <Manager IP Address> 29120 <Agent IP Address> /Host <admin> <password>`

- To create a host under a domain:

  Syntax: `./unifi regclnt register <Manager IP Address> 29120 <IP or hostname of agent></DomainPath/HostName of the agent> <admin> <password>`

  DomainPath: If you want to register an agent to a domain, you must specify the domain path in the format *`Domain/SubDomain1/SubDomain2/AgentName`*. If the domain or sub domains does not exist, registration process creates the domain automatically and places the agent under them. DomainPath is case insensitive.

Registry Manager Options

The registry command allows you to promote the registry on a backup host to primary status from the command line. After you have promoted the registry to primary, you can log in to the backup console and promote the remaining packages to primary.

Syntax: ./unifi -n registry promote

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u <*username*> -p <*password*> options and specify the name and password of a Framework Manager user who has the rights to perform this task.

Compliance Auditor Options

The command line options for the Compliance Auditor allow you to perform the following tasks:

- "Exporting and Importing Compliance Auditor Settings" on page 186
- "Managing Compliance Auditor Records" on page 187

Exporting and Importing Compliance Auditor Settings

The Compliance Auditor now supports the ability to export and import its settings from the command line. You can export and import the following settings:

- Audit Rules
- Audit Reports
- Access Control Levels

Exporting: The export command exports only configuration settings; the audit records are not exported. The export includes all rules and reports, even those that have been disabled. The Compliance Auditor does not allow rules or reports to be deleted, because they might be associated with audit records. The exported file is in XML format.

Importing: You should import the settings only on a system that hasn't been configured or on a system where the current configuration is not needed. Every rule and report contains a unique ID, but if that ID already exists on the current system, the rule or report is overwritten by the imported configuration.

Commands: The commands use the following syntax:

```
./unifi -n secaudit import -f <file>
./unifi -n secaudit export -f <file>
```

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u *<username>* -p *<password>* options and specify the name and password of a Framework Manager user who has the rights to perform this task.

Replace *<file>* with the name of the file to import or to create for the export.

Managing Compliance Auditor Records

The compliance auditor now supports the ability to archive, restore, and purge the audit records from the command line. These commands can be performed on the Framemaker Manager console machine or from a backup host. When executed from a backup host, a command is actually execute on the primary host.

If a backup host is promoted to be a primary host, the archived database can be placed on the promoted manager and restored.

The `secaudit` command has the following syntax:

```
./unifi -n secaudit [list] [listarchive] [archive] [restore] [purge]
```

If you have not mapped your local account to a Framework Manager user (see "Modify User: Native Maps" on page 64), replace the -n option with -u *<username>* -p *<password>* options and specify the name and password of a Framework Manager user who has the rights to perform this task.

The `secaudit` command supports the following options:

Option	Description
`list <format>`	Displays all of the audit records currently stored, including any records already archived, unless archived records have been purged. To view a format other than the default, specify one of the following: **-x:** `For XML output.` **-D *<date>*:** For modifying the date format. For example, if you replace *<date>* with %D for the format, the time stamp is displayed as `07/14/09` rather than `2009-07-14_11-52-56`. For possible options, see strftime(3C). **-F *<fmt>*:** For specifying what template information is displayed. By default, the following information is displayed. ◆ **id:** The unique ID of the archive. ◆ **who:** The ID of the user who created the archive. ◆ **reason:** The reason for the archive, if provided by the user. ◆ **timestmp:** The date and time when the archive occurred. Replace *<fmt>* with one or more of these options. Individual options are enclosed with ${ }$ and separated from other options with a comma. The entire string is enclosed in single quotes. For example: `-F '${id}$,${reason}$'`
`archive -n <from:to> -p <pwd> -r "<reason>"`	Creates a database in the `/opt/netiq/npum/service/local/secaudit` directory with the following format: `sa-2009-06-05_11-38-43.db` Each archived database can then be taken offline (moved to another storage area) and put back in place at any point. Specify values for the following parameters: **-n *<from:to>*:** Specifies the records to archive. To archive one record, specify its ID. To archive a range of records, replace *<from:to>* with the range. For example to archive records 20 to 40, specify `20:40`. Use the `list` option to view the IDs of the records. **p *<pwd>*:** (Optional) Specifies a password. If a password is specified for an archive, the same password must be used to restore the archive. **-r *"<reason>"*:** (Optional) Specifies a reason for the archive. The text must be included in double quotes.
`listarchive <format>`	Displays each of the archives that have been created. To view a format other than the default, replace *<format>* with a supported format. See the `list` option for valid values.

Option	Description
`restore -n <archid> -p <pwd>`	Restores an archive set of audit records so that they are displayed in the Compliance Auditor console. **-n *<archid>*:** Specifies the archive to restore. Use the `listarchive` option to view the IDs of the archives. **p *<pwd>*:** (Conditional) Specifies a password. If a password is specified for an archive, the same password must be used to restore the archive.
`purge`	Purges audit records that have been archived. Records that have been purged no longer appear in the Compliance Auditor console. A restore of the archive makes these records viewable again.

sreplay Command Line Options

The sreplay option is used to view the audit records from the command line. The sreplay binary is located in the `/opt/netiq/npum/sbin/` directory for Linux and Unix platforms.

Syntax: `sreplay <options> <host>`

The various options are:

Option	Description
`-U user`	Username
`-P passwd`	Password
`-N`	Uses native account for authorization
`-l`	Lists available logs
`-g <logfile>`	Gets available session entries in log
`-u <user>,<logfile>`	Gets available session entries for a particular user
`-r <session#>,<logfile>`	Replays a particular session
`-f`	Date format
-C	csv output
-Z	csv separator

Options that can be used with `-g` and `-u`

Option	Description
`-F <FMT>`	Displays extra info, specified by FMT (comma seperated list)
`groupid[=n]`	Display group id of session
`time[=n]`	Displays time of start of session

Option	Description
`key[=n]`	Displays session number
`user[=n]`	Displays submit user
`host[=n]`	Displays submit host
`runas[=n]`	Displays run user
`runhost[=n]`	Displays run host
`cmd[=[-]n]`	Displays command
`term[=n]`	Displays term type
`size[=n]`	Displays size of session in Kb
	NOTE: This can cause high CPU utilization on large files.
`all`	Lists all events

Option that can be used with `-g` and `-r`

Option	Description
`-z`	Get using group ID

Options that can be used with `-r`

Option	Description
`-i`	Displays stdin
`-o`	Displays stdout
`-e`	Displays stderr
-s	Displays signals
`-p`	Displays passwords
`-d <# ms>`	Sets display delay
`-c <charset>`	Enables character set conversion
`-a`	Displays all data
`-l`	Displays character by character, waiting for keypress
`-m`	Displays line by line, waiting for keypress
`-x`	Displays x11 capture

Sample Commands

- To list all the available logs

  Syntax: `./sreplay -l -U admin -P netiq123`

Sample output:

```
Audit Group: cmdctrl
Archive: cmdctrl.db - available
```

- To get the available sessions stored in log file

  Syntax: `./sreplay -l -U admin -P netiq123 -g cmdctrl.db`

  Sample output:

```
root 1 "25-Feb-2011 11:05:29"
root 161 "25-Feb-2011 11:08:51"
user2 331 "25-Feb-2011 11:09:07"
```

13 Managing Shared Keys

A shared key can be any key value that an organization requires to share with their users. For example, Windows license keys, SSH host keys, and so on.

Consider a scenario in which an administrator has to share one license key with multiple users. This is a manual process and requires a lot of effort. But by using the **Key Checkout** feature, an enterprise administrator or a Privileged Account Manager administrator can create this license key as a shared key and share it with single or multiple enterprise users.

The shared keys are securely saved within a domain for easy access to the same type of keys at one place. If a rule is created for a key checkout, single or multiple users can access the same key based on the configuration.

When the shared keys are configured for privileged users, they can access the keys from the user console.

- "Types of Shared Key" on page 193
- "Enabling the Key Checkout for Shared Key" on page 194
- "Managing Credentials for Shared Key" on page 195

Types of Shared Key

Privileged Account Manager provides three default, and a custom key type. These types are created for the quick and easy grouping for the shared keys. The key types include some definite set of fields for the key values. The list of the types of shared keys are as following:

- **SSH Key:** This key type includes the fields that are used in communicating with Secure Shell. You can use this key type for any key that may require the same fields. The SSH key type contains the following fields for the shared key:
  - Name
  - Private Key
  - Passphrase
- **Windows Key:** This key type includes the fields that are used in a Windows key. You can use this key type for the keys that require the similar fields that are used in a Windows key. The Windows key type contains the following fields:
  - Name
  - Key
- **VMWare Key:** This key type is same as Windows key type. This key type can be used for creating a separate group where you can add the keys that have the values similar to VMware key. The VMWare key type contains the following fields:
  - Name
  - Key

- **Custom Key:** This key type is helpful in adding additional custom fields for a key value. The custom key type contains the following fields:
  - Name
  - Key
  - *Custom field* (any number of custom fields that are required for a key can be added.)

Enabling the Key Checkout for Shared Key

You can create a rule to enable key checkout for privileged users. This rule enables the privileged users to checkout the available key simultaneously till the key usage exceeds the user limit. You can use the policy templates such as, **SSH Key CheckIn-CheckOut**, **Windows Key CheckIn-CheckOut**, and **VMWare Key CheckIn-CheckOut** for key checkout then, customize it as per the requirement. For more information about adding a policy template refer, "Adding a Policy Template" on page 54.

To enable key checkout, perform the following:

1. Configure the shared Key.

   For information about configuring a shared key, see the Contextual Help of Credential Vault.
2. In the navigation bar, click **Consoles > Command Control**.
3. Create a rule at a required level. For more information about rules, refer "Rules" on page 107.

   You can also use the default policy template instead of creating a new rule.
4. Create a new command by using the Key_<*domain type*> command. Where, *domain type* is the name that you specify for the type of the shared key domain.

   or

   use any of the following default commands and modify the fields as per the requirement:
   - **SSH Key Check Out**
   - **Windows Key Check Out**
   - **VMWare Key Check Out**

   If you selected **Create Command for Custom Key** while configuring shared key, the command is created with the same name as the domain type.
5. Modify the created rule with the required details.

   Account Domain: Leave this field blank.

   Credentials: Leave this field blank.

   Run User: If you want users to use only a specific key, specify the shared key name. If you want different users to use the different keys available in a domain, specify the asterisk (*) symbol.

   Run Host: Specify the shared key domain.

   If the key domain has the **Multiuser** option enabled in **Shared Key Resource** of **Credential Vault**, different users can simultaneously check out the same key that is specified in the domain.

   Risk Level: Set a **Risk Level** of 0 to 99. This option allows you to set a value representing the relative risk of a rule with the session auditing option (see "cpcksh" on page 213). When viewing a Command Control Keystroke Report, you see commands controlled by rules with different risk values represented in different colors.

   Audit Group: Define an **Audit Group**. This setting is for use in Compliance Auditor reports.

NOTE: To configure video capturing refer section "Video Capture" on page 91

Managing Credentials for Shared Key

When you add a single or multiple shared keys to a domain, users can checkout those keys simultaneously based on how many users can access the shared key.

You can use the shared key feature to share any type of value with single or multiple users. The following are the scenarios to manage shared keys:

Multiple keys for multiple users: You can define multiple keys in a domain for multiple users and each shared key can have maximum user limit. During the checkout process, multiple users can checkout any of the available keys. The same key can be used multiple times till it reaches the user limit. For allowing other users The users must check in the key. To configure multiple users, refer "Types of Accounts Discovered" on page 307.

Single key for multiple users: You can define a single key in a domain for multiple users and assign the maximum user limit. During the checkout process, multiple users can checkout the same key till the key usage reaches the maximum limit. After reaching the maximum usage, Privileged Account Manager does not allow further checkout of the keys. A succeeding user can check out the key only after a user checks in the key.

Privileged Account Manager does not reset the values for the shared key when users check in the key. This is called key check-in.

14 Privileged Access to Windows

Using Privileged Account Manager (PAM), you can provide access to a Windows computer in the following ways:

- **Remote Desktop Protocol Relay (RDP relay):** Using this method, you can create a policy for a windows RDP relay which can be accessed by the user from the User Console.

  This approach can be used when the direct access to the target Windows system is blocked using the Windows Firewall.

  For information about configuring RDP Relay, see Remote Desktop Protocol Relay.
- **Direct Remote Desktop Protocol (Direct RDP):** Using this method, you cannot provide privileged access to the user but you can monitor and audit user actions in the Windows server. The user can access this Windows server using any remote desktop client with their Windows account credentials.

  This approach can be used, when you want to avoid storing the credentials of the privileged users in PAM and avoid using proxy.

  For information about configuring Direct RDP, see Direct Remote Desktop Protocol.
- **Run as Privileged User:** Using this method, you can provide privileged access to a specific application in the Windows server. The user can access this application as a privileged user by connecting directly to the Windows server using any remote desktop client with their Windows account credentials.

  This approach can be used, when you want to provide privileged access to a specific application in the target Windows system.

  For information about configuring Run as Privileged User, see Run as Privileged User.
- **Credential Provider (CP):** Using this method, you can provide privileged access to a Windows server which can be accessed by the user using Privileged Account Manager credentials.

  This approach can be used, when you have host-based firewall in the target system and proxy cannot be used to connect with the system. It can also be used in a scenario of a lab environment, where you need direct privileged access to the system without knowing the admin credentials.

  For information about configuring Credential Provider, see Credential Provider.
- **Application SSO:** Using this method, you can provide privileged access to a Windows server and monitor the actions performed in the windows machine without installing a PAM agent.

  For information about configuring application SSO, see Application SSO.

Based on the information in the following table, you can choose the appropriate method to establish privileged session in windows system:

Method	Audit	Video Capture	Privileged Access	Command Risk & Automatic Session Disconnect	Access Through		Authentication Through	
					User Console	RDP Client	PAM Account	System Account
RDP Relay (Agent based)	✓	✓	✓	✓	✓	✗	✓	✗
Credential Provider (Agent based)	✓	✓	✓	✓	✗	✓	✓	✗
Direct RDP (Agent based)	✓	✓	✓	✓	✗	✓	✗	✓
Run as Privileged User (Agent based)	✓ (Audits only privileged application access)	✗	✓ (Privileged access to specific application)	✓	✗	✓	✗	✓
Application SSO (Agentless)	✓	✓	✓	✗	✓	✓	✓	✗

NOTE: Keystrokes are not audited in the Windows Command Prompt.

Workflow to Configure Privileged Access for Windows

This is the generic workflow that must be followed to configure privileged access for Windows:

1 **Register the agent**

For steps to register the agent, refer Installing and Registering a Framework Agent

2 **Add a Windows resource and its credentials**

For information about adding a Windows resource, see the Contextual Help of Credential Vault.

3 **Add a User Group (Optional)**

Add a user group with a list of Windows system users, who must get privileged access.

For steps to add a user group, refer "Adding a User Group" on page 117

4 **Add a Command**

- You can use the commands that are preloaded by Privileged Account Manager thats has default configurations, such as Windows Credential Provider Session, Windows Direct Session and RDP Session.

  (or)

- Add and Modify a Command

  For detailed information on adding a command, refer "Adding a Command" on page 122

  For detailed information on modifying a command, refer "Modifying a Command" on page 122

5 **Add and Modify a Rule**

For steps to add a rule, refer "Adding a Rule" on page 108

NOTE: When adding a rule, ensure that you choose the correct value for the **Run User**. Based on the value of the **Run User**, the user gets appropriated privileged access.

For steps to modify a rule, see "Modifying a Rule" on page 109

NOTE: When modifying a rule for Run as privileged user, ensure to modify the **Run Host** as `Submit Host`

---

6 **Add Command and User Groups to the Rule**

After creating the rule, drag and drop the appropriate command and user group to the rule.

After making appropriate configurations in the Privileged Account Manager, you can access the target host using any RDP client or user console as appropriate.

Session Management

Using the following methods you can provide a privileged session to a user and capture the user actions in the privileged session:

- "Remote Desktop Protocol Relay" on page 199
- "Credential Provider" on page 201
- "Direct Remote Desktop Protocol" on page 202

Remote Desktop Protocol Relay

The Remote Desktop Protocol Relay (RDP Relay) feature offers Single Sign-on capability and remote access to desktops through a secured connection.

In a privileged session, an administrator user who is allowed to access various devices can sign on to many managed devices from a single workstation without knowing the authentication passwords of those devices. In addition, the user can remotely view the desktops of the managed devices and work on them.

You enable privileged sessions for an administrator user with the user's information. Then you associate the privileged session with a rule that controls the commands that the user can run on permitted devices and applications.

NOTE: RDP Relay is supported with the following installers:

- Windows Installers
- Generic Linux Installers

- "Configuring the RDP Relay" on page 200
- "Accessing the RDP Relay" on page 200

Configuring the RDP Relay

You can configure a RDP Relay for Windows machines to allow users to remotely access these machine without the privileged account credentials.

For steps to configure, see "Workflow to Configure Privileged Access for Windows" on page 198

NOTE: In Windows 2008 R2, configure the following User Account Control settings:

- Disable **Switch to the secure desktop when prompting for elevation**.
- Set **UAC: Behavior of the elevation prompt for administrators in Admin Approval Mode** to a value other than `Prompt for credentials on the secure desktop` and `Prompt for consent on the secure desktop`.

If RDP Relay to Windows 10 or Windows 2016 fails with an error, see the section RDP Relay to Windows 10 or Windows 2016 Fails with a Network Authentication Error to workaround the issue.

Accessing the RDP Relay

After a RDP relay is configured by an administrator, the user can access the privileged session as follows:

1. Launch the My Access page.

   In a browser specify the IP address of the Framework Manager in the address bar in the following format:

   `https:// <IP address of the Framework Manager>/pam`
2. Press **Enter**. A Login screen appears.
3. Specify the username and password to log in to Privileged Account Manager and click **Login**.
4. Click **Windows** and click the icon before the appropriate resource name.

   An RDP file is downloaded.
5. Save and open the RDP file to launch the session.

NOTE: ◆RDP Relay Manager name is always shown in the RDP connection bar.

- When connecting to the remote session specify the username in capital letters.
- When establishing a remote session through RDP Relay, the following error may be displayed:

  `The remote computer disconnected the session because of an error in the licensing protocol`

To continue establishing a remote session, perform the following steps before starting an RDP session:

1. Install the latest version of Privileged Account Manager.
2. Launch Internet Explorer in **Run as administrator mode**.

Credential Provider

The Credential Provider feature helps the users to single sign-on to any Windows server or desktop through a secured Remote Desktop Connection. With Credential Provider, users can login to Windows server or desktop as a Privileged user by using Privileged Account Manager credentials.

Configuring Credential Provider

You can create rule to allow/deny access to specific users on a Windows server or desktop to connect to the required server. To disconnect a session refer, "Disconnecting a Privileged Session" on page 151.

To configure the rule for a Windows server or desktop, perform the following:

1 Ensure that the Windows computer which you want to access is registered to Privileged Account Manager as a agent. For more information, see Installing and Registering a Framework Agent .

2 Ensure that you have added the resource for the Windows computer. For more information, see the Contextual Help of Credential Vault.

3 In the home page of the administrator console, click **Command Control**.

4 (Conditional) If you want to control who can access a particular Windows computer, create a user group with the user name in capital letters.

4a If you want to deny specific users to access the server or desktop, create a separate user group and add the user names (in capital letters) in the **Users** field. By default all the users are granted access to the server.

5 Add a rule:

5a In the Command Control pane, click **Rules**.

5b In the details pane, click **Add**.

5c Specify a name for the rule, then click **Add**.

5d Select the newly added rule, then click edit icon in the details pane.

5e (Conditional) Configure the following for the users, who are allowed to access the Windows computer:

Session Capture: Yes

Authorize: Yes

Run Hosts: Submit User

Run Hosts: Submit Host

For more information about the rule configuration fields, see Modifying a Rule.

5f (Conditional) Configure the following for the users, who are denied access to the Windows Computer:

Session Capture: No

Authorize: No

5g Click **Modify**.

5h In the middle pane, click the commands icon.

5i From the list of commands, drag the **Windows Credential Provider Session** command and drop it to the newly added rule.

NOTE: If some of the users are not part of any defined user group, the actions of that user is not monitored but in the reporting console you can view the users who are connecting to the server or desktop, and the time when they started the session.

Direct Remote Desktop Protocol

When a user connects to a remote Windows server through any **Remote Desktop Connection Client**, the user's actions are not monitored. But, with the Direct Remote Desktop Protocol (Direct RDP) feature you can control the authorization, and monitor the actions of users connecting to a remote Windows server or desktop through remote desktop connection client.

You can connect to a Windows server or desktop by using your account credentials that are set up on the server. If you require to monitor the actions of the users, then you can use the direct remote desktop protocol feature. The **Windows Direct Session** command object is included with the `rdpDirect` command, which helps in monitoring the direct sessions. You can create a rule and specify who is authorized to connect to a Windows server or desktop and also disconnect the session when any malicious activity is detected.

Configuring Direct RDP

You can create rule to allow/deny access to specific users on a Windows server or desktop to connect to the required server. To disconnect a session refer, "Disconnecting a Privileged Session" on page 151.

To configure the rule for a Windows server or desktop, perform the following:

1. Ensure that the Windows computer which you want to access is registered to Privileged Account Manager as a agent. For more information, see Installing and Registering a Framework Agent .
2. In the home page of the administrator console, click **Command Control**.
3. (Conditional) If you want to control who can access a particular Windows computer, create a user group with the user name in capital letters.
   - 3a If you want to deny specific users to access the server or desktop, create a separate user group and add the user names (in capital letters) in the **Users** field. By default all the users are granted access to the server.
4. Add a rule:
   - 4a In the Command Control pane, click **Rules**.
   - 4b In the details pane, click **Add**.
   - 4c Specify a name for the rule, then click **Add**.

4d Select the newly added rule, then click edit icon in the details pane.

4e (Conditional) Configure the following for the users, who are allowed to access the Windows computer:

Session Capture: Yes

Authorize: Yes

Run User: Submit User

Run Hosts: Submit Host

For more information about the rule configuration fields, see Modifying a Rule.

4f (Conditional) Configure the following for the users, who are denied access to the Windows Computer:

Session Capture: No

Authorize: No

4g Click **Modify**.

4h In the middle pane, click the commands icon.

4i From the list of commands, drag the **Windows Direct Session** command and drop it to the newly added rule.

NOTE: If some of the users are not part of any defined user group, the actions of that user is not monitored but in the reporting console you can view the users who are connecting to the server or desktop, and the time when they started the session.

Application Management

Using the following method you can provide privileged access to a specific application in windows system and capture the user actions:

Application SSO

Application SSO allows you to provide privileged access to specific application in a Windows server and monitor the actions performed in the application without installing a PAM agent.

For information about configuring application SSO, see Application SSO.

Run as Privileged User

The administrator can use the run as privileged user feature to provide privileged access to users for a specific process, system tools, or specific files. For example, `service.msc` or `notepad.exe`.

- "Configuration to Run as Privileged user" on page 204
- "Accessing Windows System to Run as privileged user" on page 204

Configuration to Run as Privileged user

For configuring the windows machine to Run as Privileged, see "Workflow to Configure Privileged Access for Windows" on page 198

Accessing Windows System to Run as privileged user

After configuring the Run as privileged user policies in Privileged Account Manager, user can execute the Run as privileged user as follows:

1. Login to the system as an administrator by using any remote desktop accessing tool.
2. Right-click the process and select **Run as privileged user** to get privileged access to the process.

NOTE: ◆In Windows 2008 R2, Shift+right-click the applications in the **Start** menu to execute Run as privileged user.

- In Windows 2012, right-click the application in the folder where the application is installed to execute **Run as privileged user**.

You can also provide privileged access to specific files.

For Example: To provide privileged access to `critical.txt` file:

1. Create a short-cut to Notepad.

   Notepad is the process that is used to open the `critical.txt` file.
2. Right-click the short-cut to Notepad, then select **Properties**.
3. In the **Target** field, add the file path of the `critical.txt` file after the file path of the process, then click **OK**.

   NOTE: For example, the path can be added in the following format:

   `C:\WINDOWS\system32\notepad.exe "C:\critical.txt"`

   ---
4. Right-click the shortcut and select **Run as privileged user** to provide privileged access to the `critical.txt` file.

LDAP Group Lookup

The LDAP Group lookup feature retrieves LDAP group membership information for a user whose details are stored in external LDAP directories, such as NetIQ eDirectory, OpenLDAP, or Microsoft Active Directory. The information fetched can be used to perform external group matching in the rules.

- "Creating the LDAP Account in the Credential Vault" on page 205
- "Defining the User Group" on page 205
- "Creating a Rule for the LDAP Group" on page 205
- "Modifying a Rule for the LDAP Group" on page 205

Creating the LDAP Account in the Credential Vault

For creating LDAP account in the vault, click **Credential Vault > LDAP / Active Directory > *Vault Name* >** click the **+** icon next to **Resources** and provide the required information. For more information about the resource fields, see Contextual Help.

Defining the User Group

After creating an LDAP account, define a group to refer to the external LDAP group. For information on creating a user group, see "Adding a User Group" on page 117.

To configure an existing user group, perform the following:

1. On the home page of the console, click **Command Control**.
2. In the navigation pane, click the **Account Groups** icon, then click **User Groups**.
3. In the details pane, select the user group that you want to modify, then click the edit icon next to the user group name.
4. Configure the following fields:

   Name: Specify a name for the group.

   Type: You must select the **External Group** check box.

   External Group:

   Description: Describe the purpose of this user group.

   Manager Name, Manager Tel., Manager Email: Specify the name, telephone number, and e-mail address of the manager of this user group.

   Users: Add or change the users you want to include in this group. You can type the user names, one on each line, or paste them from elsewhere.

   For example, the external group can be matched by using the `%:=~/^[Cc][Nn]=G*/` regular expression,. This expression matches all external groups starting with `Cn=G` and followed by anything where user is part of the group.

