Legal Notice

Copyright 2009 - 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text 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/.
8 Managing Reports 289

8.1 Creating Reports 289
8.1.1 Creating Reports for Sessions 290
8.1.2 Creating Reports for Administrator Activities 291
8.1.3 Creating Reports for Credential Checkouts 292
8.1.4 Creating Reports for Shared Key Checkouts 293
8.1.5 Customizing Reports 294

8.2 Using Reports Settings 296
8.2.1 Using Audit Settings 296
8.2.2 Using Encryption Settings 297
8.2.3 Using Video Report Filter Settings 297
8.2.4 Configuring Video Capture 303
8.2.5 Viewing the Videos 306
8.2.6 Video Off-Load 307
8.2.7 Change Log Reports 310
8.2.8 Password Management 311
8.2.9 Enabling Password Management 311
8.2.10 Viewing Report Data 311
8.2.11 Shared Key Management 312
8.2.12 Enabling Shared Key Management 312

8.3 Using Compliance Auditor 313
8.3.1 Controlling Access to the Compliance Auditor 314
8.3.2 Compliance Audit Rules 314
8.3.3 Adding or Modifying an Audit Rule 315
8.3.4 Compliance Audit Reports 316
8.3.5 Compliance Auditor Records 322
8.3.6 Viewing a Compliance Audit Record 323
8.3.7 Deploying the Compliance Auditor 327
9 Integration with External Services

9.1 Integrating with ArcSight Intelligence .............................................................. 329
  9.1.1 Example Scenarios ...................................................................................... 329
  9.1.2 Configuring ArcSight Intelligence Details .................................................. 331
9.2 Integrating with Identity Manager ................................................................. 331
  9.2.1 Benefits of Integration with Identity Manager ........................................... 332
9.3 Integrating with Syslog Server ...................................................................... 333
  9.3.1 Configuring Syslog Server Settings ............................................................ 333
9.4 Integration with Ticketing Systems ............................................................... 335
  9.4.1 Configuration for Normal Access .............................................................. 335
  9.4.2 Configuration for Elevated Access ........................................................... 336
9.5 Integrating with NetIQ Access Manager ....................................................... 337

10 Command Line Options

10.1 The unifi Options ......................................................................................... 340
10.2 Command Control Options ........................................................................ 340
  10.2.1 Importing and Exporting Command Control Settings ............................ 341
  10.2.2 Backing Up and Restoring a Command Control Configuration ............ 341
  10.2.3 Running Test Suites ................................................................................ 343
10.3 Package Distribution Options ..................................................................... 343
10.4 Package Manager Options .......................................................................... 344
  10.4.1 Install and Uninstall Packages ................................................................. 344
  10.4.2 Upgrade and Rollback Packages ............................................................. 345
10.5 Registry Agent Options ................................................................................ 346
  10.5.1 Registering an Agent ............................................................................... 346
  10.5.2 Finding a Primary Manager Package ..................................................... 347
  10.5.3 Agent Status ............................................................................................ 347
  10.5.4 Adding Hosts and Domains .................................................................... 348
10.6 Registry Manager Options ........................................................................... 348
10.7 Compliance Auditor Options ....................................................................... 348
  10.7.1 Exporting and Importing Compliance Auditor Settings ........................ 349
  10.7.2 Managing Compliance Auditor Records ................................................ 349
10.8 sreplay Command Line Options ................................................................ 351

11 Troubleshooting

11.1 General Issues ............................................................................................. 355
  11.1.1 The Agent Is In An Offline State .............................................................. 356
  11.1.2 The Audit Events Are Not Displayed In The Reports Console Even When The Events Are Generated ............................................................ 356
  11.1.3 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. ......................................................... 356
  11.1.4 The RDP Relay Session Does Not Start From The User Console .......... 357
  11.1.5 The RDP Relay To a Windows Server 2012 Server Fails ......................... 357
  11.1.6 The Privileged Session Is Not Established Through The Backup Manager .................................................................................................................... 357
  11.1.7 The Changes To The Syslog Settings Do Not Get Applied ........................ 358
  11.1.8 The Manual Disconnect For a Windows Session Does Not Work ............ 358
  11.1.9 The Run As privileged User Option Is Not displayed On A Windows 2012 Server .............................................................................................................. 358
  11.1.10 Agent Registration Fails In Windows Platform ........................................ 358
  11.1.11 Direct RDP Sessions Are Enabled For All Users By Default .................. 358
  11.1.12 Issues When Updating Or Downloading The License Summary ............ 358
11.1.13 Failed To Connect To A Module ................................................................. 359
11.1.14 The System Cannot Process The Details Because One or More Agents With DB
Audit Module is in Offline State ................................................................. 359
11.1.15 The System Cannot Process The Details Because Of A Disconnect With The
Credential Vault Modules. ........................................................................... 359
11.1.16 SSL Connection to Microsoft SQL Sever Fails with a Timeout Error .............. 359
11.1.17 RDP Relay to Windows 10 or Windows 2016 Fails With a Network Authentication
Error ........................................................................................................... 360
11.1.18 SSO to Application Does Not Happen When There are multiple Concurrent
Sessions to the Application SSO Host .......................................................... 360

11.2 Troubleshooting Issues Related with Managing Hosts ........................................ 360
11.2.1 Promoting Managers When the Primary Manager Fails ............................... 361
11.2.2 Viewing Store and Forward Messages ...................................................... 361
11.2.3 Managing Low Disk Space ..................................................................... 362
11.2.4 Restarting the Agent .............................................................................. 363
11.2.5 Managing the Registry Cache ................................................................. 363
11.2.6 Time Synchronization .......................................................................... 365
11.2.7 Direct RDP is Disallowed When Privileged Account Manager Agents are Unable to
Reach the Manager ....................................................................................... 365

11.3 Issues While Integrating with Advanced Authentication ................................. 365
11.3.1 Advanced Authentication Server is Inactive and Users Cannot Log In to Privileged
Account Manager End-Points ................................................................. 366

A Appendix: Legacy Roles ............................................................................... 367

B Appendix: Policy Templates ....................................................................... 373
B.1 Understanding Sample Policy template ..................................................... 373
B.1.1 Importing Sample Policy Templates ....................................................... 374
B.2 Adding a Policy Template ......................................................................... 374

C Appendix: IPv6 Support .............................................................................. 377
About This Book and the Library

This guide explains how to use the Privileged Account 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
Privileged Account Manager User Guide
Privileged Account Manager 4.4 System Requirements and Sizing Guidelines
Privileged Account Manager 23.3.0 (v4.4.0) Release Notes
Privileged Account Manager Business Use Case Guide
Privileged Account Manager Overview
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 have remained unused for a long time. The untracked privileged accounts might be a risk to the enterprise. Discovering these privileged accounts and putting them to best use or minimizing them is necessary. Privileged Account Sniffer enables you to identify and analyze the privileged accounts in an enterprise.

An enterprise can have a system infrastructure with a wide range of operating systems, such as UNIX, Linux, and Windows. These operating systems contain several privileged accounts that are not used for a long time. These unused privileged accounts might be a risk to the enterprise.

Discovering these privileged accounts and putting them to best use or minimizing them is necessary. Privileged Account Sniffer is an independent tool to identify and analyze the privileged accounts in an enterprise. You can run this tool on any computer to discover the privileged accounts in the configured target systems. The discovery results are available in an easy-to-read excel report containing the details of privileged accounts and corresponding system.

You can use these reports to perform the following tasks:

- 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 contains the system details and the respective credentials. Therefore, you must secure these files.

1.1 Types of Accounts Discovered

Privileged Account Sniffer discovers the following privileged accounts in the target systems:

1.1.1 Administrative Accounts

Privileged Account Sniffer discovers 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 machine.
  - **Domain**: Discover administrative accounts in all the servers and the computers that are associated to the domain.
  - **Range of IP Addresses**: Discover all the administrative accounts in the computers that are within 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 are 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.

### 1.1.2 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 that are used by the following applications:

- Windows services
- Windows Task Scheduler
- COM+
- Internet Information Services (IIS)

### 1.2 Launching Privileged Account Sniffer

**Prerequisites**

- Supported on Windows computers with Microsoft .NET 4.5 and later versions 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 performed 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.zip from the NetIQ Downloads website. Privileged Account Sniffer is available as an individual downloadable package in Privileged Account Manager.

2. Extract the contents of the downloaded privileged_account_sniffer.zip file and run the PrivilegedAccountSniffer.exe.


1.3 Configuring Privileged Account Sniffer

For discovering the privileged accounts in the target system, you must configure an administrator account 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 specify 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 the 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.

1.4 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 download.

Privileged Account Sniffer preserves the reports of the previously run discovery. These reports are overwritten when you run discovery. Therefore, if you want the older 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 an overview of 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.

1.5 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 a 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.

1.5.1 Filtering Report Data

After account discovery, you can click the Reports tab to filter and download the reports based on the following criteria:

- **Hosts**: Generates the list of privileged accounts in the specific host.
- **Locked Accounts**: Generates the list of privileged accounts that have been locked for a specific number of days.
- **Password**: Generates the list of accounts for which the password has not been changed from 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.

**NOTE**: The exported file must be stored securely as it contains the system details and its privileged account credentials.
Managing Hosts

The Hosts console provides a hierarchical view of all the defined hosts. You must add all host machines with managers and agents to the Framework Manager console through the Hosts console.

Each host has a unique agent name specified during the registration process after installing the host. The Framework Manager console recognizes hosts by their unique agent names.

In the Hosts console, you can add hosts into domains and organize the 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 panes:

- **Task**: Displays the tasks or actions you can perform on the host server.
- **Navigation**: Displays a hierarchical view of all defined hosts and domains.
- **Details**: Displays the details of selected hosts.

This section describes the following host management capabilities:

- Section 2.1, “Managing Domains,” on page 15
- Section 2.2, “Managing and Monitoring Hosts,” on page 17
- Section 2.3, “Managing System Alerts,” on page 26
- Section 2.4, “Enabling Crash Dump Capture,” on page 28
- Section 2.5, “Managing Packages Using New Console,” on page 28
- Section 2.6, “Managing Host Packages Using the Legacy Console,” on page 29
- Section 2.7, “Managing Audit Zones,” on page 35
- Section 2.8, “Securing Access to the Framework Manager Console,” on page 36
- Section 2.9, “SSL Renegotiation DOS Attack Protection,” on page 37

### 2.1 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.

- Section 2.1.1, “Creating a Domain,” on page 16
- Section 2.1.2, “Modifying a Domain,” on page 16
- Section 2.1.3, “Deleting a Domain,” on page 17
2.1.1 Creating a Domain

When you install Privileged Account Manager, a top-level domain Hosts is automatically created. To rename this domain, see Section 2.1.2, “Modifying a Domain,” on page 16. You can create subdomains under the top-level domain.

1. Click Hosts on the home page of the console.
2. Select an existing domain to add a subdomain to it.
3. Click Add Domain in the task pane and on the Add Domain page specify the subdomain name.
4. Click Add.
5. Perform one of the following tasks based on your requirement:
   - To configure the domain, continue with Section 2.1.2, “Modifying a Domain,” on page 16.
   - To add hosts to the domain, continue with Section 2.2.2, “Adding a Host,” on page 19.
   - To move existing hosts to this domain, continue with Section 2.2.7, “Moving a Host,” on page 22.

2.1.2 Modifying a Domain

Use this page to modify the domain name and encryption settings. The encryption settings applied 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 Section 2.7, “Managing Audit Zones,” on page 35.

   **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 till when the host key can be used before generating a new key for the hosts in this domain.
   - Db Key Rollover(days): Specify till when 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 Reports console.

5. Click Finish.

### 2.1.3 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 Section 2.2.7, “Moving a Host,” on page 22.

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.

### 2.2 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. You can monitor your hosts using Deployment Dashboard. This 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.

- Section 2.2.1, “Deployment Dashboard,” on page 18
- Section 2.2.2, “Adding a Host,” on page 19
- Section 2.2.3, “Viewing Host Details,” on page 19
- Section 2.2.4, “Modifying a Host,” on page 20
- Section 2.2.5, “Registering Hosts,” on page 21
- Section 2.2.6, “Deleting a Host,” on page 22
- Section 2.2.7, “Moving a Host,” on page 22
- Section 2.2.8, “Finding a Host,” on page 23
- Section 2.2.9, “Monitoring Hosts,” on page 23
2.2.1 Deployment Dashboard

Deployment Dashboard helps the administrators to view the geographical deployment of the Privileged Account Manager Hosts and also identify the hosts on which a risky activities were 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.

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.
Customizing 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.

2.2.2 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 might 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.

2.2.3 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.
In the navigation pane, select the host to display the Packages option on the right pane.

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

### 2.2.4 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 Section 2.7, “Managing Audit Zones,” on page 35.

- **Vault:** Select the local/domain vault created for Windows agents from the dropdown list.

- **RDP Port:** Enter the RDP port which the host uses for Privileged Account Manager communication.

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 the number of days till when the host key can be used before generating a new key.

- **DB Key Rollover (days):** Specify the number of days till when 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** - Contains 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 Reports console.

6 Click **Finish**.

### 2.2.5 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:

- **Privileged Account Manager Admin Username:** Username to access the Framework Manager.
- **Privileged Account Manager 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 Section 2.2.7, “Moving a Host,” on page 22.

### 2.2.6 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 the loss of audit data that is received from the domain or audit zone.

### 2.2.7 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.
2.2.8 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.

2.2.9 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 23
- “Viewing the Host Log” on page 24
- “Modifying Log Settings” on page 25
- “Example Rollover Script” on page 25

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>:green:</td>
<td>The host is online.</td>
</tr>
<tr>
<td>:green:</td>
<td>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.</td>
</tr>
<tr>
<td>:red:</td>
<td>The host is offline.</td>
</tr>
<tr>
<td>:blue:</td>
<td>The host is unregistered.</td>
</tr>
</tbody>
</table>
4 Select the **Online**, **Offline** and **Unregistered** check box 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 becomes less than the value specified 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 **Section 10.5.3, “Agent Status,” on page 347**.

### 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 to refresh the screen. 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 Select **Pause** to pause the screen display.

6 Select **Clear** 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 25.

4. Click Next to apply the changes.
   - If the changes are applied successfully, a green indicator is displayed next to the agent name.
   - If the changes are not applied successfully (for example, if the host is not online), a red indicator 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;
}

2.3

Managing System Alerts
The System Alerts page shows system status alert messages from all hosts in the Framework. This
mechanism works in conjunction with other solutions for data center security, such as SIEM, DAM,
vulnerability management, etc.
This page displays the following details of the system alert:
 Time of the alert
 Host from where the alert originated
 Type of the alert
 Additional 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 are 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 check box 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.

26

Managing Hosts


2.3.1 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 26 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 off this setting.
   - **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 Regular expression 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) time standard 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.