   User Groups: From the list of groups you have already defined, select the user groups you want to include as subgroups of this user group. You can also add subgroups to a by dragging and dropping the groups to the target user group in the navigation pane.
5. Click **Finish**.

   You can now use this user group in rule conditions or as a script entity.

Creating a Rule for the LDAP Group

After creating a user group, you need to set up rules to use the created External User Group in Commands. For detailed information on adding a rule, see "Adding a Rule" on page 108.

Modifying a Rule for the LDAP Group

1. On the home page of the console, click **Command Control**.
2. In the Command Control pane, click **Rules**.
3. Select the rule that you want to modify.

4 In the details pane, click **Modify**.

5 Make the following changes:

Name: Change the name of the rule.

Description: Specify a description of the rule.

User Message: Specify the user message as `$<ExtGroups>$`.

Session Capture: Select either **On** or **Off**.

Authorize: Select either **Yes** or **No**, depending on whether you want the command protected by the rule to be authorized or not authorized if the rule conditions are met.

Run User: Select **Submit User** from the drop-down list.

Credentials: From the drop-down list, select the required resource. The Run User is automatically populated with the domain user provided in the resource.

Run Host: Define a run host by selecting the name of the host on which you want to run this command (this overrides any hostname defined through a set command).

Risk Level: Set a **Risk Level** of 0 to 99.

Audit Group: Define an **Audit Group**. This setting is for use in Compliance Auditor reports.

6 Click **Finish**. The settings you have defined for the rule are displayed in the console.

A typical result of the LDAP group lookup rule when a rule is created for a user to run the ID command as a `root` user is displayed below:

```
user1@pum-sles10sp3:/root> usrun id

<ExtGroups>

<groupname="CN=GROUP3,CN=Users,DC=pum,DC=com"/>

<groupname="CN=GROUP2,CN=Users,DC=pum,DC=com"/>

<groupname="CN=GROUP1,CN=Users,DC=pum,DC=com"/>

<groupname="cn=G1,o=netiq"/>

<groupname="cn=G2,o=netiq"/>

</extroups>

uid=1001(user1) gid=100(users) groups=0(root), 16(dialout), 33(video),
100(users)

user1@pum-sles10sp3:/root>
```

15 Privileged Access to UNIX and Linux

Using Privileged Account Manager you can provide UNIX and Linux users with controlled access to privileged commands in a secure manner across the enterprise. You can enable complete lockdown of user privilege by providing rules to determine the commands that are authorized to run, and a powerful account delegation feature that removes the need for common access to the `root` account.

You can provide access to UNIX, Linux, Network devices and Mainframe computers in the following ways:

- **pcksh and cpcksh:** Using these shells, you can provide privileged access to UNIX, Linux, Mainframe and network devices and monitor the actions performed in the target machine in the form of keystrokes. These shells are based on the Korn shell (ksh) and are installed as part of the Command Control Agent.

  For information about configuring `pcksh` and `cpcksh`, see pcksh and cpcksh respectively.
- **`usrun` Command:** Using this command, you can provided privileged access to specific UNIX or Linux command. This package is installed as part of the Command Control Agent.

  For information about configuring `usrun`, `usrun`.
- **Secure Shell Relay (SSH Relay):** Using this method, you can provide access to the target SSH machine through a standard SSH client.

  For information about configuring SSH Relay, see Secure Shell Relay.
- **Application SSO:** Using this method, you can allow user to access UNIX, Linux, Mainframe and network device using any protocol, such as SSH, telnet, and so on.

  For information about configuring application SSO, see Application SSO.

Based on the information in the following table, you can choose the method to establish privileged session in Unix or Linux system:

Methods	Audit	Video Capture	Privileged Access	Command Risk & Automatic Session Disconnect	Access Through		Authentication Through	
					SSH Client	User Console	System Account	PAM Account
pcksh (Agent-based)	✓ (Audits all the user actions in the privileged shell)	✗	✓	✓	✓	✗	✓	✗

Methods	Audit	Video Capture	Privileged Access	Command Risk & Automatic Session Disconnect	Access Through		Authentication Through	
					SSH Client	User Console	System Account	PAM Account
cpcksh (Agent-based)	✓	✗	✗	✗	✓	✗	✓	✗
usrun (Agent-based)	✓ (Audits only the commands that has usrun as a prefix)	✗	✓	✓	✓	✗	✓	✗
SSH Relay (Agentless)	✓	✓ (Session replay* of SSH session along with video capture of X11 window.)	✗	✗	✓	✓	✗	✓
Application SSO (Agentless)	✓	✓	✓	✗	✓	✓	✗	✓

Session Replay: Session replay is replay of the SSH user's terminal input and output.

Workflow to Configure UNIX and Linux Privileged Sessions

The generic workflow to configure the UNIX and Linux privileged sessions are as follows:

1. **Register the agent (Conditional)**

   If you are using cpcksh, pcksh, or usrun methods, you must register the agent to the Framework Manager. For steps to register an agent, refer Installing and Registering a Framework Agent

2. **Add the Privileged Accounts of SSH Resources (Conditional)**

   If you are using SSH Relay, you must add SSH resource and add its privileged account credentials. For steps to create a SSH resource and its credentials, see the Contextual Help of Credential Vault.

3. **Add a User Group (Optional)**

Add a user group with a list of UNIX or Linux system users, who are intended to get privileged access. For steps to add a user group, refer "Adding a User Group" on page 117.

4 **Add and Modify the Command**

For steps to add a command, see "Adding a Command" on page 122. For SSH relay, you can also use the preloaded SSH Session command instead of adding a new command.

For steps to modify a command, see "Modifying a Command" on page 122.

5 **Add a Rule**

For steps to add a rule, see "Adding a Rule" on page 108.

NOTE: Ensure that you choose the correct value for the **Run User**. Based on the value of the **Run User**, the user gets appropriated privileged access.

---

6 **Add Commands and User Groups to the Rule**

After creating the rule, drag and drop the appropriate command and user group to the rule.

After making appropriate configurations in the Privileged Account Manager, you can access the target host using the SSH Client or User console appropriately.

Session Management

Privileged session and session capture can be achieved through the following methods:

- "pcksh" on page 209
- "cpcksh" on page 213
- "Secure Shell Relay" on page 215

pcksh

pcksh is used by administrator to grant privileges to a non-privileged system user, such as the ability to run commands as `root` and to perform a complete session capture of all the user actions. A user logs in as a non-privileged user, then issues a `usrun pcksh` command to access the root ksh shell and all the user actions in this shell are audited.

In addition, you can also configure rules to set up command risks and disconnect the session when executing specific commands.

Using pcksh shell you can perform the following:

- "Privileged Session Using pcksh" on page 210
- "Complete Session Control Using pcksh" on page 211

Privileged Session Using pcksh

Using pcksh method the administrator can grant privileged session to a non-privileged system user and all the user action in the privileged session are captured.

- "Configuring `pcksh for a Privileged Session`" on page 210
- "Accessing `pcksh for a Privileged Session`" on page 210
- "Usage Scenario" on page 210

Configuring pcksh for a Privileged Session

To grant privileged session to a non-privileged system user, the administrator must configure pcksh privileged session in Privileged Account Manager. For steps to configure the `pcksh` privileged session in Privileged Account Manager, see "Workflow to Configure Privileged Access for Windows" on page 198

Accessing pcksh for a Privileged Session

To access pcksh privileged session in Linux or UNIX system perform the following,

1. Log into the UNIX system as a non-privileged user.
2. Use `usrun` command to gain privileged shell access to perform administrative functions.

   For example, specify `usrun pcksh` or `usrun shell` command. The command is rewritten to `/usr/bin/pcksh` and Command Control Audits set to 1 based on the policy created in Privileged Account Manager.
3. Execute the commands that require privileged access and perform the required operations in the UNIX or Linux system. These actions that are performed within the pcksh shell are audited based on the Command Control policy and can be viewed in Command Control Reports. For steps more information on the Command Control Reports, see "Command Control Reports" on page 86

If the users need different environment variables to run some of their privileged commands, you can use a script to set up the values.

By default, Command Control uses the environment variables of the executing user. If the users receive a "not found" message for a command, you need add environment variables to the rule. For configuration information, see "Scripts" on page 131 and "Modify Environment Script" on page 134.

You can also define illegal commands, including built-in shell commands, in a script assigned to the rule. For configuration information, see "Scripts" on page 131 and "pcksh Illegal Commands Script" on page 135.

Usage Scenario

Consider a scenario where the administrator has to provide privileged access to a part of the user session and monitor that privileged session.

For this scenario, the administrator must perform the following configuration in the command control:

1. Register the agent to Privileged Access Manager
2. Add a pcksh command `pcksh_cmd` with the following field values:

Description: Explain the purpose of this command. For example, `When a user submits a usrun pcksh command or a usrun shell command, the command is rewritten to /usr/bin/pcksh. The Command Control Audit level is set to 1, which enables an additional level of audit to use with the Command Risk.`

Rewrite: `/usr/bin/pcksh -o audit 1`

Commands:

`pcksh`

`shell`

3 Create a user group `pcksh_usrgrp` with the following field values:

Description: Explain the purpose of the user group. For example, `Defines the user accounts that can run the usrun pcksh command to access root privileges.`

Users: Specify the usernames of the users on the Linux and UNIX hosts that have the permission to use the usrun pcksh command.

4 Add a rule `pcksh_rule` with the following field values:

Description: Explain the purpose of the rule. For example, `Matches users who submit a usrun pcksh or usrun shell command. It authorizes their session and enables session capture as root. The command assigned to this rule also included a rewrite that enables the additional level of audit to be used in conjunction with the command risk list.`

Session Capture: Select **On**.

Authorize: Select **Yes**, then select **Stop from the drop-down menu**.

Run User: Specify `root`.

5 Drag and drop the command `pcksh_cmd` and user group `pcksh_usrgrp` to the rule `pcksh_rule`.

After the administrator has configured the authorization rule in Privileged Account Manager, the non-privileged Linux or UNIX user can gain privileged session as following:

1 Log into the Linux or UNIX system as a non-privileged user.

2 Enter the command `usrun pcksh` to start a privileged session.

All the user actions in this privileged session are audited and the administrator can view these reports in the admin console.

Complete Session Control Using pcksh

You can use pcksh to get complete session capture of the non-privileged UNIX or Linux system user. For complete session capture of the user, the user's login shell should be modified to pcksh client. The pcksh client executes commands as a normal Korn shell.The functions and the aliases that replace normal system commands are read from `/etc/profile.pcksh`.When the user issues a command that needs privileges to run, it is authorized through the Framework.

- "Configuring `pcksh for Complete Session Capture`" on page 212
- "Accessing `pcksh for Complete Session Capture`" on page 212

Configuring pcksh for Complete Session Capture

To get complete session capture using pcksh, the administrator must make appropriate configurations in Privileged Account Manager.For steps to configure the pcksh in Privileged Account Manager, see "Workflow to Configure Privileged Access for Windows" on page 198

Accessing pcksh for Complete Session Capture

To access pcksh for complete session capture perform the following,

1. Log into the UNIX or Linux system as a non-privileged user.
2. Use the tool provided in the UNIX or Linux environment to set the users' shell to the following:

   ```
   /usr/bin/pcksh
   ```

3. To ensure that configured commands are authorized at the Framework, add the following line to either the user's profile file or to the central `profile.pcksh` file in the `/etc` directory on the appropriate UNIX or Linux servers:

   ```
   set -o remote
   ```

   IMPORTANT: The `set -o remote` option forces all commands that are not built in to the user's shell to be authorized at the Framework. Commands for which a defined rule does not exist are not permitted to execute. To prevent all commands in the `profile.pcksh` file or `.profile file` from being passed to the Framework for authorization, add the `set -o remote` command at the end of the file.

4. (Optional) Set the following additional options in the profile file:

Option	Description
`set -o host <hostname>`	Specifies that all authorized commands are executed on the defined host, if permitted.
`set -o user <username>`	Specifies that all authorized commands are executed as the defined user if permitted.
`set -o audit <n>`	Enables auditing, Set <n> to one of the following values: ◆ **1:** Enables auditing of all commands that are not built into the user's shell. ◆ **2:** Enables auditing of all commands including commands that are built into the user's shell. This level of auditing can affect login times. After the audit value has been set, it cannot be changed. If it is turned on in the profile, the user cannot turn it off later.
`set -o ignoreperm`	Enables commands that have not been successfully authorized at the Framework to execute according to the local permissions in effect on the server where the command was issued.

Option	Description
`set -o test`	Allows typed commands to be checked to see if they would be accepted by the rule structure. A yes or no output to screen indicates the result. The `set -o test` option is normally used in conjunction with the `set -o remote` option.
`set -o test '${}$'`	Returns the complete metadata result that is generated by the Command Control manager.

Rule definitions override the settings for user and host. If a successfully matched rule specifies a run user or a run host, this user or host is used to execute the command, and not those specified in the `set -o` commands.

You can use rule conditions to match the run user or run host to the username or hostname defined by using these commands (see "Setting Conditions for a Rule" on page 111), but if a run user or run host is defined in the rule configuration, these are the ones that are used.

You can define a list of illegal commands, including built-in shell commands, in a script assigned to a rule. Users using the pcksh shell cannot run these commands, even if they are `root`.

Using Shell Scripts

You can hide some of the complexities of the privileged command syntax from the users by using scripts and aliases to wrap privileged tasks. Using this technique, the end user can log in with their non-privileged account and use what appear to be standard commands to perform privileged tasks. Alternatively, you could create a script that provides a menu system to access a set of administrative tasks. With this method, the user would simply select options from the menu to perform their privileged tasks.

Either method requires a shell script that executes under the `pcksh` shell and performs remote authorization. For example:

```
#!/usr/bin/pcksh
set –o remote
passwd $*
```

This script executes the `pcksh` client, sets it to use Command Control, and executes the `passwd` command.

cpcksh

cpcksh is used to audit the complete user's session. With NetIQ Privileged Account Manager, you can change a user's login shell to `cpcksh` (`/usr/bin/cpcksh`), then configure a Command Control rule to authorize `cpcksh` and enable session capture. When the users log in, the commands are captured and audited through NetIQ Privileged Account Manager.

This method of integration provides the most auditing functionality. By changing the user's shell to the `cpcksh` client instead of the `pcksh` client, Command Control can be configured to capture the user's complete session, in addition to all other audit and control features.When the user logs in to the server, the session is started with the `cpcksh` client, which executes as a normal Korn shell. A request is sent to the Command Control Manager for authorization.

Functions and aliases that can replace normal system commands are read from `/etc/profile.pcksh`. When the user issues a command that needs privileges to run, it is executed through the Command Control system.

- "Configuring `cpcksh` for Complete Session Capture" on page 214
- "Accessing `cpcksh` for Complete Session Capture" on page 214
- "Usage Scenario" on page 214

Configuring cpcksh for Complete Session Capture

To get complete session capture using `cpcksh`, the administrator must make appropriate configurations in Privileged Account Manager.For steps to configure the `cpcksh` in Privileged Account Manager, see "Workflow to Configure UNIX and Linux Privileged Sessions" on page 208

Accessing cpcksh for Complete Session Capture

To access cpcksh for complete session capture perform the following,

1. Log into the UNIX or Linux system as a non-privileged user.
2. Use the tool provided in the UNIX or Linux environment to set the user login shell to

   `/usr/bin/cpcksh`

3. Perform the required operation and all these user actions are audited and can be viewed in Command Control Reports. For more information on the Command Control Reports, see "Command Control Reports" on page 86

Usage Scenario

Consider a scenario where the administrator has to provide a privileged session and complete session when a non-privileged user logs in.

For this scenario, the administrator must perform the following configuration in the command control:

1. Register the agent to Privileged Access Manager
2. Add a pcksh command `cpcksh_cmd` with the following field values:

   Description: Explain the purpose of this command. For example, `When a user's shell is set to /usr/bin/cpcksh and the user logs in, a Command Control request is sent with a submitting command of -cpcksh to indicate login. The user's login shell is rewritten to /usr/bin/pcksh. The Command Control Audit level is set to 1, which enables an additional level of audit to use with the Command Risk.`

   Rewrite: `/usr/bin/pcksh -o audit 1`

Commands:

`-cpcksh`

3 Create a user group `cpcksh_usrgrp` with the following field values:

Description: Explain the purpose of the user group. For example, `Defines the user accounts that can use the cpcksh command.`

Users: Specify the usernames of the users on the Linux and UNIX hosts that have the permission to use the usrun pcksh command.

4 Add a rule `cpcksh_rule` with the following field values:

Description: Explain the purpose of the rule. For example, `Authorizes the matching of submit users who have /usr/bin/cpcksh as their defined login shell. It authorizes their session and enables session capture, when they are still running as their original login ID.`

Session Capture: Select **On**.

Authorize: Select **Yes**, then select **Stop if authorized** from the drop-down menu. These settings allow subsequent commands to be executed without authorization checks whenever the user has had one command authorized.

5 Drag and drop the command `cpcksh_cmd` and user group `cpcksh_usrgrp` to the rule `cpcksh_rule`.

After the administrator has configured the authorization rule in Privileged Account Manager, the non-privileged Linux or UNIX user can gain privileged session as following:

1 Log into the Linux or UNIX system as a non-privileged user.

2 Use the tool provided in the UNIX or Linux environment to set the users' shell to the following:

`/usr/bin/cpcksh`

3 Perform the required action in the Linux or UNIX system.

All the user actions in this privileged session are audited and the administrator can view these reports in the admin console.

Secure Shell Relay

Secure Shell Relay (SSH Relay) provides the ability to access privileged accounts using a standard SSH client. This feature provides the ability to access Privileged Account Manager functionality without an agent for Privileged Account Manager on the target host.

SSH Relay allows users to connect to a remote host by using secure shell without knowing the privileged account credentials such as password or identity certificate of the user.

SSH Relay session videos can be captured only if the PAM manager is in Linux environment.

- "Configuring an SSH Relay Session" on page 216
- "Accessing an SSH Relay Session" on page 216
- "Usage Scenarios" on page 217

Configuring an SSH Relay Session

The packages are:

- SSH Relay Agent
- SSH Agent

SSH Relay listens on port 2222. You need to verify port 2222 is assigned for hosts running the SSH `Relay Agent` package.

For steps to configure an SSH Relay in Privileged Account Manager, refer "Workflow to Configure UNIX and Linux Privileged Sessions" on page 208

Accessing an SSH Relay Session

After making appropriate SSH relay configuration, you can access the SSH relay session in the following ways:

- "Accessing an SSH Relay Session from My access console" on page 216
- "Accessing an SSH Relay Session from SSH Client" on page 216

Accessing an SSH Relay Session from My access console

Start an SSH client by selecting the policy for the SSH relay session on My Access page. A JAVA Webstart program will then launch the downloaded JNLP file, which will then launch the JAVA UI.

1. Launch the My Access page and specify the IP address of the Framework Manager in the address bar in the following format:

   ```
   https:// <IP address of the Framework Manager>/pam
   ```

2. Press **Enter**. A login screen appears.
3. Enter the username and password and click `Login` to log in to the Privileged Account Manager.

   A list of rules defined for that particular user is displayed in the following format:
   `<rulename>(<username>@<machinename>)`
4. Click on the rule required for accessing the Non Windows machine.

NOTE: ◆In Chrome browser, you have to open the downloaded JNLP file to launch the JAVA UI.

- In Mozilla Firefox and Internet Explorer, the JNLP file opens automatically and launches the JAVA UI.
- In Edge browser, you must modify the default program for launching the JNLP file to javaws.exe.

After the UI launches, the user must provide the credentials of the SSH Relay user to start the session.

Accessing an SSH Relay Session from SSH Client

1. You can initialize an SSH relay session by using the following command:

   ```
   ssh -t -p2222 <PUMframeworkuser@sshrelayhost> <root@hostname>
   ```

   To initialize an SSH relay session with X11 forwarding, use the following command:

```
ssh -X -t -p2222 <PUMframeworkuser@sshrelayhost> <root@hostname>
```

2 A list of all the available SSH sessions are displayed. Enter the appropriate option to start the respective SSH relay session and provide the credentials of the SSH Relay user.

NOTE: When you exit from the current SSH Relay session, all the available SSH Relay sessions are displayed again enabling you to connect to a different target system.

Usage Scenarios

Scenario 1:

Consider a scenario where the administrator has to provide privileged access to a PAM user.

For this scenario, the administrator must perform the following configuration in the command control:

1 Create an SSH `type Credential Vault` resource for the Linux or UNIX system and add the respective credentials.

2 Add the `ssh_relay_rule` rule with the following field values:

Session Capture: Select **On**.

Authorize: Select **Yes** and select **Stop if authorized**.

Use the drop-down list below to define what happens next:

- **Blank:** Checks the next rule in the hierarchy.
- **Stop:** No more rules are checked for the command.
- **Return:** The next rule to be checked is up one level in the hierarchy.
- **Stop if authorized:** If **Authorize** is set to **Yes**, no more rules are checked for the command.
- **Stop if unauthorized:** If **Authorize** is set to **No**, no more rules are checked for the command.

Account Domain: *<Credential Vault SSH Resource Name>*

Credentials: Select a credential from the drop-down list. **Run User** and **Run Host** are automatically populated based on the selection.

3 Drag and drop the preloaded SSH `Session` command to the `ssh_relay_rule` rule.

After the administrator configures the authorization rule in PAM, the PAM user can gain privileged session as follows:

1 Launch the My Access page using the following URL:

```
https:// <IP address of the Framework Manager>/pam
```

2 Log in using the PAM user credentials.

3 Click **Home > SSH/Telnet**, and then click the **Launch** icon to launch the respective resource.

4 Enter the PAM user password to access the SSH relay session.

The administrator audits the user actions in this privileged session and views these reports in the administration console.

Scenario 2:

Consider a scenario where the administrator has to provide privileged access with X11 application access to a PAM user.

For this scenario, the administrator must perform the following configuration in the command control:

1. Create a resource for the Linux or UNIX system and add the respective credentials.
2. Add a rule `ssh_relay_rule` with the following field values:

   Session Capture: Select **On**.

   X11 Enable: Select **Yes**.

   Capture the X11 application videos using the global videos settings. For information about modifying the video settings, see "Configuring the Video Conversion Settings" on page 94.

   Authorize: Select **Yes** and select **Stop if authorized**.

   Use the drop-down list below to define what happens next:

   - **Blank:** Checks the next rule in the hierarchy.
   - **Stop:** No more rules are checked for the command.
   - **Return:** The next rule to be checked is up one level in the hierarchy.
   - **Stop if authorized:** If **Authorize** is set to **Yes**, no more rules are checked for the command.
   - **Stop if unauthorized:** If **Authorize** is set to **No**, no more rules are checked for the command.

   Account Domain: *<Credential Vault SSH Resource Name>*

   Credentials: Select the required resource from the drop-down list. The **Run User** is automatically populated with the domain user provided in the resource.

   Run Host: *<Resource Name>*
3. Drag and drop the preloaded command SSH `Session` to the rule `ssh_relay_rule`.

After the administrator configures the authorization rule in PAM, the non-privileged Linux or UNIX user can gain privileged session as follows:

1. Launch the My Access page using the following URL:

   `https:// <IP address of the Framework Manager>/pam`
2. Log in using the PAM user credentials.
3. Click **Home > SSH/Telnet**, and then click the **Launch** icon to launch the respective resource.
4. Enter the PAM user password to access the SSH relay session.

   The administrator audits the user actions in this privileged session and views these reports in the administration console.

Scenario 3:

Consider a scenario where the administrator has to provide access to multiple PAM users with a single command control rule. The framework user gets access to the target resource with the same user account name only if this user account is also available in the target resource.

NOTE: In this case, the user accounts need not be added to the Credential Vault SSH Resource. If there are credentials created in the Credential Vault with the same name as the PAM login user name, login to the target server using these passwords.

For this scenario, the administrator must perform the following configuration in the command control:

1. Create a resource for the Linux or UNIX system.
2. Add a rule `ssh_relay_rule` with the following field values:

   Session Capture: Select **On**.

   Authorize: Select **Yes** and select **Stop if authorized**.

   Use the drop-down list below to define what happens next:

   - **Blank:** The next rule in the hierarchy is checked.
   - **Stop:** No more rules are checked for the command.
   - **Return:** The next rule to be checked is up one level in the hierarchy.
   - **Stop if authorized:** If **Authorize** is set to **Yes**, no more rules are checked for the command.
   - **Stop if unauthorized:** If **Authorize** is set to **No**, no more rules are checked for the command.

   Run User: `Submit User`

   Run Host: *<Credential Vault SSH Resource Name>*
3. Drag and drop the preloaded command SSH `Session` to the rule `ssh_relay_rule`.

After the administrator configures the authorization rule in PAM, the PAM user can gain access to the session as follows:

1. Launch the My Access page using the following URL:

   `https:// <IP address of the Framework Manager>/pam`
2. Log in using the PAM user credentials.
3. Click **Home > SSH/Telnet**, and then click the **Launch** icon to launch the respective resource.
4. Enter the PAM user password to access the SSH relay session.

   The administrator audits the user actions in this privileged session and views these reports in the administration console.

Scenario 4:

Consider a scenario where the administrator has to provide access of a specific user to a PAM user.

NOTE: You can specify the Run User as an account name or a Command Control user group containing the list of account names. The **Run Host** can be a specific target host name or a Command Control Host Group containing the list of target names. The target host names are the SSH type Credential Vault resource names.

For this scenario, the administrator must perform the following configuration in the command control:

1. Create a resource for the Linux or UNIX system.
2. Add a rule `ssh_relay_rule` with the following field values:

   Session Capture: Select **On**.

   Authorize: Select **Yes** and select **Stop if authorized**.

   Use the drop-down list below to define what happens next:

   - **Blank:** The next rule in the hierarchy is checked.
   - **Stop:** No more rules are checked for the command.
   - **Return:** The next rule to be checked is up one level in the hierarchy.
   - **Stop if authorized:** If **Authorize** is set to **Yes**, no more rules are checked for the command.
   - **Stop if unauthorized:** If **Authorize** is set to **No**, no more rules are checked for the command.

   Run User: *<Credential name from SSH Resource>/<Command Control User Group containing list of credential name>*

   Run Host: *<Credential Vault SSH Resource Name/Host Groups>*
3. Drag and drop the preloaded command `SSH Session` to the rule `ssh_relay_rule`.

After the administrator configures the authorization rule, the PAM user can gain access to the session as follows:

1. Launch the My Access page using the following URL:

   `https:// <IP address of the Framework Manager>/pam`
2. Log in using the PAM user credentials.
3. Click **Home > SSH/Telnet**, and then click the **Launch** icon to launch the respective resource.
4. Enter the PAM user password to access the SSH relay session.

   The administrator audits the user actions in this privileged session and views these reports in the administration console.

Command Management

You can gain privileged access to a specific command using the following method:

usrun

The `usrun` command is a function provided by Privileged Account Manager for executing specific commands in the UNIX and Linux system with privileges.

By using the `usrun` command, you can elevate the access privilege of a specific command based on the policies defined in Privileged Account Manager. You must specify `usrun` before any command in the Linux or UNIX system to elevate the access rights of that command.

When you use `usrun` command, Privileged Account Manager audits only the commands that are appended with the `usrun` and other operations in the session are not audited.

- "usrun Command Syntax" on page 221
- "Configuring usrun Command for Privileged Access" on page 221
- "Accessing usrun for Privileged Access" on page 221
- "Usage Scenario" on page 222

usrun Command Syntax

The usrun function can be used with the following options:

```
usrun [-b] [-p] [-t] [-x] [-u <user>] [-h <host>] <command>
```

Option	Description
`-b`	Puts the execution of the command into the background.
`-p`	Provides a pipe compatibility option for competitive products. It is only used for a competitive swap-out.
`-t`	Provides a test command option that tests the specified command against the rule structure. A yes or no is printed to the screen, indicating whether the command would be accepted or not.
`-x`	Enables the X11 forwarding option.
`-u <user>`	Specifies the user you want the command to run as, although this can be overwritten by the Command Control rules.
`-h <host>`	Specifies the host you want the command run on, although this can be overwritten by the Command Control rules. For *<host>* you can use either the hostname of the server or the agent name specified in the Hosts console.
<command>	Specifies the command to pass to the Command Control Manager.

Configuring usrun Command for Privileged Access

To provide privileged access to a specific set of command, you must make appropriate configurations in Privileged Account Manager. For steps to configure `usrun` in Privileged Account Manager, see "Privileged Access to UNIX and Linux" on page 207

Accessing usrun for Privileged Access

To use usrun to get privileged access,

1. Log into the target system as a non-privileged user
2. Execute the commands with prefix `usrun` to get privileged access to the command. For example, `usrun passwd`.

Privileged access is provided only to the specific set of commands that you have defined in the `usrun` Command Control policy.

3 All the privileged actions that is the commands executed with the prefix `usrun` are audited and can be viewed in the Command Control Reports. For more information about the Command Control Reports, see "Command Control Reports" on page 86.

Usage Scenario

Consider a scenario where the administrator has to provide a privileged access to a specific command such as passwd.

For this scenario, the administrator must perform the following configuration in the command control:

1 Register the agent to Privileged Access Manager.

2 Add a command and name it `usrun_pwd_cmd` with the following field values:

Description: Explain the purpose of this command. For example:

Allows a user to submit a usrun passwd command to change account passwords.

Commands: `passwd *`

3 Create a user group `usrun_pwd_usrgrp` with the following field values:

Description: Explain the purpose of the user group. For example:

Defines the user accounts that can run the usrun passwd command to change account passwords.

Users: Specify the usernames of the users on the Linux and UNIX hosts that have the permission to use the `usrun passwd` command.

4 Add a rule `usrun_pwd_rule` with the following field values:

Description: Explain the purpose of the rule. For example:

Matches users who submit a usrun passwd command. It authorizes their session and sets the run user to root.

Session Capture: Select **On**.

Authorize: Select **Yes**, then select **Stop from the drop-down menu**.

Run User: Specify `root`.

5 Drag and drop the command `usrun_pwd_cmd` and user group `usrun_pwd_usrgrp` to the rule `usrun_pwd_rule`.

After the administrator has configured the authorization rule in Privileged Account Manager, the non-privileged Linux or UNIX user can gain privileged access as following:

1 Log into the Linux or UNIX system as a non-privileged user.

2 Execute the command `usrun passwd`.

You can access the `passwd` command with elevated access and this user action is recorded and the administrator can view these reports in the admin console.

Enhanced Access Control

Command Control policies give you additional options to control the execution of commands. For example, you can use a policy to restrict the rights and roles of a command so that the command works only for one particular directory, file, network address, or system call.

Prerequisite

For using Enhanced Access control, you must install 32bit `glibc` library in 64 bit RHEL agent and manager.

- "Configuring a Command Control Policy" on page 223
- "Configuring a Path Policy" on page 223

Configuring a Command Control Policy

A command control policy is defined by using the policy script arguments. A policy script argument specifies the access rights of the applications based on the path, network, and capability.

1. On the home page of the console, click **Command Control**.
2. From the **Command Control Sample Scripts**, add the **Enhanced Access Control Policy** script.
3. Drag and drop the **Enhanced Access Control Policy** script from **Scripts** to **Authorizing Rule**.
4. Click the **Authorizing Rule** and access the **Script Arguments**.
5. Create a script argument with a name *policy* and add that policy to the **Value** field.

Configuring a Path Policy

A Path policy is a type of command control policy that restricts an application from accessing a specific directory based on the path.

The syntax of a Path policy is as follows:

```
path [owner] <path> <capability:capability:!capability>
```

owner specifies the file or directory ownership that should match with the current user ID.

path specifies a particular directory based on the path. Replace *path* with any of the following options:

Table 15-1 Path Options

Option	Description
`/dir/file`	Specifies the file that the application can access in the `/dir/`directory.
`/dir/`	Specifies the directory that the application can access.
`/dir/f*`	Specifies a file that begins with `f` in the `/dir/`directory that the application can access.
`/dir/*`	Specifies that the application can access all the files in the `/dir/` directory.
`/dir/**`	Specifies that the application can access all the files and the subdirectories within the `/dir/`directory.
`/dir/**/`	Specifies that the application can access all subdirectories that are recursively searched for in the `/dir/`directory.
`/dir/**/*`	Specifies that the application can access all the files that are recursively searched for in any subdirectory within the `/dir/`directory.

`capability` specifies the rights of the application. You can use the `!` symbol in the syntax to denote a logical *not*. For example, `all:!write` grants all the rights except the *write* role.

Replace `capability` with any of the following options:

Table 15-2 Capability Options

Option	Description
`privperms`	Enables the application with the `read`, `write`, and `ownership` permissions for the specified directory or file. The `privperms` command limits two areas of functionality: 1. Using the `chmod` command to set a file to setuid or setgid. 2. Using the `chown` or `chgrp` command to change the ownership of a file.
`perms`	Enables the application to assign the permissions of a specified directory or file.
`read`	Enables the application to assign the `read` permission for a specified directory or file.
`write`	Gives the application the `create` and `write` permissions for the specified directory or file.
`unlink`	Gives the application the `deletion` rights for the specified directory or file.
`mknod`	Enables the application to create system files in the specified directory.
`exec`	Enables the application to execute the shared files and files for which the application does not have `read` and `write` permission.

Option	Description
`unsafe`	Enables the application to execute any file that does not inherit the policy.
`link`	Enables the application to create a symbolic link or hard link to another file.
`log[=<0-9>]`	Enables the application to audit system calls, with an optional risk value of `0-9`.
`all`	Enables the application to have all permissions.

You can use wildcards, regular expressions, and strings in the Path policy. For example, using the word `default` in the following example specifies the default policy.

```
path default all:log
path /opt/oracle/private/** !all:log=9
```

When administering EAC policy, do not restrict the following permissions to the listed folders:

Read / Write Permission	Read Permission
`/tmp/`	`/etc/resolv.conf`
`/dev/zero`	`/etc/hosts`
`/dev/null`	`/etc/passwd`
`/dev/tty`	`/etc/groups`
`/devices/**`	`/dev/random`
`/proc/<pid>/**`	`/dev/urandom`
`/tmp/**`	`/etc/utmp`
`/var/tmp/**`	`/etc/utmpx`
	`/usr/share/**`
	`/usr/lib/**`
	`/lib/**`
	`/usr/lib64/**`
	`/lib64/**`

NOTE: `Solaris 9/sbin/sh` is a static binary and therefore cannot enforce EAC.

16 Privileged Access to Databases

When users access a database with privileged credentials, the chances for data loss or sensitive information misuse go up. The administrators need to ensure that the connection to the database is secure and the database credentials are not misused. Privileged Account Manager provides the database monitoring feature where administrators can protect the database by controlling and monitoring the activities of the users who connect to the database.

In addition, Privileged Account Manager allows you to assign the risk to a specific query or a table in the database. Based on the risk configuration, you can identify any suspicious activities in the database and disconnect the session or block the respective user from accessing the database.

Privileged Account Manager enables you to control and monitor database accesses by granting access to the database as follows:

- **Database Access Through Credential Checkout:**

  This method enables you to provide privileged access to the database using the credentials checked out from Privileged Account Manager. In this method, the privileged account credentials are reset after every check-in to avoid misuse of credentials. For more information about configuring credential checkout for the database, see Database Access Through Credential Checkout.

- **Database Access Through PAM Proxy:**

  Using this method, you can allow users to access the database through PAM proxy where PAM monitors the activities performed on the database. For more information about configuring database access through PAM proxy, see Database Access Through PAM Proxy.

- **SSO to the Database:**

  Using this method, you can allow users to SSO to a database session and monitor the activities performed on the database. For more information about configuring privileged SSO to database, see Application SSO.

Based on the information in the following table, you can choose the appropriate database access method:

Method	Keystroke Audit	Command Audit	Video Capture	Command Risk & Automatic Session Disconnect	Manual Disconnect
Database Access Through PAM Proxy (Agentless)	✗	✓	✗	✓	✓
Database Credential Checkout (Agentless)	✗	✗	✗	✗	✗
Privileged SSO to Database (Agentless)	✓	✗	✓	✗	✓

Database Access Through Credential Checkout

Credential Checkout for databases allows you to provide elevated access to a database and monitor user actions on the database. This feature is supported only on Linux environments.

- Configuring Credential Checkout for Oracle Database
- Configuring Credential Checkout for Other Databases
- Checking Out Database Credentials

Configuring Credential Checkout for Oracle Database

To enable credential checkout for Oracle, perform the following:

1 Download and install the Oracle database client:

1a Download and install the Oracle database client by using the `instantclient-basic-linux.x64-x.x.zip` package.

NOTE: You can download the Oracle database client from the Instant Client at http://www.oracle.com/technetwork/indexes/downloads/index.html#database. All the files that you retrieve through the Oracle client zip/ tar file should be saved in `/lib64` for 64-bit machine and `/lib` for 32-bit machine.

1b Create a symbolic link `libclntsh.so` for the `libclntsh.so.xx.x` file in /lib64 or /lib.

For example, for `libclntsh.so.12.1` create a symbolic link `libclntsh.so` (`libclntsh.so -> libclntsh.so.12.1`).

2 Configure the Oracle client library path in PAM:

2a On the home page of the Privileged Account Manager administration console, click **Hosts**.

2b On the middle pane, select the Privileged Account Manager host.

2c On the right pane, click **Packages**.

2d Select the **dbaudit** package.

2e On the left pane, click **Settings**.

2f In the **Oracle Client Library Path** field, specify the path where oracle client is installed. By default the path is `/lib64` for a 64-bit machine or `/lib` for a 32-bit machine.

This library must be installed on a Privileged Account Manager server.

3 Add the database server details as a resource and add the privileged account of the database server. To add database resource and its credentials, click **Credential Vault > Database > *Database Type*** and click **+** next to the **Resources**. For more information about the resource configuration fields, see the contextual help.

4 Create a database rule:

4a On the home page of the console, click **Command Control**.

4b In the Command control pane, click **Rules**.

4c In the details pane, click **Add Rule**.

4d Specify a name for the database rule, then click **Finish**.

4e To configure the rule, select the rule, then in the details pane, click **Modify**.

Configure only the following:

Run User: Select **Everyone** from dropdown list.

Run Host: Specify the name of the Database resource created above.

Authorize: Select **Yes**, then select **Stop** from the drop-down list.

4f Click **Finish**. The settings you have defined for the rule are displayed in the console.

5 Add database password check out command to the rule:

5a On the middle pane, click the **Commands** icon.

5b For database password check out rule, From the drop down list of commands, drag the **Oracle DB Password Check Out** command and drop it to the database rule

Configuring Credential Checkout for Other Databases

To enable credential checkout for databases, such as Microsoft SQL Server, MySQL, PostgreSQL, MariaDB, Sybase, and IBM Db2 perform the following:

1 In the agent that has the `dbaudit` module, perform the following:

1a Install the ODBC (Open Database Connectivity) package that is unixODBC rpm package which is part of the OS distribution.

1b Create the Symbolic links for ODBC Libraries in `/lib64` or in `/usr/lib64` as explained below:

1b1 Create a link `libodbc.so` for `libodbc.so.x.x.x`

1b2 Create a link `libodbcinst.so` for `libodbcinst.so.x.x.x`

1c Install the supporting ODBC driver of the respective database. This ODBC driver is available as part of the database provider's server distribution.

For Microsoft SQL Server, choose the drivers as follows:

1. Microsoft SQL Driver is supported only on Linux 64-bit.
2. Free TDS Driver is supported on Linux 32 bit and 64-bit.

1d Configure the database driver in ODBC by using `odbcinst.ini` file.

1e Configure Data Source Name (DSN) of the database in the `odbc.ini` file.

For more information about how to configuring `odbcinst.ini` and `odbc.ini` files, see the Knowledge Base Article.

NOTE: To enable password change for a Linux IBM Db2 database, refer to the IBM Db2 documentation. For more information on setting up ODBC application connectivity on Linux using the IBM Data Server Driver, refer to the IBM Support pages.

---

2 In the Privileged Account Manager administration console:

2a Set the ODBC library path:

2a1 On the home page of the Privileged Account Manager administration console, click **Hosts**.

On the middle pane, select the Privileged Account Manager host.

On the right pane, click **Packages**.

2a2 Select the `dbaudit` package.

2a3 On the left pane, click **Settings**.

2a4 In the **ODBC Library Path** field, specify the path where the symbolic links are created.

You can use the appropriate policy template to automatically create a resource and rule for databases. This resource and rule can be customized as required. For more information about adding the policy template, see "Adding a Policy Template" on page 54. To create the resource and rule manually, continue with the following steps.

2b Add the database server details as a resource and add the privileged account of the database server. To add database resource and its credentials, click **Credential Vault > Database > *Database Type*** and click **+** next to the **Resources**. For more information about the resource configuration fields, see the contextual help.

2c Create a database rule:

2c1 On the home page of the console, click **Command Control**.

2c2 In the Command control pane, click **Rules**.

2c3 In the details pane, click **Add**.

2c4 Specify a name for the database rule, then click **Add**.

2c5 To configure the rule, select the rule, click edit icon in the details pane and configure the following:

Run User: Select **Everyone** from the drop-down list.

Run Host: Specify the name of the Database resource created above.

Authorize: Select **Yes**, then select **Stop** from the drop-down list.

2c6 Click **Modify**. The settings you have defined for the rule are displayed in the console.

2d To add database password check out command to the rule, perform the following:

2d1 In the middle pane, click the **Commands** icon.

2d2 From the drop-down list of commands, drag the appropriate database command and drop it to the database rule.

Checking Out Database Credentials

Privileged Account Manager (PAM) allows users to checkout the database credentials in the following ways:

- Credential Checkout from the user console
- Checkout credentials using API tokens.

  For more information about AAPM, see Application to Application Password Management.
- Checkout credentials using REST API.

  To view the REST API documentation:

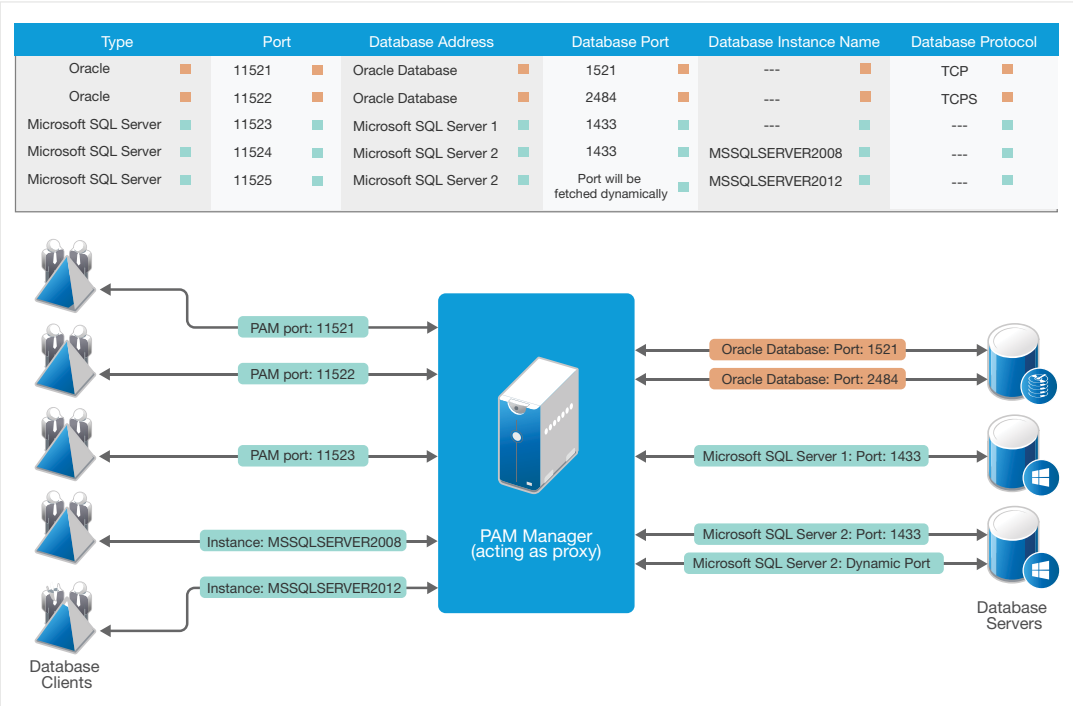
  1. In the new administration or user console, click the logged in user on the top-right corner.
  2. Click REST API.

     The REST API document opens in a new tab.

Database Access Through PAM Proxy

You can use this feature to protect a database by controlling and monitoring the activities of the users who connect to the database through database connector. A database connector acts as a proxy between the user's database client and the database server. This PAM proxy IP address and port number must be communicated to the user to whom you are providing access.

Figure 16-1 *Database Connector*



Type	Port	Database Address	Database Port	Database Instance Name	Database Protocol
Oracle	11521	Oracle Database	1521	---	TCP
Oracle	11522	Oracle Database	2484	---	TCPS
Microsoft SQL Server	11523	Microsoft SQL Server 1	1433	---	---
Microsoft SQL Server	11524	Microsoft SQL Server 2	1433	MSSQLSERVER2008	---
Microsoft SQL Server	11525	Microsoft SQL Server 2	Port will be fetched dynamically	MSSQLSERVER2012	---

After you provide database access through PAM proxy, you can allow the user to log into the database using:

- Their own database credentials.
- Credentials checked out from PAM.

  In this method, you are enhancing the database security by allowing PAM to manage database credentials. To configure credential checkout through PAM, see Database Access Through Credential Checkout.

For configuring the database access thrpogh PAM proxy to monitor the database activities, perform the following:

- Prerequisite
- Adding Database Connectors
- Adding Rules for Database
- Managing Database Connectors

Prerequisite

- Direct access from database client to the database server should be blocked.

  The database server should only accept the data transfer through the Privileged Account Manager server.
- If the database is connected over SSL to the Oracle database, import Privileged Account Manager certificate to the database client's wallet.

- If the database is connected over SSL to the Microsoft SQL server, import Privileged Account Manager certificate to the database client.
- If the database is connected over SSL to Microsoft SQL server, ensure that the Microsoft SQL server supports TLS 1.2.

Adding Database Connectors

You can add the database connectors for any required agent which has the `dbaudit` module to connect to the supported database.You can add any number of database connectors to an agent listed on the Database Connectors page.

- Adding Database Connector for Oracle
- Adding Database Connector for Microsoft SQL Server
- Adding Database Connector for Other Databases

Adding Database Connector for Oracle

1. On the home page of the console, click **Hosts**.
2. In the left pane, click **Database Connectors**.

   The Database Connectors page displays all the agents that have `dbaudit` package installed with the list of connectors.
3. Click **Add** on the bar for the required agent.

   If you have already added a connector, you can modify it as required by clicking the required connector field.
4. Specify the following:
   - **Type:** **Select Oracle** from the drop-down menu.
   - **DB Proxy Port:** Specify the port on which the Privileged Account Manager accepts the connection from database clients to connect to a specific database server. Privileged Account Manager maps this port number to a specific database that has a specific **DB address** and **DB Port**.
   - **DB Server Address:** Specify the IP address or host name of the Oracle database.
   - **DB Server Port:** Specify the port number of the Oracle database.
   - **Connection Protocol:** Select **TCP** for non-SSL connection or **TCPS** for an SSL connection.
   - **DB SSL Version:** Specify the SSL version used on the Oracle database server.

   NOTE: ◆To use SSL, import the Privileged Account Manager certificate to the database client's wallet.
   - If you are using Oracle 11.x or earlier versions of Oracle for an SSL connection, PAM supports only the TLS1V0 SSL version.
   - If you are using Oracle 12.x, PAM supports the TLS1V0, TLS1V1 and TLS1V2 versions.

   ---
5. Click **Save**.

   When you save the configuration, the agents containing the `dbaudit` package restarts.

Adding Database Connector for Microsoft SQL Server

For Microsoft SQL Server database you can add a Microsoft SQL Server database connector using the port number or using the Microsoft SQL Server instance.

Adding Database Connector Using Port Number

1. On the home page of the console, click **Hosts**.
2. In the left pane, click **Database Connectors**.

   The Database Connectors page displays all the agents that have `dbaudit` package installed with the list of connectors.
3. Click **Add** on the bar for the required agent.

   If you have already added a connector, you can modify it as per requirement by clicking the required connector field.
4. Specify the following:
   - **Type:** Select **Microsoft SQL Sever** from the dropdown menu.
   - **Use with Instance:** The **Use with Instance** checkbox is selected by default. Uncheck this to configure the connector with the database port number.
   - **DB Proxy Port:** Specify the port number on which the Privileged Account Manager accepts the connection from database clients to connect to a specific database server. Privileged Account Manager maps this port number to a specific database that has a specific **DB address** and **DB Port**.
   - **DB Server Address:** Specify the IP address or host name of the Microsoft SQL server.
   - **DB Server Port:** Specify the port number of the Microsoft SQL server.
   - **Network Packet Size:** The default value is 4096. You can enter any value within the range 512 to 16000.

     NOTE: You need to enter the same value as specified here in the client, while connecting through this connector.

Adding Microsoft SQL Server Connector Using Named Instance

1. (Optional) If you know the Microsoft SQL Server instance name, perform the following:
   1. On the home page of the console, click **Hosts**.
   2. In the left pane, click **Database Connectors**.

      The Database Connectors page displays all the agents that have `dbaudit` package installed with the list of connectors.
   3. Click **Add** for the required agent.
   4. Specify the following:
      - **Type:** Select **Microsoft SQL Sever** from the dropdown menu.
      - **Use with Instance:** The **Use with Instance** checkbox is selected by default.

- **DB Proxy Port:** Specify the port number on which the Privileged Account Manager accepts the connection from database clients to connect to a specific database server. Privileged Account Manager maps this port number to a specific database that has a specific **DB address** and **DB Port**.
- **DB Server Address:** Specify the IP address or host name of the Microsoft SQL server.
- **Instance Name:** Enter the Database Instance name and click **Fetch Details**.

  NOTE: The SQL Server Browser service should be enabled in the SQL Server for which the instances are being fetched.

- **DB Server Port:** Specify the port number of the Microsoft SQL server.
- **Dynamic Port:** Click the **Dynamic Port** checkbox if a dynamic port is set for the configured server.
- **Network Packet Size:** The default value is 4096. You can enter any value within the range 512 to 16000.

  NOTE: You need to enter the same value as specified here in the client, while connecting through this connector.

2 (Optional) If you do not know the Microsoft SQL Server instance name, you can search and fetch the instance as follows:

   1. On the home page of the console, click **Hosts**.
   2. In the left pane, click **Database Connectors**.

      The Database Connectors page displays all the agents that have `dbaudit` package installed with the list of connectors.
   3. Click **Microsoft SQL Server Instances**.The Microsoft SQL Server Instances window is displayed.
   4. Enter the host name or the IP for which you want to fetch the instances and click **Fetch**.

      NOTE: The SQL Server Browser service should be enabled in the SQL Server for which the instances are being fetched.

   5. Select the desired instance and click **Ok**.

      NOTE: Click the **Dynamic Port** checkbox if a dynamic port is set for the configured server.

   6. Click **Save**.

Adding Database Connector for Other Databases

Perform the following for adding the connectors for the databases MySQL, PostgreSQL, MariaDB, Sybase, and IBM Db2:

1 On the home page of the console, click **Hosts**.

2 In the left pane, click **Database Connectors**.

The Database Connectors page displays all the agents that have `dbaudit` package installed with the list of connectors.

3 Click **Add** on the bar for the required agent.

If you have already added a connector, you can modify it as required by clicking the required connector field.