2.4 Enabling Crash Dump Capture

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

```xml
<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.

2.5 Managing Packages Using New Console

You can now manage packages using the new Privileged Account Manager console easily.

2.5.1 Viewing and Managing Host Packages

On the home page of the console, click 📦.

You can view all the host packages present in your environment with additional details, such as, Title, Description, Version, Platform, and Package.

Clicking on a specific package or a group of packages enables the Publish button. Confirm by clicking Publish to proceed with downloading and publishing the package/packages. The published packages are signified by green color whereas unpublished packages are signified cloud icon. Clicking the cloud icon again the necessary package publishes the package.

On the left navigation pane, you can click on the specific Privileged Account Manager release to import the packages updated with that specific release. For example, selecting 4.2.0.1, auto populates all the packages that were updated as part of Privileged Account Manager 4.2.0.1 release. You can select the packages from the right pane and click Publish to publish the selected packages.

You can also filter the packages based on the Platform and Status.

Status signifies whether the selected package is published or not.
The Platform filter allows you to select based on the following platforms:

- Windows
- Linux
- HP-UX
- AIX
- Solaris
- All

Selecting All allows you to view all the platforms’ packages.

**NOTE:** Privileged Account Manager server might be slow to respond when you publish large number of packages using the new Package Manager user interface.

### 2.5.2 Package Source Settings

You can select the package source from the following options:

- **Default Update Server:**
  
  This option allows you to use the default settings that are displayed on the console and the settings are not editable.

- **Custom Update Server:**
  
  This option allows you to customize the repository which fetches the package.

- **Local PAM Manager:**
  
  This option allows you to use local PAM Manager as the repository as Package source.

Enabling Agent Package Management option allows you to retrieve the packages from another instance of PAM manager.

### 2.6 Managing Host Packages Using the Legacy Console

- Section 2.6.1, “Finding Packages on Hosts,” on page 30
- Section 2.6.2, “Updating Packages for a Host,” on page 30
- Section 2.6.3, “Rolling Back Packages,” on page 31
- Section 2.6.4, “Committing Packages,” on page 31
- Section 2.6.5, “Registering and Unregistering Packages for a Host,” on page 32
- Section 2.6.6, “Installing Packages on a Host,” on page 32
- Section 2.6.7, “Uninstalling Packages from a Host,” on page 33
- Section 2.6.8, “Modifying Audit Settings for the Audit Manager Package,” on page 33
- Section 2.6.9, “Configuring SMTP Server Settings,” on page 34
- Section 2.6.10, “Configuring Settings for the dbaudit Package,” on page 34
2.6.1 Finding Packages on Hosts

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

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 dropdown 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.

2.6.2 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 adequate 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.
   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.
2.6.3 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 prior 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 prior version, first rollback all the packages except distrib and framework (`spf`) and at last 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.

2.6.4 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 appropriately in your environment. (See Section 2.6.3, “Rolling Back Packages,” on page 31.)

If the current package performs appropriately 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.
2.6.5 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 represented with a green check mark: 

Unregistered packages are represented 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.

2.6.6 Installing Packages on a Host

Ensure that the packages have been downloaded to the Framework Package Manager by viewing packages available to deploy.

The distribution agent performs a number of checks to ensure that the host has sufficient 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 Section 10.4, “Package Manager Options,” on page 344.

2.6.7 Uninstalling Packages from a Host

It is not required to uninstall a package to disable it. You can disable it by unregistering the package. See Section 2.6.5, “Registering and Unregistering Packages for a Host,” on page 32.

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 Section 10.4, “Package Manager Options,” on page 344.

2.6.8 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, because 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.
2.6.9 Configuring SMTP Server Settings

SMTP Settings enables you to specify email server information and automate the emailing of reports such as Compliance Auditor and Custom Command Control reports to the necessary personnel.

To configure the SMTP settings:

1. On the home page of the console, click Settings > External Services > SMTP Server.
2. Configure the following fields:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Specify the IP address of your E-mail server.</td>
</tr>
<tr>
<td>Domain</td>
<td>If you are using a Lotus Notes server, specify the name of your SMTP domain.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Move the slider to the right to enable SSL communication with a SMTP server. Import the certificate authority (CA) certificates into primary and backup managers for verifying the SMTP server certificate.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port of your E-mail server.</td>
</tr>
<tr>
<td>Username</td>
<td>SMTP server username.</td>
</tr>
<tr>
<td>Password</td>
<td>SMTP server password.</td>
</tr>
<tr>
<td>Server E-mail ID</td>
<td>SMTP server Email ID.</td>
</tr>
<tr>
<td>E-mail Body</td>
<td>Select either HTML or Plain Text as the E-mail body.</td>
</tr>
</tbody>
</table>

3. Click Update.

2.6.10 Configuring Settings for the dbaudit Package

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

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

For more information, refer to “Password Management for Database and Applications” on page 128.
2.7 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. The advantages of configuring an audit zone for your domain include:

- Defining destination criteria for domain's audit data based on geographical and organizational demographics. Defining this criteria allows restricting access to audit data, ensuring it reaches only the intended recipients.
- Preventing distribution of huge audit data to audit managers.

You can configure one or more audit zones for a domain. If you have not configured any, the default audit zone is zero for all the domains, Privileged Account Manager agents, and Privileged Account Manager managers.

**IMPORTANT:** You must maintain at least one audit manager within audit zone 0 at all times. This precaution is necessary because if there are no audit managers in the audit zone of any domain, the audit data for that domain is automatically routed to audit zone 0 preventing data loss.

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 associated.

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 for Privileged Account Manager agent and sent to the audit managers of your audit zone when they are up.

If you move an agent host such as an audit manager from one domain to another during a session, audit data is still sent to the audit manager. A new session data is sent to audit managers.

Here are few recommendations for configuring audit zones:

- Each audit zone must have more than one audit manager.
- 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.
2.8 Securing Access to the Framework Manager Console

The following options enhance 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.

- Section 2.8.1, “Requesting a Certificate for the Framework Manager Console,” on page 36
- Section 2.8.2, “Modifying the Connector,” on page 37

2.8.1 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). Privileged Account Manager uses OpenSSL to generate a Certificate Signing Request (CSR). When requesting a certificate in Privileged Account Manager, 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 37.

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.

2.8.2 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 required changes:
   - Define the address of a specific interface card
   - Define which port to use
   - Select SSL if you want to use SSL.
6 Click Finish.

2.9 SSL Renegotiation DOS Attack Protection

Clients can attack the SSL server by sending many renegotiation (SSL handshake) requests to it. This can overload 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.
Managing Users and Groups

Privileged Account Manager provides comprehensive user management capabilities to control access to the consoles. Privileged Account Manager provides comprehensive user management capabilities to control access to the Framework consoles. The administrator user belongs to the administrator group, which has access to all consoles and can perform all tasks.

You can set up different permissions for each user group. These permissions determine whether a group can access a console and perform actions.

This section describes the following user management capabilities:

- Section 3.1, “Managing Groups,” on page 39
- Section 3.2, “Managing Users,” on page 50
- Section 3.3, “Changing a User’s Password,” on page 53
- Section 3.4, “Assigning Permissions for LDAP Users,” on page 54

3.1 Managing Groups

Privileged Account Manager users must be assigned to one or more groups with the appropriate permissions defined before they can access any resources or perform any tasks.

- Section 3.1.1, “Predefined User Groups,” on page 39
- Section 3.1.2, “Adding a User Group,” on page 40
- Section 3.1.3, “Modifying a User Group,” on page 40
- Section 3.1.4, “Configuring Permissions,” on page 41
- Section 3.1.5, “Deleting a User Group,” on page 50

3.1.1 Predefined User Groups

The following predefined user groups and users are already created for the default * user. Not all predefined user groups contain users. The predefined user groups have default permissions. The following default groups implicitly have “*” permissions to the relevant modules:

- **Access Administrators**: Administrators who manage privileged access to resources.
- **Admin**: Global Administrators.
- **Agent Administrators**: Administrators who manage agents.
- **API Users**: Group membership that has the role which gives permission to make API calls using a secret key that the user generates. The key would be used for authentication in place of user ID and password.
- **Audit Administrators**: Auditors who monitor user activities.
- **Auditors**: Auditors who manage user activities.
• **Compliance Auditors**: Auditors who review user activities.
• **Package Management Administrators**: Administrators who manage package repository.
• **SSO Administrators**: Application SSO Administrators.
• **User and Group Administrators**: Administrators who manage local users, groups and their permissions.
• **User Requests Administrators**: Administrators who manage user access requests.
• **Vault Administrators**: Administrators who manage Credential Vaults and password management.

### 3.1.2 Adding a User Group

1. On the home page of the console, click **Users > Users & Groups > Create Group > General**.
2. **Group Name**: Specify the group name. This is a mandatory field.
3. (Optional) **Comment**: Add an explanatory text.
4. (Optional) **Group Manager Name**: Specify the name of the group manager.
5. (Optional) **Group Manager E-mail ID**: Specify the email address of the group manager.
6. (Optional) **Group Manager Contact Number**: Specify the contact number of the group manager.
7. (Optional) **Bypass Secondary Authentication**: This property is inherited from the parent group. Select **Bypass Secondary Authentication** option if you have enabled secondary authentication for the Administration Console and want to bypass it. See “Benefits of Integration with Advanced Authentication” on page 58 for more details.
8. Click **Next**.
9. In the **Members** page, select the members you want to add in the user group.
10. Click **Next**.
11. In the **Sub Groups** page, select the sub groups you want to add to the user group.
12. Click **Next**.
13. In the **Advanced Settings** page, select the permissions based on the assignments from the list.
14. In the **Role(s)** field, select the **Module** and the **Role**.
15. Click **Next** to select the **Group Maps**.
16. Click **Create**.

### 3.1.3 Modifying a User Group

Modifying a user group allows you to:

• Add a comment describing the group
• Add users and subgroups to the group
• Define administrative permissions for the group
• Specify group maps for the group
• Modify the advanced setting involving the module level permissions
To modify a Framework user group:

1. On the home page of the console, click Users > Users & Groups. Select the group from the left pane, click the edit icon. The Edit Group page is displayed.

2. In the General pane, select the details you want to modify. You cannot modify the Group Name field.

3. In the Members section, select to add or remove the users you want to be members of this group.

4. In the Sub Groups section, select the groups you want to be subgroups of the user group.

5. In the Advanced Settings section, select the Descriptive Permissions 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 Section 3.1.4, “Configuring Permissions,” on page 41 for more details.

6. In the Group Maps section, add the LDAP users and groups. See “Assigning Permissions for LDAP Users” on page 54 for more details.

7. Click Save.

### 3.1.4 Configuring Permissions

From Privileged Account Manager 4.0, "roles" and the associated access to modules have been described to improve the new user interface's readability. These "roles" refer to the administrative permissions used while deploying Privileged Account Manager.

**NOTE:** Every time a new permission is added the user has to log out and log in for the new permission to take effect.

When you create a user group, you must assign at least one permission to the group.

To allow access, you can define one or more permissions according to the tables below:

- “Administration” on page 42
- “Access Control Permissions” on page 42
- “Agent Management Permissions” on page 42
- “Audit Reports Permissions” on page 43
- “Compliance Audit Reports Permissions” on page 45
- “Credential Vault Permissions” on page 45
- “Package Distribution Permissions” on page 46
- “Package Manager Permissions” on page 48
- “Password Management Permissions” on page 48
- “User and Group Manager Permissions” on page 48
- “User Access Requests Permissions” on page 49
Administration

The following permissions can be assigned to any module if you want to delegate administrative rights.

<table>
<thead>
<tr>
<th>Descriptive Permissions</th>
<th>Allows users to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Administrator</td>
<td>Have permission to access all modules and permissions.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Have permission to view and modify superusers, and view and modify groups with the super role defined. This role should also be able to add or delete users and groups, and assign users to groups.</td>
</tr>
</tbody>
</table>

Access Control Permissions

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

<table>
<thead>
<tr>
<th>Descriptive Permissions</th>
<th>Allows users to…</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Permissions on Access Control and Command Control</td>
<td>Have permissions to perform all operations. This implies you have “*” permission to Access Control or Command Control console.</td>
</tr>
<tr>
<td>View, Modify Objects and Transaction Permissions in Access Control and Command Control</td>
<td>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 permissions. This implies you have read permission to auth module.</td>
</tr>
<tr>
<td>View Access Control or Command Control Console</td>
<td>View the Access Control and Command Control console. This implies you have console permission to Access Control and Command Control console as applicable.</td>
</tr>
<tr>
<td>View Access Control Objects</td>
<td>View the Access Control and Command Control objects.</td>
</tr>
<tr>
<td>Manage Access Control and Command Control Objects</td>
<td>Configure the resources and credentials in the command control rules. This implies you have read permission to prvrdvlt module.</td>
</tr>
</tbody>
</table>

Agent Management Permissions

The following permissions can be assigned to the agent management module.
### Descriptive Permissions

| All permissions on Agent Management | Have permissions to perform all operations. This implies you have “*” permission to Agent management. |
| View the listed agents and perform administrative actions | View the listed agents and perform administrative actions. This implies you have administrator permission to unifi module. |
| View Host Console | View the Hosts console. This implies you have console permission to unifi module. |
| Check agents status using command line utility | Check agents status using command line utility. |
| Allow addition of Agents and Domains directly from the command line during registration | Allow addition of Agents and Domains directly from the command line during registration. |
| Allow creation of Agent records during registration | Allow creation of Agent records during registration. |
| Allow creation of Domain records during registration | Allow creation of Domain records during registration. |

### Audit Reports Permissions

The following permissions can be assigned to the auditing module to control access to the Reports console. For a group to manage auditing, the group also needs read permission to the auditing and authentication modules.

<table>
<thead>
<tr>
<th>Descriptive Permissions</th>
<th>Allows users to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Permissions on audit reports</td>
<td>Have permissions to perform all operations. This implies you have “*” permission to audit reports.</td>
</tr>
<tr>
<td>View audit sessions and manage settings</td>
<td>View the Compliance Auditor console. This implies you have console permission to secaudit module.</td>
</tr>
<tr>
<td>View Reports Console</td>
<td>View the Reports console. This implies you have the console permission for audit module.</td>
</tr>
<tr>
<td>View audit sessions</td>
<td>Read the audit database. You must use console along with read. This implies you have read permission for audit module.</td>
</tr>
<tr>
<td>Create new audit reports and adjust filter settings in reports</td>
<td>Read and update the reports defined in the Reports console. This role is only useful when used in conjunction with the report permission.</td>
</tr>
<tr>
<td>View command control reports</td>
<td>Read and update the reports defined in the Reports console. This role is only useful when used in conjunction with the report permission.</td>
</tr>
<tr>
<td>View change log reports</td>
<td>View Account Logon reports. In conjunction you must use console and read permission. This implies you have logon permission for audit module.</td>
</tr>
</tbody>
</table>
You can use these Audit Report permissions 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 permissions 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 permissions 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 permissions 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 not 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 specify them here. The console does not provide any error checking, so you need to ensure to specify the valid name.
Compliance Audit Reports Permissions

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

<table>
<thead>
<tr>
<th>Descriptive Permissions</th>
<th>Allows users to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Permissions on Compliance Auditor</td>
<td>Perform the console, audit, and admin permissions. This implies you have “*” permission to <code>secaudit</code> module.</td>
</tr>
<tr>
<td>Add and modify audit rules in Compliance Auditor</td>
<td>View and edit records. This implies you have audit permission to <code>secaudit</code> module. Access reports with the report defined permissions. This implies you have report permissions to <code>audit</code> module.</td>
</tr>
<tr>
<td>View Compliance Auditor console</td>
<td>View the Compliance Auditor console. This implies you have console permission to <code>secaudit</code> module.</td>
</tr>
<tr>
<td>View and edit records in Compliance Auditor</td>
<td>Access the records collected by audit rules with this permission defined in the <code>Modify Audit Rule</code> page. This implies can choose your own name for the permission in the <code>secaudit</code> module.</td>
</tr>
</tbody>
</table>

Credential Vault Permissions

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

<table>
<thead>
<tr>
<th>Descriptive Permissions</th>
<th>Allows users to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Permissions on Credential vault</td>
<td>Have permissions to perform all operations. In conjunction you have to use <code>cmdctrl</code> module with admin permission. Must be used in conjunction with <code>userreqdashboard</code> module and admin role. This implies you have “*” permission to <code>prvcrdvlt</code> module.</td>
</tr>
</tbody>
</table>
### Descriptive Permissions

<table>
<thead>
<tr>
<th>Permission</th>
<th>Allows users to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>View, Add and Modify Resources and Credentials in Credential Vault</td>
<td>View, add, and modify the domains and credentials in Credential Vault.</td>
</tr>
<tr>
<td></td>
<td>Must be used in conjunction with userreqdashboard module and admin role.</td>
</tr>
<tr>
<td></td>
<td>To add, modify, delete scripts user requires module taskmanager in conjunction with the admin role.</td>
</tr>
<tr>
<td></td>
<td>This implies you have admin permission to prvcrdvlt module.</td>
</tr>
<tr>
<td>View Credential Vault Console</td>
<td>View the Credential Vault console. This implies you have console permission to prvcrdvlt module.</td>
</tr>
<tr>
<td>View Resources and Credentials in Credential Vault</td>
<td>View the resources and credentials in Credential Vault.</td>
</tr>
<tr>
<td></td>
<td>You must use console role along with read role to view the Credential Vault console and its content.</td>
</tr>
<tr>
<td></td>
<td>This implies you have read permission to prvcrdvlt module.</td>
</tr>
<tr>
<td>Add and Modify Resources and Credentials in Credential Vault</td>
<td>Add and modify the resources and credentials in Credential Vault.</td>
</tr>
<tr>
<td></td>
<td>Must be used in conjunction with the prvcrdvlt read role.</td>
</tr>
<tr>
<td></td>
<td>This implies you have write permission to prvcrdvlt module.</td>
</tr>
<tr>
<td>Application SSO Administration</td>
<td>Add and modify the resources of Application SSO credentials in Credential Vault.</td>
</tr>
</tbody>
</table>

### Package Distribution Permissions

The following permissions can be assigned to the host module in order to control access to the Package Distribution console. Select from the following permissions when creating a group to manage the packages.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Allows users to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricts Deployment of Packages to Specified Modules</td>
<td>Restricts deployment of packages to specified modules. This implies you have permission to distrib module.</td>
</tr>
<tr>
<td>Install or patch the Administration Manager (admin)</td>
<td>This implies you have install or patch permission to admin module.</td>
</tr>
<tr>
<td>Install or patch the Application Single Sign-On Manager (appssso)</td>
<td>This implies you have install or patch permission to appssso module.</td>
</tr>
<tr>
<td>Install or patch the Audit Manager (audit)</td>
<td>This implies you have install or patch permission to audit module.</td>
</tr>
<tr>
<td>Descriptive Permissions</td>
<td>Allows users to...</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Install or patch the Authentication Manager (auth)</td>
<td>This implies you have install or patch permission to auth module.</td>
</tr>
<tr>
<td>Install or patch the Access Control (Command Control) Manager (cmdctrl)</td>
<td>This implies you have install or patch permission to cmdctrl module.</td>
</tr>
<tr>
<td>Install or patch the Database Monitoring Manager (dbaudit)</td>
<td>This implies you have install or patch permission to dbaudit module.</td>
</tr>
<tr>
<td>Install or patch the Package Distribution Agent (distrib)</td>
<td>This implies you have install or patch permission to distrib module.</td>
</tr>
<tr>
<td>Install or patch the LDAP Agent (ldapagnt)</td>
<td>This implies you have install or patch permission to ldapagnt module.</td>
</tr>
<tr>
<td>Install or patch the Messaging Component Agent (msgagnt)</td>
<td>This implies you have install or patch permission to msgagnt module.</td>
</tr>
<tr>
<td>Install or patch the Package Manager (pkgman)</td>
<td>This implies you have install or patch permission to pkgman module.</td>
</tr>
<tr>
<td>Install or patch the Privileged Credentials Manager (prvcrdvlt)</td>
<td>This implies you have install or patch permission to prvcrdvlt module.</td>
</tr>
<tr>
<td>Install or patch the RADIUS Agent (radiusagnt)</td>
<td>This implies you have install or patch permission to radiusagnt module.</td>
</tr>
<tr>
<td>Install or patch the RDP Relay Module (rdprelay)</td>
<td>This implies you have install or patch permission to rdprelay module.</td>
</tr>
<tr>
<td>Install or patch the Registry Agent (regclnt)</td>
<td>This implies you have install or patch permission to regclnt module.</td>
</tr>
<tr>
<td>Install or patch the Registry Manager (registry)</td>
<td>This implies you have install or patch permission to registry module.</td>
</tr>
<tr>
<td>Install or patch the Resource Request Agent (resreqagnt)</td>
<td>This implies you have install or patch permission to resreqagnt module.</td>
</tr>
<tr>
<td>Install or patch the Access Control (Command Control) Agent. (revec)</td>
<td>This implies you have install or patch permission to revec module.</td>
</tr>
<tr>
<td>Install or patch the Compliance Auditor. (secaudit)</td>
<td>This implies you have install or patch permission to secaudit module.</td>
</tr>
<tr>
<td>Install or patch the SSH Agent. (sshtagnt)</td>
<td>This implies you have install or patch permission to sshagnt Agent module.</td>
</tr>
<tr>
<td>Install or patch the SSH Relay Module. (sshrelay)</td>
<td>This implies you have install or patch permission to sshrelay module.</td>
</tr>
<tr>
<td>Install or patch the Store and Forward Agent. (strfwd)</td>
<td>This implies you have install or patch permission to strfwd module.</td>
</tr>
<tr>
<td>Install or patch the System Information Agent. (sysinfo)</td>
<td>This implies you have install or patch permission to sysinfo module.</td>
</tr>
<tr>
<td>Install or patch the Syslog Emitter. (syslogemit)</td>
<td>This implies you have install or patch permission to syslogemit module.</td>
</tr>
</tbody>
</table>
### Package Manager Permissions

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:

<table>
<thead>
<tr>
<th>Descriptive Permissions</th>
<th>Allows users to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install or patch the Password Management Module. (taskmanager)</td>
<td>This implies you have install or patch permission to taskmanager module.</td>
</tr>
<tr>
<td>Install or patch the Video Offload Manager. (videoprocessor)</td>
<td>This implies you have install or patch permission to videoprocessor module.</td>
</tr>
</tbody>
</table>

### Password Management Permissions

The following permissions can be assigned to the task manager module in order to view and modify scripts.

<table>
<thead>
<tr>
<th>Descriptive Permissions</th>
<th>Allows users to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Permissions on Package Manager console</td>
<td>Have permissions to perform all operations. This implies you have “*” permission to audit reports.</td>
</tr>
<tr>
<td>Manager Packages in Package repository</td>
<td>View the Package Manager console. This implies you have console permission to pkgman module.</td>
</tr>
<tr>
<td>View Package Manager Console</td>
<td>View, add, update, or remove packages. This implies you have admin permission to pkgman module.</td>
</tr>
</tbody>
</table>

### User and Group Manager Permissions

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

<table>
<thead>
<tr>
<th>Descriptive Permissions</th>
<th>Allows users to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Permissions on Framework user manager console</td>
<td>Have permissions to perform all operations. This implies you have “*” permission to auth module.</td>
</tr>
<tr>
<td>Manage Users and Groups in Framework</td>
<td>Add or delete users and groups, and assign users to groups. This implies you have admin permission to auth module.</td>
</tr>
<tr>
<td>Descriptive Permissions</td>
<td>Allows users to...</td>
</tr>
<tr>
<td>------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>View Users and Groups Management console</td>
<td>View the Users and Groups Management console. This implies you have console permission to auth module.</td>
</tr>
<tr>
<td>Modify Attributes of Framework Users and Groups</td>
<td>Modify account settings.</td>
</tr>
<tr>
<td></td>
<td>You must use admin role to view the Framework User Manager and its content.</td>
</tr>
<tr>
<td></td>
<td>This implies you have act_settings permission to auth module.</td>
</tr>
<tr>
<td>Add or Remove Permissions in Framework</td>
<td>Read the auth database.</td>
</tr>
<tr>
<td></td>
<td>You must use console role along with read role to view the Framework User Manager and its content.</td>
</tr>
<tr>
<td></td>
<td>This must be used with all other auth permissions.</td>
</tr>
<tr>
<td></td>
<td>This implies you have read permission to auth module.</td>
</tr>
<tr>
<td>View and Modify Super Users and Groups with Super Role in Framework</td>
<td>Add or remove permissions.</td>
</tr>
<tr>
<td></td>
<td>You must use console role along with read and admin role to view the Framework User Manager and its content.</td>
</tr>
<tr>
<td></td>
<td>This implies you have admin permission to auth module.</td>
</tr>
<tr>
<td>Modify Account Settings in Framework</td>
<td>Modify superusers, and view and modify groups with the super role defined. This role should also be able to add or delete users and groups, and assign users to groups.</td>
</tr>
<tr>
<td></td>
<td>This implies you have super permission to auth module.</td>
</tr>
<tr>
<td>View Framework Users and Groups</td>
<td>View superusers, and view groups with the super role defined.</td>
</tr>
<tr>
<td>Generate API Tokens</td>
<td>Generate API tokens. This implies you have api_token permission to auth module.</td>
</tr>
</tbody>
</table>

**User Access Requests Permissions**

The following permissions can be assigned to control access to the Requests console. Select from the following permissions when you are creating a group to manage the Requests.
### 3.1.5 Deleting a User Group

1. On the home page of the console, click Users > Users & Groups and select the group you want to delete from the left pane.
2. Click delete icon.
3. Click Yes to confirm the deletion.

### 3.2 Managing Users

When you add a new user, the user cannot access any of the Privileged Account Manager 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 permissions, 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 permissions. 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.

- Section 3.2.1, “Adding a User,” on page 51
- Section 3.2.2, “Modifying User,” on page 51
- Section 3.2.3, “Removing a User from a User Group,” on page 53
- Section 3.2.4, “Deleting a User,” on page 53
3.2.1 Adding a User

When you add a 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 Privileged Account Manager console. You can change this setting for individual users by using the Edit User option.
- The user cannot access any of the Privileged Account Manager consoles until you have added the user to a group with the required permissions defined. For more information, see Section 3.2.2, “Modifying User,” on page 51 and Section 3.1.4, “Configuring Permissions,” on page 41.

To add a new user:

1. Click Users on the home page of the console.
2. Click Create User, task pane is displayed.
3. In the General page, specify a name of the user in the User Name field and a password for the user in the Password field.
4. Specify the password in the Confirm Password field for confirmation.
5. (Optional) Set the slider to the right if you want to Change Password at Next Login. This invalidates the user’s current password immediately, forcing the user to change it on the next login.
6. (Optional) Set the slider to Disable Account to deactivate a user account.
7. (Optional) Set the slider to elevate the user as Super User.

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.

8. (Optional) Set the Inactive Session timeout in minutes.
9. (Optional) Click Next to proceed to configure additional settings for the user’s account.

3.2.2 Modifying User

The Edit User option allows you to override the default account settings for an individual user. It 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 user account:

1. Click Users on the home page of the console.
2. Select the preferred user.
3. Click Edit icon.
4. Change the following settings as required:
General

4a Edit Password: Select this option to change the current password.

4b Change Password at Next Login: Select this option to enable a prompt for changing password when a user logs in.

4c Disable Account: Select this option to disable the user’s account.

4d Last Successful Login: Displays the time stamp of last successful login.

4e Last Unsuccessful Login: Displays the time stamp of last unsuccessful login.

4f Super User: You can use this option to make the user as Super user during creation. You can add the user to a group later.

4g Bad Logons: The number of unsuccessful logons attempted by the user.

4h Reset Bad Logon Count: Use this option to reset the count to 0.

5 To configure additional options, click Next. The Membership page is displayed:

5a Add the user to the listed groups. You can also search for the groups using the Search icon.

6 Click Next. The Details page is displayed.

6a 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.

6b Email: Specify the user’s e-mail address. If an e-mail address is defined here, it can also be used in Command Control.

6c Staff ID: Specify the user’s staff ID, for example, the user’s unique company identifier.

6d Telephone Number: Specify the user’s telephone number. If a telephone number is defined here, it can also be used in Command Control.

6e Description: Specify a detailed description in the text box.

7 Click Next. The Password Validation and Timeout page is displayed.

7a Set the slider to the right to Modify Default User Settings.

7b Lock Account after This security setting determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out.

7c Password Validation: Allows you to define the minimum number of alphabetic and numeric characters required in the user’s password. 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.

7d Timeout: Allows you to define the time limit in days required for either disabling or deleting the user account if it remains in inactive state.

8 Click Save.
Modify User: Groups

To assign a user to one or more groups:

1. Click Users on the home page of the console.
2. Select the user group you want to modify, and click Edit Group. The Edit Group page is displayed.
3. Click Sub Groups.
4. Select the preferred groups to assign this user.
5. Click Save.

3.2.3 Removing a User from a User Group

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

1. Click Users on the home page of the console.
2. Select the group you want to remove from the user’s account.
3. Click Delete Group icon next to the group you selected to delete.
4. Click Yes in the confirmation dialog box. The user is removed.

3.2.4 Deleting a User

1. Click Users on the home page of the console.
2. In the Users task pane, select the user you want to delete.
3. Click Delete User in the task pane.
4. Click Yes in the confirmation dialog box. The user is deleted.

3.3 Changing a User’s Password

Users can change their own passwords and if a user belongs to a group with the appropriate auth permissions defined (see Section 3.1.4, “Configuring Permissions,” on page 41), they can also change other users’ passwords by using the Edit User option.

To change your own password:

1. Click Users > Edit User.
2. In the General page, click Edit Password.
3. In the 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 Save.
3.4 Assigning Permissions for LDAP Users

LDAP users (Windows Directory, NetIQ eDirectory, or OpenLDAP) can get administration privileges on Privileged Account Manager through their LDAP group membership. To achieve this, see Section 4.1, “Configuring LDAP Server Settings,” on page 55. Assign the permissions 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 permissions for LDAP users by mapping those LDAP groups in the Privileged Account Manager framework.

For more information on mapping, refer to Step 6 on page 41 in “Modifying a User Group” on page 40.

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

Through external authentication, Privileged Account Manager adds the following capabilities:

- **Authentication through an LDAP system**: LDAP user authentication is the process of validating a username and password combination with a directory server such as Windows Active Directory, NetIQ eDirectory, and OpenLDAP.

- **Multifactor authentication**: Privileged Account Manager integrates with NetIQ Advanced Authentication to provide secure access to the following resources by using multi-factor authentication methods:
  - Privileged Account Manager endpoints (systems, applications, databases, keys)
  - Administration Console
  - Privileged credential to connect to a server (credential checkout and shared key checkout)
  - Authentication through third-party RADIUS servers, such as Duo, RSA, Gemalto, and Yubico

This section includes the following information:

- Section 4.1, “Configuring LDAP Server Settings,” on page 55
- Section 4.2, “Advanced Authentication,” on page 58
- Section 4.3, “Configuring RADIUS Server Settings,” on page 64
- Section 4.4, “OAuth2,” on page 65

### 4.1 Configuring LDAP Server Settings

- Section 4.1.1, “Exporting the Certificate From the Active Directory Server,” on page 56
- Section 4.1.2, “Exporting the Certificate From the NetIQ eDirectory Server,” on page 57
- Section 4.1.3, “Importing Active Directory or eDirectory Certificates on RHEL or SLES Servers,” on page 57

You can configure multiple LDAP Servers using the **LDAP Servers** settings page.

- Click **Settings > LDAP Servers** on the home page of the console. In the **External Services** page click **Add New** and specify the following fields:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Enter the Domain Name.</td>
</tr>
<tr>
<td>Type</td>
<td>Select from the three drop down list</td>
</tr>
<tr>
<td></td>
<td>- Windows Active Directory</td>
</tr>
<tr>
<td></td>
<td>- NetIQ eDirectory</td>
</tr>
<tr>
<td></td>
<td>- OpenLDAP</td>
</tr>
</tbody>
</table>
4.1.1 Exporting the Certificate From the Active Directory Server

You must export the CA certificate from the Active Directory server and import it to your PAM manager server to enable communication over Secure Sockets Layer (SSL).

1. Log in to Active Directory domain server as a domain administrator.
2. In the Active Directory server, launch the Certificate Authority application using Start | Run | certsrv.msc.
3. Right click the Certificate Authority you created and select Properties.
4. Click General > View Certificate.
5. Select Copy to File from the Details tab.
6. Follow the wizard prompts and select the DER Encoded binary X.509 (.cer) format.
7. Click browse and specify a path and filename to save the certificate.
4.1.2 Exporting the Certificate From the NetIQ eDirectory Server

You must export the CA certificate from the NetIQ eDirectory server and import it to your PAM manager server to enable communication over Secure Sockets Layer (SSL).

1. Log in to iManager as an admin user.
2. On the iManager console, navigate to Roles and Tasks.
4. Click Next without selecting any option on the page.
5. Click Certificates.
6. Enable the check box next to the certificate you want to export.
7. Click Export. The certificate is typically marked as Organizational CA.
8. Select the certificate from Certificates drop down list.
9. De-select Export private key and select base64 as the Export format.
10. Click the link Save the exported certificate to save the exported certificate.
11. Rename the saved file with .cer extension for easy identification.

4.1.3 Importing Active Directory or eDirectory Certificates on RHEL or SLES Servers

For importing certificates on RHEL server:

1. Copy the rootCA.cer certificate file to /etc/pki/ca-trust/source/anchors/ directory.
2. Run the update-ca-trust extract command to update the system certificates.

For importing certificates on SLES server:

1. Copy the rootCA.cer certificate file to /etc/pki/trust/anchors directory.
2. Run the update-ca-certificates command to update the system certificates.

**NOTE:** If you are using an older version of the operating system, use the below commands:

1. The LDAP CA certificate must be placed in the /etc/ssl/certs/ folder
2. Run command c_rehash.

The c_rehash command is deprecated in newer versions of Linux operating system.

**TIP:** In case you face any issue, ensure that host names used in certificates are resolvable from your PAM manager server to the target LDAP server.
4.2 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. 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.

**NOTE:** Advanced Authentication with Access Control is supported only for LDAP users.

4.2.1 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 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.

Multi factor authentication is one of the steps to the Zero Trust model.

4.2.2 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:
<table>
<thead>
<tr>
<th>Term</th>
<th>Usage in Advanced Authentication</th>
<th>Usage in Privileged Account Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository</td>
<td>Used for storing user information. This information can be retrieved from any LDAP directory such as eDirectory, and Active Directory.</td>
<td>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 Settings &gt; LDAP Server configuration, the repository name must be the same as the domain name mentioned in the Credential Vault. For more information, see Section 4.1, “Configuring LDAP Server Settings,” on page 55. <strong>NOTE:</strong> 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.</td>
</tr>
<tr>
<td>Methods</td>
<td>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.</td>
<td>The chains must be a combination of only the supported methods. If there is a combination of supported and unsupported methods, the user authentication is unsuccessful.</td>
</tr>
<tr>
<td>Chain</td>
<td>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.</td>
<td>Privileged Account Manager uses a single endpoint for primary and backup servers. <strong>NOTE:</strong> Privileged Account Manager facilitates adding the endpoint to the Advanced Authentication server. This endpoint must be available to create an event.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Used for identifying a device or server that contains a database.</td>
<td></td>
</tr>
</tbody>
</table>
### 4.2.3 Checklist to Follow Before Enabling Secondary Authentication

- To integrate Advanced Authentication, you must install NetIQ Advanced Authentication 6.0 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.

### 4.2.4 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 Settings > LDAP Servers of Privileged Account Manager console.

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.

**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 Section 4.2.6, “Configuring Advanced Authentication Server Settings,” on page 62.

6 In Advanced Authentication server, edit the event for Privileged Account Manager and add the same endpoint in Endpoints Whitelist.

### 4.2.5 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.
4.2.6 Configuring Advanced Authentication Server Settings

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. Click **Settings > External Services** from the home page of the Privileged Account Manager Console, and then click **NetIQ Advanced Authentication**.

2. In the right pane, specify the **Advanced Authentication Configuration** details:
   - **Hostname/IP Address and Port Number**: 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 already existing as repository in 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:
     - **LDAP Password**: This is the default option selected. Use this option for all other certified Section 4.2.5, “Supported Authentication Methods,” on page 61.
     - **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**.

   - **Retrieve Authorization Attributes from LDAP Server**: By default this option is enabled.
     Ensure that the domain name configured in Advanced Authentication matches with the domain name of LDAP Server configured in Privileged Account Manager. Move the slider to the left if you do not want to retrieve the authorization attributes from the LDAP server.
4.2.7 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 Section 4.2.3, “Checklist to Follow Before Enabling Secondary Authentication,” on page 60. 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

4.2.8 Secondary Authentication Server Setting

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, Section 4.2.7, “Enabling Advanced Authentication for Privileged Access,” on page 63. 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 policy. 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 policies. To enforce this global policy perform the following procedure:

1. On the home page of the administration console, click Settings > Server Settings > Authentication.
2. In the details pane, move the Secondary Authentication Required slider to the right.
4.2.9 Enabling Advanced Authentication for Privileged Account Manager

You can enable Advanced Authentication for the Privileged Account Manager to allow access only to the users who pass the secondary authentication.

To enable Advanced Authentication, Privileged Account Manager administrator must perform the following:

1. On the home page of the Privileged Account Manage console, click **Settings > Server Settings > Authentication**.

2. In the right pane, move the **Secondary Authentication Required** slider to the right.
   - To use this, ensure that Netiq Advanced Authentication is enabled.
   - This setting ensures that the users are prompted for secondary authentication to log into the Administration Console.

3. **Inactivity Session Timeout**: Set the time in minutes to timeout the session when in inactive state.

4.3 Configuring RADIUS Server Settings

On a UNIX or Windows server, a RADIUS Server is a background process that operates. It enables you to keep track of user profiles in a main database. As a result, if you have a RADIUS Server, you can decide who can access your network. NetIQ Privileged Account Manager also supports a variety of MFA products such as RADIUS protocol support, including Duo, RSA, Gemalto, and Yubico.

The RADIUS Client makes requests to the RADIUS Server whenever a user tries to connect to it. Only once the RADIUS Server authenticates and approves the user can establish a connection to the RADIUS Client.

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 Privileged Account Manager environment, you must add a backup Privileged Account Manager Linux manager to the deployment.

- If Advanced Authentication is configured and you want to configure Privileged Account Manager 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 **Settings**.
2. Click **External Services > RADIUS Server**.
3 In the right pane, specify the **RADIUS Server Configuration** details:

- **Hostname/IP Address and Port Number**: Specify the hostname or IP address of the RADIUS and the port where the RADIUS authentication request is sent. The default port is 1812 server.
- **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.
- **Retrieve authorization attributes from LDAP server**: Move the slider to left if you want to disable this option. Setting this to enable, retrieves authorization attributes from the LDAP server.

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.

### 4.4 OAuth2

OAuth2 is an authorization framework that grants restricted access to the protected resource. In this framework, the client delegates authentication to an authorization server and obtains the access token to grant access to an application or a web service. The client can be web applications, mobile phones, hand-held devices, and desktop applications.

While using the OAuth2 framework, the OAuth server validates users and grants access to the corresponding account of Privileged Account Manager. Here, Privileged Account Manager serves as the OAuth2 client.

In order for OAuth 2.0 to be used, the Client must first obtain its own credentials from the Authorization Server, a client id and client secret, in order to identify and authenticate itself when requesting an Access Token.

The Client, such as a smartphone app, website, smart TV app, desktop programme, etc., initiates access requests using OAuth 2.0. This is the usual flow for the token request, exchange, and response:

The Client submits an authorization request (authorization request) to the Authorization server along with the client id, client secret, scopes, and an endpoint URI (redirect URI) to which the Access Token or the Authorization Code should be sent.
The Authorization server validates the Client’s identity and confirms that the requested scopes are legal.

### 4.4.1 OAuth2 Roles

OAuth2 consists of the following four roles:

- **Resource Owner**: A system or a person (end-user) who owns the resource and grants access to it.
- **Resource Server**: A server that hosts the protected resources. It accepts and validates requests from the Client to grant access to the resource.
- **Client**: An application that requests and gets authorization on behalf of the resource owner to access the protected resource. For example, Privileged Account Manager.
- **Authorization Server**: A server that provides access tokens to the Client after validating the resource owner and obtaining authorization. For example, Advanced Authentication server.

The following diagram describes the flow of authorization:

*Figure 4-1  Flow of Authorization Code*

When a resource owner wants to access the client website or application, the following steps describe the flow of authorization code:

1. PAM initiates the flow and directs the user agent of the resource owner to the authorization server. PAM includes its client identifier, requested scope, local state, and a redirection URI.
2. The authorization server authenticates the resource owner through the user agent and recognizes whether the resource owner grants or denies the access request.
3 If the resource owner grants access, PAM uses the redirection URI provided earlier to redirect the user agent back to the corresponding account or resource. The redirection URI includes an authorization code and any local state previously provided by PAM.

4 PAM requests an access token from the authorization server through the token endpoint. Then PAM authenticates with its client credentials and includes the authorization code received in the previous step. PAM also includes the redirection URI used to obtain the authorization code for verification.

5 The authorization server validates the client credentials and the authorization code. The server also ensures that the redirection URI received matches the URI used to redirect the client in Step 3. If valid, the authorization server responds back with an access token.

### 4.4.2 OAuth2 Server Settings

To integrate Privileged Account Manager with OAuth2 server, it is necessary to configure the authorization server details in Privileged Account Manager. You can fetch the OSP OAuth server cfg using the API: `curl --insecure https://10.71.16.158/osp/a/TOP/auth/oauth2/.well-known/oauth-authorization-server`

**NOTE:** Privileged Account Manager 4.2 supports only the Advanced Authentication server as the OAuth2 server. In the upcoming releases, support will extend for other authorization servers. Also, PAM can leverage Risk Service configured in Advanced Authentication.

**NOTE:** You can obtain the following details while configuring the OAuth2 authorization server.

To configure the authorization server details, perform the following:

1. Click **Settings > External Services > OAuth2 Server** on the Privileged Account Manager console.
2. Specify the following details:
### Client Configuration

- **Client ID**: A unique ID that is generated when you configure the authorization server.
- **Client Secret**: A unique value that is generated when you configure the authorization server. This value is shared between the OAuth client (Privileged Account Manager) and the authorization server.
  
  Select [Edit Secret](#) to edit the Client Secret post integration with the authorization server.

### Server Endpoints

- **OAuth2 Authorization Login URL**: Login URL of the authorization server to prompt the users for authentication and directs to the Redirect URL. Login URL must be specified in the following format:
  
  ```
  https://<authorization server ip address>/osp/a/TOP/auth/oauth2/grant
  ```

- **OAuth2 Token URL**: Token URL that the client uses to initiate the request. This token is issued by the authorization server. Token URL must be specified in the following format:
  
  ```
  https://<authorization server ip address>/osp/a/TOP/auth/oauth2/token
  ```

- **OAuth2 User Info URL**: An endpoint from where you can retrieve the user information after authentication. User info URL must be specified in the following format:
  
  ```
  https://<authorization server ip address>/osp/a/TOP/auth/oauth2/userinfo
  ```

- **OAuth2 Logout URL**: URL that logs the user out of authentication session. Logout URL must be specified in the following format:
  
  ```
  https://<authorization server ip address>/osp/a/TOP/auth/oauth2/logout
  ```

- **Enforce OAuth for Web Authentication**: The OAuth authentication framework is applied for web-based applications by default. With this option disabled, the administrator allows users to the web console login by other external authentication that is configured, such as LDAP, RADIUS, and so on. Users can log in with the URL `https://<privileged-account-manager-ipaddress>/pam`.

  **NOTE**: This option does not apply to local users, ssh relay, and credential providers.
4.4.3 Integrating with NetIQ Advanced Authentication and Risk Service Using the OAuth2 Settings

Using the OAuth2 framework, you can integrate NetIQ Advanced Authentication with Privileged Account Manager to use multi-factor authentication and utilize Risk Service capabilities. Advanced Authentication delivers various authentication mechanisms that enable identity assurance in addition to typical username and password-based authentication. Risk Service evaluates the contextual information associated with an access attempt, detects unknown risks, and takes necessary action based on the defined rules.

The Risk Service allows you to accomplish the following:

- Prevent fraudulent access to a web application or network and improve its security.
- Determine the level of risk based on several criteria and user behavior patterns (for example, browser type, time of login).
- Enhance the user experience. Users are only required to give additional information for authentication when the associated risk is high.

The Risk Service also facilitates in detecting different malicious activities listed in Integrating with ArcSight Intelligence.

To integrate Privilege Account Manager with Advanced Authentication, perform the following tasks:

- “Configuring the Advanced Authentication OAuth 2.0 Event” on page 70
- “Configuring the OAuth2 Server Settings in Privileged Account Manager” on page 70

Prerequisite

Ensure that Advanced Authentication 6.3.5.1 and later versions with the supported version of Risk Service are installed and configured.


Configuring the Advanced Authentication OAuth 2.0 Event

1. Open the Advanced Authentication Administration portal.
2. Click Events > New Event.
3. Specify a name for the event.
4. Select OAuth2 from Event type.
5. Select the required chains to assign to the event.
6. In Risk Policy, select the policy that you want to assign to this event for assessing the risk associated with a login attempt.