4 Specify the following:

- **Type:** Select the desired database from the drop-down menu.
- **DB Proxy Port:** Specify the port number on which the Privileged Account Manager accepts the connection from database clients to connect to a specific database server. Privileged Account Manager maps this port number to a specific database that has a specific **DB address** and **DB Port**.
- **DB Server Address:** Specify the IP address or host name of the database.
- **DB Server Port:** Specify the port number of the database.
- **Connection Protocol:** Select **TCP** for non-SSL connection and **TLS** for an SSL connection.

  This option is visible only for the databases for which you can choose the connection methods.

Databases	Connection Protocols
Sybase	You can choose **TCP** or **TLS** (SSL Connection) connection protocol.
MySQL and MariaDB	Privileged Account Manager dynamically selects the protocol based on the database client and database server configuration.
PostgreSQL	Privileged Account Manager supports only TCP protocol in this release.
IBM Db2	Privileged Account Manager supports only TCP protocol in this release.

- **Enable SHA Cipher Suites:** This option allows Privileged Account Manager to use SHA cipher suites lower than SHA256 for communicating with database client and server.

  By default, this option is enabled because most of the third party database clients use SHA cipher suites for SSL communication.

5 Click **OK**.

When you save the configuration, the agents containing the `dbaudit` package restarts for the connector configurations to take effect.

Adding Rules for Database

After adding the appropriate database connector, you must add rules to provide access to the database. You can add the database rule manually or by using the policy template. :

1 On the home page of the administration console, click **Command Control**.

2 To add a rule and provide the access to supported databases, perform the following:

2a (Conditional) To add the rules automatically using policy template, perform the following:

2a1 In the Command control pane, click **Rules**.

2a2 In the details pane, click **Add Policy Template** and then select the required policy from the drop-down list. For example, select **Oracle DB Session** to add rules for Oracle database.

2a3 Click **Import**.

When you click import a new rule is added and based on the type of policy selected, the appropriate command is also added to the rule. You can further edit the rule as required.

2b (Conditional) To add the rules manually, perform the following:

2b1 In the Command control pane, click **Rules**.

2b2 In the details pane, click **Add**.

2b3 Specify a name for the database rule, then click **Add**.

2b4 To configure the rule, select the rule, click edit icon in the details pane.

Configure only the following:

Session Capture: Select **On** to capture the activities done by the user.

Authorize: Select **Yes**, then select **Stop** from the drop-down list.

2b5 Click **Modify**.

The settings that are defined for the rule are displayed in the console.

2b6 In the middle pane, click the **Commands** icon.

2b7 From the list of commands, drag the required database command and drop it to the database rule.

NOTE: In case the user needs to have restricted access for specific instances of Microsoft SQL Server, you can create custom commands and drag it to the database rule. For example, if you want to provide restricted access to user for one of the two instances, then you need to add **<DBMSSQLAccess> InstanceName1** under **Commands** field when creating the custom command.

Managing Database Connectors

You can remove or edit the database connectors for any required agent which has the `dbaudit` module to connect to the supported database.

Viewing Database Connectors

To view a database connector, perform the following:

1. On the home page of the Administration console, click **Hosts**.
2. In the middle pane, select the root domain, **Hosts.**
3. In the left pane click **Database Connectors**.

   The Database Connectors page lists all the agents and its connectors on which `dbaudit` module is installed.
4. (Conditional) If you can view only the agents, but not the connectors then you can click on the bar. The page expands the view and displays all the database connectors for the specific agent.

   It expands the view and all database connectors for the specific agent gets displayed.
5. (Conditional) If you want to expand the view to display all the connectors for all the agents, click **Expand All**.
6. (Conditional) If you want to collapse the view to display only the agents that contain the `dbaudit` package, click **Collapse All**.

If any agent that contains the `dbaudit` package is offline, Privileged Account Manager displays the agent with offline message on the database connectors page.

Removing Database Connectors

To remove a database connector, perform the following:

1. On the home page of the Administration console, click **Hosts**.
2. In the left pane, click **Database Connectors**.

   The Database Connectors page displays all the agents that have dbaudit package installed with the list of connectors.
3. To delete a connector, click on the required connector for the required agent, then click **Remove > Save**.

Modifying Database Connectors for an Agent

You can add, remove, or modify the database connectors for any specific agent that has the dbaudit module. To add or modify connectors for multiple agents through a single page, see "Adding Database Connectors" on page 233.

To view, add, remove, or modify the database connector for a specific agent, perform the following:

1. On the home page of the administration console, click **Hosts**.
2. In the left pane, click **Database Connectors**.The Database Connectors page displays all the agents that have dbaudit package installed with the list of connectors.
3. Click on the **dbaudit** package to display the **Modify** and **Remove** options.
4. Click **Modify** to display the Modify Database Connector window.

   NOTE: For Microsoft SQL Server database connector, **Database Address** and **Instance Name** fields cannot be modified. The Instance Details will be displayed.

5 Click **Remove** to delete an added connector.

If you have already added a connector, you can modify it by clicking the required field.

Viewing Database Activity

To view the activities of a database user, perform the following:

1 In the **Reporting** console, select the appropriate database command, such as `DBOracleAccess` command for Oracle database, `DBMSSQLAccess` command for Microsoft SQL Server database, and so on.

Command control keystroke reports appears, which displays all the commands executed by the user on the database on that particular session.

2 (Conditional) If **Command Risk** for database query/ table is defined in the Command Control console, based on the level of risk a color is displayed against a particular input.

You can disconnect a session if the activity of a user is suspicious. For more information, refer "Disconnecting a Privileged Session" on page 151.

NOTE: 1.When a user logs in to any database server through Privileged Account Manager, the database session can contain multiple connections. If the user executes any suspicious query (for which auto-disconnect is configured in the **Command Risk**), Privileged Account Manager disconnects the connection on which the query is executed. The user can still use the existing session, or establish a new database session. If the suspicious query results in blocking the user (if **Auto Block** is also configured in the **Command Risk**), Privileged Account Manager will not allow any new session, or any new connections within the existing sessions.

2. For any database, Privileged Account Manager disconnects a session if auto-disconnect is configured for a user. In case of such progressive session with multiple active connections, if the Privileged Account Manager terminates any connection, the remaining connections of the session won't be affected.

---

17 Privileged Access to Applications and Cloud Services

In an enterprise when a user uses the shared account credentials for privileged access to any application or database, this can lead to security vulnerability as the users can use the shared account credentials without any time limit. If the privileged access to shared accounts are not managed, auditing becomes difficult and leads to security risk.

Privileged Account Manager (PAM) manages the access and the security of the privileged account credentials through the Credential Vault. Privileged Account Manager securely stores the shared account credentials of the application or database in Credential Vault.

You can grant privileged access to applications or cloud services in the following ways:

- **Credential Checkout**

  This method enables you to provide privileged access to applications and cloud services using the password checked out from Privileged Account Manager. In this method, the privileged account passwords are reset after every check-in to avoid misuse of checked out passwords.

  For more information about credential checkout, see Credential Checkout.

- **Application SSO**

  Using this method, you can allow users to SSO to an application or a cloud service and monitor the activities performed on them.

  For more information about configuring application SSO, see Application SSO.

Based on the information in the following table, you can choose the appropriate method:

Method	Keystroke Audit	Command Audit	Video Audit	Command Risk & Automatic Session Disconnect	Manual Disconnect
Credential Checkout (Agentless)	✗	✗	✗	✗	✗
Privileged SSO (Agentless)	✓	✗	✓	✗	✓

Credential Checkout

The credential checkout feature helps in retrieving the credentials from Credential Vault. The credential checkout feature helps in managing the account credentials and provides the following capabilities:

- Provide available shared account credentials and deny access if all the credentials are in use.
- Provide users access to application or database for a fixed time period.
- After every session, reset the password of the account in the target application to maintain the password security.

A Privileged Account Manager administrator can create a privileged account for an application/ database and save the application/ database administrator credential. These credentials will be used only when resetting or checking-in the password. So, when a user requests for credentials to connect to Oracle database or any application, Privileged Account Manager checks for the login credentials that are available for that application, then provides the credentials to the user. An administrator can monitor the commands that a user runs on any application and audit the report based on the defined risk score.

The following sections provide details on configuring, accessing and managing shared account credentials by using the credential checkout feature.

- "Configuring Credential Checkout for Applications" on page 242
- "Configuring Credential Checkout for Cloud Services" on page 245
- "Configuring Credential Checkout Settings" on page 247
- "Checking Out Credentials" on page 247
- "Password Reset Scripts" on page 248

Configuring Credential Checkout for Applications

The privileged accounts that are set up on the following applications/ database can be managed through PAM. To manage those accounts, you must customize the sample script and add it to the PAM rule. For more information about customizing the script refer, "Password Reset Scripts" on page 248.

Following are the tested applications on which you can reset the password of the accounts that are existing for those applications:

IMPORTANT: Privileged Account Manager server must have Java 1.6 or higher for password reset to work on the following applications:

- SAP
- VMWare ESXi

- **eDirectory**

  NetIQ eDirectory is a list of objects that represent network resources, such as network users, servers, printers, print queues, and applications.You can enable password check-out feature to access the eDirectory server.

To enable credential checkout feature for eDirectory, you can add the rules by using the eDirectory policy template. For more information about using the policy template refer, "Adding a Policy Template" on page 54.

- **Active Directory**

  Active Directory is a directory service that authenticates and authorizes all users and computers in a Windows domain type network. It assigns and enforces security policies for all computers and installs, or updates software.You can enable password check-out feature to access the Active Directory server.

  To enable credential checkout feature for Active Directory, you can add the rules by using the Active Directory policy template. For more information about using the policy template, see "Adding a Policy Template" on page 54.

- **System Applications Products**

  System Applications Products (SAP) is an Enterprise Resource Planning System (ERP). You can enable the password check-out feature to access the SAP application.

  To connect PAM with the Systems, Applications, and Products (SAP) application, ensure that you download the following files on the PAM manager server:

  - SAP Java connector (JCO)

    You can download the JCO from the SAP Connectors site

  - The following files must be downloaded from the SAP Service Marketplace Web site (http://www.sap-ag.de/services) to the location `/opt/netiq/npum/service/local/cmdctrl/lib/` (for Linux) and `c:\Program Files\npum\opt\netiq\npum\service\local\cmdctrl\lib` (for Windows):

    - sapjco3.jar
    - (For Linux) libsapjco3.so
    - (For Windows) sapjco3.dll

NOTE: The download is free to any SAP software customer or development partner, but you are required to log in to the mentioned website.

To enable credential checkout feature for SAP, you can add the rules by using the SAP policy template. For more information about using the policy template, see "Adding a Policy Template" on page 54.

- **VMware ESXi**

  The VMware ESXi is a type-1 hypervisor that is used for the hardware virtualization. You can enable password check-out feature to access the ESXi server.

  PAM bundles the VMWare Infrastructure Java API to communicate with VMware ESXi server. The default location to VMWare Infrastructure Java API is `/opt/netiq/npum/service/local/cmdctrl/lib/` (for Linux) and `c:\Program Files\npum\opt\netiq\npum\service\local\cmdctrl\lib` (for Windows).

  To enable credential checkout on ESXi, you can add the rules by using the ESX policy template. For more information about using the policy template, see "Adding a Policy Template" on page 54.

- **Local Accounts on Linux**

  PAM supports Credential Checkout feature for local user accounts on any Linux Operating System running SSH.

- **Local Accounts on Unix**

  PAM supports Credential Checkout feature for local user accounts on AIX Operating System.

  Prerequisite

  In AIX machine, configure the following:

  - Specify `AcceptEnv LC_ALL` in the `sshd_config` file.
  - Restart `sshd` service.

- **Local Accounts on Windows**

  Prerequisite

  For **RHEL 8** (64-bit) and **RHEL 7** (64 bit), install the `redhat-lsb-core` package.

  For **RHEL 8** (64-bit) and **SLES 15** (64-bit), install the `lsb-release` package.

  - **On Windows Manager**:
    - Ensure that the `Windows Remote Management (WinRM)` service is running on Windows. To start `winrm` service, run the following command:

      ```
      Enable-PSRemoting –force
      ```

    - Add the target machine, where the password must be changed, to the `WinRM` trusted host. To add all servers as trusted host, run the following command:

      ```
      winrm set winrm/config/client '@{TrustedHosts="*"}'
      ```

    - Set the PowerShell execution policy to `Remotesigned` using the following command:

      ```
      Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
      ```

  - **On Linux Manager**:

    Install the `taskmanager` package.

  - **On Target Machine**:

    Ensure the following is done:

    - Powershell 2.0 or later must be installed in all the windows target machines as PAM uses PowerShell scripts to change password.
    - Windows Remote Management (WinRM) service must be running on the Windows machine. To start WinRM service, use the command:

      ```
      Enable-PSRemoting –force
      ```

    - IP address of the task manager must be added to the trusted host of the target machine. To add trusted host, use the command:

      ```
      winrm set winrm/config/client '@{TrustedHosts="x.x.x.x"}'
      ```

  PAM supports Credential Checkout feature for local user accounts on Window Operating System.

Enabling Credential Checkout for Applications

The credential checkout feature can be customized for the applications such as Salesforce, and so on.

To enable credential checkout for applications such as LDAP, Active Directory, SAP, ESXi you can import the respective policy template. When you import the policy template, all the components required for configuring a credential checkout, such as resource, and rule are added with default values. You must customize these according to your requirement. For more information about adding a policy template refer, "Adding a Policy Template" on page 54.

To enable credential checkout for application whose policy template is not available, you need to add the application server as a resource in the credential vault and add a rule for credential checkout. For information about adding a resource, see contextual help. For information about adding a rule, see "Adding a Rule" on page 108.

Configuring Credential Checkout for Cloud Services

The privileged accounts that are set up on the following cloud services can be managed through PAM. To manage those accounts, you must customize the sample script and add it to the PAM rule. For more information about customizing the script refer, "Password Reset Scripts" on page 248.

Following are the tested applications on which you can reset the password of the accounts that are existing for those applications:

IMPORTANT: Privileged Account Manager server must have Java 1.6 or higher for password reset to work on the following:

- OpenStack
- Amazon Web Services
- Microsoft Azure

- **OpenStack**

  OpenStack is a set of software tools designed for building and managing cloud computing platforms. You can enable the password check-out feature to access the OpenStack server.

  To enable the credential checkout feature for OpenStack, you can add the rules by using the OpenStack policy template or add an OpenStack resource and rule manually. For more information about enabling the credential checkout for OpenStack, see "Enabling Credential Checkout for OpenStack" on page 246

- **Amazon Web Services**

  Amazon Web Services (AWS) is a bundled remote computing service that provides cloud computing infrastructure over the Internet with storage, bandwidth, and customized support for Application Programming Interfaces (API). You can enable the password check-out feature to access services in AWS cloud.

  To enable credential checkout feature for AWS, you can add the rules by using the AWS policy template or add a AWS resource and rule manually. For more information about enabling the credential checkout for AWS, see "Enabling Credential Checkout for Amazon Web Services" on page 246

- **Microsoft Azure**

Microsoft Azure is a bundled remote computing service that provides cloud computing infrastructure over the Internet with storage, bandwidth, and customized support for Application Programming Interfaces (API). You can enable the password check-out feature to access services in Microsoft Azure.

To enable credential checkout feature for Microsoft Azure, you can add the rules by using the Microsoft Azure policy template or add a Microsoft Azure resource and rule manually. For more information about enabling the credential checkout for Microsoft Azure, see "Enabling Credential Checkout for Microsoft Azure" on page 246.

Enabling Credential Checkout for OpenStack

To enable credential checkout feature for the OpenStack server perform the following:

1. In the OpenStack server, create a user and assign the user to a project (tenant) with a role. For information about user creation and project and role assignment, see OpenStack Documentation.
2. In the PAM Administration Console,

   Add the OpenStack policy template to automatically add a resource and rule for OpenStack. This OpenStack resource and rule can be customized as required. For more information about adding the policy template, see "Adding a Policy Template" on page 54.

   Or

   Add a resource in the credential vault and a rule manually for OpenStack. For information about adding a resource, see contextual help. For information about adding a rule, see "Adding a Rule" on page 108.

   NOTE: For the password check out of accounts belonging to different OpenStack projects (tenants), you must create a different resource for each tenant.

Enabling Credential Checkout for Amazon Web Services

To enable credential checkout feature for Amazon Web Services (AWS) perform the following:

1. In the Amazon Web Services cloud, create a user and assign permissions or policies to the user. For information about AWS user creation, see AWS Documentation.
2. In the Privileged Account Manager Administration Console,

   Add the AWS policy template to automatically add a resource and rule for AWS. This resource and rule can be customized as required. For more information about adding the policy template, see "Adding a Policy Template" on page 54.

   Or

   Add a resource in the credential vault and a rule manually for AWS. For information about adding a resource, see contextual help. For information about adding a rule, see "Adding a Rule" on page 108.

Enabling Credential Checkout for Microsoft Azure

Prerequisite: Ensure that PAM password policies adhere to the Microsoft Azure password policies.

To enable credential checkout feature for Microsoft Azure:

1. In the Microsoft Azure cloud, create a user and assign permissions or policies to the user. For information about Microsoft Azure user creation, see Microsoft Azure documentation.
2. In the Privileged Account Manager Administration Console,

   Add the Microsoft Azure policy template to automatically add a resource and rule for Microsoft Azure. You can customize this resource and rule as required. For more information about adding the policy template, see "Adding a Policy Template" on page 54.

   or

   Add a resource in the Credential Vault and a rule manually for Microsoft Azure. Edit the resource in PAM and update the following fields:

   - Client ID: Microsoft Azure application ID. For more information, see Microsoft Azure documentation.
   - Authority: For example, https://login.microsoftonline.com/common/
   - AuthenticationTokenURL: For example, https://graph.windows.net

   For information about adding a resource, see the contextual help. For information about adding a rule, see "Adding a Rule" on page 108.

Configuring Credential Checkout Settings

1. On the home page of the Privileged Account Manager console, click **Access Dashboard**.
2. Click the **Configuration** tab.
3. In the **Delete Request After** field, select the number of days after which the request should be deleted from the list under **All**. For example, if you select **15 Days** all the requests that are 15 days old is deleted from the list of requests.
4. In the **Allow Grace Period of** field, select the extra duration that a user can access the password, after the requested time period expires.
5. In the **Server Email Id** field, enter the email id that is defined for the Privileged Account Manager server. This is the email id from which emails are sent to the users.
6. In the **Admin Email Id** field, enter the email id of the administrator for Privileged Account Manager.

Checking Out Credentials

Privileged Account Manager (PAM) allows users to checkout the credentials in the following ways:

- Checkout credentials from the user console
- Checkout credentials using API tokens.

  For more information about AAPM, see Application to Application Password Management.
- Checkout credentials using REST API.

  To view the REST API documentation:

  1. In the new administration or user console, click the logged in user on the top-right corner.
  2. Click REST API.

     The REST API document opens in a new tab.

Password Reset Scripts

You can use required policy templates to reset the password of the privileged accounts that are set on the supported application server. The password check-in process includes generating random password, resetting the password on the PAM database, and resetting password on the application. The password check-in process can either use the script to reset the password on the application and return the value to PAM database, or use Identity Manager to send the reset password on PAM database and synchronize the password with an active Identity manager application.

This section contains Perl Script for Customizing the Password Reset of Accounts in Applications.

- "LDAP Password Reset Script" on page 248
- "Active Directory Password Reset Script" on page 249
- "Openstack Password Reset Script" on page 251
- "AWS Password Reset Script" on page 253
- "Microsoft Azure Password Reset Script" on page 255
- "ESXi User Password Reset Script" on page 257
- "SAP User Password Reset Script" on page 259
- "Linux User Password Reset Script" on page 261
- "Windows User Password Reset Script" on page 263

LDAP Password Reset Script

Following is an example script for resetting the password of the accounts on all the LDAP directory except Active Directory. To reset Active Directory account password, you can use the script "Active Directory Password Reset Script" on page 249.

```
## PAM script to reset password of an LDAP user

## global variables
my $ldapURL = "";
my $retVal = 0;
my $ldap = "";
## arguments
my $host = $args->arg("host");
my $port = $args->arg("port");
my $secure = $args->arg("secure");
my $adminDN = $args->arg("adminName");
my $adminPasswd = $args->arg("adminPasswd");
my $userDN = $args->arg("userName");
my $userPasswd = $args->arg("userPasswd");
$ctx->log_info("START PASSWD RESET");
$ctx->log_debug("Input LDAP parameters : host - $host :: port - $port ::
secure -
$secure :: adminDN - $adminDN :: userDN - $userDN ");
$ctx->log_info("Resetting the password of the LDAP user $userDN");
## validate inputs
if ($host eq "" or $adminDN eq "" or $adminPasswd eq "" or $userDN eq "" or
$userPasswd eq "") {
$ctx->log_error("Incomplete LDAP inputs - following parameters are
```

```
mandatory -
host, adminDN, adminPasswd, userDN and userPasswd are passed.");
return 0;
}
# set default ldap port numbers
if ($port eq "") {
if ($secure eq "" || $secure != 0) {
$port = 636;
} else {
$port = 389;
}
}
# create ldap url
if ($secure != 0) {
$ldapURL = "ldaps://".$host.":".$port;
} else {
$ldapURL = "ldap://".$host.":".$port;
}
# Login as LDAP admin
$ctx->log_debug("Authenticating to the LDAP server...");
$ldap = ldap_bind($ctx, $ldapURL, $adminDN, $adminPasswd, 100);
if ($ldap->arg('err') != 0) {
my $le = $ldap->arg('err');
$ctx->log_error("LDAP authentication failed - $le");
return 0;
} else {
$ctx->log_debug("LDAP authentication to $ldapURL as $adminDN successful.");
}
# Reset the user password
$ctx->log_debug("Modifying the password of the user $userDN ...");
$ldap = ldap_modify($ctx, $userDN, "userpassword", $userPasswd);
if ($ldap->arg('err') != 0) {
my $le = $ldap->arg('err');
$ctx->log_error("LDAP modify failed - $le ");
return 0;
} else {
$ctx->log_debug("LDAP modify successful in resetting the password of the
user
$userDN.");
}
# Logout LDAP admin
$ctx->log_debug("Logging out $adminDN from $ldapURL");
ldap_unbind($ctx);
$ctx->log_info("END PASSWD RESET");
return 1;
```

Active Directory Password Reset Script

Following is an example script for resetting the password of the accounts on Active Directory:

```
## PAM script to reset password of Microsoft ActiveDirectory LDAP user
use MIME::Base64;
use Encode qw(encode);

## global variables
my $ldapURL = "";
my $retVal = 1;
my $ldap = "";

## arguments
my $host = $args->arg("host");
my $port = $args->arg("port");
my $secure = $args->arg("secure");
my $adminDN = $args->arg("adminName");
my $adminPasswd = $args->arg("adminPasswd");
my $userDN = $args->arg("userName");
my $userPasswd = $args->arg("userPasswd");
my $userPasswdEncoded = encode_base64(encode("UTF-16le",
"\"$userPasswd\""));

$ctx->log_info("START PASSWD RESET");
$ctx->log_debug("Input LDAP parameters : host - $host :: port - $port ::
secure - $secure :: adminDN - $adminDN :: userDN - $userDN ");
$ctx->log_info("Resetting the password of the LDAP user $userDN");

## validate inputs
if ($host eq "" or $adminDN eq "" or $adminPasswd eq "" or $userDN eq "" or
$userPasswd eq "") {
  $ctx->log_error("Incomplete LDAP inputs - following parameters are
mandatory - host, adminDN, adminPasswd, userDN and userPasswd are
passed.");
  return 0;
}
# set default ldap port numbers
if ($port eq "") {
  if ($secure eq "" || $secure != 0) {
    $port = 636;
  } else {
    $port = 389;
  }
}

# create ldap url
if ($secure != 0) {
  $ldapURL = "ldaps://".$host.":".$port;
} else {
  $ldapURL = "ldap://".$host.":".$port;
}

# Login as LDAP admin
$ctx->log_debug("Authenticating to the LDAP server...");
$ldap = ldap_bind($ctx, $ldapURL, $adminDN, $adminPasswd, 100);
if ($ldap->arg('err') != 0) {
  my $le = $ldap->arg('err');
  $ctx->log_error("LDAP authentication failed - $le");
```

```
  return 0;
} else {
  $ctx->log_debug("LDAP authentication to $ldapURL as $adminDN
successful.");
}

# Reset the user password
$ctx->log_debug("Modifying the password of the user $userDN ...");
$ldap = ldap_modify($ctx, $userDN, "unicodePwd", $userPasswdEncoded);
if ($ldap->arg('err') != 0) {
  my $le = $ldap->arg('err');
  $ctx->log_error("LDAP modify failed - $le ");
  $retVal = 0;
} else {
  $ctx->log_debug("LDAP modify successful in resetting the password of the
user $userDN.");
}

# Logout LDAP admin
$ctx->log_debug("Logging out $adminDN from $ldapURL");
ldap_unbind($ctx);

$ctx->log_info("END PASSWD RESET");
return $retVal;
```