7. Click Create New Policy to create a new risk policy for this event.


8. In Redirect URIs, specify https://<privilege-account-manager-ipaddress>/sso. After successful authentication, users are directed to this URL.
   If there are multiple PAM managers, you can specify all URLs as the Redirect URI. So, users can access the preferred instance of PAM.
   For example, if there two PAM managers https://www.pam-abc.com/sso and https://pam-123/sso, specify both the URLs in Redirect URIs.

   **NOTE:** The Client ID and Client secret are generated automatically. You cannot view the Client secret later, therefore you must make a note of this value as these are required to complete the configuration in Privileged Account Manager.

9. Click Save.

Configuring the OAuth2 Server Settings in Privileged Account Manager

1. Log in to the Privileged Account Manager console.
2. Navigate to Settings > External Services > OAuth2 Server.
3. Specify the Client ID and Client Secret that are generated while configuring the OAuth2 event in Advanced Authentication.
4. Specify login URL of the Advanced Authentication server to direct the users for authentication in OAuth2 Authorization URL.

   **NOTE:** Privileged Account Manager 4.2 supports the Advanced Authentication server with OSP as the OAuth2 server. Therefore, examples include IP address of AA/OSP. In the upcoming releases, support will extend for other authorization servers.

   For example, https://<ip-address-or-dns-or-advanced-authentication>/osp/a/TOP/auth/oauth2/grant
5. Specify the token URL that initiates the authentication request in **OAuth2 Token URL**.
   For example, https://<ip-address-or-dns-or-advanced-authentication>/osp/a/POP/auth/oauth2/token

6. Specify the location from where the information of users are retrieved post authentication in **OAuth2 User Info URL**.
   For example, https://<ip-address-or-dns-or-advanced-authentication>/osp/a/POP/auth/oauth2/userinfo

7. Specify the URL to log users out of the authentication session in **OAuth2 Logout URL**.
   For example, https://<authorization server ip address>/osp/a/POP/auth/oauth2/logout

8. Retain default settings for **Enforce OAuth for Web Authentication** and **Retrieve authorization attributes from LDAP Server**.

9. Save the settings.

**NOTE:** After completing the configurations, you must map the LDAP servers to assign the browsing capability to User roles in **Access Control**.

**NOTE:** Use one of the following URLs to authenticate to Privileged Account Manager using the OAuth2 authorization protocol:

- Old console: https://pam_ip_or_dns/sso?console=legacy
- New console: https://pam_ip_or_dns/sso/
Privileged Account Manager stores credentials of privilege accounts, such as administrator accounts, to a secure central repository (vault). After the privileged credential is added to the vault, the users need to access their credentials through Privileged Account Manager. They get authenticated before checking out the privileged credentials, and their access is logged. After a user checks in the credential, it is reset to ensure that users cannot reuse it the next time and must check it out through Privileged Account Manager when they require the credential. Keeping privileged credentials in a secure and centralized vault enables you to perform the following tasks:

- Strongly protect the credentials
- Limit who has access to the credentials
- Track any unusual activity

Privileged Account Manager supports the following vault types:

- **Application configuration**: Configuration for application credential checkout and application SSO.
- **Database**: Configuration for database credential checkout.
- **Keys**: Configuration for Windows license keys, SSH, or host keys.
- **LDAP/Active Directory**: Configuration for all the directory servers.
- **UNIX/Linux/Network**: Configuration for Linux, Unix, network device configuration.
- **Windows**: Configuration for a Windows machine that is not part of any directory services.

Click **Privileged Account Manager > Credential Vault** to view all the vaults configured. Each vault provides a preview of the resources and credentials stored within.

### 5.1 Credential Vault

A credential vault is a storage location for shared accounts and resource credentials such as, user IDs and passwords. Privileged Account Manager uses the Enterprise Credential Vault database to manage and secure details and credentials of various domains. This solution helps you not to rely on a third party component for database as credential vault supports embedded database. A privileged user can use these credentials to connect to the endpoints such as systems, databases, and applications. You can encrypt this database. By default, the credentials are securely stored in an encrypted form. On the home page of the console, click **Credential Vault** to view all the credentials of the resources available in Privileged Account Manager.

#### 5.1.1 Adding a Resource in Credential Vault

1. On the home page of the console, click **Credential Vault**.
2. Click **+Add**.
3 Select one or more resources based on your requirement.

- **Application**
  - Applications
  - SSO
- **Certificate Issuer**
  - PKI
  - SSH
- **Cloud**
  - Amazon Web Services
- **Database**
  - Oracle
  - Microsoft SQL Server
  - MySQL Server
  - Sybase
  - PostgreSQL
  - MariaDB
  - IBM DB2
- **Key**
  - SSH Keys
  - Windows Keys
  - VMWare Keys
  - Custom Keys
- **LDAP/Active Directory**
  - Active Directory
  - NetIQ eDirectory
  - OpenLDAP
- **Linux/Unix/Network Device**
  - **SSH**: Select from the following Terminal types.
    - ansi
    - Linux
    - vt100
    - vt220
    - xterm
    - xterm-256color
  - Telnet
- **Windows**
  - Windows Host
Click Credential Vault > Resources > Name > Credentials to add the Username, Password and Privileged Type. Resource Details displays more information about the resource such as Resource Name, Type, and Extended Attributes.

Consider you have a number of resources and want to filter only specific type of keys. Select the resource from the left pane and you can view all the resource type on the right pane.

For more information about Resources, see “Resource Pools” on page 134.

To delete a resource, you can select the delete icon for the resource or select one or more resource for bulk deletion and click Delete.

To modify a resource, you can select the edit icon against the resource and modify.

**Adding Extended Attributes**

Extending the schema by defining the attributes for resources. These attributes help the resources to hold different values. You can filter and search resources based on the attributes. Consider you have a high number of similar type of Resources at a specific location, but there is no way to filter those resources. You could use extended attributes such as, location to filter out specific resources from specific location.

You can add these extended attributes by clicking Credential Vault > Extended Attributes. You can only add five attributes. After you add the extended attributes you can define them in the resources with values.

**NOTE:** At least one resource should be present only then the Extended Attributes button will be enabled.

Go to Resources > Add Resource. You can also click Extended Attributes icon on the right pane of Credential Vault tab from the home page of Privileged Account Manager. You can add only a maximum of five entries for extended attributes.

If you want to define the Extended Attribute for an existing resource:

1. Click the edit icon on the Resource name row. The Edit Resource page is displayed
2. Select Extended Attributes from the left pane.
3. Click Define. The extended attributes you have created are displayed.
4. Select the attribute/attributes that you want to add for the resource.
5. Click Define.
6. Define the value for the selected attributes.
   - If you have already mapped a value for a specific resource, it is displayed for you to select. If you are entering a new value, you can enter that at this point.
7. Click Finish.

The value you added and the Extended Attribute is updated and displayed in the Resources page.

**NOTE:** Another way to define Extended Attributes is when you are creating a Resource. Click Credential Vault > Resource > +Add and Save. The maximum attributes you can enter are five.
After you have defined the extended attributes, the values are displayed on the screen for easy filtering. For example, if you select the location attribute of Bangalore from the left pane of the console, the resources located in Bangalore are displayed on the right pane.

**NOTE:** You must always provide a unique value for the attribute.

### Modifying Extended Attributes

You can click single resource you wish to modify, or select multiple resources and update the extended attributes at one go.

**Bulk Modification**

Select the resource attributes you want to update from Credential Vault > Resource page. Click Modify Resource Attributes. Move the slider to the right to allow you to enter the value in the Enable Edit column, provide a value and click Save. The attribute is then applied for all the selected Resources. For example you have selected 100 resources and want to update the attribute value such as, department=finance, you can do this at one go. The attribute value will be applied to all the selected 100 resources as a batch update.

**NOTE:** When you click Modify Resource Attribute and do not define any value the attribute removes the previous value, if any.

### Deletion of Extended Attributes

You can either delete a single resource or select multiple resources and delete at one go.

**Bulk Deletion**

Select the resources for which you want to delete the resource attributes from Credential Vault > Resource page. Click Delete Resource Attributes. Select the attributes to be deleted from the Delete the Resource Attribute(s) page. Click Delete. The deletion now is applicable to all the selected Resources. For example you have selected 100 resources and want to delete the attribute value such as, location=India, you can do this at one go. The attribute value will be applied to all the selected 100 resources as a batch deletion.

### 5.1.2 Sample Use Cases

The following use case illustrates the work flow of Credential Vault user journey:

**Configuring Oracle Database Vault Type Using Credential Vault**

This use case helps you to configure the Oracle database vault type using the following procedure:

1. Click Credential Vault > Resources > +Add New and select the resource.
2. In the General tab, specify the name of the database. This name is used along with the Credential to authenticate. If you do not provide the correct domain name, user authentication fails.
Complete the details.

- **Connection Details**
  - **Connect String:** You can specify the string that will reset the password in the database and check in the password.
  - **Connect As:** Select SYSDBA. If you want Privileged Account Manager to perform the password check in process then, to check the connection to the database server, click Test Connection or select Default.

- **Password Change on Check in:**
  Based on the following selection the password of the application will be changed automatically every time a credential is checked in.
  - **Never**
    You can use this option if you do not want to change the password after every credential check-in.
  - **Delegate to Identity Manager**
    If you want to delegate the password check-in process to Identity Manager, select Delegate to Identity manager. Once a resource is created in Identity Manager, it gets synced to Privileged Account Manager. Resource permission is created in Privileged Account Manager but during check in and checkout password is rotated and handled by Identity Manager Driver Implementation guide on the PAM documentation page.

  **NOTE:** Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

  **NOTE:** Before you delegate password check-in to Identity Manager ensure that both the Privileged Account Manager IDM driver and database driver are operational.

  - **Internal**
    Use this option, if you want Privileged Account Manager to manage password change.
    Select the appropriate **Password Policy** that must be used when Privileged Account Manager generates a new password. By default Default Password Policy is selected. You can either modify the default password policy or create a new password policy.
    - **Password Policy**
      **NOTE:** Ensure not to use ‘%’, percentage character in the special characters list of the password policy.

    - **User Name**
    - **Password**

3 Click **Next**.
4 In the **Proxy Connector** tab, complete the details.
   - **Database IP Address**: Specify the IP address or the Host Name of the Database.
   - **Database Port**: Specify the Database port number.
   - **Connection Protocol**: Select TCP or TCPS.
   - **Database SSL Version**: In case you have selected TCPS, specify if it is **Any** Database SSL version, or the specific one from the dropdown list.
   - **DBAudit Servers**: You can either select **All** or **Selected** server. Specify the proxy port.

5 Click **Next**.

6 In the **Custom Attributes** tab, click **Add**.
   - In the **Name** field, specify the name of the custom attribute. For example, *Expiration date*.

7 In the **Value** field, specify the value for the attribute. For example, the date you want the entity to expire.

8 Repeat the steps through 4-6 for any other custom attributes you want to add.

9 Click **Next**.

10 In the **Extended Attributes** tab, click **+Define** and select the relevant attributes from the list.

11 Click **Finish**.

12 Enter Privileged Account Manager user credentials and log into the user interface.

13 Click **icon on Privileged Account Manager console** My Access > Checkouts icon against the Oracle resource.

14 A **Credential Checkout** pop-up page is displayed. Enter **Access Duration**, **Email ID**, and **Reason** for accessing the resource and click **Check Out**.

**NOTE**: From Privileged Account Manager 4.2 onwards, an option is provided for you to select the user or the role whose password can be checked out. To see this option, you must have added privilege type. Additionally you should have already enabled **Allow selection by user** option from **Access Control > Assignments > Permissions > Checkout Options** page. For more information see, Section 5.1.3, “Defining Privileged Type for a Credential,” on page 79.

15 Note the credentials provided and open Oracle server and enter the same credentials in the **Credential Checkout** page and click **sign in**. Now you are successfully logged into the AWS Database and can proceed with completing the tasks.

16 You can check-in the credentials after the use of the credentials using the following procedure.

   16a Enter Privileged Account Manager user credentials and log into the user interface.

   16b Click **icon on Privileged Account Manager console** My Access > Check-in icon against the Oracle resource. The message "Credentials Checked in successfully" is displayed. Now you can verify and note that you can no longer access the Oracle database using the earlier credentials.

      The administrator can monitor this activity by navigating to **Reports > Built-in Reports > Credential Checkouts** to access the report using the Privileged Account Manager console.
Selecting Resource and Credentials Using Filter

This resource filter feature simplifies search-ability in scenarios where there are 1000s of locations with more than 400 odd location-based networks.

Consider Mike, a network administrator. The operational equipment such as sensors, actors, and controller is located in the production network. Privileged Account Manager is located in both the office network and in the standard client. But there is no connection between office network and internal network. Mike requires access to a resource from the production network. He uses his network device to access Privileged Account Manager. He selects the credentials based on the three components of location, network, and resource. Consider Mike has 1000s of Resources based out of same location with the same application type. It gets challenging to select the specific resource. You can type the Resource type in the Find Types search field for easy filtering. You can also select a combination of Key Type, Location, and Department for further granular filtering.

Allowing Delegated Resource and Credential Creation

Consider Susan, a network administrator in a chemical plant. A resource is added in the production environment and Susan has to add that resource along with the credentials in Privileged Account Manager. She can define a privileged type for a single resource. She can categorize the credentials in the resource based on the attributes such as finance, HR, or engineering.

5.1.3 Defining Privileged Type for a Credential

You can assign a role for a credential. For example, consider that Luke is a Shift Leader of a chemical plant. What is the privileged role you want to assign to Luke based on his responsibilities? If you want to delegate both modify and delete permissions, you can assign an Admin role to Luke. In a similar way if Susan is a Shift Leader also in the chemical plant, to distinguish her role from Luke’s and based on her responsibilities, you can assign an Associate’s role to Susan. This is referred to as Privileged Type of the Resource. A string is associated with a credential and this value will be displayed during credential checkout. An administrator can restrict the credential based on the privileged type.

While checking out a credential, as an administrator you can select which role or user credential you want to check out.

NOTE: Privileged Type is mainly used for Check-in and Check-out for Application and Database. For other functions you can store it to use as a filter etc...

Follow the procedure to add the privilege type.

1 Go to Credential Vault.
2 Click an Application or Database credential count from the second column. The Credentials page is displayed.
3 Click + icon.
4 In the Add Credential page enter the User Name, Password and Privilege Type.
5 Click Add.

The credential gets listed under the Privilege Type column. These credentials are populated when you are checking out a resource’s credentials or if you want to change a specific user’s password from > My Access page.
View Policy

Clicking on the root path (/) allows you to View Policy.

You must click +Add Policy to create a policy for the specific resource group from the Policy and Path Details page. Specify the details in the Create Policy dialog box.

- **Name:** Specify a name for the policy.
- **+Add** Add the groups by selecting from Local or LDAP Groups.

The policy that you created will be applicable for the specific groups you have selected, ex: API users.

Create Path

Only if the user is a path administrator or a owner for a path, he will be able to view the respective path, else the user gets the “access denied” error. A user should be part of a permission to be able to view the path. To get the appropriate permission, create a user group with the following mandatory permissions. Go to Users, click edit to modify Permissions. Under Credential Vault, select the following:

- View Credential Vault Console
- View Resources and Credentials in Credential Vault
- Add and Modify Resources and Credentials in Credential Vault

You can create path using the following procedure:

1. Go to Credential Vault.
2. From the left pane, click +.
3. Add the Path name.
4. Add the groups by selecting from Local or LDAP Groups.
   - Enable Recursive if you want to populate the resources of the select path recursively.
5. Click Create.

Configuring Privilege Type

You can configure privilege type clicking Credential Vault > Resources. If you have defined credentials in the vault, you can use the credential as the privilege type. Edit any resource to define the privilege type. The privileged type attribute allows the user to access only certain privileges attributed to that role.

Follow the procedure to add the privilege type.

1. Go to Credential Vault.
2. Click an Application or Database credential count from the second column. The Credentials page is displayed.
3. Click + icon again the Resource Count column
4. In the Add Credential page enter the User Name, Password and Privilege Type.
5 Click Add.

The credential gets listed under the Privilege Type column. These credentials are populated when you are checking out a resource’s credentials or if you want to change a specific user’s password from > My Access page.

5.1.4 Encryption Methods in Credential Vault

Currently the default and the only encryption method in Credential Vault is AES-256 in CBC mode.

You can now use additional encryption methods in Credential Vault. If you want to set a specific encryption method globally, you can select the option from Settings > Server Settings Default Credential Vault Cipher field. These encryption methods are FIPS compliant ensuring both product security and seamless functionality, even when the product is switched to FIPS mode.

You can also set different encryption methods for different resources in the Credential Vault.

1 From the home page of the Privileged Account Manager, click Credential Vault.
2 Select the specific resource for which you want to set this option, for example: Windows Host.
3 Click the Edit icon to modify the credential’s details.
4 Select the encryption method for the resource using the Encryption Type drop down list.

NOTE: The selected cipher is used by default to all the new credentials.

5.2 Just In Time Access Framework

This section outlines the procedure needed to enable just-in-time (JIT) access for Amazon Web Services, and Public Key Infrastructure.

Organizations can grant enhanced privileged access to an application or system in real-time to both human and non-human users in order to carry out a necessary task by using the just-in-time (JIT) access approach. JIT access enables businesses to supply access so that users can only access privileged accounts and resources when they are actually needed. Organizations can employ JIT access to restrict access to a particular resource for a defined amount of time rather than allowing always-on (or standing) access (or standing access). By drastically lowering the time it takes a hacker or malicious insider to get access to privileged accounts before moving laterally through a system and acquiring unauthorized access to critical data, this granular method reduces the risk of privileged account abuse. The dangers of standing privileges are reduced by just-in-time access.

The following explains the difference between emergency access and Just-in-Time access:

Emergency Access Requests

When a user requires access to a privileged session, database server, or to application server but does not have rules defined, then they can request emergency access.
Just-in-time Access

Also known as JIT, is an essential cybersecurity process where users, applications, or systems are granted privileged access, only for a limited period of time on an as-needed basis. The user need not even have an existing account or access to a specific target.

5.2.1 The Principle of Least Privilege

We must comprehend the least privilege principle to appreciate the value of just-in-time access (PoLP). More entry points for cybercriminals are a consequence of giving users in an organization too much access. The industry discourages standing access for this reason.

With PoLP, you can only grant privileged access to a single resource or during a defined window of time with each grant. As a result, a malevolent insider has less leeway to maneuver and cause harm. Since most cyberattacks rely on abusing privileged accounts, PoLP generally lowers the likelihood of cybercrime. Additionally, when privileges expire, malware cannot spread as quickly.

5.2.2 Resource Types Supporting Different Types of Dynamic Secret

- A dynamic secret is a short-lived secret based on the Time-to-Live (TTL) value.
- A dynamic secret should not be a reconciled account. Reconcile account contains credentials that can be used to provision a dynamic secret. Example: AWS root password, SSH Certificate Authority are the Reconcile account credentials that will be used to provision dynamic credentials. These cannot be dynamic credentials.

5.3 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 the application or database for a fixed period.
- After every session, reset the account’s password in the target application to maintain password security.

A Privileged Account Manager administrator can create a privileged account for an application or database and save the application or 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 available for that application and 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 a shared account credentials by using the credential checkout feature.
5.3.1 Configuring Credential Checkout for Application and Database Type Credentials

You can map credentials to permissions. For more information about permissions, see “Permissions” on page 135.

This section is only for Application and Database checkout feature. When you click the Application or Database type resource from Credential Vault > Resources, a fly-out is displayed if you are creating a resource and credential for the first time. The Credentials tab requires you to add the privileged type for the respective credential. If you have already created a credential, click on the resource name and the resource details open in a fly-out and when you click on the Credential Count, a Credential fly-out is displayed.

To create a permission:

In Access Control (enable the Access Control Policy engine from Settings > Policy Engine > Server Settings), follow the below procedure.

1. Create a Resource Pool for Application/Database type. You can add resources to the Resource Pool. For more information see, “Configuring a Resource Pool” on page 144
2. Add a User Role. For more information see, “Configuring a User Role” on page 146
3. Create an Assignment and assign permissions for Application/Database credential type. For more information see, “Configuring Permissions” on page 148.
4. In the Access Control > Assignments > Permissions > Checkout Options page, select the options as required.
   - Allow Password Change During Check-in: Move the radio button to the right to enable this option. By default this option is set to disabled and does not allow user to change the password while checking in. Enabling this option allows you to change the password while check in and provides the following options.

   NOTE: For users upgrading from Privileged Account Manager 4.1 to 4.2 version, and want to continue using the same Check in and Check out behavior for credentials, do not enable the Allow Password Change During Check in option.

Whereas enabling the Allow Password Change During Check in is a new behavior of functionality from Privileged Account Manager 4.2 version onwards.

   - Credential Checkout Mode: Selected by System option allows system to select the user for checkout.
   - Allow Selection by User option allows you to select the user for which you want to perform password check-in and check-out function.
   - Credentials Allowed for Checkout This option allows you to either allow All credentials to perform Check in and Check Out function.

The Restrict Credentials to a Privilege Type option is only applicable if you have already defined privilege type and want to select for which user you want to change the password while check out. For more information about privilege type, see Section 5.1.3, “Defining Privileged Type for a Credential,” on page 79.
5.3.2 Configuring Credential Checkout for Applications

The privileged accounts that are set up on the following applications or database can be managed through Privileged Account Manager. To manage those accounts, you must customize the sample script and add it to the Privileged Account Manager rule.

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 the credential checkout feature for eDirectory, you can add the rules by using the eDirectory policy template.

Follow the procedure, after importing the vault:

**General:**

In the **General** tab, enter the name, example: *DOM-APP_LDAP*. Click **Next**.

**Connection Details:**

In the **Connection** tab, specify the following details:

- **Application Type**: Enter the application type as *LDAP*.
- **Host Name/IP Address**: Enter either the host name or the IP address of the E-Directory.
- **Port**: Enter the port number. If you enable SSL, the port number is 636, else the port number is 389.
- **SSL**: Enable or disable by moving the button to the left or to the right.
- **Password Change on Check in**: Based on the following selection the password of the application will be changed automatically every time a credential is checked in.
  - **Never**
    
    You can use this option if you do not want to change the password after every credential check-in.
  - **Delegate to Identity Manager**
If you want to delegate the password check-in process to Identity Manager, select Delegate to Identity Manager. Once a resource is created in Identity Manager, it gets synced to Privileged Account Manager. Resource permission is created in Privileged Account Manager but during check in and checkout password is rotated and handled by Identity Manager Driver Implementation guide on the PAM documentation page.

**NOTE:** Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

**NOTE:** Before you delegate password check-in to Identity Manager ensure that both the Privileged Account Manager IDM driver and database driver are operational.

- **By Script**
  
  Enter the E-Directory script in the text box provided.

- Select the appropriate Password Policy that must be used when Privileged Account Manager generates a new password. By default Default Password Policy is selected. You can either modify the default password policy or create a new password policy.
  
  - User DN
  - Password

  **NOTE:** Ensure not to use '%', percentage character in the special characters list of the password policy.

**NOTE:** Enter the user DN and password in the Credentials fly out.

- Reconcile Account: Select based on the account.

- **Script Arguments:** Select any relevant script argument.

- In the Extended Attributes tab, click +Define and select the relevant attributes from the list. Click Finish

### 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 the software. You can enable the password check-out feature to access the Active Directory server.

To enable the credential checkout feature for Active Directory, you can add the rules by using the Active Directory policy template.

Follow the procedure, after importing the vault:

**General:**

In the General tab, enter the name, example: DOM-APP_Active-Directory_LDAP. Click Next.
Connection Details:

- **Application Type**: Enter the application type as LDAP.
- **Host Name/IP Address**: Enter either the host name or the IP address of the Active Directory.
- **Port**: Enter the port number. If you enable SSL, the port number is 636, else the port number is 389.
- **SSL**: Enable or disable by moving the button to the left or to the right.
- **Password Change on Check in**: Based on the following selection the password of the application will be changed automatically every time a credential is checked in.
  - **Never**
    You can use this option if you do not want to change the password after every credential check-in.
  - **Delegate to Identity Manager**
    If you want to delegate the password check-in process to Identity Manager, select Delegate to Identity Manager. Once a resource is created in Identity Manager, it gets synced to Privileged Account Manager. Resource permission is created in Privileged Account Manager but during check in and checkout password is rotated and handled by Identity Manager Driver Implementation guide on the PAM documentation page.

**NOTE**: Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

**NOTE**: Before you delegate password check-in to Identity Manager ensure that both the Privileged Account Manager IDM driver and database driver are operational.

- **By Script**
  Enter the Active Directory script in the text box provided.
  - **Select the appropriate Password Policy** that must be used when Privileged Account Manager generates a new password. By default Default Password Policy is selected. You can either modify the default password policy or create a new password policy.
    - **User DN**
    - **Password**

**NOTE**: Enter the user DN and password in the Credentials fly out.

- **Reconcile Account**: Select based on the account.

**Script Arguments**:

- In the Extended Attributes tab, click *Define* and select the relevant attributes from the list. Click Finish
System Applications Product

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 Privileged Account Manager with the Systems, Applications, and Products (SAP) application, ensure that you download the following files on the Privileged Account 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.

Follow the procedure, after importing the vault:

**General:**

In the **General** tab, enter the name, example: *DOM-APP_SAP*. Click **Next**.

**Connection Details:**

- **Application Type:** Enter the application type as *SAP*.
- **Host Name/IP Address:** Enter either the host name or the IP address of the SAP machine.
- **Port:** Enter the port number as 3309.
- **SSL:** Enable or disable by moving the button to the left or to the right.
- **Password Change on Check in:**
  
  Based on the following selection the password of the application will be changed automatically every time a credential is checked in.
  - **Never**
    
    You can use this option if you do not want to change the password after every credential check-in.
  - **Delegate to Identity Manager**
If you want to delegate the password check-in process to Identity Manager, select **Delegate to Identity manager**. Once a resource is created in Identity Manager, it gets synced to Privileged Account Manager. Resource permission is created in Privileged Account Manager but during check in and checkout password is rotated and handled by Identity Manager **Driver Implementation guide** on the PAM documentation page.

**NOTE:** Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

**NOTE:** Before you delegate password check-in to Identity Manager ensure that both the Privileged Account Manager IDM driver and database driver are operational.

- **By Script**
  Enter the SAP script in the text box provided.

- Select the appropriate **Password Policy** that must be used when Privileged Account Manager generates a new password. By default **Default Password Policy** is selected. You can either modify the default password policy or create a new password policy.
  - **User Name**
  - **Password**
  - **Reconcile Account:** Select based on the account.

- **Script Arguments:** Specify the **Language**, **clientNumber**, and **systemNumber** of the SAP machine.

- In the **Extended Attributes** tab, click **+Define** and select the relevant attributes from the list.

### 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.

Privileged Account Manager 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.

Follow the procedure, after importing the vault:

**General:**

In the **General** tab, enter the name, example: **DOM-APP_ESXi**. Click **Next**.

**Connection Details:**

- **Application Type:** Enter the application type as ESXi.
- **Host Name/IP Address:** Enter either the host name or the IP address of the ESXi machine.
- **Port:** Enter the port number as 443.
- **SSL:** Enable or disable by moving the button to the left or to the right.
• **Password Change on Check in:**
  Based on the following selection the password of the application will be changed automatically every time a credential is checked in.
  
  • *Never*
    You can use this option if you do not want to change the password after every credential check-in.
  
  • **Delegate to Identity Manager**
    If you want to delegate the password check-in process to Identity Manager, select Delegate to Identity Manager. Once a resource is created in Identity Manager, it gets synced to Privileged Account Manager. Resource permission is created in Privileged Account Manager but during check in and checkout password is rotated and handled by Identity Manager *Driver Implementation guide* on the PAM documentation page.

  **NOTE:** Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

  **NOTE:** Before you delegate password check-in to Identity Manager ensure that both the Privileged Account Manager IDM driver and database driver are operational.

• **By Script**
  Enter the ESXi script in the text box provided.
  
  • Select the appropriate Password Policy that must be used when Privileged Account Manager generates a new password. By default Default Password Policy is selected. You can either modify the default password policy or create a new password policy.
    
    • User Name
    • Password
    
    • Reconcile Account: Select based on the account.

  • **Script Arguments:**
    • In the Extended Attributes tab, click +Define and select the relevant attributes from the list.

**Local Account on Linux**

Privileged Account Manager supports Credential Checkout feature for local user accounts on any Linux Operating System running SSH.

Follow the procedure, after importing the vault:

**General:**

In the General tab, enter the name, example: *DOM-APP_Linuxlocal*. Click Next.

**Connection Details:**

• **Application Type**: Enter the application type as linuxlocal.

• **Host Name/IP Address**: Enter either the host name or the IP address.
• **Port**: Enter the port number. If you enable SSL, the port number is 636, else the port number is 22.

• **SSL**: Enable or disable by moving the button to the left or to the right.

• **Password Change on Check in**: Based on the following selection the password of the application will be changed automatically every time a credential is checked in.
  
  • **Never**: You can use this option if you do not want to change the password after every credential check-in.
  
  • **Delegate to Identity Manager**: If you want to delegate the password check-in process to Identity Manager, select Delegate to Identity Manager. Once a resource is created in Identity Manager, it gets synced to Privileged Account Manager. Resource permission is created in Privileged Account Manager but during check in and checkout password is rotated and handled by Identity Manager. See the [PAM documentation page](#) for more details.

  **NOTE**: Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

  **NOTE**: Before you delegate password check-in to Identity Manager ensure that both the Privileged Account Manager IDM driver and database driver are operational.

• **By Script**: Enter the Linux script in the text box provided.

  • Select the appropriate **Password Policy** that must be used when Privileged Account Manager generates a new password. By default, Default Password Policy is selected. You can either modify the default password policy or create a new password policy.

    • **User Name**
    
    • **Password**

  • **Reconcile Account**: Select based on the account.

    • **Script Arguments**:  

    • In the **Extended Attributes** tab, click +Define and select the relevant attributes from the list.

**Local Accounts on Unix**

Privileged Account Manager 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.

Follow the procedure, after importing the vault:
General:
In the General tab, enter the name, example: DOM-APP_Unixlocal. Click Next.

Connection Details:

• Application Type: Enter the application type as Unixlocal.
• Host Name/IP Address: Enter the host name and IP of the Unix machine.
• Port: Enter the port number as 22.
• SSL: Enable or disable by moving the button to the left or to the right.
• Password Change on Check in:
  Based on the following selection the password of the application will be changed automatically every time a credential is checked in.
  • Never
    You can use this option if you do not want to change the password after every credential check-in.
  • Delegate to Identity Manager
    If you want to delegate the password check-in process to Identity Manager, select Delegate to Identity manager. Once a resource is created in Identity Manager, it gets synced to Privileged Account Manager. Resource permission is created in Privileged Account Manager but during check in and checkout password is rotated and handled by Identity Manager Driver Implementation guide on the PAM documentation page.

NOTE: Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

NOTE: Before you delegate password check-in to Identity Manager ensure that both the Privileged Account Manager IDM driver and database driver are operational.

• By Script
  Enter the Unix script in the text box provided.
• Select the appropriate Password Policy that must be used when Privileged Account Manager generates a new password. By default Default Password Policy is selected. You can either modify the default password policy or create a new password policy.
  • User Name
  • Password
  • Reconcile Account: Select based on the account.
• Script Arguments: Enter the relevant script argument.
• In the Extended Attributes tab, click +Define and select the relevant attributes from the list.

Local Accounts on Windows

Prerequisites for adding local accounts on Windows machine:
For RHEL 8 (64-bit) and RHEL 7 (64 bit), install the redhat-1sb-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 a 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 Privileged Account Manager 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
    ```
  - The IP address of the task manager must be added to the trusted host of the target machine. To add a trusted host, use the command:
    ```
    winrm set winrm/config/client '@{TrustedHosts="x.x.x.x"}'
    ```

Follow the procedure, after importing the vault:

**General:**

In the **General** tab, enter the name, example: **DOM-APP_WINDOWS**. Click **Next**.

**Connection Details:**

- **Application Type**: Enter the application type as **WINDOWS**.
- **Host Name/IP Address**: Enter the host name and IP of the Windows machine.
- **Port**: Enter the port number as 3389.
- **SSL**: Enable or disable by moving the button to the left or to the right.
- **Password Change on Check in**:
  - Based on the following selection the password of the application will be changed automatically every time a credential is checked in.
    - **Never**
      - You can use this option if you do not want to change the password after every credential check-in.
    - **Delegate to Identity Manager**
If you want to delegate the password check-in process to Identity Manager, select Delegate to Identity manager. Once a resource is created in Identity Manager, it gets synced to Privileged Account Manager. Resource permission is created in Privileged Account Manager but during check in and checkout password is rotated and handled by Identity Manager Driver Implementation guide on the PAM documentation page.

**NOTE:** Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

**NOTE:** Before you delegate password check-in to Identity Manager ensure that both the Privileged Account Manager IDM driver and database driver are operational.

- **By Script**
  Enter the Windows script in the text box provided.
- Select the appropriate **Password Policy** that must be used when Privileged Account Manager generates a new password. By default Default Password Policy is selected. You can either modify the default password policy or create a new password policy.
  - User Name
  - Password
- Reconcile Account: Select based on the account.
  - **Script Arguments:** Enter the ClientID, Authority, and AuthenticationTokenURL.
  - In the **Extended Attributes** tab, click +Define and select the relevant attributes from the list.
  - Click Finish.

Privileged Account Manager supports Credential Checkout feature for local user accounts on Window Operating System.

**Enabling Credential Checkout for Applications**

You can be customize the credential checkout feature for the applications such as Salesforce and so on.

To enable credential checkout for 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.

To enable credential checkout for an application whose policy template is not available, you need to add the application server as a resource in the credential vault and add a credential checkout rule. For information about adding a resource, see contextual help. For information about adding a rule, see “Add a Permission” on page 280 in Access Control or “Adding a Rule” on page 164 in Command Control.
5.3.3 Configuring Credential Checkout for Cloud Services

The privileged accounts that are set up on the following cloud services can be managed through Privileged Account Manager. To manage those accounts, you must customize the sample script and add it to the Privileged Account Manager rule.

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.

- 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 the AWS cloud.

To enable credential checkout feature for AWS, you can add the rules by using the AWS policy template or add an AWS resource and rule manually.

- 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.

**Enabling Credential Checkout for OpenStack**

To enable the 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 Privileged Account Manager Administration Console, Add the OpenStack policy template to add a resource and rule for OpenStack automatically. This OpenStack resource and rule can be customized as required.
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 164.

**NOTE:** For the password check out of accounts belonging to different OpenStack projects (tenants), you must create a different resource for each tenant.

Follow the procedure, after importing the vault:

**General:**

In the General tab, enter the OpenStack URL, example: http://myOpenstack.com/dashboard/auth/login/_openstack. Click Next.

**Connection Details:**

- **Application Type**: Enter the application type as openstack.
- **Host Name/IP Address**: Enter the host name and IP of the openstack machine.
- **Port**: Enter the port number as 35357.
- **SSL**: Enable or disable by moving the button to the left or to the right.
- **Password Change on Check in**:

  Based on the following selection the password of the application will be changed automatically every time a credential is checked in.

  - **Never**
    
    You can use this option if you do not want to change the password after every credential check-in.

  - **Delegate to Identity Manager**
    
    If you want to delegate the password check-in process to Identity Manager, select Delegate to Identity manager. Once a resource is created in Identity Manager, it gets synced to Privileged Account Manager. Resource permission is created in Privileged Account Manager but during check-in and checkout password is rotated and handled by Identity Manager Driver Implementation guide on the PAM documentation page.

  **NOTE:** Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

  **NOTE:** Before you delegate password check-in to Identity Manager ensure that both the Privileged Account Manager IDM driver and database driver are operational.

  - **By Script**
    
    Enter the OpenStack script in the text box provided.
Select the appropriate Password Policy that must be used when Privileged Account Manager generates a new password. By default Default Password Policy is selected. You can either modify the default password policy or create a new password policy.

- User Name
- Password
- Reconcile Account: Select based on the account.

Script Arguments: .

In the Extended Attributes tab, click Define and select the relevant attributes from the list.

Enabling Credential Checkout for Amazon Web Services

To enable credential checkout feature for Amazon Web Services (AWS), perform the following:

1. Create a user and assign permissions or policies to the user in Amazon Web Services. For information about AWS user creation, see AWS Documentation.

2. In the Privileged Account Manager Administration Console, add the AWS policy template to add a resource and rule for AWS automatically. This resource and rule can be customized as required.

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 164.

Follow the procedure, after importing the vault:

General:

In the General tab, enter the name, example: https://ACCOUNT-ID.signin.aws.amazon.com/console_AWS. Click Next.

Connection Details:

- Application Type: Enter the application type as AWS.
- Host Name/IP Address: Enter account ID and the URI. Example: https://ACCOUNT-ID.signin.aws.amazon.com/console
- Port: Enter the port number as 443.
- SSL: Enable or disable by moving the button to the left or to the right.
- Password Change on Check in:
  Based on the following selection the password of the application will be changed automatically every time a credential is checked in.
  - Never
    You can use this option if you do not want to change the password after every credential check-in.
  - Delegate to Identity Manager
If you want to delegate the password check-in process to Identity Manager, select Delegate to Identity Manager. Once a resource is created in Identity Manager, it gets synced to Privileged Account Manager. Resource permission is created in Privileged Account Manager but during check in and checkout password is rotated and handled by Identity Manager Driver Implementation guide on the PAM documentation page.

NOTE: Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

NOTE: Before you delegate password check-in to Identity Manager ensure that both the Privileged Account Manager IDM driver and database driver are operational.

- **By Script**
  Enter the AWS script in the text box provided.
  - Select the appropriate Password Policy that must be used when Privileged Account Manager generates a new password. By default Default Password Policy is selected. You can either modify the default password policy or create a new password policy.
    - User Name
    - Password. Enter the access key name and the ID. Example: AWS-ACCESS-KEY-ID.
  - Reconcile Account: Select based on the account.
  - **Script Arguments:**
  - In the Extended Attributes tab, click +Define and select the relevant attributes from the list.

**Enabling Credential Checkout for Microsoft Azure**

**Prerequisite:** Ensure that Privileged Account Manager password policies adhere to the Microsoft Azure password policies.

To enable credential checkout feature for Microsoft Azure, follow the procedure:

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 add a resource and rule for Microsoft Azure automatically. You can customize this resource and rule as required.
   or
   Add a resource in the Credential Vault and a rule manually for Microsoft Azure. Edit the resource in Privileged Account Manager 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 164.
Follow the procedure, after importing the vault:

**General:**

In the General tab, enter the name, example: \https://portal.azure.com/_MSAzure. Click Next.

**Connection Details:**

- **Application Type:** Enter the application type as MSAzure.
- **Host Name/IP Address:** Enter account ID and the URI. Example: ADAccountDomainName.onmicrosoft.com
- **Port:** Enter the port number as 443.
- **SSL:** Enable or disable by moving the button to the left or to the right.
- **Password Change on Check in:**
  
  Based on the following selection the password of the application will be changed automatically every time a credential is checked in.
  
  - **Never**
    
    You can use this option if you do not want to change the password after every credential check-in.
  
  - **Delegate to Identity Manager**
    
    If you want to delegate the password check-in process to Identity Manager, select Delegate to Identity manager. Once a resource is created in Identity Manager, it gets synced to Privileged Account Manager. Resource permission is created in Privileged Account Manager but during check in and checkout password is rotated and handled by Identity Manager Driver Implementation guide on the PAM documentation page.

**NOTE:** Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

**NOTE:** Before you delegate password check-in to Identity Manager ensure that both the Privileged Account Manager IDM driver and database driver are operational.

- **By Script**
  
  Enter the Azure script in the text box provided.
  
  - Select the appropriate Password Policy that must be used when Privileged Account Manager generates a new password. By default Default Password Policy is selected. You can either modify the default password policy or create a new password policy.
    
    - **User Name:** Example, adminuser@dn.onmicrosoft.com
    
    - **Password**
    
    - **Reconcile Account:** Select based on the account.
    
    - **Script Arguments:** Enter the ClientID, Authority, and AuthenticationTokenURL.
    
    - In the Extended Attributes tab, click +Define and select the relevant attributes from the list.
5.3.4 Configuring Credential Checkout Settings

1. On the home page of the Privileged Account Manager console, click Requests.
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.

5.3.5 Checking Out Credentials

Privileged Account Manager 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” on page 127.
- 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.

5.3.6 Dynamic Credentials

Your users and applications can request just-in-time credentials by using dynamic database credentials. These requests also have the ability to be audited and have a defined TTL that causes them to expire automatically. You can also filter from a large number of records using the select box on the left pane.

This field contains ephemeral account details:

- Requester
- Resource Name
- User Name
- Type
- Status
- Creation Time
- Expiry Time
For an active account you can revoke the credentials if you see any malicious or unwanted activity using the revoke icon against the credential.

### 5.3.7 View Policy

Clicking on the root path (/) allows you to View Policy. You must click **Add Policy** to create a policy for the specific resource group from the Policy and Path Details page. Specify the details in the Create Policy dialog box.

- **Name**: Specify a name for the policy.
- **+Add**: Add the groups by selecting from Local or LDAP Groups.
  
  The policy that you created will be applicable for the specific groups you have selected, ex: API users.

### Create Path

Only if the user is a path administrator or an owner for a path, he will be able to view the respective path, else the user gets the “access denied” error. A user should be part of a permission to be able to view the path. To get the appropriate permission, create a user group with the following mandatory permissions. Go to Users, click edit to modify Permissions. Under Credential Vault, select the following:

- View Credential Vault Console
- View Resources and Credentials in Credential Vault
- Add and Modify Resources and Credentials in Credential Vault

You can create path using the following procedure:

1. Go to Credential Vault.
2. From the left pane, click +.
3. Add the Path name.
4. Add the groups by selecting from Local or LDAP Groups.
   
   Enable Recursive if you want to populate the resources of the select path recursively.
4. Click Create.
Configuring Privilege Type

You can configure privilege type clicking Credential Vault > Resources. If you have defined credentials in the vault, you can use the credential as the privilege type. Edit any resource to define the privilege type. The privileged type attribute allows the user to access only certain privileges attributed to that role.

Follow the procedure to add the privilege type.

1. Go to Credential Vault.
2. Click an Application or Database credential count from the second column. The Credentials page is displayed.
3. Click + icon again the Resource Count column.
4. In the Add Credential page enter the User Name, Password and Privilege Type.
5. Click Add.

The credential gets listed under the Privilege Type column. These credentials are populated when you are checking out a resource’s credentials or if you want to change a specific user’s password from > My Access page.

5.3.8 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 a random password, resetting the password on the Privileged Account Manager database, and resetting the 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 the Privileged Account Manager database, or use Identity Manager to send the reset password on Privileged Account Manager 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.

- “Active Directory Password Reset Script” on page 101
- “AWS Password Reset Script” on page 103
- “ESXi User Password Reset Script” on page 105
- “LDAP Password Reset Script” on page 107
- “Linux User Password Reset Script” on page 108
- “Microsoft Azure Password Reset Script” on page 110
- “Openstack Password Reset Script” on page 112
- “SAP User Password Reset Script” on page 114
- “Windows User Password Reset Script” on page 116

Active Directory Password Reset Script

Following is an example script for resetting the account’s password 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");
}
```