Openstack Password Reset Script

Following is an example script for resetting the password of the accounts on Openstack:

```
# Sample perl script for Password Reset of a user on Openstack system

## global variables
my $retVal = 1;
my $OS = $^O;
my $cmd_output = "";

## arguments
my $host = $args->arg("host");
my $port = $args->arg("port");
my $secure = $args->arg("secure");
my $keystone_version = $args->arg("keystone_version");
my $admin = $args->arg("adminName");
my $adminPasswd = $args->arg("adminPasswd");
my $user = $args->arg("userName");
my $userPasswd = $args->arg("userPasswd");
my $tenant = $args->arg("tenant");

# Set passwords as environment variables
$ENV{ADMIN_PASSWORD} = $adminPasswd;
$ENV{NEW_PASSWORD} = $userPasswd;

$ctx->log_info("*** START Openstack PASSWD RESET");
$ctx->log_info("*** Privileged Account Manager running on the OS $OS");
$ctx->log_info("Openstack System input parameters : Openstack Host - $host
:: Port Number - $port :: Secure - $secure :: keystone_version -
```

```
$keystone_version :: admin - $admin :: user - $user :: tenant - $tenant");
$ctx->log_info("Resetting the password of the Openstack user $user ...");

## validate inputs
if ($host eq "" or $port eq "" or $secure eq "" or $admin eq "" or
$adminPasswd eq "" or $user eq "" or $userPasswd eq "" or $keystone_version
eq "" or $tenant eq "") {
   $ctx->log_error("Incomplete inputs - following parameters are mandatory
- Openstack host, port number, secure(1/0), keystone version, admin,
adminPasswd, userName, userPasswd and tenant name.");
    return 0;
}

# Execute the java command for password reset
if ($OS =~ "^MSWin") {
    $cmd_output = `java -jar C:/\"Program Files\"/NetIQ/npum/service/local/
cmdctrl/lib/NPUM_Openstack_api.jar  $host $port $secure $keystone_version
$admin $user $tenant`;
} else {
    my $point;
    my @new_pwd = ();
    my @pwd;;

#escape single quote ''' in user password
    @pwd = ();
    @pwd = split(//, $userPasswd);
        $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
        }
        $point++;
    }
    $userPasswd = join("", @new_pwd);

#escape single quote ''' in admin password
    @pwd = ();
    @new_pwd = ();
    @pwd = split(//, $adminPasswd);
        $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
```

```
        }
        $point++;
    }
    $adminPasswd = join("", @new_pwd);

   $cmd_output = `ADMIN_PASSWORD='$adminPasswd' NEW_PASSWORD='$userPasswd'
java -jar /opt/netiq/npum/service/local/cmdctrl/lib/NPUM_Openstack_api.jar
$host $port $secure $keystone_version $admin $user $tenant`;
}

if ($? != 0) {
    $ctx->log_error("Password reset for the user $user failed.");
    $retVal = 0;
} else {
    $ctx->log_info("Succesfully reset the password of the Openstack user
$user .");
}

$ctx->log_info("Command execution output as below : $cmd_output ");

$ctx->log_info("*** END Openstack PASSWD RESET");
return $retVal;
```

AWS Password Reset Script

Following is an example script for resetting the password of the accounts on AWS:

```
# Sample perl script for Password Reset of a user on AWS system

## global variables
my $retVal = 1;
my $OS = $^O;
my $cmd_output = "";

## arguments
my $host = $args->arg("host");
my $port = $args->arg("port");
my $secure = $args->arg("secure");
my $admin = $args->arg("adminName");
my $adminPasswd = $args->arg("adminPasswd");
my $user = $args->arg("userName");
my $userPasswd = $args->arg("userPasswd");

$ctx->log_info("*** START AWS PASSWD RESET");
$ctx->log_info("*** Privileged Account Manager running on the OS $OS");
$ctx->log_info("AWS System input parameters : AWS Host - $host :: Port
Number - $port :: Secure - $secure :: admin - $admin :: user - $user");
$ctx->log_info("Resetting the password of the AWS user $user ...");

## validate inputs
if ($user eq "" or $admin eq "" or $adminPasswd eq "" or $userPasswd eq "")
{
   $ctx->log_error("Incomplete inputs - following parameters are mandatory
- admin, adminPasswd, userName and userPasswd");
    return 0;
```

```
}

# Set passwords as environment variables
$ENV{AWS_ACCESS_KEY_ID} = $admin;
$ENV{AWS_SECRET_ACCESS_KEY} = $adminPasswd;
$ENV{NEW_PASSWORD} = $userPasswd;

# Execute the java command for password reset
if ($OS =~ "^MSWin") {
    $cmd_output = `java -jar C:/\"Program Files\"/NetIQ/npum/service/local/
cmdctrl/lib/NPUM_AWS_api.jar $user`;
} else {
    my $point;
    my @new_pwd = ();
    my @pwd;;

#escape single quote ''' in user password
    @pwd = ();
    @pwd = split(//, $userPasswd);
    $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
        }
        $point++;
    }
    $userPasswd = join("", @new_pwd);

#escape single quote ''' in admin password
    @pwd = ();
    @new_pwd = ();
    @pwd = split(//, $adminPasswd);
    $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
        }
        $point++;
    }
    $adminPasswd = join("", @new_pwd);

    $cmd_output = `AWS_ACCESS_KEY_ID='$admin'
AWS_SECRET_ACCESS_KEY='$adminPasswd' NEW_PASSWORD='$userPasswd' java -jar
```

```
/opt/netiq/npum/service/local/cmdctrl/lib/NPUM_AWS_api.jar $user`;
}

if ($? != 0) {
    $ctx->log_error("Password reset for the user $user failed.");
    $retVal = 0;
} else {
   $ctx->log_info("Succesfully resetted the password of the AWS user $user
.");
}

$ctx->log_info("Command execution output as below :
        $cmd_output ");

$ctx->log_info("*** END AWS PASSWD RESET");
return $retVal;
```

Microsoft Azure Password Reset Script

Following is an example script for resetting the password of the accounts on Microsoft Azure:

```
# Sample perl script for Password Reset of a user on Microsoft Azure
Account

## global variables
my $retVal = 1;
my $OS = $^O;
my $cmd_output = "";

## arguments
my $host = $args->arg("host");
my $port = $args->arg("port");
my $secure = $args->arg("secure");
my $admin = $args->arg("adminName");
my $adminPasswd = $args->arg("adminPasswd");
my $user = $args->arg("userName");
my $userPasswd = $args->arg("userPasswd");
my $Authority = $args->arg("Authority");
my $ClientID = $args->arg("ClientID");
my $AuthenticationTokenURL = $args->arg("AuthenticationTokenURL");
my $pam_home = getcwd;

# Set passwords as environment variables
$ENV{ADMIN_PASSWORD} = $adminPasswd;
$ENV{NEW_PASSWORD} = $userPasswd;

$ctx->log_info("*** START Microsoft Azure PASSWD RESET");
$ctx->log_info("*** Privileged Account Manager running on the OS $OS at
location $pam_home");
$ctx->log_info("Microsoft Azure System input parameters : Microsoft Azure
Host - $host :: Port Number - $port :: Secure - $secure :: admin - $admin
:: user - $user :: Authority - $Authority :: ClientID - $ClientID ::
AuthenticationTokenURL - $AuthenticationTokenURL ");
$ctx->log_info("Changing the password of the Microsoft Azure user $user
...");
```

```
## validate inputs
if ($host eq "" or $port eq "" or $secure eq "" or $admin eq "" or
$adminPasswd eq "" or $user eq "" or $userPasswd eq "" or $Authority eq ""
or $ClientID eq "" or $AuthenticationTokenURL eq "") {
   $ctx->log_error("Incomplete inputs - following parameters are mandatory
- Microsoft Azure host, port number, secure(1/0), keystone version, admin,
adminPasswd, userName, userPasswd ,Authority name, ClientID name and
AuthenticationTokenURL.");
    return 0;
}

# Execute the java command for password reset
if ($OS =~ "^MSWin") {
    $cmd_output = `java -jar \"$pam_home\"/service/local/cmdctrl/lib/
NPUM_AzureAD_api.jar $admin '$ClientID' '$AuthenticationTokenURL/$host/
users/$user?api-version=1.6' $Authority $AuthenticationTokenURL`;
} else {
    my $point;
    my @new_pwd = ();
    my @pwd;;

#escape single quote ''' in user password
    @pwd = ();
    @pwd = split(//, $userPasswd);
        $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
        }
        $point++;
    }
    $userPasswd = join("", @new_pwd);

#escape single quote ''' in admin password
    @pwd = ();
    @new_pwd = ();
    @pwd = split(//, $adminPasswd);
        $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
        }
```

```
        $point++;
    }
    $adminPasswd = join("", @new_pwd);

   $cmd_output = `ADMIN_PASSWORD='$adminPasswd' NEW_PASSWORD='$userPasswd'
java -jar /opt/netiq/npum/service/local/cmdctrl/lib/NPUM_AzureAD_api.jar
$admin '$ClientID' '$AuthenticationTokenURL/$host/users/$user?api-
version=1.6' $Authority $AuthenticationTokenURL`;
}

if ($? != 0) {
    $ctx->log_error("Password reset for the user $user failed.");
    $retVal = 0;
} else {
    $ctx->log_info("Successfully changed the password of the Microsoft
Azure user $user .");
}

$ctx->log_info("Command execution output as below : $cmd_output ");

$ctx->log_info("*** END Microsoft Azure PASSWD RESET");
return $retVal;
```

ESXi User Password Reset Script

Following is an example script for resetting the password of the accounts on ESXi:

```
# Sample perl script for Password Reset of a user on ESXi system

## global variables
my $retVal = 1;
my $OS = $^O;
my $cmd_output = "";

## arguments
my $host = $args->arg("host");
my $port = $args->arg("port");
my $secure = $args->arg("secure");
my $admin = $args->arg("adminName");
my $adminPasswd = $args->arg("adminPasswd");
my $user = $args->arg("userName");
my $userPasswd = $args->arg("userPasswd");

# Set passwords as environment variables
$ENV{ADMIN_PASSWD} = $adminPasswd;
$ENV{USER_NEW_PASSWD} = $userPasswd;

$ctx->log_info("*** START ESXi PASSWD RESET");
$ctx->log_info("*** Privileged Account Manager running on the OS $OS");
$ctx->log_debug("ESXi System input parameters : ESXi Host - $host :: Port
Number - $port :: Secure - $secure :: admin - $admin :: user - $user ");
$ctx->log_info("Resetting the password of the ESXi user $user ...");

## validate inputs
if ($host eq "" or $port eq "" or $secure eq "" or $admin eq "" or
```

```
$adminPasswd eq "" or $user eq "" or $userPasswd eq "") {
   $ctx->log_error("Incomplete inputs - following parameters are mandatory
- ESXi host, port number, secure(1/0), admin, adminPasswd, userName and
userPasswd.");
    return 0;
}

# Execute the java command for password reset
if ($OS =~ "^MSWin") {
    $cmd_output = `java -jar C:/\"Program Files\"/NetIQ/npum/service/local/
cmdctrl/lib/NPUM_ESXi_api.jar  $host $port $secure $admin $user`;
} else {
    my $point;
    my @new_pwd = ();
    my @pwd;;

#escape single quote ''' in user password
    @pwd = ();
    @pwd = split(//, $userPasswd);
    $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
        }
        $point++;
    }
    $userPasswd = join("", @new_pwd);

#escape single quote ''' in admin password
    @pwd = ();
    @new_pwd = ();
    @pwd = split(//, $adminPasswd);
    $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
        }
        $point++;
    }
    $adminPasswd = join("", @new_pwd);

    $cmd_output = `ADMIN_PASSWD='$adminPasswd'
USER_NEW_PASSWD='$userPasswd' java -jar /opt/netiq/npum/service/local/
```

```
cmdctrl/lib/NPUM_ESXi_api.jar $host $port $secure $admin $user`;
}

if ($? != 0) {
    $ctx->log_error("Password reset for the user $user failed.");
    $retVal = 0;
} else {
    $ctx->log_info("Succesfully resetted the password of the ESXi user
$user .");
}

$ctx->log_debug("Command execution output as below :
        $cmd_output ");

$ctx->log_info("*** END ESXi PASSWD RESET");
return $retVal;
```

SAP User Password Reset Script

Following is an example script for resetting the password of the accounts on SAP:

```
# Sample perl script for Password Reset of a user on SAP system

## global variables
my $retVal = 1;
my $OS = $^O;

my $cmd_output = "";

## arguments
my $host = $args->arg("host");
my $systemNumber = $args->arg("systemNumber");
my $clientNumber = $args->arg("clientNumber");
my $lang = $args->arg("lang");
my $admin = $args->arg("adminName");
my $adminPasswd = $args->arg("adminPasswd");
my $user = $args->arg("userName");
my $userPasswd = $args->arg("userPasswd");

# Set passwords as environment variables
$ENV{ADMIN_PASSWD} = $adminPasswd;
$ENV{USER_NEW_PASSWD} = $userPasswd;

$ctx->log_info("*** START SAP PASSWD RESET");
$ctx->log_info("*** Privileged Account Manager running on the OS $OS");
$ctx->log_debug("SAP System input parameters : SAP Host - $host :: System
Number - $systemNumber :: Client Number - $clientNumber :: Language ::
$lang :: admin - $admin :: user - $user ");
$ctx->log_info("Resetting the password of the SAP user $user ...");

## validate inputs
if ($host eq "" or $systemNumber eq "" or $clientNumber eq "" or $admin eq
"" or $adminPasswd eq "" or $user eq "" or $userPasswd eq "") {
   $ctx->log_error("Incomplete inputs - following parameters are mandatory
- SAP host, systemNumber, clientNumber, admin, adminPasswd, userName and
```

```
userPasswd.");
    return 0;
}

# set default language
if ($lang eq "") {
    $lang = "EN";
}

# Execute the java command for password reset
if ($OS =~ "^MSWin") {
    $cmd_output = `java -jar "C:/\"Program Files\"/NetIQ/npum/service/
local/cmdctrl/lib/NPUM_SAP_api.jar" $host $systemNumber $clientNumber
$lang $admin $user`;
} else {
    my $point;
    my @new_pwd = ();
    my @pwd;;

#escape single quote ''' in user password
    @pwd = ();
    @pwd = split(//, $userPasswd);
    $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
        }
        $point++;
    }
    $userPasswd = join("", @new_pwd);

#escape single quote ''' in admin password
    @pwd = ();
    @new_pwd = ();
    @pwd = split(//, $adminPasswd);
    $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
        }
        $point++;
    }
    $adminPasswd = join("", @new_pwd);
```

```
    $cmd_output = `ADMIN_PASSWD='$adminPasswd'
USER_NEW_PASSWD='$userPasswd' java -jar /opt/netiq/npum/service/local/
cmdctrl/lib/NPUM_SAP_api.jar $host $systemNumber $clientNumber $lang
$admin $user`;
}

if ($? != 0) {
    $ctx->log_error("Password reset for the user $user failed.");
    $retVal = 0;
} else {
   $ctx->log_info("Succesfully resetted the password of the SAP user $user
.");
}

$ctx->log_debug("Command execution output as below :
        $cmd_output ");

$ctx->log_info("*** END SAP PASSWD RESET");
return $retVal;
```

Linux User Password Reset Script

Following is an example script for resetting the password of the accounts on Linux:

```
#Sample perl script for Password Reset of a user on Linux local Account

## global variables
my $retVal = 1;
my $OS = $^O;
my $cmd_output = "";

## arguments
my $host = $args->arg("host");
my $port = $args->arg("port");
my $admin = $args->arg("adminName");
my $adminPasswd = $args->arg("adminPasswd");
my $user = $args->arg("userName");
my $userPasswd = $args->arg("userPasswd");
my $pam_home = getcwd;

# Set passwords as environment variables - SSHPASS and LC_ALL
$ENV{SSHPASS} = $adminPasswd;
$ENV{LC_ALL} = $userPasswd;

$ctx->log_info("*** START Linux Local Account PASSWD RESET");
$ctx->log_info("*** Privileged Account Manager running on the OS $OS at
location $pam_home");
$ctx->log_info("Linux System input parameters : Linux Host - $host :: Port
Number - $port :: admin - $admin :: user - $user");
$ctx->log_info("Changing the password of the Linux user $user ...");

## validate inputs
if ($host eq "" or $port eq "" or $admin eq "" or $adminPasswd eq "" or
$user eq "" or $userPasswd eq "") {
   $ctx->log_error("Incomplete inputs - following parameters are mandatory
```

```
- Linux host, port number, admin, adminPasswd, userName, userPasswd.");
    return 0;
}

if ($OS =~ "^MSWin") {
    $cmd_output = `\"$pam_home\"/bin/ssh.exe -p $port -n -o SendEnv=LC_ALL
-o StrictHostKeyChecking=no -Z -l $admin $host "echo -e
\$LC_ALL\\\\n\$LC_ALL | passwd $user 2>&amp;1"`;
} else {
    my $point;
    my @new_pwd = ();
    my @pwd;;

    #escape single quote ''' in user password
    @pwd = ();
    @pwd = split(//, $userPasswd);
    $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
            }
            else{
            $new_pwd[$point] = $_;
            }
        $point++;
    }
    $userPasswd = join("", @new_pwd);

    #escape single quote ''' in admin password
    @pwd = ();
    @new_pwd = ();
    @pwd = split(//, $adminPasswd);
    $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
        }
        $point++;
    }
        $adminPasswd = join("", @new_pwd);
        $cmd_output = `SSHPASS='$adminPasswd' LC_ALL='$userPasswd' /opt/
netiq/npum/service/local/sshrelay/bin/ssh -p $port -o SendEnv=LC_ALL -o
StrictHostKeyChecking=no -Z -l $admin $host
\"usr=$user;myrootuser=$admin;\" 'echo -e \$LC_ALL\\\\n\$LC_ALL | passwd
$user 2>&1'`;
```

```
}

if ($? != 0) {
    $ctx->log_error("Password reset for the user $user failed.");
    $retVal = 0;
} else {
    $ctx->log_info("Successfully changed the password of the Linux Local
Account Password Reset");
}

$ctx->log_info("Command execution output as below : $cmd_output ");

$ctx->log_info("*** End Linux Local Account PASSWD RESET");
return $retVal;
```

Windows User Password Reset Script

Following is an example script for resetting the password of the accounts on Windows:

```
# Sample perl script for Password Reset of a user on Windows system

## global variables
my $retVal = 1;
my $OS = $^O;

my $cmd_output = "";
my $pam_home = getcwd;

## arguments
my $host = $args->arg("host");
my $admin = $args->arg("adminName");
my $adminPasswd = $args->arg("adminPasswd");
my $user = $args->arg("userName");
my $userPasswd = $args->arg("userPasswd");
my $pam_home = getcwd;

# Set passwords as environment variables
$ENV{ADMIN_PASSWD} = $adminPasswd;
$ENV{USER_NEW_PASSWD} = $userPasswd;

$ctx->log_info("*** START WINDOWS PASSWD RESET");
$ctx->log_info("*** Privileged Account Manager running on the OS $OS at
location $pam_home");
$ctx->log_info("WINDOWS System input parameters : WINDOWS Host - $host ::
admin - $admin :: user - $user :: pam_home - $pam_home");
$ctx->log_info("Changing the password of the Windows user $user ...");


## validate inputs
if ($host eq "" or $admin eq "" or $adminPasswd eq "" or $user eq "" or
$userPasswd eq "") {
   $ctx->log_error("Incomplete inputs - following parameters are mandatory
- WINDOWS host, admin, adminPasswd, userName and userPasswd.");
    return 0;
}
```

```
# Execute powershell script for password reset
if ($OS =~ "^MSWin") {
    $ctx->log_info("*** running powershell $adminPasswd $userPasswd");
    $cmd_output = `powershell.exe -file "$pam_home/service/local/cmdctrl/
template/exports/winPwdChangeLocal.ps1" $host $admin $user`;
    $ctx->log_info("$cmd_output");
} else {
    my $point;
    my @new_pwd = ();
    my @pwd;;

#escape single quote ''' in user password
    @pwd = ();
    @pwd = split(//, $userPasswd);
    $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
        }
        $point++;
    }
    $userPasswd = join("", @new_pwd);

#escape single quote ''' in admin password
    @pwd = ();
    @new_pwd = ();
    @pwd = split(//, $adminPasswd);
    $point = 0;
    foreach (@pwd){
        if($_ eq "'"){
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = '\\';
            $new_pwd[$point++] = "'";
            $new_pwd[$point++] = "'";
        }
        else{
            $new_pwd[$point] = $_;
        }
        $point++;
    }
    $adminPasswd = join("", @new_pwd);
    $cmd_output = `ADMIN_PASSWD='$adminPasswd'
USER_NEW_PASSWD='$userPasswd' /usr/bin/pwsh -file "/opt/netiq/npum/
service/local/cmdctrl/template/exports/winPwdChangeLocal.ps1" $host $admin
$user`;
}
```

```
if ($? != 0) {
    $ctx->log_error("Password reset for the user $user failed.");
    $retVal = 0;
} else {
    $ctx->log_info("Successfully changed the password of the Windows user
$user .");
}

$ctx->log_debug("Command execution output as below :
        $cmd_output ");

$ctx->log_info("*** END WINDOWS PASSWD RESET");
return $retVal;
```

18 Privileged Single Sign-On

Privileged Account Manager allows you to grant privileged access to an application and enable single sign-on (SSO) to the application seamlessly.

Based on the information in the following table, you can choose the appropriate method to perform SSO for various targets:

Target	Agent-Based	Agentless
Windows	◆ RDP Relay (Remote Desktop Protocol Relay) ◆ Credential Provider (Credential Provider)	Application SSO (Application SSO) For example, you can enable SSO to any Windows server by granting access to the Remote Desktop Connection application.
UNIX, Linux, Mainframes, and Network Devices		◆ SSH Relay (Secure Shell Relay) ◆ Application SSO (Application SSO) For example, you can enable SSO to any UNIX or Linux server by granting access to PuTTY.
Database		Application SSO (Application SSO) For example, you can enable SSO to any database by granting access to appropriate database clients.
Enterprise Applications		Application SSO (Application SSO) For example, you can enable SSO to any application by granting access to appropriate application clients.
Web Applications		Application SSO (Application SSO) For example, you can enable SSO to any web application by granting access to appropriate web browsers.

Application SSO

Using application SSO, you can achieve the following:

- Privileged SSO to any target resource using the appropriate application.

- Privileged access without the PAM agent on the target.
- Complete session capture, such as keystroke and video capture.

For understanding and setting up application SSO, see the Configuring Application Single Sign-On section in the Privileged Account Manager Installation Guide.

You can configure application SSO in the following modes:

- RemoteApp Mode
- Direct Access Mode

RemoteApp Mode

In Remoteapp mode, the user launches the application from the user console and PAM does a SSO to the application using the SSO module installed in the server. For more information about remoteapp mode, see the RemoteApp Mode section in the Privileged Account Manager Installation Guide.

Prerequisites

CAUTION: Ensure that you disable Sticky Keys and Keyboard Shortcut keys for Task Manager in Windows while configuring Remote Application SSO feature. For more information, see "Disabling Task Manager Keyboard Shortcut Keys and Sticky Keys in Windows" on page 268.

Disabling Task Manager Keyboard Shortcut Keys and Sticky Keys in Windows

You can disable Sticky keys using Group Policy or through Control Panel for Windows.

To disable the Keyboard Shortcut keys for Task Manager, you can use Group policy or one of the following methods:

1. Access the Windows Registry by typing `regedit` in the Windows search box on the taskbar and press `Enter`.
2. Go to `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System`.
3. Create a new `DWORD(32-bit)` value with `Name` as `DisableTaskMgr` and `Data` value as `1`.

To disable the use of Keyboard Shortcut Keys for Task Manager, using a script, follow the below procedure:

1. Copy the following text in a notepad:

   ```
   Windows Registry Editor Version
   5.00[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
   "DisableTaskMgr"=dword:00000001
   ```

2. Save the file with a `.reg` extension.

   For example:

`DisableCtrlShiftEscape.reg`

3 In a different notepad, copy `REGEDIT /s \\servername\share\filename.reg`. Replace the `servername`, `share`, and `reg` file information appropriately.

4 Save the file with a `.bat` extension.

5 Double-click on the saved batch file and the registry key will be imported.

6 Verify the procedure by entering the key combination **Ctrl + Shift + Esc**.

Configuring RemoteApp Mode

The following sections explain how to configure application SSO using RemoteApp mode and how to view application SSO reports:

- Prerequisite
- Adding a Credential Vault
- Adding a Rule

Prerequisite

Ensure that you have completed all the steps mentioned in the section Configuring Application Single Sign-On in the Privileged Account Manager Installation Guide.

Adding a Credential Vault

You must add a credential vault for each and every application to which you want to enable SSO. To add an Application SSO resource to the vault, click **Credential Vault > Application > Application SSO** and click **+** next to **Resources** in the new administration console.

Adding a Rule

You must add a rule for every application to which PAM must perform SSO.

To add an application SSO rule:

1 Click **Command Control > Rules**.

2 Click **Add** in the last pane.

3 Specify a name for the rule and click **Add**.

4 To configure the rule, select the rule and click the edit icon in the last pane.

5 Make the following changes:

Session Capture: Set this option to **ON** to enable session capture.

Video Capture: Set this option to **ON** to enable video capture.

Authorize: Select **Yes** and select **Stop if authorized**.

Define what happens next by using the drop-down list as follows:

- **Blank:** The next rule in the hierarchy is checked.
- **Stop:** No more rules are checked for the command.
- **Return:** The next rule to be checked is up one level in the hierarchy from the current rule.
- **Stop if authorized:** If **Authorize** is set to **Yes**, no more rules are checked for the command.

- **Stop if unauthorized:** If **Authorize** is set to **No**, no more rules are checked for the command.

Application SSO: Select **Yes**.

If you are creating nested rules, ensure that you set the **Application SSO** to **Yes** in each and every rule in the nested hierarchy.

Application Details: Select the appropriate application SSO vault.

Application Credentials: Select the appropriate credentials to perform SSO.

Application Host: Specify the host and the port number that must be included during SSO. You must specify the host and port number in the format *<Host Name or IP Address>*:*<Port Number>*

This option appears only when you have selected **Use Host from Policy** when creating the application SSO credential vault.

Account Domain: Select the domain which you used when configuring the application SSO installation attributes.

Credentials: Select the domain credential created for SSO.

Run Host: Select **All Host** as PAM would perform load balancing when connecting to Remoteapp servers.

For more information about all the rule configuration fields, see "Modifying a Rule" on page 109.

6 Click **Modify**.

7 Click the command icon on the middle pane.

8 Drag the **Application SSO** command and drop it on the application SSO rule.

If you are creating nested rules, ensure that you drag the **Application SSO** command and drop it on the parent application SSO rule.

This rule is accessible by all the PAM users. If you want to restrict the application access to specific users, create a user group and drag and drop the user group to this rule. For more information about creating user groups, see "User Groups" on page 116.