## Working with Credentials
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;

AWS Password Reset Script

Following is an example script for resetting the account’s password 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(/\s/, $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(/\s/, $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("Successfully 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;

ESXi User Password Reset Script

Following is an example script for resetting the account’s password 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;

LDAP Password Reset Script

Following is an example script for resetting the accounts’ password 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 101.

## PAM script to reset password of an LDAP user

```perl
## 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;

---

**Linux User Password Reset Script**

Following is an example script for resetting the account’s password 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");
```
# 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>&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++;
    }
    # 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>&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);

    $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>&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);

$new_pwd[$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\" | 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;

Microsoft Azure Password Reset Script

Following is an example script for resetting the account’s password 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
Working with Credentials

```perl
$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++] = "'";
    } else{
      $new_pwd[$point] = $_;
    }
    $point++;
  }
  $userPasswd = join("", @new_pwd);
  
  #escape single quote ''' in admin password
  @pwd = ();
  @new_pwd = ();
```
@pwd = split(/\s/, $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;

Openstack Password Reset Script

Following is an example script for resetting the account’s password 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;

SAP User Password Reset Script

Following is an example script for resetting the account’s password 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_info("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(/\n/, $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("Successfully 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;

Windows User Password Reset Script

Following is an example script for resetting the account’s password 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;

5.4 What is Delegated Administrator Access

- Delegated administration helps defend against internal attacks that escalate privileges and exploit them by eliminating endpoint-specific built-in administrative access and rights.
- Delegated administration helps enforce the "least privilege" concept to only grant users the access and privileges they require to do their tasks in an efficient manner.

Present capabilities of Privileged Account Manager involves the capability to store and access resources and their secrets, but resource management is still a flat/lateral structure which does not offer the ability for delegated administration.

In the new capability, all the resources are organized in a tree-based structure called Path and the policies are defined on top of this path. The ownership is defined for each Path based on which the resources will be managed.

In an organization, if you want a specific set of people to manage resources but can access credentials, such as, API users to access the credentials for resources...it is easier to delegate such granular permissions.
In addition to Access Control, in the secrets vault, you can provide delegated access for users wanting JIT access, etc. Vault Management itself can be segregated based on certain users and their policies.

Both LDAP and local users are supported for this capability.

All the resources so far were stored from the home page of Privileged Account Management, Credential Vault Resources.

Now, on top of Resources, there is the path that helps organize and manage resources using the path we can give granular and specific policies to differentiate vault administrators as delegated administrators Vault administrators are no longer the whole and sole owners managing path and resource.

As a user Adam can do this by clicking on Credential Vault Resources search path using / which is the root path and add additional paths in the root path by clicking, Access Create Path owner (who is a super administrator for a particular path). Path administration, unlike the super administrator will have restrictive permissions. For example, if Adam, the path administrator wants to provide delegated administrator permissions to Alice, he will follow the procedure:

1. Create a Path > Add to create a policy to create a path. Navigate to the path and click on View Policy to add a new policy where the groups and privilege types are listed.
2. Edit the created path.
3. Add users to this created path from Users and Groups.
4. Create a group (add permissions from the user and group management, view add, modify resources and credentials in Credential Vault). Credential Vault permission and users and group permission are mandatory.
5. Edit Access path and either enable recursive or disable recursive.

**NOTE:** Enabling Recursive allows the path owner to manage the delegated path and the inherited child paths.

6. Log out from Privileged Account Manager as administrator.

When Alice logs in she gets Credential Vault permission (but no path management permission). Which means Alice as a delegated administrator has been given only permission to create a policy and not manage a path and at that particular level, she can manage as a delegated administrator. Additionally Alice can log in and manage the resources and credentials for the particular path when is given path administrator rights for a path.

### 5.5 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. 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 in 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.

5.5.1 Types of Shared Key

Privileged Account Manager provides three default and a custom key types. These types are created for the quick and easy grouping of 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 consists of 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.)

5.5.2 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 simultaneously check out the available key until 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.

To enable key checkout, perform the following:

1. Configure the shared Key.
For more 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 164. 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 other 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 user 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 247). 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.

### 5.5.3 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 various users:** You can define multiple keys in a domain for multiple users, and each shared key can have a 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 11.
**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.

### 5.6 Password Management

Using Privileged Account Manager, you can grant privileged access to Privileged Account Manager users either by elevating the user privilege or by providing privileged account credentials for checkout. The resource and credential details 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 Privileged Account Manager are unknown to any administrator. Hence, these credentials must be rotated automatically by Privileged Account Manager 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 the password management feature of Privileged Account Manager, you can automate periodic rotation of service account password.

Password rotation is the process of regularly changing or resetting passwords (s). By reducing the amount of time a stolen password might be used, limiting the lifespan of a password lowers the danger from and efficacy of password-based attacks and exploits.

The solution supports password updates for a wide range of platforms, including databases, routers, switches, operating systems (Windows and Unix), routers, and firewalls.

#### 5.6.1 Understanding Password Management for Windows, Active Directory, Linux, and Network Devices

For changing these resource passwords, Privileged Account Manager 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 Change Password Policy option enabled.

In addition, if you want to perform any automated task after a 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 creating a custom script and adding it to the task. For more information about the template for creating a custom script, contact Customer Support.

- **For Windows and Active Directory:**

  Privileged Account Manager provides out-of-the-box scripts to the change password of Windows local machine and Active Directory.
In addition to windows account password change, Privileged Account Manager also offers the capability to change the password of service accounts. Privileged Account Manager provides out-of-the-box scripts to change the password of service accounts, such as such as Windows Services, COM+, Task Scheduler, and IIS Pool. You can define a custom script for password change for other service accounts and associate it to a service task.

These service account tasks are executed only for those credential with the appropriate service account associated with it. This association can be defined when adding a credential. When you are adding a credential for an active directory, Privileged Account Manager 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:**

  Privileged Account Manager provides out-of-the-box script to change password of Linux and Network devices that can be connected using SSH protocol. Privileged Account Manager can rotate both the password or the SSH key that is configured for a credential.

  If you want to change the 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.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Password Management</th>
<th>Schedule Password Change</th>
<th>Change Password in Associated Services</th>
<th>Custom Task Execution after Password change</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>UNIX, Linux and Network Device</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux and Network Devices using SSH connection</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Telnet</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>(Linux and Network Devices using Telnet connection)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNIX</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>LDAP</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Active Directory</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NetIQ eDirectory</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>OpenLDAP</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Database</strong></td>
<td>Yes</td>
<td>No</td>
<td>You can only enable the password to be changed immediately after credential check-in.</td>
<td>No</td>
</tr>
</tbody>
</table>

For more information about configuring tasks and scripts, see Contextual Help.
5.6.2 Prerequisites for Configuring Password Management

- Ensure that the Task Manager module is installed.
  - The task manager component of Privileged Account Manager (taskmanager) is supported only on Windows, SLES 12 (64-bit), SLES 15 (64-bit), RHEL 7.5 (64-bit), or RHEL 8 (64-bit).
    - For RHEL 8 (64-bit) and RHEL 7 (64 bit), install the redhat-1sb-core package.
    - For SLES 12 (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 Privileged Account Manager, you must have Task Manager module installed on every host domain.
    For more information about installing a package in Privileged Account Manager, 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:
    ```sh
    Enable-PSRemoting -force
    ```
  - Add a target machine, where the password must be changed, to the WinRM trusted host. To add all servers as trusted host, use the command:
    ```sh
    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 Privileged Account Manager 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

**Prerequisites**

You must install the gssntlmssp package for upgrade and for fresh install of Privileged Account Manager. Download the appropriate versions from gssntlmssp (https://software.opensuse.org/package/gssntlmssp).

**Example 5-1  Installing the gssntlmssp Package**

```
>> wget --no-check-certificate https://download.opensuse.org/repositories/openSUSE:/Backports:/SLE-15-SP4:/Update/standard/x86_64/gssntlmssp-1.2.0-bp154.2.3.1.x86_64.rpm
>> rpm -i gssntlmssp-1.2.0-bp154.2.3.1.x86_64.rpm
```

For RHEL, install using the `yum install gssntlmssp` command.

Test powershell authentication to AD server using the following command: cd /opt/netiq/npum/service/local/taskmanager/framework/powershell

LD_LIBRARY_PATH=/opt/netiq/npum/bin/ ./pwsh

New-PSSession -ComputerName <ad_server_ip> -Credential <ad_domain\administrator -Authentication Negotiate

To configure Privileged Account Manager to change (rotate) the password of any resource, you must enable the Password Change option value in the Credential Vault > Resources > Edit icon Password Management resource configuration 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 > Password Management > Vault Name > edit icon next to the required resource.
## Configuring Password Management in an Upgraded Setup

After upgrading Privileged Account Manager, if you want to enable password management, perform the following:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Go To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Review the prerequisites and ensure all the required configurations are complete.</td>
<td>“Prerequisites for Configuring Password Management” on page 124</td>
</tr>
<tr>
<td>2. Review all password change and service tasks associated with the vault and update when the task must be scheduled for execution.</td>
<td>Credential Vault &gt; Password Management</td>
</tr>
<tr>
<td>3. (Conditional) By default, the out-of-the-box password policy provided by Privileged Account Manager is associated with every vault. You can choose to use the default policy or create a new policy and associate with the vault. Ensure not to use '%', percentage character in the special characters list of the password policy.</td>
<td>Credential Vault &gt; Password Policies &gt; Help icon</td>
</tr>
<tr>
<td>4. Perform the following on all the resources:</td>
<td></td>
</tr>
<tr>
<td>1. Edit the resource and enable the Password Change option value in the Credential Vault &gt; Resources &gt; Edit icon Password Management. Also, review and modify all password management options, such as reconcile the account and so on. These password management values will be inherited by all credentials in the resource.</td>
<td>Credential Vault &gt; Vault Type &gt; Vault Name &gt; click edit icon of the required resource</td>
</tr>
<tr>
<td>2. (Conditional) If you do not want Privileged Account Manager to change reconcile account password, disable the Password Change option value in the Credential Vault &gt; Resources &gt; Edit icon Password Management in the appropriate resource credential. It is recommended that you disable the Password Change option value in the Credential Vault &gt; Resources &gt; Edit icon Password Management. Also, you must have one local administration account, which Privileged Account Manager does not manage to resolve any password change issue.</td>
<td>Credential Vault &gt; Vault Type &gt; Vault Name &gt; Resource Name &gt; click edit icon of the required credential</td>
</tr>
<tr>
<td>3. (Conditional) For Windows, if the credential is used as a service account, you must edit the credential and modify the service association.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
Disabling Password Management

You can disable password management at task level or resource level.

- You can disable password rotation (change) of all credentials or a specific credential in a resource at resource level.

To disable password management of all accounts in a resource, edit the resource configuration and disable the Password Change option value in the Credential Vault > Resources > Edit icon Password Management. Similarly, to disable password management for a credential, edit the credential configuration and set the Password Change to disabled.

- At the task level, you can disable the password change task of any vault to stop the 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.

5.7 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 passwords without any manual intervention.

The following illustration explains the working of the AAPM feature:
5.7.1 Password Management for Database and Applications

Privileged Account Manager provides the capability to change the password of the database and application credentials after every check-in. You can configure to either allow the Privileged Account Manager to perform the password change or delegate this task to the Identity Manager. If you want Privileged Account Manager 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 automatically imported when you use a policy template to configure a resource. If you have added the resource manually, you can copy the out-of-the-box password change scripts from “Password Reset Scripts” on page 101.

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.

5.7.2 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 Privileged Account Manager users to the appropriate user group. For more information, see “Enabling Users to Generate API Tokens” on page 129.
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
- Cloud services
- Applications
- Shared Keys

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 Privileged Account Manager allows multiple credentials checkout for an application, you must have an adequate number of credentials in Privileged Account Manager for simultaneous access to the application.

### Enabling Users to Generate API Tokens

You can allow Privileged Account Manager 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.

**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 User Group” on page 40.

### 5.7.3 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 Reports > 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 Privileged Account Manager reports, see Managing Reports.
Working With Access Policies

For any privileged access management product, defined policies or rules determines how various privileges are accessed across the enterprise. NetIQ Privileged Account Manager provides a method of creating policies to enable the granular control of privilege access.

Before you configure a policy, you must consider the following points:

- Privilege access is required for multiple resources having similar privilege access and security requirements, their usage, locations, criticality to business, and other factors.
- There are users across the organization who require different privileges across different systems. These users can be individuals such as, particular system administrator, or might be a group of users like contract employees, and Helpdesk administrators.

You can create policies in two ways:

- **Access Control**: This is the latest and recommended way to define policies and steps. For more information, see Section 6.2, “Access Control,” on page 133.
- **Command Control**: Using this capability, you can create a flexible set of policies. The granular hierarchy of policies enables you to define as many policies as possible in a tree manner. You can edit any policy to grant or deny access to a user, host, and command. For more information, see Section 6.3, “Command Control,” on page 160.

Some key differences in capabilities of Access Control and Command Control in Privileged Account Manager are mentioned in the following table:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Access Control</th>
<th>Command Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structure of Policy set</td>
<td>Linear</td>
<td>Hierarchical</td>
</tr>
<tr>
<td>Defining Host/Resources</td>
<td>Resource Pools</td>
<td>Host Groups</td>
</tr>
<tr>
<td></td>
<td>Type defined</td>
<td>Heterogeneous</td>
</tr>
<tr>
<td></td>
<td>Browsable Agents/Vaults</td>
<td>Non-Browsable Agents/Vaults</td>
</tr>
<tr>
<td>Defining Users/Groups</td>
<td>Based on Resource Pool type</td>
<td>Generic definition for all policies</td>
</tr>
<tr>
<td></td>
<td>Type defined permissions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Relevant attributes for each permission</td>
<td></td>
</tr>
<tr>
<td>Defining Policies</td>
<td>User Roles</td>
<td>Generic definition for all policies</td>
</tr>
<tr>
<td></td>
<td>Based on authentication source</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Browsable authentication source</td>
<td></td>
</tr>
</tbody>
</table>
6.1 Enabling or Disabling the Policy Engine

You can either use Command Control or Access Control based on the relevance and the environment. You can enable or disable either Command Control or Access Control policy engine, by going to Settings > Server Settings > Policy Engine. Use the slider to enable the status of the Access Control Engine or the Command Control Engine.

NOTE: The Command Control policy engine is enabled by default. If you disable both Access Control and Command Control engines, then no privileged access request is processed by either of the policy engines. Only emergency access requests will be evaluated.

Impact on Accessing Windows Resources on Which PAM Agent is Installed

- Prior to Privileged Account Manager 4.1, any Windows resource with the PAM agent installed on it could be accessed by Direct RDP without any authorizing Command Control rule.
- Privileged Account Manager 4.1 onwards, an authorizing Command Control rule or an Access Control permission is mandatory to access any resource.

Therefore, if you have not configured any authorizing Command Control rule or Access Control permission or you have disabled both the policy engines, then you cannot access any Windows resource. In case you have configured the authorizing Command Control rule or Access Control permission, but Command Control manager connection is disrupted, then the Windows...
resource can be accessed only using TROUBLESHOOT user. For more information, see Section 11.2.7, “Direct RDP is Disallowed When Privileged Account Manager Agents are Unable to Reach the Manager,” on page 365.

6.2 Access Control

Access Control is the latest policy engine introduced in Privileged Account Manager, which enables administrators to configure privileged access permissions in a simpler, easier and meaningful manner. It also provides quick insights into Privilege Governance (Who has what access) details.

Access Control engine emphasizes on grouping the Resources based on similar access requirements of an organization and then granting the access to users by defining the criteria such as allowed time of access, privilege level, monitoring needs etc.

Designing Access Permissions

In an organization, consider there are several Resources such as, Windows Servers, UNIX Servers, and Network devices, and various Users with different access levels, who require access on these servers.

The first step of designing access permissions is to group all the Resources based on similar access requirements or attributes such as:

- Operating system
- Specific software installed in those Resources
- Location of the Resources
- Department to which these Resources belong
- Users who need the access on those Resources, etc

The second step is to group the users based on their access requirements on the Resources or attributes such as:

- Tasks assigned to users on the Resources
- Privilege level allowed on the Resources
- Location of the Users
- Department of the users

The third step is to configure permissions to grant access on these Resource Groups to one or more User Groups, by defining the criteria such as:

- Allowed time of access
- Privilege level required on the Resources
- Access restrictions on file system or executables
- Activity monitoring
- Remediation in case of risks found in users’ activities, etc
6.2.1 Components of Access Control

Access Control depends on four primary components to enable privileged access to users on various types of resources.

- “Resource Pools” on page 134
- “User Roles” on page 135
- “Assignments” on page 135
- “Permissions” on page 135

Resource Pools

Resource Pools contain similar kind of resources with similar access requirements.

**NOTE:** A resource cannot be part of more than one Resource Pool.

Resource Pool types are categorized as below:

- Agents
  - Windows Agents – Contains Windows Agents only
    
    **NOTE:** Windows Agents are Windows systems where Privileged Account Manager - agent or manager is installed
  
  - UNIX Agents – Contains any Linux or UNIX Agents
- Agent-less
  - SSH Servers – Resources configured in Credential Vault within Generic UNIX category
    
    **NOTE:** SSH and Telnet servers can be any Linux, UNIX machines, Network devices, or Mainframe.

  - Telnet Servers – Resources configured in Credential Vault within Telnet category
  
  - Terminal SSH – Resources configured in Credential Vault within Terminal SSH category. To specify the starting directory for a SSH session invoked by Windows Terminal
  
  - Windows Systems – Resources configured in Credential Vault within Windows Hosts category

- Database
  
  - Oracle
  
  - Microsoft SQL Server
  
  - My SQL
  
  - Sybase
  
  - PostgreSQL
  
  - MariaDB
  
  - IBM Db2
• Applications
  • Applications
  • Application SSO
• Keys
  • SSH Keys
  • Windows Keys
  • VMWare Keys
  • Custom Keys

User Roles

User Roles contain users and groups, collectively called as members, from various sources who have similar access requirements. A User role can contain members from one or more sources. The supported sources are:

• **Local Users**: Users created locally in Privileged Account Manager.
• **Agent Users**: Users from any Agent registered to Privileged Account Manager.
• **LDAP Users and Groups**: Users or Groups from LDAP Servers configured for Authentication. Administrators can configure **Excluded Members** from LDAP Users and Groups, if there is a Group already added in **Included Members** section of a role.
• **Database Users**: Users created for authorizing access to database while co-ordination and monitoring it’s use. Administrators can configure **Excluded Members** from LDAP Users and Groups, if there is a Group already added in **Included Members** section of a role.

Assignments

Assignment is a relationship between a single Resource Pool and a User Role, which enables to configure one or more permissions under it.

**NOTE**: An assignment created for a Resource Pool and a User Role is unique, hence the same assignment cannot be created again.

Permissions

Under an assignment, one or more permissions define the access criteria such as Privilege Level, Allowed Access time, Monitoring options, File or Folder access control, Customization etc. Below is the list of permissions based on the Resource Types.

**NOTE**: Every time a new permission is added the user has to log out and log in for the new permission to take effect.

Privilege Elevation

• **Default**: Default Privileges selected for Resource in Resource Pool
• **Submit User**: No Elevation of Privileges
- **Common Run User or Common Credential**: A Common privilege for all the Resources authorized through this permission
- **Custom Run User or Custom Credential**: Custom Credentials per Resource

### Time Restrictions

- All Days – 24 hours and 7 days access
- Time Range – Selecting a specific start time and end time, recurring every week
- Custom – A recurring time slot for each selected day

**NOTE:** If a Permission is defined for All Days which is 24 hours and 7 days, another permission of same type is not allowed under an assignment.

**NOTE:** The time specified is always treated as GMT.

### Access and Monitoring Options

- Session Capture – Capture Key Strokes and Low level audits
- Low-level Session Audits – Enabling this option allows you to access the audits related to File System, Registry, Network, and Memory. This action might slow system performance
- Screen Shot Capture – Capture Screen Shot
- X11 – Applicable for Terminal SSH only
- Video Capture – Capture Videos
- Video FPS – Frames Per Second to use while capturing Videos
- Secondary Authentication – Move the slider to the left if you do not want this option to be enabled. By default, this option is set to enabled. To use this, ensure that Netiq Advanced Authentication is enabled. This setting ensures that the users are prompted for secondary authentication to log in to the Administration Console.
- User Message – Display a message to the Users while accessing the session authorized by this permission. This is applicable for selected permissions only
- Shell Options – Applicable for UNIX Agent permissions, to change the shell behavior

**NOTE:** Low Level Audits, also called as Command Audits are applicable only for Agents.

### Enhanced Access Control

Administrators can enforce access restrictions on files, folders or executables in Agents, by defining the allowed operations such as read, write, delete and execute.

**NOTE:** Unless the user logs off and logs in again, the EAC Policy is not effective. Non-English characters are not supported with Enhanced Access Control on Windows.
Command Lists

Command Lists are useful to allow or deny access on specific commands or applications within privileged sessions.

- On Agents, Privileged Applications or Privileged Commands permissions can be configured using Command Lists, to allow privileged access to specific applications or commands, rather than providing a complete privileged session.
- On Agent-less scenarios, Command Lists are helpful to allow or deny specific commands within privileged sessions.

Customization

Administrators can add Perl scripts to permissions, to customize the behavior of the permission before authorizing the privileged access. For example, a script added in the permission can verify a user’s attribute such as location or department, before authorizing the access.

Figure 6-1  Overview of Privileged Access Permissions

Windows Agents

Below is the list of permissions under Windows Agents Resource Pools.

- Credential Provider
  - Users must use the Credential Provider provided by Privileged Account Manager Agent installation.
  - Users must use the Credential Provider provided by Privileged Account Manager Agent installation.
- Direct RDP
  - Users can directly login into the Windows system using own accounts.
  - Privilege Elevation is not applicable.
Web Agent RDP

- Users need to login into Privileged Account Manager's User Console.
- Users' are authenticated by authentication sources configured in Privileged Account Manager.

Privileged Applications

- Users can directly login into the Windows system using own accounts. Users need to request a specific application to run with privileges supplied by Privileged Account Manager, using the Run as privileged user option, that appears when you right click on any application.

The table highlights the differences of each permissions with respective options and user experience:

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Authentication</th>
<th>Secondary Authentication</th>
<th>Privileged Elevati on</th>
<th>Mode of Access</th>
<th>Mode of session</th>
<th>Sessio n Captu re</th>
<th>Video Captur e</th>
<th>Enhanc ed Access Control</th>
<th>Application Commands</th>
<th>Application Lists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Provider</td>
<td>Privileged Account Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Thick Client</td>
<td>RDP Session</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>Direct RDP</td>
<td>Windows Authentication</td>
<td>NA</td>
<td>NA</td>
<td>Thick Client</td>
<td>RDP Session</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>Web Agent RDP</td>
<td>Privileged Account Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Web Browser</td>
<td>RDP Session</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>Privileged Applications</td>
<td>NA</td>
<td>NA</td>
<td>Yes</td>
<td>Thick Client</td>
<td>Requested Application</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

UNIX Agents

The List of permissions under Linux or UNIX Agents Resource Pools are:

- Privileged Shell
  - Users can directly login into the Linux or UNIX systems using own accounts.
  - Users need to request for privileged shell using the command - usrun pcksh.

- Login Shell
  - Users can directly login into the UNIX or Linux systems using own accounts.
  - Users' default shell should be set to /usr/bin/cpcksh.

- Privileged Commands
  - Users can directly login into the UNIX or Linux systems using own accounts.
  - Users must request for privileged commands using the command - usrun.
The table highlights the differences of each permissions with respective options and user experience:

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Authentication</th>
<th>Secondary Authentication</th>
<th>Privilege Elevation</th>
<th>Mode of Access</th>
<th>Mode of Session</th>
<th>Session Capture</th>
<th>Enhanced Access Control</th>
<th>Application Command Lists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged Shell</td>
<td>Local Accounts on Agent</td>
<td>NA</td>
<td>Yes - On Demand</td>
<td>Terminal SSH</td>
<td>Yes</td>
<td>PCKSH Shell</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Login Shell</td>
<td>Windows Authentication</td>
<td>NA</td>
<td>Yes - On Login</td>
<td>Terminal CPCKSH SSH</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
</tr>
<tr>
<td>Privileged Command Manager</td>
<td>Privileged Account Manager</td>
<td>NA</td>
<td>Yes - On Execution</td>
<td>Terminal Requested Command</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
</tr>
</tbody>
</table>

**SSH Servers**

The List of permissions under SSH Resource Pools are:

- **Terminal SSH**
  - Users can list or access SSH Sessions from any terminal, by connecting to the port of SSH Relay - `ssh -t -p 2222 username@pamhost`
  - Users' are authenticated by authentication sources configured in Privileged Account Manager.

- **Web SSH**
  - Users must login into Privileged Account Manager's User Console.
  - Users' are authenticated by authentication sources configured in Privileged Account Manager.

The table highlights the differences of each permissions with respective options and user experience:

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Authentication</th>
<th>Secondary Authentication</th>
<th>Privilege Elevation</th>
<th>Mode of Access</th>
<th>Mode of Session</th>
<th>Session Capture</th>
<th>X11 Video Capture</th>
<th>Application Command Lists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal SSH</td>
<td>Privileged Account Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Thick Client</td>
<td>SSH Session</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Web SSH</td>
<td>Privileged Account Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Web Browser</td>
<td>SSH Session</td>
<td>Yes</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>
Telnet Servers

The List of permissions under Telnet Resource Pools are:

- **Terminal Telnet**
  - Users can list or access SSH Sessions from any terminal, by connecting to the port of SSH Relay - `ssh -t -p 2222 username@pamhost`
  - Users' are authenticated by authentication sources configured in Privileged Account Manager.

- **Web Telnet**
  - Users must login into Privileged Account Manager's User Console.
  - Users are authenticated by authentication sources configured in Privileged Account Manager.

The table highlights the differences of each permissions with respective options and user experience:

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Authentication</th>
<th>Secondary Authentication</th>
<th>Privilege Elevation</th>
<th>Mode of Access</th>
<th>Mode of session</th>
<th>Session Capture</th>
<th>Application Command Lists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Telnet</td>
<td>Privileged Account Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Thick Client</td>
<td>Telnet Session</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Web Telnet</td>
<td>Privileged Account Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Web Browser</td>
<td>Telnet Session</td>
<td>Yes</td>
<td>NA</td>
</tr>
</tbody>
</table>

Windows Servers

The List of permissions under Windows (Agent-less) Resource Pools are:

- **Web RDP**
  - Users need to login into Privileged Account Manager's User Console.
  - Users' are authenticated by authentication sources configured in Privileged Account Manager.

The table highlights the differences of each permissions with respective options and user experience:

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Authentication</th>
<th>Secondary Authentication</th>
<th>Privilege Elevation</th>
<th>Mode of Access</th>
<th>Mode of session</th>
<th>Video Capture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web RDP</td>
<td>Privileged Account Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Thick Client</td>
<td>RDP Session</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Database Servers

- Oracle Database Access
- Oracle Database Credentials
- Microsoft SQL Server Database Access
- Microsoft SQL Server Database Credentials
- MySQL Database Access
- MySQL Database Credentials
- Sybase Database Access
- Sybase Database Credentials
- PostgreSQL Database Access
- PostgreSQL Database Credentials
- MariaDB Database Access
- MariaDB Database Credentials
- IBM DB2 Database Access
- IBM DB2 Database Credentials

The List of permissions under Database Resource Pools are:

- Database Access
  - Users can access database from any thick client or command line tools, by connecting to the port of Database connector configured in the Resource.
  - Users are authenticated by the database.
  - Users from the below User Roles are authorized if specified in the respective Assignments to the Resources:
    - Local users or LDAP users, if the credentials are checked out.
    - Agent users, if the credentials are not checked out and an agent is present in the resource where the database client is invoked.
    - Database users, if the credentials are not checked out and agent is not present.

- Database Credentials
  - Database Credentials
    - Users need to login into Privileged Account Manager’s User Console.
    - Users are authenticated by authentication sources configured in Privileged Account Manager.
    - Users can check out the Credentials of authorized Resources from the User Console.

The table highlights the differences of each permissions with respective options and user experience:
Defining Privilege Type for Database Credential Type Resource

1. In the Access Control > Assignments > Permissions > Checkout Options page, select the options as required.
   - **Allow Password Change During Check-in**: Move the radio button to the right to enable this option. By default this option is set to disabled and does not allow user to change the password while checking in. Enabling this option allows you to change the password while check in and provides the following options.

   **NOTE**: For users upgrading from Privileged Account Manager 4.1 to 4.2 version, and want to continue using the same Check in and Check out behavior for credentials, do not enable the **Allow Password Change During Check in** option. Whereas enabling the **Allow Password Change During Check in** is a new behavior of functionality from Privileged Account Manager 4.2 version onwards.

   - **Credential Checkout Mode**: Selected by System option allows system to select the user for checkout.
   - **Allow Selection by User** option allows you to select the user for which you want to perform password check-in and check-out function.
   - **Credentials Allowed for Checkout** This option allows you to either allow All credentials to perform Check in and Check Out function.

     The **Restrict Credentials to a Privilege Type** option is only applicable if you have already defined privilege type and want to select for which user you want to change the password while check out.

Applications

- Applications
- Application SSO

The list of permissions under Applications are:

- **Application Credentials**
  - Users need to login into Privileged Account Manager’s User Console.
  - Users are authenticated by authentication sources configured in Privileged Account Manager.
  - Users can check out the Credentials of authorized Resources from the User Console.
For more information, see Section 5.3.1, “Configuring Credential Checkout for Application and Database Type Credentials,” on page 83.

The table highlights the differences of each permissions with respective options and user experience:

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Authentication</th>
<th>Secondary Authentication</th>
<th>Mode of session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Credentials</td>
<td>Privileged Account Manager</td>
<td>Yes</td>
<td>Web Browser/REST API</td>
</tr>
</tbody>
</table>

The list of permissions under Application SSO are:

- **Application SSO over Web**
  - Users need to login into Privileged Account Manager's User Console.
  - Users are authenticated by authentication sources configured in Privileged Account Manager.

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Authentication</th>
<th>Secondary Authentication</th>
<th>Privilege Elevation</th>
<th>Mode of Access</th>
<th>Mode of Session</th>
<th>Session Capture</th>
<th>Video Capture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application SSO over Web</td>
<td>Privileged Account Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Web Browser/REST API</td>
<td>Requested Application</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Defining Privilege Type for Application Type Resource**

1. In the Access Control > Assignments > Permissions > Checkout Options page, select the options as required.

- **Allow Password Change During Check-in:** Move the radio button to the right to enable this option. By default this option is set to disabled and does not allow user to change the password while checking in. Enabling this option allows you to change the password while check in and provides the following options.

**NOTE:** For users upgrading from Privileged Account Manager 4.1 to 4.2 version, and want to continue using the same Check in and Check out behavior for credentials, do not enable the **Allow Password Change During Check in** option.

Whereas enabling the **Allow Password Change During Check in** is a new behavior of functionality from Privileged Account Manager 4.2 version onwards.

- **Credential Checkout Mode:** **Credential Checkout Mode:** Selected by System option allows system to select the user for checkout.
- **Allow Selection by User** option allows you to select the user for which you want to perform password check-in and check-out function.
- **Credentials Allowed for Checkout** This option allows you to either allow All credentials to perform Check in and Check Out function.

The **Restrict Credentials to a Privilege Type** option is only applicable if you have already defined privilege type and want to select for which user you want to change the password while check out.
Keys

- SSH Keys
- Windows Keys
- VMWare Keys
- Custom Keys

The List of supported Keys are:

- SSH Keys
- Windows Keys
- VMWare Keys
- Custom Keys

The list of permissions for the above mentioned keys are:

- Users need to login into Privileged Account Manager’s User Console.
- Users are authenticated by authentication sources configured in Privileged Account Manager.
- Users can check out the Keys of the authorized Resources from the User Console.

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Authentication</th>
<th>Secondary Authentication</th>
<th>Mode of Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>All permissions under Keys</td>
<td>Privileged Account Manager</td>
<td>Yes</td>
<td>Web Browser/REST API</td>
</tr>
</tbody>
</table>

6.2.2 Configuring Access Control

The following sections explain how you can manage resource pools, user roles, assignments, and permissions.

Configuring a Resource Pool

Resource Pools contain resources of similar type.

The following procedure explains how to manage resource pools:

1. On the home page of the console, click Access Control.
2. In the navigation pane, click Resource Pools.
3. In the details pane, click Create. A left pane with Create Resource pool is displayed with General and Resources settings.
4. In the Resources page, specify a name for the Resource Pool.
5. Add a Description.
6. Specify the Type of resource pool from the list.
7. Click Next. Resources page is displayed for configuration.
8. Click Add. Select the resources.
9 Click Add.

10 Select or enter the Default Credential. For more information, see “Default Credential” on page 145.

11 Click Create.

To modify a resource pool: In the details pane, select the resource pool you want to modify, then click the edit icon next to the resource pool name or click on the resource pool you want to modify and Edit Resource Pool page opens up on the right pane. Optionally, you can also modify the default credential at this point.

Configure the following fields:

Name: Specify a name for the resource pool.

Description: Describe the purpose of this resource pool.

Add, Remove or Delete resources.

**NOTE:** You cannot delete a Resource Pool if it is a part of an assignment.

**NOTE:** You cannot modify the type of the resource pool.

**Default Credential**

A credential with least privileges, should be selected as a Default Credential, for each resource added in a Resource Pool. This would help organizations in implementing the least privilege model as per the security recommendations and also minimizes the effort required to select a Credential while creating the access permissions.

**Windows Agents**

To create permissions in Access Control, each Windows Agent must be linked with a Credential Vault, where the Credentials are stored for single sign-on purposes for respective Agents. To link a Windows Agent with a Credential Vault follow the procedure:

1 Go to Hosts select Windows Agent.

2 Click Modify Host and select a value for the Vault.

3 Click Finish.

You can link the following two types of Windows Agents:

- Active Directory type Credential Vaults can be used for linking, if the Windows Agent is connected to an Active Directory Domain and to reference only Active Directory accounts in the Agent.

- Windows Hosts type Credential Vaults can be used for linking, if the Windows Agent is a stand-alone Windows Host or a Windows Agent which is part of a Domain but also has Local Accounts. To reference both the Local Accounts and Active Directory accounts in the Agent, the Windows Host type vault in Credential Vault should be linked to an Active Directory domain.

**Linux/Unix Agents**

- These Resources can use a username as Default Credential, which should be typed-in. For example, root or administrators.
SSH or Telnet Servers

- These Resources can use any Credential, which belongs to them in the Credential Vault.

Windows Servers

- These Resources can use any Credential, which belongs to them in the Credential Vault or the linked Active Directory domain.

**NOTE:** Default credentials are not required for the following resource pools:

- Database
- Applications
- Keys

Configuring a User Role

To add a new user role:

1. On the home page of the console, click Access Control.
2. In the navigation pane, click User Roles.
3. In the details pane, click Create. A Create User Role page with General, Included Members, and Excluded Members setting is displayed.
   - **General:** Specify the name and description of the user role. Click Next.
   - **Included Members:** Click Add to select users from the dropdown list which should be included in the user role. The drop down list consists of Local Users, LDAP Users and Groups, Database Users, and Agent Users.
     - Browse to users or groups and select a source.
     - Click Next.
   - **Excluded Members:** This field is only applicable for LDAP Users and groups. An LDAP user or group can be excluded, if that user or group is part of the LDAP groups selected Included Members in the previous section
4. Click Create.

To modify a user role: In the details pane, select the user role you want to modify and click the edit icon on that row or click on the user role you want to modify. Edit User Role page is displayed on the right pane.

5. Modify the following fields:
   - **General:** Modify the Name and Description of the user role and click Next.
   - **Included Members:** Click Add to select users from the dropdown list which should be included in the user role.
     - The drop down list shows Local Users, Agent Users, LDAP Users and Groups, and Database Users sources.
     - Browse to the users or groups and select a source. Click Add.
     - To remove, select existing users or groups from the table and click Remove.
     - Click Next.
Excluded Members: This field is applicable only for LDAP users and groups.

To delete a user role: In the details pane, select the user role that you want to delete and click the delete icon next to the user role name.
To select multiple user roles, click Delete multiple.

NOTE: You cannot delete a user role if it is a part of an assignment.

Configuring Assignments

Assignment is a relationship between a single Resource Pool and a User Role, which enables to configure one or more permissions under it.

1 On the home page of the console, click Access Control.
2 In the access control pane, click Assignments.
3 In the details pane, click Create.
4 To create an assignment, you must select a User Role, Resource Pool, and provide a Description. This Description is shown to the users while listing their permissions.
5 Click Add and select a Permission. Configure the permission options using the wizard. For more information, see “Configuring Permissions” on page 148.
6 Click Create to add the new assignment.

7 NOTE: After creating the assignment or permissions, you cannot modify the User Role and Resource Pool.

To modify an assignment: In the details pane, select the assignment you want to modify and then click the Edit icon on that row or click on the assignment you want to modify and Edit Assignment page is displayed on the right pane. You can edit the Description and the Priority, click Save.

- Priority is helpful to prioritize the assignments of the same Resource Pool and if one or more members are included in more than one User Role involved in these assignments.
  - For example: Consider that a Resource Pool (RP) is assigned to two User Roles UR1 and UR2, through the Assignments A1 (RP + UR1) and A2 (RP + UR2).
  - Members m1 and m2 are part of both User Roles.
  - A1 and A2 are configured to deliver the access with similar privileges on the target servers, but A2 has higher level of monitoring.
  - If A2 is expected to provide access to m1 and m2, with higher level of monitoring, A2 should have higher priority value over A1.
- The assignment with highest priority value will authorize the access request.
- The allowed values are - 1 to 99.

To delete an assignment: Select the assignment you want to delete and click Delete to delete the assignment and all child assignments.

For more information, see “Configuring Assignments” on page 147.
Configuring Permissions

Under an assignment, one or more permissions define the access criteria such as Privilege Level, Allowed Access time, Monitoring options, File or Folder access control, Customization etc. Below is the list of permissions based on the Resource Types.

While configuring permissions, only the applicable options are available for configuration. The wizards on the console are helpful in navigating to a particular section of options for a permission and selecting, enabling or disabling the required options.

1 On the home page of the console, click Access Control.
2 In the access control pane, click Assignments.
3 In the details pane, click Create Assignment or modify an existing Assignment.
4 Click Add and select a Permission. Configure the permission options using the wizard. For more information, see “Configuring Permissions” on page 148.
5 Click Save.

To modify a permission: In the details pane, select the permission you want to modify and then click the Edit or Delete icon on that row to modify the permission.

Example Scenarios to Configure Access Control

Scenario 1

Consider the following scenario:

- An organization contains two user roles named consultants and contractors, need access on ten resources
- Consultants role need access on four resources where software A installed
- Contractors role need access on four resources where software B installed.
- Both roles need access on two shared resources where both software A and B are installed.

Steps to provide privileged access in this scenario:

Resource Pools

- Create a Resource Pool (A) with four Resources where software A is installed.
- Create a Resource Pool (B) with four Resources where software B is installed.
- Create a Resource Pool (AB) with two Resources where both software A and B are installed.