Configuring Application SSO Agents for Load Balancing

In RemoteApp mode, PAM load balances the application SSO requests. For PAM to load balance the application SSO requests, you must configure the application SSO agents among which the application SSO requests must be distributed.

To configure agents for application SSO load balancing:

1 Click **Hosts > Application SSO > Remote App Servers.**

Displays all the agents with the `appsso` package.

2 Select the required agents for load balancing.

If you do not select the agent, all the agents that are listed are taken for load balancing application SSO requests.

3 Click **Finish**.

Viewing Reports

PAM audits all the activities performed in the application SSO session. Based on the rule configuration, the reports can show keystroke and video audits.

To view application SSO reports:

1. Click **Reporting > Command Control Reports.**
2. All report instances are displayed. You can interpret the SSO report columns as follows:

   User: PAM user who has logged into the user console.

   Host: Host where the user console is launched.

   RunAs: The user who logs into the application.

   RunHost: Host to which the application connects. If the application does not connect to any host, then asterisk (*) is displayed.

   Command: Application.
3. Double-click the appropriate report.
4. (Conditional) If you have configured video capture, select **Output** and click **Playback** to play the audit video.

For more information about reports, see Command Control Reports.

Direct Access Mode

In direct access mode, the application is installed on a remote server. The user performs an RDP connection to the remote server with the AD account, launches the application as a privileged user, and PAM performs SSO. For more information about direct access mode, see the section Direct Access Mode in the Privileged Account Manager Installation Guide.

The following sections explain the configurations required for application SSO using direct access mode and how to view application SSO reports:

- Configuring Direct Access Mode
- Viewing Reports

Configuring Direct Access Mode

- Prerequisite
- Adding a Credential Vault
- Adding Rules

Prerequisite

Ensure that you have completed all the steps in the section Configuring Application Single Sign-On in the Privileged Account Manager Installation Guide.

Adding a Credential Vault

You must add a credential vault for every application to which you want to allow SSO. To add an Application SSO resource to the vault, click **Credential Vault > Application > Application SSO** and click **+** next to **Resources** in the new administration console.

Adding Rules

You must add the following rules for application SSO using direct access mode:

- Adding a Direct RDP Rule
- Adding a Rule to Run Application as a Privileged User
- Adding an Application SSO Rule

Adding a Direct RDP Rule

This rule authorizes the RDP session to the application SSO agent.

To add a direct RDP rule:

1. Click **Command Control > Rules**.
2. Click **Add** in the last pane.
3. Specify a name for the rule and click **Add**.
4. To configure the rule, select the rule and click the edit icon in the last pane.
5. Make the following changes:

   Session Capture: Set this option to **ON** to enable session capture.

   Video Capture: Set this option to **ON** to enable video capture.

   Authorize: Select **Yes**.

   Define what happens next by using the drop-down list as follows:

   - **Blank:** The next rule in the hierarchy is checked.
   - **Stop:** No more rules are checked for the command.
   - **Return:** The next rule to be checked is up one level in the hierarchy from the current rule.
   - **Stop if authorized:** If **Authorize** is set to **Yes**, no more rules are checked for the command.
   - **Stop if unauthorized:** If **Authorize** is set to **No**, no more rules are checked for the command.

   Run User: Select **Submit User** to monitor actions of any user logging into the desktop.

   Run Host: Select **Submit Host** to monitor actions on any host that has a PAM agent.

   For information about other rule configuration fields, see "Modifying a Rule" on page 109.
6. Click **Modify**.
7. Click the command icon in the middle pane.
8. Drag the **Windows Direct Session** command and drop it on the direct RDP rule.

Adding a Rule to Run Application as a Privileged User

This rule enables privileged access to the application.

To add a rule to run application as privileged user:

1. Click **Command Control > Rules**.
2. Click **Add** in the last pane.
3. Specify a name for the rule and click **Add**.
4. To configure the rule, select the rule and click the edit icon in the last pane.
5. Make the following changes:

   Session Capture: Set this option to **ON** to enable session capture.

   Authorize: Select **Yes**.

   Define what happens next by using the drop-down list as follows:

   - **Blank:** The next rule in the hierarchy is checked.
   - **Stop:** No more rules are checked for the command.
   - **Return:** The next rule to be checked is up one level in the hierarchy from the current rule.
   - **Stop if authorized:** If **Authorize** is set to **Yes**, no more rules are checked for the command.
   - **Stop if unauthorized:** If **Authorize** is set to **No**, no more rules are checked for the command.

   Account Domain: Select the appropriate domain.

   Credentials: Select the domain credential created for SSO.

   Run User: Select the domain user created for SSO.

   Run Host: Select **Submit Host**.

   For information about other rule configuration fields, see "Modifying a Rule" on page 109.
6. Click **Modify**.
7. Click the command icon in the middle pane.
8. Click **Add** in the last pane and specify a name for the command. For example, pamrun.
9. Click **Add**.
10. Select the command that you created in step 8 in the middle pane and click the edit icon in the last pane.
11. Specify the path of all the applications that must be authorized using this rule.

    To improve security, you can provide the absolute path of the application. For example, `C:\Windows\System32\mstsc.exe`. If the absolute path of the application contains space, include the absolute path between quotes. For example, `"C:\Program Files (x86)\WinSCP\WinSCP.exe"`.
12. Click **Modify**.
13. Drag the newly created command and drop it on the run application as a privileged user rule.

Adding an Application SSO Rule

This rule authorizes application user and performs SSO. You must add this rule for every application to which you want to allow SSO. For example, if you want to allow SSO to WinSCP and Remote Desktop Connection, you must create two application SSO rules.

To add an application SSO rule:

1. Click **Command Control > Rules**.
2. Click **Add** in the last pane.
3. Specify a name for the rule and click **Add**.
4. To configure the rule, select the rule and click the edit icon in the last pane.
5. Make the following changes:

   Application SSO: Select **Yes** as this rule is used for application SSO.

   Session Capture: Set this option to **ON** to enable session capture.

   Video Capture: Set this option to **ON** to enable video capture.

   Authorize: Select **Yes**.

   Define what happens next by using the drop-down list as follows:

   - **Blank:** The next rule in the hierarchy is checked.
   - **Stop:** No more rules are checked for the command.
   - **Return:** The next rule to be checked is up one level in the hierarchy from the current rule.
   - **Stop if authorized:** If **Authorize** is set to **Yes**, no more rules are checked for the command.
   - **Stop if unauthorized:** If **Authorize** is set to **No**, no more rules are checked for the command.

   If you are creating nested rules, ensure that you set the **Application SSO** to **Yes** in each and every rule in the nested hierarchy.

   Application Details: Select the appropriate application SSO vault.

   Application Credentials: Select the appropriate credential that must be used to perform SSO.

   Application Host: Specify the host and the port number that must be included during SSO. You must specify the host and port number in the format *<Host Name or IP Address>*:*<Port Number>*

   This option appears only when you have selected **Use Host from Policy** when creating the application SSO credential vault.

   Run User: Select everyone.

   Run Host: Select **All Host**.

   For more information about the rule fields, see "Modifying a Rule" on page 109.
6. Click **Modify**.
7. Click the command icon on the middle pane.
8. Drag the **Application SSO** command and drop it on the application SSO rule.

   If you are creating nested rules, ensure that you drag the **Application SSO** command and drop it on the parent application SSO rule.

Viewing Reports

PAM audits all the activities performed in the application SSO session. Based on the rule configuration, the report can show keystroke and video audits.

PAM generates the following reports for every application SSO session using direct access mode:

- Report for launching Windows direct RDP session
- Report for launching the application as a privileged user
- Report for the operations performed in the application

To view activities performed in the application SSO session:

1. Click **Reporting > Command Control Reports.**
2. All the report instances are displayed. You can interpret the SSO reports columns as follows:

   User: User who has logged into the remote server.

   Host: Remote server where the application is launched.

   RunAs: Application user who has logged into the application.

   RunHost: Host to which the application is connected.

   Command: Application.
3. Double-click the appropriate report.
4. (Conditional) If you have configured video capture, click **Linked Session > Output > Playback** to view the keystrokes and play audit video.

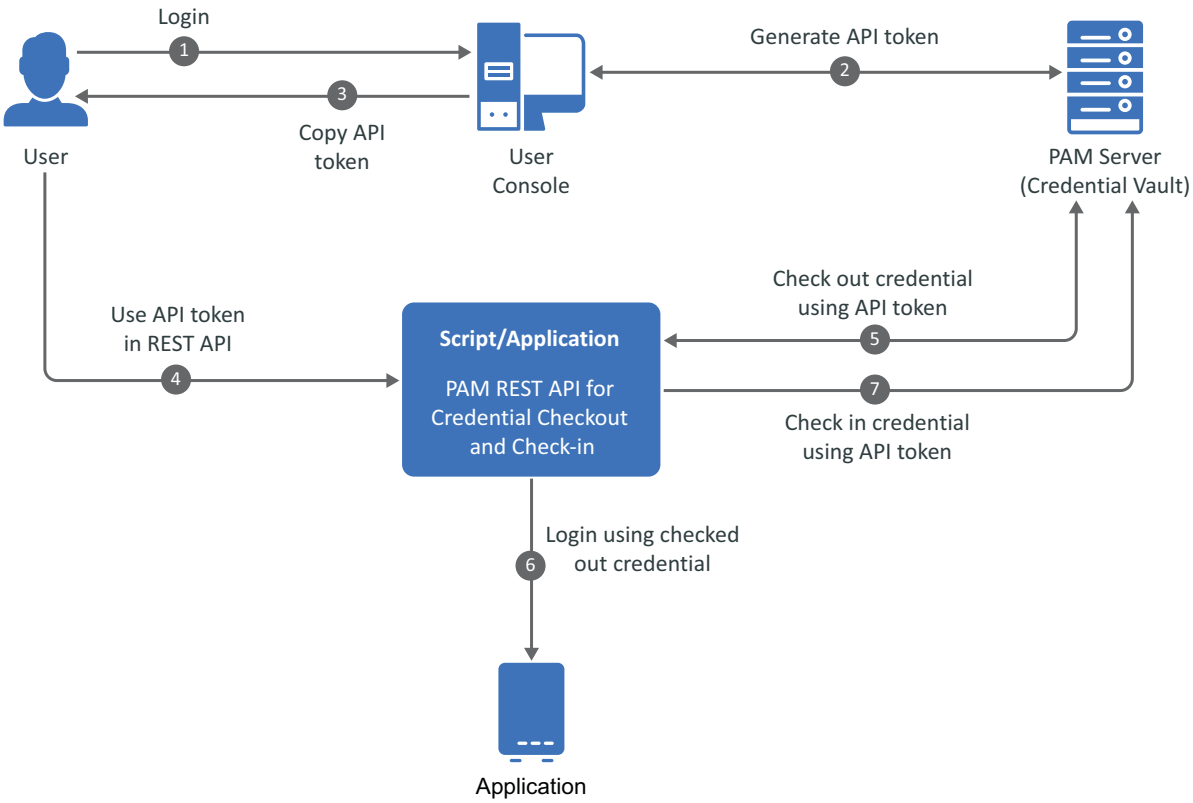
For more information about reports, see Command Control Reports.

19 Application to Application Password Management

Organizations depend on a large number of business applications, web services, and custom software to fulfill business communications and other transactions. These applications require access to other applications and database servers to get business-related information. This communication process is usually automated by including the application credentials in clear text in configuration files and scripts. It is difficult for the administrators to identify, change, and manage these credentials. As a result, the credentials are left unchanged, which might lead to unauthorized access to sensitive systems.

The Application to Application Password Management (AAPM) feature eliminates the need to store credentials in clear text in the application. Instead the application can query Privileged Account Manager for the credentials using REST API. In this way, the application credentials are secured, and you can achieve password rotation automatically by assigning strong and unique password without any manual intervention.

The following illustration explains the working of AAPM feature:



Configuring AAPM

By using API tokens in the REST API request, users can check out credentials of applications such as databases, LDAP, cloud services, and shared keys.

To enable a user to generate an API token:

1. Add PAM users to the appropriate user group. For more information, see "Enabling Users to Generate API Tokens" on page 278.
2. Create a resource for the required application, add credentials for check out, and add appropriate rules for application credential checkout.

   For more information about credential checkout configurations, see the following:

   - Database: "Database Access Through Credential Checkout" on page 228
   - Cloud services: "Enabling Credential Checkout for OpenStack" on page 246 and "Enabling Credential Checkout for Amazon Web Services" on page 246.
   - Applications: "Configuring Credential Checkout for Applications" on page 242.
   - Shared Keys: "Enabling the Key Checkout for Shared Key" on page 194

   For more information about how to add a credential, see Contextual Help.

   Using this feature a user can check out multiple credentials for the same application either by directly checking out the application credentials from the user console or checking out credentials using API tokens. As PAM allows multiple credentials checkout for an application, you must have adequate number of credentials in PAM for simultaneous access to the application.

Enabling Users to Generate API Tokens

You can allow PAM users to generate API tokens from the user console by adding them to the **API Users** group, which is created by default.

To allow LDAP users to generate API tokens, you must first add these users to the Framework User Manager and then continue with the following procedure. For more information about how to add LDAP users to PAM, see "LDAP Account Mapping" on page 65.

To add a user to API Users group:

1. Click **Framework User Manager > API Users**.
2. Click **Edit** in the **Group Information** task pane.
3. In the **Members** section, select the user whom you want to generate API tokens from the user console.

   You can also add a user to the group by dragging and dropping the user onto the **API Users** group.
4. To allow API tokens to skip secondary authentication, select **Bypass Secondary Authentication** in the **Secondary Authentication** section.

   For more information about the Framework User Group configuration, see "Modifying a Framework User Group" on page 70.

Viewing Activities Performed Using API Tokens

You can run a report that lists the activities performed using API tokens, such as credential check in and check out. You can identify the operation performed using the API token by using the value in the column **Password Check Out Token Details** and **Password Check In Token Details**.

1. Click **Reporting > Password Management**.
2. Select **Settings > Filter**.
3. Select the optional columns **Password Check Out Token Details** and **Password Check In Token Details**.
4. Select **Apply**.

For more information about PAM reports, see Managing Audit Reports.

20 Password Management

Using Privileged Account Manager, you can grant privileged access to PAM users either by elevating the user privilege or by providing privileged account credential for checkout. The resource and credential details that are required to provide privileged access are stored securely in the Credential Vault formerly known as Enterprise Credential Vault. The password of these credentials can be rotated periodically based on the compliance rule of the organization.

The credentials that are used to perform SSO by PAM are unknown to any administrator. Hence, these credentials must be rotated automatically by PAM to improve security. Similarly, the credentials used in service accounts are left unchanged, as it is tedious to detect all the service accounts, rotate their password and restart the services. Using password management feature of PAM, you can automate periodic rotation of service account password.

Understanding Password Management

Password Management feature allows you to change the password of credentials configured in PAM. To change the password, PAM uses scripts associated with the vault or the resource. PAM by default provides out-of-the-box scripts to change password of few resources. In addition, PAM provides capability to define custom password change scripts.

For some of the resources, in addition to privileged account password change, you can also change the password in the associated services or service accounts. This password change task can be scheduled for execution automatically at periodic intervals. In addition, you can also configure execution of an automated task (service task), after password change is complete. For example, if you want to perform backup after changing the password, it can be defined as a service task.

The following table helps you understand the password management capabilities provided by PAM based on the type of resource:

Resource	Password Management	Schedule Password Change	Change Password in Associated Services	Custom Task Execution after Password change
Windows	Yes	Yes	Yes	Yes
UNIX, Linux and Network Device				
Linux and Network Devices using SSH connection	Yes	Yes	No	Yes
Telnet (Linux and Network Devices using Telnet connection)	No	No	No	No
UNIX	No	No	No	No
LDAP				

Resource	Password Management	Schedule Password Change	Change Password in Associated Services	Custom Task Execution after Password change
Windows Active Directory	Yes	Yes	Yes	Yes
NetIQ eDirectory	No	No	No	No
OpenLDAP	No	No	No	No
Database	Yes	No You can only enable the password to be changed immediately after credential check-in.	No	No
Application				
Application Credential Checkout	Yes	No You can only enable the password to be changed immediately after credential check-in.	No	No
Application SSO	No	No	No	No
Key	No These are static keys that cannot be rotated.	No	No	No

Password Management for Windows, Active Directory, Linux, and Network Devices

For changing these resource passwords, PAM uses tasks. Tasks contains the script that must be executed for password change and the scheduling option required to execute the script. The tasks are associated to a vault. For more information about vaults, see Contextual Help. By default, every vault will have a password change task associated with it. This task is executed for the credentials in the vault which has the **Password Change** option set to **Yes**.

In addition, if you want to perform any automated task after password change, it can be added as a service task. For example, if you want to perform backup after changing the account password, it can be defined as a service task. These service tasks are custom tasks for which you need to create a custom script and add it in the task. For more information about the template for creating a custom script, contact Customer Support.

- **For Windows and Active Directory:**

  PAM provides out-of-the-box scripts to change password of Windows local machine and Active Directory.

  In addition to windows account password change, PAM also provides the capability to change the password of service accounts. PAM provides out-of-the-box scripts to change password of service accounts, such as such as Windows Services, COM+, Task Scheduler, and IIS Pool. For other service accounts, you can define a custom script for password change and associate it to a service task.

  These service account tasks are executed only for those credential which have the appropriate service account associated with it. This association can be defined when adding a credential. When you are adding a credential for active directory, PAM provides a capability for you to define the machines where the credential is used for service accounts. This will help in end to end password change of the Active Directory accounts.

- **For Linux and Network Devices:**

  PAM provides out-of-the-box script to change password of Linux and Network devices that can be connected using SSH protocol. PAM can rotate both the password or the SSH key that is configured for a credential.

  If you want to change password of associated service accounts, you can define a custom script for service account password change and associate it to a service task.

For more information about configuring tasks and scripts, see Contextual Help.

The following section explains in detail the prerequisite for configuring Password Management and also the checklist for configuring Password Management in an upgraded environment of PAM.

- Prerequisites
- Configuring Password Management
- Configuring Password Management in an Upgraded Setup
- Disabling Password Management

Prerequisites

- Ensure that the Task Manager module is installed.
  - The task manager component of PAM (`taskmanager`) is supported only on Windows, SLES 12 (64-bit), SLES 15 (64-bit), RHEL 7.5 (64-bit), or RHEL 8(64-bit).

    NOTE: ◆For **RHEL 8** (64-bit) and **RHEL 7** (64 bit), install the `redhat-lsb-core` package.
    - For **RHEL 8** (64-bit) and **SLES 15** (64-bit), install the `lsb-release` package.
  - If you want to configure task manager on a separate agent, you must first install Privileged Credential Manager package (`prvcrdvlt`) and Access Manager package (`auth`), and then install Task Manager (`taskmanager`) module in the agent.
  - If you have multiple host domains in PAM, you must have Task Manager module installed on every host domain.

    For more information about installing a package in PAM, see Installing Packages on a Host.
  - If you have configured a Windows machine as task manager, ensure the following:
    - Powershell 4.0 or later must be installed in the Windows machine where you are installing the Task Manager module.
    - Windows Remote Management (WinRM) service must be running on the Windows machine. To start winrm service, use the command:

      ```
      Enable-PSRemoting –force
      ```
    - Add target machine, where the password must be changed, to the WinRM trusted host. To add all servers as trusted host, use the command:

      ```
      winrm set winrm/config/client '@{TrustedHosts="*"}'
      ```
    - Set the PowerShell execution policy to `Remotesigned` using the command:

      ```
      Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
      ```
- Ensure the following is done on the target machine where the password must be changed.
  - **In Windows machine:**
    - Powershell 2.0 or later must be installed in all the windows target machines as PAM uses PowerShell scripts to change password.
    - Windows Remote Management (WinRM) service must be running on the Windows machine. To start WinRM service, use the command:

      ```
      Enable-PSRemoting –force
      ```
    - IP address of the task manager must be added to the trusted host of the target machine. To add trusted host, use the command:

      ```
      winrm set winrm/config/client '@{TrustedHosts="x.x.x.x"}'
      ```
  - **In AIX machine, configure the following**:
    - Specify `AcceptEnv LC_ALL` in the `sshd_config` file.
    - Restart `sshd` service.

Configuring Password Management

To configure PAM to change (rotate) password of any resource, you must set the **Password Change** option value in the resource configuration to **Yes** and ensure that all the password change tasks are enabled. If the password change option is set to yes in a resource, this configuration will be inherited by all credentials in that resource. However, you can override them in the credential configuration. To modify the password management option of a resource, click **Credential Vault** > *Vault Type* > *Vault Name* > edit icon next to the required resource.

Configuring Password Management in an Upgraded Setup

After upgrading PAM, if you want to enable password management, perform the following:

	Tasks	Go To
❑	1. Review the prerequisites and ensure all the required configurations are complete.	Prerequisites
❑	2. Review all password change and service tasks associated with the vault and update when the task must be scheduled for execution.	**Credential Vault** > ***Vault Type*** > ***Vault Name*** > **Associated Task** > **click edit icon next to the task**
❑	3. (Conditional) By default, the out-of-the-box password policy provided by PAM is associated with every vault. You can choose to use the default policy or create a new policy and associate with the vault.	**Credential Vault** > **Password Policies** > **Help icon**
❑	4. Perform the following on all the resources:	
	1. Edit the resource and set the **Password Change** option as **Yes**. Also, review and modify all password management options, such as reconcile account and so on. These password management values will be inherited by all credentials in the resource.	**Credential Vault** > ***Vault Type*** > ***Vault Name*** > **click edit icon of the required resource**
	2. (Conditional) If you do not want PAM to change reconcile account password, set **Password Change** option as **No** in the appropriate resource credential. We recommended you to set **Password Change** to **No** for reconcile account. Also, you must have one local administration account, which is not managed by PAM to resolve any password change issue.	**Credential Vault** > ***Vault Type*** > ***Vault Name*** > ***Resource Name*** > **click edit icon of the required credential**
	3. (Conditional) For Windows, if the credential is used as a service account, you must edit the credential and modify the service association.	
	4. (Conditional) For Active Directory, if the credential is used as a service account in any of the Windows machine, you must add the Windows machine to the credential and update the service association.	

Disabling Password Management

You can disable password management at task level or resource level.

- At resource level, you can disable password rotation (change) of all credentials or a specific credential in a resource.

  To disable password management of all accounts in a resource, edit the resource configuration and set the **Password Change** to **No**. Similarly, to disable password management for a credential, edit the credential configuration and set the **Password Change** to **No**.

- At task level, you can disable the password change task of any vault to stop execution of the task.

  Before you disable any task, review and resolve all the errors related to the task in the failed reports page. As the reports relates to failed reports are not displayed when the task is disabled.

Password Management for Database and Applications

PAM provides capability to change password of the database and application credentials after every check in. You can configure to either allow PAM to perform the password change or delegate this task to the Identity Manager. If you want PAM to perform password change after every check in, you must add the password change script as part of the resource configuration.

These password change scripts are imported automatically when you use a policy template to configure a resource. For information about policy template, see Policy Templates. If you have added the resource manually, you can copy the out-of-the-box password change scripts from Password Reset Scripts.

For more information about configuring password management for database and application, see Contextual Help. To see the contextual help, click **Credential Vault > Application or Database >** ***Vault Name*** **>** Help icon.

21 Integration with Ticketing Systems

Privileged Account Manager provides capability to integrate with the ticketing tool, ServiceNow. This allows you to create privileged access request for Linux Machines through ServiceNow instead of using Emergency Access Request of PAM. In addition, PAM allows the user to create a ServiceNow access request directly from the SSH terminal. The user can request for either normal or elevated access directly from the SSH terminal. These session details are captured in the ServiceNow incident for auditing. In addition, the complete session is monitored and commands that are executed in the session are logged in PAM.

The following sections explain the configuration that must be done to provide access to the user using ServiceNow incident:

- Configuration for Normal Access
- Configuration for Elevated Access

Configuration for Normal Access

To provide normal access to a Linux machine through ServiceNow request, configure the following:

1. Click **Command Control > Rules > Add Policy Template** and import the following Policy Templates:
   - **ServiceNow Request Access:** This is used to provide elevated access.
   - **ServiceNow Update Incident:** This is used to allow user to add comments to the ServiceNow incident.
   - **ServiceNow Close Incident:** This is used to resolve the ServiceNow incident.

   For more information about using the policy template, see Adding a Policy Template.
2. Edit the ServiceNow application configuration in the new Administration Console:
   - **2a** Click **Vault > Application > Applications**.
   - **2b** Select the edit icon next to the newly added resource **ServiceNow_Credentials**.
   - **2c** Specify the **HostName** and **Port** of ServiceNow.
   - **2d** Click edit icon next to the appropriate credentials.
   - **2e** Specify the **User Name** and **Password** of ServiceNow
3. Edit ServiceNow rules, RL-SERVICENOW-PRIV-ACCESS, RL-SERVICENOW-UPDATE, and RL-SERVICENOW-CLOSE as follows:
   - **3a** Click **Rules** and select the required rule.
   - **3b** Click **Script Arguments** in the last pane and modify the following:

     Account: This is the credential that is used to access ServiceNow. This value must be the user name mentioned in Step 2e.

     Vault: The resource which contains the ServiceNow connection details such as, IP address, and port number. This must be the name of the resource configured in Step 2b.

Strict_Check: If this option is set to false, any user is granted access and the session is monitored by PAM.

If you set this to true, the access to the machine is granted only when the following conditions are satisfied:

- The user must be configured in ServiceNow.
- The ServiceNow incident must be assigned to the user who has created the request.
- The machine to which the access is provided must be configured in ServiceNow.
- The ServiceNow incident must be in the active state.

3c Click **Finish**.

3d Deselect **Disable** to enable the rule and click **Apply**.

Configuration for Elevated Access

Prerequisites:

- The user to whom you are providing access should be configured in ServiceNow.
- The machine to which you are granting access must be configured in ServiceNow.
- The user can get access to the machine only when the ServiceNow incident is in the active state.

To provide elevated access to a Linux machine through ServiceNow incident, configure the following:

1. Click **Command Control > Rules > Add Policy Template** and import the following policy templates:
   - **ServiceNow Request Elevated Access:** This is used to provide elevated access.
   - **ServiceNow Update Incident:** This is used to allow user to add comments to the ServiceNow incident.
   - **ServiceNow Close Incident:** This is used to resolve the ServiceNow incident.

   For more information about using the policy template, see Adding a Policy Template.
2. Edit the ServiceNow application configuration in the new Administration Console:

   2a Click **Vault > Application > Applications**.

   2b Select the edit icon next to the newly added resource **ServiceNow_Credentials**.

   2c Specify the **HostName** and **Port** of ServiceNow.

   2d Click edit icon next to the appropriate credentials.

   2e Specify the **User Name** and **Password** of ServiceNow.
3. Edit the ServiceNow rules, RL-SERVICENOW-PRIV-ACCESS, RL-SERVICENOW-UPDATE, and RL-SERVICENOW-CLOSE as follows:

   3a Click **Rules** and select the required rule.

   3b Click **Script Arguments** in the last pane and modify the following:

   Account: This is the credential that is used to access ServiceNow. This must be same as the user name mentioned in Step 2e.

   Vault: The resource which contains the ServiceNow connection details such as, IP address, and port number. This must be the name of the resource configured in Step 2b.

Users: Linux users as whom the user can be elevated. You can enter multiple values separated by space. For example, User1 User2 User3.

3c Click **Finish**.

3d Deselect **Disable** to enable the rule and click **Apply**.

22 Managing Emergency Access Requests

When a user requires access to privileged session, database server, or to any application server but do not have rules defined, then they can request for an emergency access. The Emergency Access feature helps the users to get access to any privileged session or application for a specific duration by creating an emergency access request. An administrator of Privileged Account Manager can create rules for a user for permanent access but for emergency access the administrator need not create any rule.

A user requests for access and administrator approves or denies the request. Administrator monitors all the requests and can revoke the approved request if there is any malicious activity detected. Privileged Account Manager audits all the activities done by the user.

Configuring Emergency Access Settings

To configure emergency access settings, perform the following:

1. On the home page of the console click **Access Dashboard**.
2. Click the **Configuration** tab.
3. Configure the following settings:

   Delete Request After: Select the number of days after which the request gets deleted. The requests that are in the expired, revoked or denied state are deleted. All the approved but not expired, and the pending requests are not deleted.

   Allow Grace Period of: Select the extra time period that a user is allowed, after the approved time period expires. User is notified about the expiry time so, grace period gives some time to the user to check in the password or end the session. For example, if an administrator has approved a request for an hour and configures this setting for 15 minutes, then the user can access the session or application for 1 hour 15 minutes.

   Disconnect after grace period: Select this check box if you want to disconnect the connection after the grace period expires.

   Server Email Id: Enter the email address that is defined for the Privileged Account Manager server. This is the email id from which emails are sent to the users with the status of the request.

   Admin Email Id: Enter the email address of the administrator. This is the email address to which an email is sent when a user requests for emergency access.

23 Deployment Dashboard

Deployment Dashboard helps the administrators to view the geographical deployment of the Privileged Account Manager Hosts and also identify the host on which a risky activity was performed.

NOTE: You can view the hosts in the **Deployment Dashboard**, only if the **Map Coordinate** details are provided in the respective domain configuration.

You can perform the following tasks using the Deployment Dashboard:

- View the deployment of the hosts geographically.
- Locate the host on which a risky activity was performed.
- Zoom in and zoom out on the dashboard to inspect the hosts in a specific region.
- Customize the dashboard to display specific region of the map.
- Set automatic page refresh through dashboard settings.

Deployment Dashboard consists of the following:

- "Deployment View" on page 293
- "Live Risk View" on page 294

Deployment View

In the Deployment Dashboard, the hosts are represented as nodes and tagged to a location based on the coordinates details provided in the respective domain configuration.You can mouse over on the host and view the complete details of the host.

To go to the Deployment view, click **Hosts > Deployment Dashboard > Deployment**.

In the Deployment view,

- You can filter the hosts that are displayed based on the packages available in the hosts. For example, you can use this filter option to display only the Privileged Account Manager agents or Framework Managers and so on.
- You can view a specific region of the map by clicking the **Change Map Region** icon and selecting the appropriate area.

To filter the hosts based on packages installed, perform the following:

1. Click **Deployment > Manage Modules**.
2. Select the required packages in the Manage Modules dialog box.

   For example, If you want to view all the Privileged Account Manager agents, click **Show Agents** and the Deployment view displays only the agent machines.

3 Click **Apply**.

The Deployment view displays the hosts based on the packages selected.

Live Risk View

Live Risk view displays the hosts on which any malicious or risky activity was performed based on the configurations in the Compliance Auditor.

To view the hosts on which a malicious activity was performed, you must create corresponding audit rules in the Compliance Auditor. For more details about how to create a compliance audit rule, see "Adding or Modifying an Audit Rule" on page 157

You can click on the host that is displayed in the Live Risk view to view the complete audit details. When you click on the host in Live Risk view, it displays the corresponding Compliance Audit records, which can be used for further analysis of the malicious activity.

Customize Deployment Dashboard

You can customize the view of the deployment dashboard and the refresh interval by modifying the dashboard settings.

To customize the Deployment Dashboard, perform the following:

1 Click **Hosts > Deployment Dashboard**.

2 Click the Settings icon in the upper right corner and make the required changes in the following fields:

- **Deployment View:** Select the appropriate refresh option for the Deployment View.

  Select Manual Refresh to refresh the Deployment view manually and set the appropriate refresh interval to refresh the Deployment view automatically.

- **Live Risk:** Select the appropriate refresh option for Live Risk view.

  Select Manual Refresh to refresh the Live Risk view manually and set the appropriate refresh interval to refresh the Live Risk view automatically.

3 Click **Apply**.

The Deployment Dashboard reflects the changes according to the settings.

24 Integrating Privileged Account Manager with Advanced Authentication

With the increasing number of security vulnerabilities and compromised identities, it becomes difficult to ensure security and control over all privileged credential access, and activity. To overcome this issue, you can use two-factor or multi-factor authentication. Privileged Account Manager integrates with the Advanced Authentication application to secure and control the access to privileged endpoints by using the multi-factor authentication methods.

Privileged Account Manager facilitates in providing advanced authentication features to access the following:

- Privileged Account Manager end-points (systems, applications, databases, keys).
- Administration Console.
- Privileged credential to connect to a server (credential checkout and shared key checkout)

For information about Advanced Authentication, refer the Advanced Authentication documentation web page.

- "Benefits of Integration with Advanced Authentication" on page 295
- "Advanced Authentication Terminologies and Their Usage" on page 296
- "Checklist to Follow Before Enabling Secondary Authentication" on page 297
- "Configuring Advanced Authentication Server" on page 298
- "Supported Authentication Methods" on page 299
- "Configuring the Advanced Authentication Server Details in Privileged Account Manager" on page 299
- "Enabling Advanced Authentication for Privileged Access" on page 300
- "Troubleshooting" on page 302

Benefits of Integration with Advanced Authentication

Privileged Account Manager can integrate with Advanced Authentication application to provide the following benefits:

- **Advanced data security:** Privileged Account Manager uses some of the Advanced Authentication methods to secure user privileged access. It prompts users for another authentication before providing privileged access to them. Hence, even when users log in with their primary password they are prompted for second-factor authentication password to get privileged access.

- **Multi-domain support:** Privileged Account Manager uses Advanced Authentication server to authenticate users from different domains. You can define rules/ policies to control access of users from different domains.

  With the integration of Advanced Authentication application, Privileged Account Manager can authenticate users on various domains including the default domain. You need not import users from various domains to Privileged Account Manager.

Advanced Authentication Terminologies and Their Usage

In this chapter we have used some terminologies which are specific to Advanced Authentication. This section helps in providing brief information on the terminologies. For detailed information about Advanced Authentication, you can refer the Advanced Authentication server guide from the Advanced Authentication documentation page.

The following table describes the Advanced Authentication terminologies that are used in this chapter:

Term	Usage in Advanced Authentication	Usage in Privileged Account Manager
Repository	Used for storing user information. This information can be retrieved from any LDAP directory such as eDirectory, and Active Directory.	You must create Advanced Authentication repositories for each domain that is used in Privileged Account Manager. If there is an account created in Privileged Account Manager's **Credential Vault**, the repository name must be the same as the domain name mentioned in the **Credential Vault**. **NOTE:** If you require secondary authentication imposed for local users of Privileged Account Manager, add those local users to the **Local** repository of Advanced Authentication server before configuring secondary authentication details.
Methods	Used for defining the type of authentication.It displays the list of available methods for authentication. You can modify the setting for each method as per your requirement.	Only the supported methods can be used for secondary authentication. For a list of supported methods in Privileged Account Manager, refer "Supported Authentication Methods" on page 299

Term	Usage in Advanced Authentication	Usage in Privileged Account Manager
Chain	Used for defining the combination of authentication methods. The users must authenticate themselves with all the authentication methods that are specified in a chain. For example, if you create a chain which is a combination of Email OTP and SMS, the user is prompted to enter the One-Time Password that is sent to his registered email address. If the OTP is correct, the system sends SMS with a One-Time-Password to the registered mobile number.	The chains must be a combination of only the supported methods. For the list of supported methods refer, "Supported Authentication Methods" on page 299. If there is a combination of supported and unsupported methods, the user authentication is unsuccessful.
Endpoint	Used for identifying a device or server that contains a database.	Privileged Account Manager uses a single endpoint for primary and backup servers. **NOTE:** Privileged Account Manager facilitates adding the endpoint to the Advanced Authentication server. This endpoint must be available to create an event. For information about adding an endpoint, refer "Configuring Advanced Authentication Server" on page 298.
Event	Used for configuring the chains and user categories that can be used for any endpoint.	There should be a separate event for Privileged Account Manager. Only the chains that have a combination of supported methods must be added to this event. You must add the endpoint that you create through Privileged Account Manager to the Endpoint whitelist of Advanced Authentication server.

Checklist to Follow Before Enabling Secondary Authentication

- ❒ To integrate Advanced Authentication, you must install NetIQ Advanced Authentication 5.2 or later on a separate server.
- ❒ The Advanced Authentication Server must be active and available.
- ❒ The users who are added locally to the Framework User Manager must be added to the **Local** repository of Advanced Authentication server.
- ❒ To use Advanced Authentication application you must perform the following in the same order:
  1. In Advanced Authentication server, create required number of repositories for local and LDAP users.

     These repositories should be the domains used in Privileged Account Manager.
  2. Modify the supported methods as per requirement.

3. Create chains. Ensure that the chain includes only the supported methods and the default chains are not deleted.
4. Create an event.
5. In Privileged Account Manager specify the Advanced Authentication server details to register Privileged Account Manager server.

   This creates new endpoint in Advanced Authentication server.
6. In Advanced Authentication server, select the Privileged Account Manager endpoint in **Events**.

❒ All Privileged Account Manager users and Administrators must access the Advanced Authentication URL and enroll the methods before using Privileged Account Manager.

Only the methods that are enrolled will be available for secondary authentication.

Configuring Advanced Authentication Server

You must configure the Advanced Authentication server to make the secondary authentication features available for Privileged Account Manager.

To configure the Advanced Authentication server for Privileged Account Manager, perform the following:

1 Add required number of repositories in Advanced Authentication server.

You must create a repository for the Local Framework users and add the same usernames as it is specified in Framework User Manager.

The repository name must match the domain name that you specify in **Credential Vault** of Privileged Account Manager.

2 In Advanced Authentication server click **Method** and configure the required methods that are supported in Privileged Account Manager.

Only the supported methods in Privileged Account Manager must be configured and used.

3 In Advanced Authentication server, click **Chains** to create the chains that includes those methods that are supported in Privileged Account Manager. For the list of supported authentication methods, refer "Supported Authentication Methods" on page 299.

NOTE: ◆Ensure that you do not delete the default chains from the list of chains.

- Ensure that you configure the **Chain** with LDAP Password method.

---

4 In Advanced Authentication server, click **Event** to create a custom event for Privileged Account Manager.

Include the required chains from the **Available** to the **Used** list.

5 In the Privileged Account Manager server, create an endpoint through Privileged Account Manager.

The endpoint gets created from Privileged Account Manager server. For information about creating endpoint through Privileged Account Manager refer "Configuring the Advanced Authentication Server Details in Privileged Account Manager" on page 299

6 In Advanced Authentication server, edit the event for Privileged Account Manager and add the same endpoint in **Endpoints whitelist**.

Supported Authentication Methods

- Email OTP
- SMS
- Smartphone
- TOTP
- HOTP
- Voice
- Fingerprint
- Smart card
- RFID card
- RADIUS

For details about these methods, see the *Advanced Authentication server guide* on the Advanced Authentication documentation page.

Configuring the Advanced Authentication Server Details in Privileged Account Manager

You must specify the details of the Advanced Authentication server in Privileged Account Manager to use the supported advanced authentication methods.

To configure the Advanced Authentication server details, perform the following:

1. On the Home page of the Administration Console, click **Framework User Manager**.
2. Select **Options**, and then click **Advanced Authentication Configuration**.
3. In the right pane, specify the Advanced Authentication configuration details:
   - **Advanced Authentication Host**: Specify the IP address or the DNS name of the Advanced Authentication Server.
   - **Name**: Specify a unique endpoint name.

     This endpoint gets created in Advanced Authentication server with the same name that is specified in this field.

     If you require to delete the endpoint, you must delete it from the Advanced Authentication server.
   - **Description**: Specify the description for the endpoint.
   - **Default Domain**: Specify any one of the Advanced Authentication repository names that must be used as the default domain to authenticate the user in that domain.

     When a user does not provide the domain name during login and if that user is not a local user in Privileged Account Manager, then this default domain is used for authenticating the user in Advanced Authentication server.

     NOTE: You must specify only the name that is existing as repository on the Advanced Authentication server.

- **Event**: Specify the same event name that is mentioned in the Advanced Authentication server for Privileged Account Manager.
- **Primary Login Method**: Specify one of the following primary login methods:
  - **RADIUS**: Use RADIUS option only if Advanced Authentication server forwards the authentication request to a third-party RADIUS server.

    NOTE: If you select RADIUS, do not enable the **Secondary Authentication Required** option under **Account Settings**.

  - **LDAP Password**: This is the default option selected. Use this option for all other certified Advanced Authentication methods.

Enabling Advanced Authentication for Privileged Access

Before enabling secondary authentication, you must ensure that you have performed all the configuration steps in the same order as mentioned in "Checklist to Follow Before Enabling Secondary Authentication" on page 297. If Advanced authentication server is not configured, there will be issues when users try to login or try to get privileged access for an endpoint.

You can enable advanced authentication feature for authenticating users who access the following:

- Administration console
- Host servers such as Windows, SSH.
- Applications or database by retrieving Passwords or shared keys from the user console

Bypassing Secondary Authentication

You can allow a framework user group or all privileged users to have privileged access without prompting for secondary authentication. To allow this access, Privileged Account Manager provides the Bypass Secondary Authentication option.

This option is helpful for framework users in the following scenario:

In case of some emergency, Privileged Account Manager administrators can log in to Privileged Account Manager Administration console without being asked for secondary authentication. This can happen only if the administrator is in a user group that has the option enabled. To enable this option for a user group refer, "Enabling Advanced Authentication for Administration Console" on page 301. The users who may require to be a part of the same group are:

- Identity Manager users using the driver for Privileged Account Manager
- Any other users who perform Privileged Account Manager administrative activities through automation.

This option is also available as a global setting where you can bypass secondary authentication on the parent rule. This is helpful so that in case of emergency such as when Advanced Authentication server is down, you can enforce bypassing secondary authentication for all the rules. To enforce this global rule perform the following procedure:

1. On the home page of the administration console, click **Command Control**.
2. In the command control pane, click **Command Control**.

3 In the details pane, click **Secondary Authentication Setting**.

4 On the **Bypass Secondary Authentication for all Policies** option, Click **Yes**.

By default this option is set to **No**.

Enabling Advanced Authentication for Administration Console

You can enable Advanced Authentication for the Administration Console to allow access only to the users who pass the secondary authentication.

To enable Advanced Authentication for Administration console, Privileged Account Manager administrator must perform the following:

1 On the home page of the Administration Console, click **Framework User Manager**.

2 In the left pane, click **Account Settings**.

3 In the right pane, click **Secondary Authentication Required**.

This setting ensures that the Framework users are prompted for secondary authentication to log in to the Administration Console.

4 Add a separate user group that has the **Bypass Secondary Authentication** option selected.

NOTE: You must create this user group so that when there is some problem with Advanced Authentication server, the users in this group must be able to login to Privileged Account Manager without being prompted for secondary authentication.

---

5 Add the primary administrator to that group.

This allows the users in that group to access Privileged Account Manager without prompting for secondary authentication. For more information about selecting the **Bypass Secondary Authentication** option refer "Modifying a Framework User Group" on page 70.

Enabling Advanced Authentication for Privileged Access to End-Points

You can enable advanced authentication for all endpoints by adding a parent rule at the beginning of the rule's tree and selecting the **Secondary Authentication** check box. Also, you can enable secondary authentication for any required rule, for example, you may choose to enable secondary authentication only when particular group of users are accessing certain servers. In this scenario, you can create a rule accordingly and enable secondary authentication only for that rule. For more information about rules, refer "Adding a Rule" on page 108.

The advanced authentication can be enabled only for the rules that include the following:

- Secure Shell Relay
- Secure Shell session initiation through the user console.
- Remote Desktop Relay
- Privileged Account Manager Credential Provider for Windows
- Password check out through user console
- Shared key check out through user console

NOTE: Secure Shell Relay and Privileged Account Manager Credential Provider rules does not support the advanced authentication methods smart card, fingerprint, and RFID card.

Privileged Account Manager does not support secondary authentication for command-based privileged access such as, pcksh, usrun, and for **Run as Privileged User**, You must not enable secondary authentication for these rules.

To enable advanced authentication on a rule for privileged access to the end-points, you must modify the required rule by selecting **Yes** for the **Secondary Authentication** option. For more information about modifying a rule, refer "Modifying a Rule" on page 109.

Troubleshooting

This section includes the probable issue that may arise when you integrate Advanced Authentication with Privileged Account Manager.

Advanced Authentication Server is Down and Users Cannot Log In to Privileged Account Manager End-Points

In a scenario where the Advanced Authentication server is down or not reachable, users cannot pass the secondary authentication. Hence, they cannot access the end-points that have secondary authentication enabled in the rule.

To overcome this issue, the primary administrator can enable the **Bypass Secondary Authentication for all Policies** option. For more information refer, "Bypassing Secondary Authentication" on page 300.

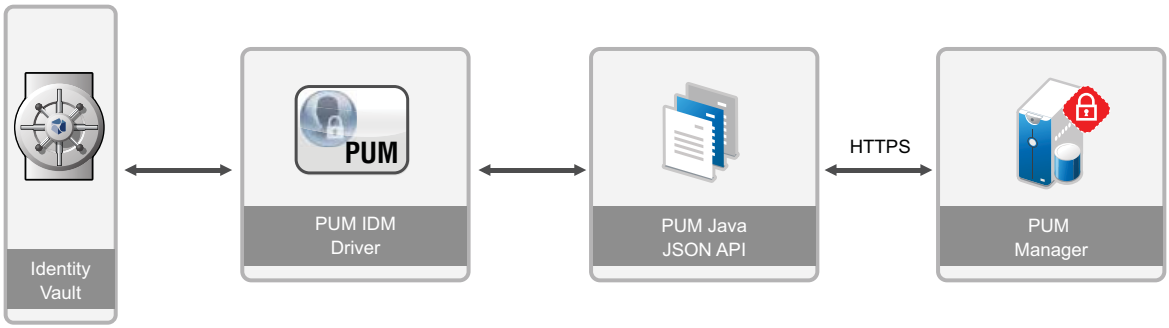
25 Integrating Privileged Account Manager with Identity Manager

Privileged Account Manager can communicate with Identity Manager () by using the Identity Manager driver for Privileged Account Manager. An Identity Manager driver is an interface between the NetIQ Identity Manager and the connected application. Here, the connected application is PAM. For more information about Identity Manager, see Identity Manager documentation page.

The PAM driver is a Java program running in Identity Manager. This driver communicates with the PAM application using Java JSON API library provided by PAM. This communication happens over HTTPS channel.

To view the high level architecture diagram of how PAM is integrated with the Identity Manager, see Figure 25-1 on page 303. For more information about the driver, see NetIQ Identity Manager® Driver for NetIQ Privileged Account Manager Implementation Guide.

Figure 25-1 *Integrating PAM with Identity manager*



From PAM 3.0.1 onwards, the PAM driver creates a channel from Identity Manager to PAM to synchronize the password that is changed through the password check-in process. The PAM driver checks for any changes performed on the PAM credential object. When a user checks-in the password, the driver generates a random password through Identity Manager and the same password gets reset on the application/ database through the driver for the respective application/ database.

Benefits of Integration with Identity Manager

The integration with Identity Manager helps us with the following:

- **Ease for access request through Entitlements:** An Entitlement defines a permission or an access that a user can have on an application. An end user requests for an Entitlement by using the web based user portal called NetIQ RBPM or UserApp. Also, the UserApp has Workflow capability that takes the request through an approval process before granting access to the user.

For PAM, the UserGroup objects are made available as Entitlements in Identity manager through the Driver. The UserGroup object is used in the PAM policy for authorizing privileged access to a server or an application. A user could login to UserApp and request for a PAM Entitlement. When the request is approved, the user gets the privileged access through the UserGroup membership. Hence, the privileged access request becomes automated through UserApp.

- **Managing multiple PAM Account Domains:** The driver for PAM can synchronize PAM's Credential Vault objects from Identity Manager to PAM. So, the resource and the respective credential object creation and management can be easily done as Identity Manager (eDirectory) objects.
- **Delegation of Password Checkin to Identity Manager:** PAM allows emergency access and credential checkout/check in to any applications. During the password check in process, PAM generates a random password and the script that is set on the resource takes care of resetting the new password on the target application. PAM supports credential checkout for few applications. For every additional application, a perl script needs to be written and set on the corresponding resource object. For more information about credential checkout/ check in process, see Chapter 17, "Privileged Access to Applications and Cloud Services," on page 241.

  In a corporate environment where Identity Manager is already used for centralized password policy definitions, management of identities and their passwords on various applications, performs the same function as the password check in process. Hence, the password check in process can be delegated to Identity Manager. The driver for PAM and Identity Manager takes care of random password generation, password policy definition for the applications, syncing the new password to the end application and finally checking in the password to PAM. Also with Identity Manager integration, the number of applications that PAM supports for credential checkout will be as many as that Identity Manager supports, which is very large. For more information about other drivers for Identity Manager, see Drivers for Identity Manager documentation page.

  For auditing the password check in event details, the PAM audit report can be used and these events can also be logged in the SIEM system like Sentinel. For more details refer to Chapter 7, "Managing Audit Reports," on page 83.

26 Virtualization Implementation

You can access the target desktop using the Citrix Virtual Desktop Infrastructure (Citrix VDI). Privileged Account Manager supports PAM agent on target desktop and PAM manager on the Cirtix VDI server.

The users can have remote access to the hosted desktop machines within an organization by using a Virtual Desktop Infrastructure (VDI) environment. You can also monitor the user sessions and define roles for different users by using Citrix VDI environment and installing Privileged Account Manager agent on the target desktop.

You can create rules on PAM Manager for different users for their access and roles. When a user logs in to the target desktop using Citrix VDI server, the defined rules are used for his access and monitoring of the session. The following two different methods demonstrates to access the target desktop:

Using Citrix's Access Control

1. Install Privileged Account Manager agent on the target desktop.
2. Install PAM manager on the Citrix VDI server or any other machine. Register the PAM agent to the installed PAM manager.
3. Install the Citrix Receiver on the user's machine to access the target desktop.
4. Configure the rules for different users to access the target desktop by using Direct RDP in the PAM manager. These rules will be used to decide the login and the privileges of the user.

   For more information about configuring rules for Direct RDP, refer to "Direct Remote Desktop Protocol" on page 202.
5. The user can access the target desktop using the Citrix receiver.

Using Privileged Account Manager's Access Control

1. Install Privileged Account Manager agent on the target desktop.
2. Install PAM manager on the Citrix VDI server or any other machine. Register the PAM agent to the installed PAM manager.
3. Add the target desktop to the machine catalog of the Citrix VDI server.
4. Configure the rules for different users in PAM manager. You can defines rules for access and role. These rules will be used to decide the login and the privileges of the user.

   For more information about rules, refer to "Rules" on page 107.
5. The user can access the target desktop using RDP Relay, Credential Provider, or Direct RDP.

27 Discovering Privileged Accounts

An enterprise can have a system infrastructure with a wide range of operating systems such as UNIX, Linux, and Windows. There can be several privileged accounts in these systems that would have been created and left unattended for a long time. These privileged accounts that are not tracked are a risk to the enterprise. It is necessary to discover these privileged accounts and put it to best use or minimize them. Privileged Account Sniffer enables you to identify and analyze the privileged accounts in an enterprise.

Privileged Account Sniffer is an independent tool, which you can run on any computer to discover the privileged accounts in the configured target systems. The discovery results are generated as an easy-to-read excel report which contains the privileged accounts and the respective system details. These reports can be further filtered using the options available in the tool.

Using the reports generated by Privileged Account Sniffer you can:

- Manage and utilize the existing privileged accounts effectively.
- Identify the stale and expired accounts and eliminate them to mitigate the misuse of privileged accounts.

The report generated by Privileged Account Sniffer contains the system details and its credentials. Hence, it is recommended to store these files securely.

Types of Accounts Discovered

Privileged Account Sniffer discovers the following privileged accounts in the target systems:

Administrative Accounts

Privileged Account Sniffer can discover the administrative accounts in the following:

- **Windows, Linux, and UNIX Computers:** Discover administrative accounts in a Windows, Linux, and UNIX computer. These computers can be any of the following:
  - **Standalone Computer:** Discover administrative accounts in a standalone Windows, Linux and UNIX computers.
  - **Domain:** Discover administrative accounts in all the servers and the computers that are part of the domain.
  - **Range of IP Addresses:** Discover all the administrative accounts in the computers that fall in the IP range. The IP range can also contain a heterogeneous mixture of Windows and Linux/UNIX computers.

- **LDAP Directory:** Discover all the accounts of a specific user group in the directory by scanning the user group and its sub groups recursively.

  For example, if you want to identify the administrative accounts of an enterprise application which is authenticated by Active Directory, you can configure the enterprise application's administrator user group in Privileged Account Sniffer. Privileged Account Sniffer scans and discovers all the accounts in the application's user group.

Service Accounts

In addition to administrative accounts, Privileged Account Sniffer can also be used to discover the user accounts used by the services in the Windows computer. Using Privileged Account Sniffer you can discover service accounts in a Windows computer that is standalone or part of a domain.

Privileged Account Sniffer discovers the service accounts used by the applications:

- Windows services
- Windows Task Scheduler
- COM+
- Internet Information services (IIS)

Launching Privileged Account Sniffer

Prerequisites

- You can launch this tool only on Windows computers.
- You must have Microsoft .NET 4.5 or later installed in the system where you are launching this tool.
- Ensure that the Windows Remote Registry service is running in the target system.
- For domain administrative account discovery, run this tool in a computer that is part of the domain.
- For Windows administrative account discovery, ensure that the WTS communication is open and firewalls are not blocking the remote discovery.
- For service account discovery, ensure that the following configurations are done in the target system:
  - IIS service account discovery:
    - Privileged Account Sniffer supports IIS version 7 or later.
    - Ensure that the `IIS Management Scripts and Tools` role service is installed.
  - COMplus service account discovery:
    - Enable the `COM+ Remote Administration (DCOM-In)` firewall policy to allow remote discovery of COM+ service accounts.
    - Set the `remoteaccess enable` registry entry value to `1`. You can find the registry entry at `regedit\hkey local machine\software\microsoft\com3`.

To launch Privileged Account Sniffer, perform the following:

1. Download the privileged_account_sniffer from the NetIQ Downloads website.

Privileged Account Sniffer is included as a separate downloadable file in Privileged Account Manager.

2 Extract the contents of the downloaded `privileged_account_sniffer.zip` file and run the `PrivilegedAccountSniffer.exe`.

3 Continue with "Configuring Privileged Account Sniffer" on page 309.

Configuring Privileged Account Sniffer

For discovering the privileged accounts in the target system, you must configure an administrator accounts of the target system and details of the target system in the tool.

To configure the target system for account discovery, click the corresponding target system icon on the left pane and enter the required details in the fields. When configuring the Windows system, you can make use of these additional options:

- **Quick Search:** Select this option to accelerate the discovery process by retrieving the nearest value for some attributes of the account.

  For example, when you select quick search, the value of last login time is retrieved from one domain controller instead of retrieving the last login time from all the domain controllers in the domain and calculating the accurate value.

- **Discover Service Accounts:** Select this option if you want to discover service accounts in the configured target system.

After adding the target system details, you can view and edit the list of target systems that are added by selecting appropriate systems from the list.

Discovering Accounts

Discovery is scanning all the configured systems and identifying the accounts in the target systems. Before you initiate discovery, this tool allows you to select the target systems from which the accounts must be discovered. For example, you can choose to discover accounts only from the servers in the domain. After you choose the target systems, the accounts are discovered and the reports are available for you to download.

Privileged Account Sniffer preserves the reports of the previously run discovery. These reports are overwritten when you run discovery. Hence, if you want the previously ran reports, you must download the reports before initiating discovery.

To review the target systems and initiate the discovery of accounts, perform the following:

1 Click **Discover**.

2 Select the required target systems from which the accounts must be discovered.

3 (Conditional) If you want to add any new target system, click **+** of the appropriate target system.

4 Click **Run Discovery**.

The tool discovers accounts on the selected target systems and displays a high level discovery details, such as total number of accounts discovered, number of target systems on which account discovery failed and so on.

5 Click **Download Report** to download the generated report.

To further refine the reports data and download the report, click **Filter Reports and Download**.

Discovery Reports

After account discovery, you can download the discovery reports. These reports contain the details of the privileged account, such as account type, last login time, account expiry status, and so on.

If you have enabled service account discovery, two kinds of reports are generated:

- **Accounts Report:** This report contains the list of all the administrative and service accounts and general information about these accounts.

  If the account is used by any service, then the Service Account attribute of the respective account is set to yes. By using this Service Account attribute in the report, you can identify the list of service accounts.
- **Service Accounts Report:** This report contains the list of all the service accounts and details of the services associated with these accounts.

Filtering Report Data

After account discovery, you can click the **Reports** tab to filter and download the reports based on the following criteria:

- **Hosts**: Generate the list of privileged accounts in the specific host.
- **Locked Accounts:** Generates the list of privileged accounts that are locked for a specific number of days.
- **Password:** Generates the list of accounts whose password was not changed for a certain period.
- **Disabled Accounts:** Generates a list of disabled accounts in the configured systems.
- **Expired:** Generates a list of expired accounts in the configured systems.
- **Service Accounts:** Generates a list of service accounts in the configured systems.

If none of the above filters are selected, then the complete report is available for download.

Importing and Exporting Configuration

Import and export configuration feature enables you to reuse the target system configuration multiple times. The exported configuration file is stored by default in the location `privileged_account-sniffer\Configuration` and the details are exported in XML format.

After exporting the configurations, it can be imported again from the local system and discovery can be performed again to identify the privileged accounts that were newly added or removed from the system. When you perform import, all the existing configurations in the tool are overwritten.

NOTE: The exported file must be stored securely as it contains the system details and its privileged account credentials.

---

28 Upgrading Privileged Account Manager

This chapter provides instructions for upgrading Privileged Account Manager.

- "Privileged Account Manager Upgrade Checklist" on page 311
- "Configuring the Package Manager" on page 312
- "Publishing Packages on the Package Manager" on page 313
- "Upgrading Privileged Account Manager" on page 315
- "Troubleshooting" on page 317

Privileged Account Manager Upgrade Checklist

Upgrade your Privileged Account Manager installation using the following checklist:

	Tasks	See
❑	1. Review the Privileged Account Manager Release Notes to see the new functionality and understand the known issues.	PAM Documentation website
❑	2. Ensure that the computers on which you want to upgrade Privileged Account Manager components meet the specified requirements.	System Requirements in PAM Documentation website.
❑	3. (Conditional) Configure the location from where the Package Manager must download the latest packages. By default, the package manager downloads packages from the Novell update server.	Configuring the Package Manager
❑	4. Download and publish the latest packages on the package manager.	Publishing Packages on the Package Manager
❑	5. Upgrade Privileged Account Manager.	Upgrading Privileged Account Manager
❑	6. (Conditional) Enabling Privileged Account Manager to run in FIPS 140-2 Mode.	Enabling FIPS Mode

Configuring the Package Manager

Package Manager acts as a repository that contains the latest packages, which can be installed on the required host. By configuring the Package Manager, you define the location from where the Package Manager must download the latest packages.

You can download packages to a Package Manager in the following ways:

- Manually download packages from the Downloads Website. To publish the downloaded packages, see Publishing Packages from the Downloads Website.
- Download packages directly from the Novell Update Server (Recommended).

  The Novell Update Sever contains all the packages of the last two major PAM releases and also the maintenance release (hot fix and service pack) packages of the second last release. For example, if the latest release of PAM is 3.2, the Novell Update Server contains the packages of the releases, such as 3.2.0.0, 3.1.0.0, 3.1.1.0, 3.1.1.1, 3.0.1.2, and so forth. You can differentiate the packages with the help of version numbering.
- Download packages from another PAM server, which contains the latest packages, that were downloaded using one of the two methods mentioned above.

To configure a Package Manager to download packages from Novell Update Server or another PAM server:

1. Click **Package Manager** on the home page of the console.
2. Click **Settings** in the task pane.
3. (Conditional) **To use the Novell Update server:**
   - **3a** Select **Novell Update Server**.
   - **3b** Specify the User Name and Password (These are the Mirrored Credentials obtained from the Novell Customer Center account for Privileged Account Manager).
   - **3c** To view the update server information, select **Advanced Settings**.
     - Select the **Packages** checkbox, the following URL is configured:

       `https://nu.novell.com:443/PUM/packages`
4. (Conditional) **To use another PAM server:**
   - **4a** Select **Local Package Manager**.
   - **4b** Fill in the following fields:

     Host name: Specify the DNS name of the host.

     Port: Specify the communication port. The default is 29120.

     The Local Package Manager is a Framework host that has been configured to store the packages.
5. Click **Finish**.
6. Continue with Publishing Packages from Novell Update Server or another PAM Server.

NOTE: By default, Package Manager connects to **Novell Update Server** for updates.

Publishing Packages on the Package Manager

You can publish the packages on the package manager in the following ways:

- Download packages from downloads website and publish the packages using command-line options. See Publishing Packages from the Downloads Website.
- If you have configured the system to download packages from the NetIQ Customer Center (NCC) or another PAM server, you can download and publish the packages from the console. See Publishing Packages from Novell Update Server or another PAM Server.

Publishing Packages from the Downloads Website

1. Download packages from the Downloads Website.
2. Create a directory such as `framework` on the Framework Manager in the `/tmp` directory.

   This directory is called `framework` in the rest of these instructions.
3. Copy the `netiq-npam-packages-3.6.tar.gz` from the Package Manager directory on the CD to the machine.
4. Extract the file to the `framework` directory.

   For UNIX and Linux platforms, use the following commands:

   ```
   gunzip netiq-npam-packages-3.6.tar.gz
   tar -xvf netiq-npam-packages-3.6.tar
   ```

   For Windows platforms, use WinZip to extract the file.

   NOTE: To deploy tunnel specific packages, use the following command:

   ```
   gunzip netiq-npam-tunnel-packages-3.6.tar.gz
   tar -xvf netiq-npam-tunnel-packages-3.6.tar
   ```

   ---

5. Use the following command to publish the packages to the Package Manager.

   Replace *<admin>* with the name of your admin user.

   For Linux and UNIX platforms:

   ```
   /opt/netiq/npum/sbin/unifi -u <admin> distrib publish -d /tmp/framework
   ```

   For Windows platforms:

   ```
   c:\Program Files\netiq\npum\bin\unifi -u <admin> distrib publish -d
   c:\tmp\framework
   ```

   For more information about the command to publish packages to the package manager, see Package Distribution Options section of the Privileged Account Manager Administration Guide.
6. When prompted, enter the password of the admin user.
7. (Optional) To view available packages, log in to the Framework Manager, then click **Package Manager**.
8. Delete the `framework` directory.
9. Continue with Upgrading Privileged Account Manager.

Publishing Packages from Novell Update Server or another PAM Server

- "Publishing Packages of Major Releases" on page 314
- "Publishing Packages of Service Packs, Patch Updates, and Hotfixes" on page 314

Publishing Packages of Major Releases

To download and publish packages of the major PAM releases, such as 3.1, 3.2, 4.0, to the Package Manager, perform the following:

1. Ensure that you have configured the appropriate server for downloading packages. For more information, see Configuring the Package Manager.
2. Click **Package Manager** on the home page of the console.
3. Click **Add Packages** in the task pane.
4. Set the **Package Filter** options:

   Platforms: Select the operating system, then use the arrow to display and select the platforms.

   Types: Select the type of package you want to add (Console, Module, Interface, Patch).

   Components: Select the component (Command Control, Framework, Miscellaneous).
5. Select the required packages from the list of packages.

   To select multiple packages, press the Ctrl key and select the packages one at a time, or press the Shift key to select a consecutive list of packages. To select all the packages, select **Select all the packages** checkbox.
6. Click **Add** to start downloading.
7. Click **Finish**.
8. To ensure that all packages are up-to-date, continue with Publishing Packages of Service Packs, Patch Updates, and Hotfixes.

Publishing Packages of Service Packs, Patch Updates, and Hotfixes

After adding the appropriate major release packages to the Package Manager, check for any updates (hot fix, patch updates or service pack) on the major releases, such as 3.1.1.1, 3.0.1.2 and publish the updated packages to the Package Manager.

To download and publish packages, perform the following:

1. Ensure that you have configured the appropriate server for downloading packages. For more information, see Configuring the Package Manager.
2. Click **Package Manager** on the home page of the console.
3. Click **Check for Updates** in the task pane.

   If updates are available, the navigation pane displays the updated packages that are available for download. Else, an Alert dialog box is displayed stating **No package updates are available**.
4. Select the packages from the list of available packages.

To select multiple packages, press the Ctrl key and select the packages one at a time, or press the Shift key to select a consecutive list of packages. To select all the packages, select **Select all the packages** checkbox.

5 Click **Update** to start downloading.

6 Click **Finish**.

7 Continue with Upgrading Privileged Account Manager.

Upgrading Privileged Account Manager

Prerequisites

- Disconnect all Privileged Account Manager sessions to the host on which you are installing the package.
- Ensure that latest packages are available in the Package Manager. For publishing packages on the Package Manager, see Publishing Packages on the Package Manager.

NOTE: When you launch the dashboard for the first time after upgrade, the dashboard widgets may take a few minutes to load depending on the size of your database.

You must upgrade all PAM manager and agent components. You can upgrade all hosts or selected hosts in the following ways:

- "Upgrading Through Command Line" on page 315
- "Upgrading Through Console" on page 315
- "Upgrading Using the Privileged Account Manager Installer" on page 317

Upgrading Through Command Line

You can upgrade Privileged Account Manager by executing certain commands in the agent or the framework manager. To use these upgrade commands, you must have the `unifi` file in your machine at the location `/netiq/npum/bin/`. This file is available as part of the Privileged Account Manager ISO. For information about the upgrade commands and its usage, refer Upgrade and Rollback Packages.

Upgrading Through Console

You can upgrade Privileged Account Manager from the console, only if the **Enable Package Management Through Host Console** is set to **Yes** in the **Package Manager > Settings > Agent Package Management**.

WARNING: An Application SSO package update, triggers an automatic restart of the computer it is installed on.

To upgrade from the console, perform the following:

1 Upgrade your Framework Manager:

   1a Click **Hosts**.

   1b Select the host that is your Framework Manager.

   1c Click **Update Packages** in the task pane.

   The Framework Patch is displayed. This must be the latest version of the package before you can update any other packages. If the Framework Patch package is not displayed, follow the steps in Publishing Packages of Major Releases and add the Framework Patch for your platform.

   1d Select the package, then click **Next**.

   Ensure that the Credential Vault package (`prvcrdvlt`) is selected. If you do not update Credential Vault package (`prvcrdvlt`), you will not be able to manage privileged credentials.

   1e When the package is installed, click **Finish**.

   1f Click **Update Packages** in the task pane.

   1g (Conditional) If Application SSO is enabled, update Administration Manager (admin) and Agent Console (servers) packages first, manually log out of the application, clear browser cache and log in again before you update any other packages.

   1h Select all required packages, then click **Next**.

   1i When the packages are installed, click **Finish**.

   1j Verify that all packages display latest version. If they don't, return to Publishing Packages on the Package Manager and download any missing package.

2 (Conditional) If there are any new packages introduced in 3.7, you must install those packages on your Framework Manager:

   New package introduced in 3.6 is Task Manager (`taskmanager`). Task Manager package is required only if you want to rotate resource password using PAM. Before installing the Task Manager package, review the Prerequisites in the Privileged Account Manager Administration Guide.

   2a Click **Hosts**.

   2b Select the host that is your Framework Manager, use the arrow to display the packages, then select **Packages**.

   2c Click **Install Packages**.

   2d Select packages newly added in 3.6 and then click **Next**.

   2e Click **Finish**.

3 Upgrade your agents:

   WARNING: An Application SSO package update, triggers an automatic restart of the computer it is installed on.

   3a Click **Hosts** on the home page of the console.

   3b Select the hosts that are agents or select the domain containing the agents.

   3c Click **Update Packages** in the task pane.

3d Select the Framework Patch, then click **Next**.

3e Click **Update Packages** in the task pane.

3f Select the listed packages, then click **Next**.

3g When the packages have installed, click **Finish**.

3h Verify that all packages display 3.6 version.

Upgrading Using the Privileged Account Manager Installer

You can upgrade Privileged Account Manager Packages using the Privileged Account Manager Installer.

Prerequisites

- You must have the administrator privilege for the `unifi` module to execute this command in the local agent machine.
- This method is supported only in Windows computer.

To upgrade Privileged Account Manager:

1. Download the Privileged Account Manager installation file from the NetIQ Downloads website.
2. (Conditional) For interactive upgrade, run the following installer file and follow the onscreen prompts:

   `<filename>.msi`

3. (Conditional) For silent upgrade, use the following command:

   Syntax: `msiexec /i <Installer Filename> /passive USERNAME=<"username">` `PASSWORD=<"password"> REINSTALL=ALL REINSTALLMODE=VOMUS`

   Example: `msiexec /i netiq_pam_manager_3.6.0_x64.msi /passive` `USERNAME="admin" PASSWORD="novell123" REINSTALL=ALL REINSTALLMODE=VOMUS`

   If you have mapped your local account to a Framework Manager user (see Modify User: Native Maps), you need not specify the user name and password.

   Example: `msiexec /i netiq_pam_manager_3.6.0_x64.msi /passive` `REINSTALL=ALL REINSTALLMODE=VOMUS`

   For more information about other `msiexec` command-line options, see Microsoft documentation.

Troubleshooting

This section contains potential problems and error codes that you may encounter when upgrading Privileged Account Manager.

AIX Agent Upgrade Through UI Fails With An Error Message

Issue: When you upgrade Framework package (`spf`) of the AIX agent through UI, the upgrade fails with the error message **Failed to receive response from the module**.

Workaround: To workaround this issue, you must perform hard restart of the AIX agent from the Host Console and try upgrading again.

29 Troubleshooting

This section contains potential problems and error codes that you may encounter when configuring or using Privileged Account Manager.

The Agent is in an Offline State

Issue: If the Agent is in an offline state, the users cannot access the agent.

Workaround: To resolve this issue, the administrator of Privileged Account Manager can perform the following:

- Ensure that the time synchronization is maintained between the Manager and the Agent.
- Ensure that you can ping the Agent from the Manager by using the DNS names with which it is registered with the Manager.

The Audit Events are Not Displayed in the Reporting Console Even When the Events are Generated

Issue: When the audit events are not getting replicated from the Agent to the Manager, the reporting console does not display the latest events. This happens when the connection between the Agent and the Manager is interrupted and large amount of data gets stored in the Store and Forward (strfwd.ldb) file.

Workaround: To resolve this issue, the administrator can perform the following:

- Check if the database is working fine by performing a db integrity check. To check this, You can use the `strfwdutil -i` command.
- Check if the msq file is working fine by using the tstdb tool. To check this, you can use the `tstdb -m strfwd.msq –V` command.

For more information about this issue, see the Knowledge Base Article 7005851.

On an AIX Platform, When the Audit Data Gets Generated in Large Amount, The Privileged Account Manager Service Restarts and an Error is Displayed in the unifid.log file.

Issue: If Manager for Privileged Account Manager is installed on an AIX platform and the AIX users try to access session simultaneously large amount of audit data gets generated and the further sessions may hang. This results in restart of the Privileged Account Manager service.

Workaround: To resolve this issue the administrator can perform the following:

1. Check the unifid.log file for the `Error, Db strfwd.ldb - SQL Error, out of memory` error.
2. Restart the Privileged Account Manager service by using the following command so that PAM can scale upto 2 GB:

   ```
   `startsrc -s npum –e "LDR_CNTRL=MAXDATA=0x70000000"
   ```

   On an AIX platform, by default each process is limited to 256MB which may not be sufficient for the Privileged Account Manager service under high load conditions.

The RDP Relay Session Does Not Start From the User Console

Issue: When a user tries to connect to an RDP relay session through the user console, the session does not start. This may happen if the target server is unreachable.

Workaround: An administrator can perform the following:

1. Ensure that the Remote Desktop Connection is enabled in the System Properties of the target machine.
2. Ask the user to check if RDP Relay host is reachable by using the DNS name and IP address.
3. Ensure that the 13389 port is not blocked by firewall in the user's computer.
4. Check if RDP relay from the Manager to the target server is working fine.
5. Check if the target server agent logs the error `agent is not initialized`. If this error exists then, restart the agent server (Windows restart).
6. Check if the target system agent logs the error `user lookup failed`. If this error exists, then ensure that the **RunAs** user is available in the target server.
7. Ensure that the Agent for Privileged Account Manager is installed on the target machine when the session capture is set to **On**. If the Agent is not installed on the target server, and the session capture is **On**, RDP relay fails, then you need to modify the policy by setting the session capture to **Off**.

The RDP Relay to a Windows Server 2012 Server Fails

Issue: If a user is starting an RDP relay session to connect to a Windows server 2012 computer and has the remote desktop client version 8.0 or higher, the session fails to connect.

Workaround: To workaround this issue, users can use Windows 7 or earlier version with mstsc version 6.1.7601 or earlier. If Windows 7 is updated to use latest version of RDP, you can downgrade to lower version by uninstalling the patch KB 2592687. This is an optional update for Windows 7 and Windows Server 2008 R2 to update RDP protocol version.

The Privileged Session is Not Established Through the Backup Manager

Issue: When users connect to a privileged session through the backup manager for Privileged Account Manager, the session is not established. But they can connect to the privileged session through the primary manager.

Workaround: The administrator can check if the replication from the primary to the backup manager is successful.

The Changes to the Syslog Settings Do Not Get Applied

Issue: In the Reporting console of Privileged Account Manager when you save the changes to syslog settings, such as select **SSL**, or **Allow Persistent Connections,** the changes are not applied.

Workaround: To workaround this issue, restart Privileged Account Manager.

The Manual Disconnect for a Windows session Does Not Work

Issue: When a Privileged Account manager administrator tries to disconnect a windows session manually, the error `No module available` is displayed.

Workaround: Ensure that **Run Host** that is configured in the policy should be same as the agent name that you have specified in the Host console.

The Run as privileged user Option is not displayed on a Windows 2012 Server

Issue: When you right-click **Start** on a Windows 2012 server, the **Run as privileged user** option does not get displayed.

Workaround: To workaround this issue, right-click the application in the folder where the application is installed to execute **Run as privileged user**.

Agent Registration Fails on a Windows Platform

Issue: When you are registering a Windows agent for Privileged account Manager to a Manager, the registration fails.

Workaround: Ensure that you launch `cmd.exe` by selecting **Run As Administrator** and log in with the administrator credentials.

Direct RDP Sessions are Enabled for all Users By Default

Issue: By default, the Direct RDP sessions are enabled for all users.

Workaround: If you want to deny specific users to access the server, create a separate user group and add the user names in the **Users** field. By default all the users are granted access to the server.

NOTE: For latest version of troubleshooting information, refer Chapter 29, "Troubleshooting," on page 319.

Issues When Updating or Downloading the License Summary

The following sections include the issues that may occur when you are updating or downloading the license summary from the License Summary page.

Failed to connect to module

Issue: When you click **Update License Summary** or **Download Detailed Report** you get an error, `Failed to connect to module`. This happens when the agent from where you are trying to update the license summary, cannot contact the primary registry.

Workaround: Verify if the primary registry is online by performing the following:

1. Click **Hosts > Find Packages**.
2. In the Package field select **Registry manager > Find**.
3. Click the registry that displays the asterisk(*) symbol.
4. Check **Status**.
5. (Conditional) If the primary registry is offline, refer TID.

The system cannot process the details because one or more agents that have the DB Audit module is in Offline state

Issue: When the agents that have the dbaudit module is offline, the license summary does not get updated.

Workaround: For updating the license summary, it is a prerequisite that all the agents that have dbaudit module must be in an online state.

To check which agent is offline, perform the following on the Hosts console:

1. In the middle pane click the root host, **Hosts**
2. In the left pane click **Database Connectors**
3. Check the required agent, if it is offline, the text, `offline` is displayed next to the agent name.

The system cannot process the details because it cannot contact any of the Credential Vault modules

Issue: The error gets displayed when there are no credential vault modules in the PAM framework, or no credential vault module is reachable from the primary registry module.

Workaround: For updating the license summary, it is a prerequisite that at-least one credential vault module is online and reachable from the primary registry module.

You need to install a credential vault module in at least one of the agents and rectify any network issues between the primary registry and the agent with credential vault module.

SSL Connection to Microsoft SQL Sever Fails with a Timeout Error

Issue: When Privileged Account Manager 3.5 tries to establish an SSL connection to Microsoft SQL server for database monitoring, the connection fails with a timeout error. This issue occurs because Privileged Account Manager uses the advanced ciphers that are supported in TLS 1.2.

Workaround: To workaround this issue, upgrade the Microsoft SQL server to support TLS 1.2.

RDP Relay to Windows 10 or Windows 2016 Fails with a Network Authentication Error

Issue: RDP Relay to Windows 10 or Windows 2016 fails with an error `the connection cannot proceed because authentication is not enabled`. This issue occurs when the network level authentication is enabled in Windows 2016 or Windows10.

Workaround: To workaround this issue, change the **Security Layer** level to 0 or 1. You can find the Security Layer registry entry at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp`.

SSO to Application Does Not Happen When There are Multiple Concurrent Sessions to the Application SSO Host

Issue: If you have multiple concurrent sessions to the application SSO host with Video capture enabled, then the resource utilization of the application SSO host increases which affects the SSO operation.

Workaround: To workaround this issue, perform one of the following:

- Disconnect unwanted sessions to the Application SSO Host.
- Offload the video creation operation from the application SSO host. For more information, see Video Off-Load.