User Roles

- Create a User Role – Consultants and include the required users
- Create a User Role – Contractors and include the required users
Assignments and Permissions

Consider a scenario where you need access to shared resources. You can configure a resource pool which overlaps one or more resource pool. For example, it there is a development and an automation resource pool, wherein development servers/resources are accessed by the developers and automation servers/resources are accessed by quality analysts. The overlapping or shared permission scenario is where there is a possibility of both developers and quality analysts accessing a share resource pool which have a mix of both development and automation servers/resources.

- Create an assignment between Resource Pool A and Consultants and define required permissions.
- Create an assignment between Resource Pool B and Contractors and define required permissions.
- Create an assignment between Resource Pool AB and Consultants and define required permissions.
- Create an assignment between Resource Pool AB and Contractors and define required permissions.

Figure 6-2  Usage Scenario Permissions
Scenario 2

Consider the following scenario:

- A user role needs access to a set of Windows Agents over weekdays with Privilege elevation. Administrator wants to monitor the activity as well as controlling file access and blocking certain applications from execution.
- The same user role needs access on those resources over weekends without elevation.

Steps to provide privileged access in this scenario:

**Resource Pools**

- Link the Agents to appropriate Credential Vaults, where all the required credentials are present.
- Create a Resource Pool with all the required Windows Agents in it.

**User Roles**

- Create a User Role with all the required users.

**Assignments**

- Create an Assignment between the created Resource Pool and User Role.

**Permissions**

- Create a Credential Provider Permission with below options
  1. Privilege Elevation as required (Example: Administrator).
  2. Define Time Restrictions with Monday 00:00 to Saturday 00:00.
3. Enable Session Capture and Video Capture.

- Create another Credential Provider Permission with below options:
  1. Privilege Elevation with any other account which does not have any higher privileges.
  2. Define Time Restrictions with Saturday 00:00 to Monday 00:00.
  3. Disable Session Capture and Video Capture.

A sample procedure is listed below:

**Configure the LDAP Repository**

1. Click **Settings** on the Administration Console.
2. Click **LDAP Servers** on the left pane and click **Add New**.
3. Perform the following actions:
   - Specify **Domain Name** of the LDAP Server.
   - Type **is set to Active Directory Services**, by default.
   - Specify **Host Name/IP Address** of the LDAP Server.
   - Select **SSL** and **Verify Certificate** to secure the connection via SSL by using the CA certificate.
   - Click **GetBaseDN** to fetch the appropriate details.
   - Set **Scope** to **Subtree**.
   - Specify **User DN, User Name**, and **Password** that are required for retrieving the user details and domain details for authentication.
4. Click **Save**.

**Add a Resource**

A resource is a network device, application, repository, or data storage device to which users can get privileged access.

1. Click **Credential Vault** on the Administration Console.
2. Click **+Add > Windows > Windows Host**.
3. In **Name**, specify a name for Windows Server.
   For this example, the resource name is set to **winsrv16.intech.com**.
4. Click **Next**.
5. Perform the following actions to configure the **Connection** details:
   - In **Host Name/IP Address**, specify the host name or IP address of Windows Server.

**NOTE:** Port is set to 636, by default.

**NOTE:** Port is set to 3389, by default.
5b Select Active Directory Domain displays the list of domains if the specified host name is associated to a domain.
In this example, Windows Server is a standalone device and does not need to be associated to any Active Directory Domain.

6 Click Next.
7 Click Finish.
8 Click the resource that you have added and click Credentials tab.
9 Click Add.
10 Specify the User Name, Password, and Privilege Type required to access Windows Server.

Defining a User Role
1 Click Access Control > User Roles > Create.
2 Specify the role name in Name and additional information about the role in Description.
3 Click Next.
4 Click +Add > LDAP Users and Groups.
5 Select the domain and select the preferred user or group.
   In this example, the user AlbertJ is selected.
6 Click Add > Create.

Create a Resource Pool
1 Click Access Control > Resource Pools > Create.
2 Specify Name and Description for this resource pool.
   For this example, the resource pool name is set to Windows Server with AD Users.
3 Select Type as Windows Servers under Agentless.
4 Click Next.
5 Click Add and select the resource that you added in “A resource is a network device, application, repository, or data storage device to which users can get privileged access.” on page 151.
6 Click Add.
7 Select Default Credentials that is required to allow users to access the resource.
8 Click Create.

Create an Assignment and Grant Permission
1 Click Access Control > Assignments > Create.
2 Select the Resource Pool that you created in “Click Access Control > Resource Pools > Create.” on page 152.
3 Select the User Role that you defined in “Click Access Control > User Roles > Create.” on page 152.
   The Description gets generated with the name that you have provided for Resource Pool and User Role.
4 Click Add and select Web RDP permission in the Privilege Elevation window.
NOTE: By default, Credential is set to Default to allow users to access Windows Server with the default credentials that is configure for the resource.

5 Click Next.
6 Select Custom Days and set the days and time frame as follows:
   6a Select Mon to Fri as the days.
   6b Specify 9 to 6 as time frame for the selected days.
7 Click Next.
8 Disable Secondary Authentication.
9 In User Message, specify a message that is displayed to users on connecting to the resource.
10 Click Next > Finish > Create.

Add LDAP Repository

1 Click Settings on the Administration Console.
2 Click LDAP Servers on the left pane and click Add New.
3 Perform the following actions:
   3a Specify Domain Name of the LDAP Server.
   3b Specify Host Name/IP Address of the LDAP Server.
   3c Select SSL and Verify Certificate to secure the connection via SSL by using the CA certificate.
   3d Click GetBaseDN to fetch the appropriate details.
   3e Set Scope to Subtree.
   3f Specify User DN, User Name, and Password that are required for retrieving the user details and domain details for authentication.
4 Click Save.

Add Linux System as a Resource

1 Click Credential Vault on the Administration Console.
2 Click +Add > Linux/Unix/Network Device > SSH.
3 In Name, specify a name for the Linux system.
   For this example, the resource name is set to inx-mchs.intech.com.
4 Click Next.
5 Perform the following to configure the Connection details:
   5a In Host Name/IP Address, specify the host name or IP address of the Linux system.
   5b Click Get Host Key to get the key of the specified machine.
6 Click Next.
7 Click Finish.
8 Click Count of the resource that you have added.
9 Click Add in the Credentials tab.

**NOTE:** Credential Type is set to Password by default, this grants elevated access to the resource using the specified Password.

10 Specify the User Name, Password, and Privilege Type required to access Linux system.
11 Click Add.

**Defining a User Role**

1 Click Access Control > User Roles > Create.
2 Specify the role name in Name and additional information about the role in Description.
3 Click Next.
4 Click +Add > LDAP Users and Groups.
5 Select the domain and select the preferred user or group.
   In this example, the user Silvia is selected.
6 Click Add > Create.

**Create a Resource Pool**

1 Click Access Control > Resource Pools > Create.
2 Specify Name and Description for this resource pool.
   For this example, the resource pool name is set to Inx-ssh-pool.
3 Select Type as SSH Servers under Agentless.
4 Click Next.
5 Click Add and select the resource that you added in Add Linux System as a Resource.
6 Click Add.
7 Select Default Credentials that is required to allow users to access the resource.
8 Click Create.

**Create an Assignment and Grant Permission**

1 Click Access Control > Assignments > Create.
2 Select the Resource Pool that you created in Create a Resource Pool.
3 Select the User Role that you defined in Defining a User Role.
   The Description gets generated with the name that you have provided for Resource Pool and User Role.
4 Click Add and select Web SSH permission.

**NOTE:** By default, the Credential is set to Default in the Privilege Elevation window.

5 Click Next.
NOTE: Time Restriction is set to All Days (24 hours) by default, allowing Linux system to be accessible for 24 hours without any restriction.

6 Click Next.
7 Disable Secondary Authentication.
8 In User Message, specify a message that is displayed to users on connecting to the resource.
9 Click Next > Finish > Create.

6.2.3 Advanced Configurations

Access Control assigns permissions to users based on their role. It provides granular control and offers a simple, manageable approach to access management that is less prone to error than assigning permissions to users individually.

The user role and permissions concept simplifies user assignments because management of users is not done individually, but instead have privileges that conform to the permissions assigned to their role(s).

All the objects in the advanced configurations can be managed using folders.

Creating a Folder for Scripts, Enhanced Access Control, and Application Command List

NOTE: You have the option to create a folder and associate objects to the created folder.

1 On the home page of the console, click Access Control.
2 In the navigation pane, click Configurations > Scripts.
3 In the left side of the details pane, click on a specific script.
4 Click the folder icon. Create New Folder dialog is displayed.
5 Enter a folder Name. Click Create.
6 You can move the existing scripts to this folder by selecting the script and clicking Move.

NOTE: You cannot delete a folder if the folder is associated with a Command list, EAC, or Scripts.

Editing the Folder

• Click on the edit icon against a specific folder to edit the folder name and then click Save.

NOTE: You cannot modify the folder type, but you can enable or disable the script.

The following configuration options are provided to assist you with Access Control configuration and management:

• “Application Command List” on page 156
• “Enhanced Access Control” on page 157
• “Scripts” on page 158
Application Command List

Keeping Windows and Linux/Unix agents in perspective, rather than elevating the entire session for the user, we have option to elevate privileges for certain applications. This may be for a command prompt or database client <SQL client> which ever application which might required granular permissions to be granted.

For agentless sessions although they are elevated sessions using SSH and Telnet, we can restrict the user functions. These command lists are easy to configure because there are wizards to guide to users.

The following procedure helps you in adding commands which you want to allow or deny.

1 Create a command list.
   1a Go to Access Control Configuration > Application Command List.
   1b Click New List > Create New List
   1c Enter the Name, optionally add the Description.
   1d Select the List Type. Either Windows or Linux.
   1e Click Create.

2 Add commands which you want to allow or deny.

3 Set the Risk Score to any of the following levels:
   ♦ Undefined
   ♦ Low
   ♦ Medium
   ♦ High

4 Go to Credential Vault. Select either Linux/Unix Network Device or Windows. as applicable.

5 Select the resource for creating the vault for which you want to add allow/deny commands.


7 Create a User Role based on the user selection from Local User, Agent User, LDAP User. For more information see, “Configuring a User Role” on page 146.

8 Create an Assignment by delegating necessary permissions.

9 In the Command List page, add the command list you created in the configuration tab and specify if you want to allow or deny those set of commands.

10 Click Finish Save.

If you log into the target machine and execute the commands, you will notice that the commands you set to deny will throw a “permission denied” error.

You can view the risk details in Reports All Sessions Details > Keystrokes.
Enhanced Access Control

Enhanced Access Control (EAC) policy can be defined at Permission level and also at an individual at the Access Control EAC object level and these can be associated to the Permission.

The EAC capability defines granular risks scores. Earlier capability included defining risk for every path (file or folder). But with the present functionality one can define the same for every operation on a given path for read, write, delete, execute, separate risk can be defined. The order of EAC policy execution is sequential. In the event of conflict, the first one takes the priority.

The Enhanced Access Control functionality includes the following four categories:

- File and Directory Level Access
- Application Process Control
- Registry Access
- Services Start/Stop Control

The earlier functionality with Command Control was limited to Linux/Unix but the present one includes support for Windows.

Enhanced Access Control Policy on Windows

This ability has control over files and directories permissions to users based on sessions. An administrator can specify a list of paths and each one has access control such as; Read, Write, Delete capabilities.

NOTE: Non-English characters are not supported with Enhanced Access Control on Windows.

Procedure to Create EAC Policy in Windows:

2. Specify the Name
3. (Optional) Specify the Description
4. Select the List Type as Windows.
5. Click Create.
6. Click Add Path: Create a path in the target machine. Modify this path rule to create appropriate permissions for file and associate this with the necessary risk score if you want.
7. Click Save.
9. Create User Role. For more information, see “Configuring a User Role” on page 146.
10. Associate the Resource Pool and User Role with an assignment by clicking permissions for the Enhanced Access Control.
11. Click Add > Add EAC Policy. The Windows policy is displayed.
12. Select the Policy and click Add.
13 Click Finish. The permission is created.
14 Log into a Windows machine and navigate to the created folder. You can verify that the permissions you had created are successfully configured.

You can view the risk details in Reports All Sessions Details > Keystrokes.

**Enhanced Access Control Policy on Linux/Unix**

For more information on Enhanced Access Control on Linux and Unix machine, see “Enhanced Access Control” on page 257.

1 Click Access Control Configuration > Enhanced Access Control > New Policy.
2 Specify the Name
3 (Optional) Specify the Description
4 Select the List Type as Linux.
5 Click Create.
6 Click Add Path: Create a path in the target machine. Modify this path rule to create appropriate permissions for file and associate this with the necessary risk score if you want.
7 Click Save.
8 Create Resource Pool. For more information see, Section 6.2.2, “Configuring Access Control,” on page 144.
9 Create User Role. For more information, see “Configuring a User Role” on page 146.
10 Associate the Resource Pool and User Role with an assignment by clicking permissions for the Enhanced Access Control.
11 Click Add > Add EAC Policy. The Windows policy is displayed.
12 Select the Policy and click Add.
13 Click Finish. The permission is created.
14 Log into a Windows machine and navigate to the created folder. You can verify that the permissions you had created are successfully configured.

You can view the risk details in Reports > All Sessions Details > Keystrokes.

**Scripts**

You can use Perl scripts to provide additional, customized functionality using relevant permissions. The Perl scripts defined as conditional can be used in permission. The return codes are limited to 1 for true and 0 for false. These conditional Scripts are executed during the permission evaluation. This conditional script runs on the PAM manager to evaluate if user has permission for the access or not. You can organize these scripts into a single level folder structure. Follow the steps to create a script:

1 On the home page of the console, click Access Control.
2 In the navigation pane, click Configurations > Scripts.
3 In the details pane, click +Script. A Create New Script page with Name, Description, and Script is displayed.
   - **Name**: Specify the name for the script.
• **Description:** Add a description for the script.
• **Script:** Write the script. Click **Create**.

4 You can add this script to a folder.

### 6.2.4 Configuring Exceptions

Exceptions are used as access deny lists in Access Control. Exceptions are created automatically when you block the user during a manual or automatic disconnect session.

Exceptions are used as access deny lists in Access Control. Exceptions are created automatically when you block the user during a manual or automatic disconnect session.

- **Blocking user access in versions earlier than Privileged Account Manager 4.0:** Till Privileged Account Manager 4.0, any privileged access request processed by Access Control, Command Control, or Emergency Access, was evaluated against Blocked Users group first. If a user was part of Blocked Users group, then all the access was denied.

- **Blocking user access from Privileged Account Manager 4.1 and later:** Exceptions are applicable only to Access Control. They are not considered while evaluating Command Control policies or Emergency Access requests. Any privileged access request processed by Command Control or Emergency Access, is evaluated against Blocked Users group.

Navigate to **Access Control > Exceptions** and click the **Configuration** icon on the right pane to set properties or exceptions.

- **Status:** You can retain the enabled status of this option if you want the exceptions to be evaluated while processing the privileged access requests by Access Control. This option is enabled by default. Move the slider to the left if you want to disable this option.

- **Deny Access On:** You can select any combination of Resources or Permissions.
  - Selection **All Resources** implies that user access is denied on all resources.
  - Selecting **Target Resource** implies that user access is denied on the target resources only.
  - Selecting **All Permissions** implies that user access is denied for all permissions.
  - Selecting **Target Permission** implies that user access using the target permission is denied for the user with any permission.

Following are all the possible combinations:

- **All Resources + All Permissions:** This combination implies that all access for the user is denied.

- **All Resources + Target Permission:** This combination implies that user access for the target permission is denied on all resources. Example: If the target permission is Direct RDP, then user access to any resource using Direct RDP is denied.

- **Target Resource + All Permission:** This combination implies that access to the target resource is denied for the user using any permission.

- **Target Resource + Target Permission:** This combination implies that user access using target permission to the target resource is denied.
• **Expire After:** You can set the validity for the exception in minutes, hours, days, week, or never. The default value *Never*, implies the exception will be applicable indefinitely.

• **Delete After:** You can set the deletion time for the exception after expiry. The exceptions will be purged from the server after the configured days of expiry. Only the expired exceptions will be deleted.

### Managing Exceptions

You can mark exceptions as *Mark Expired* from the *Active* tab. *Expired* exceptions indicate that the validity for the exception has expired.

To mark an exception as expired:

1. On the home page of the console, click **Access Control > Exceptions**.
2. Select the exceptions that you want to mark as expired.
3. In the details pane, click **Mark Expired**.
4. Click **Yes** to confirm.

### 6.3 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?

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.

### 6.3.1 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**

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.
- **Reports Console**: Installed into the Framework Manager console. Required for viewing audit information.
- **Command Reports Console**: Installed into the main Reports 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 Command Control” on page 162 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 Section 2.6.6, “Installing Packages on a Host,” on page 32 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.

6.3.2 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.
6.3.3 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 164.
- Account groups, user groups, and host groups, which determine who matches the rule. For configuration information, see “Command Control Groups” on page 171.
- Commands. For configuration information, see Section 6.3.4, “Commands,” on page 177.
- Credential Vault. For configuration information, see Contextual Help.
- Scripts for additional functionality. For configuration information, see “Scripts” on page 187.
- Access time to define specific time interval during which access is denied or granted. For configuration information, see “Access Times” on page 191.

**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 Section 3.1.4, “Configuring Permissions,” on page 41 for details.

The following additional features are provided to assist you with Command Control configuration and management:
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 167 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 165 for details.

You can also create and assign Perl scripts to the rule to provide additional functionality. See “Adding a Script” on page 188 and “Assigning a Script to a Rule” on page 169 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")-&gt;arg("job_default_env",0);
return 1;
```

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 165.

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 188.

**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 Reports 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 247). 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 **Section 8.2.4, “Configuring Video Capture,”** on page 303

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 to 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 188).

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 188). 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 168.

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 170 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 164 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.
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

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 wildcards 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:

User Groups

- “Adding a User Group” on page 172
- “Modifying a User Group” on page 173
- “Deleting a User Group” on page 173

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 173.

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, 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 Section 3.1.4, “Configuring Permissions,” on page 41).

   - 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,

```plaintext
=~/^vi .*$/
=~/w+\.netiq\.com
```

The following sections explain how to manage host groups:

- “Adding a Host Group” on page 174
- “Modifying a Host Group” on page 174
- “Deleting a Host Group” on page 175

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 174.

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.**

4 Specify a name for the account group.

5 Click **Add.**

Account groups are represented by the ** nº ** icon.

6 To configure the group, continue with “Modifying an Account Group” on page 175.

### 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, 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 Section 3.1.4, “Configuring Permissions,” on page 41).

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.

6.3.4 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 177
- “Adding a Command” on page 178
- “Modifying a Command” on page 178
- “Setting the Command Risk” on page 182
- “Removing a Command Risk” on page 183
- “Copying a Command” on page 183
- “Moving a Command” on page 183
- “Deleting a Command” on page 183
- “Importing Sample Commands” on page 183
- “Finding a Reference” on page 184
- “Defining Custom Attributes” on page 184
- “Functions” on page 184
- “Adding a Category” on page 186
- “Deleting a Category” on page 186
- “Blocked Users” on page 187
- “Adding Users in Blocked Users Group” on page 187
- “Deleting Users in Blocked User Group” on page 187
- “Scripts” on page 187
- “Access Times” on page 191
- “Command Control Reports” on page 193

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 178.

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 181. To use the **Rewrite** field to enable auditing of the command, see “Configuring Auditing with the Rewrite Functionality” on page 182
   **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 181
- “Configuring Auditing with the Rewrite Functionality” on page 182
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>
<thead>
<tr>
<th>Function</th>
<th>Rewrite</th>
<th>Submitted Command</th>
<th>Executed Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert all arguments ($0 is not displayed)</td>
<td>echo $*</td>
<td>1s passwd shadow fstab echo passwd shadow fstab</td>
<td></td>
</tr>
<tr>
<td>Insert argument 'r;n'</td>
<td>echo $3</td>
<td>1s passwd shadow fstab echo fstab</td>
<td></td>
</tr>
<tr>
<td>Insert all but argument 'n' ($0 is not displayed)</td>
<td>echo ${^2}</td>
<td>1s passwd shadow fstab echo passwd fstab</td>
<td></td>
</tr>
<tr>
<td>Insert arguments from 'n' to end</td>
<td>echo ${2-}</td>
<td>1s passwd shadow fstab echo shadow fstab</td>
<td></td>
</tr>
<tr>
<td>Insert arguments from 0 to 'n'</td>
<td>echo ${-2}</td>
<td>1s passwd shadow fstab echo 1s passwd shadow</td>
<td></td>
</tr>
<tr>
<td>Insert arguments from 'm' to 'n'</td>
<td>echo ${1-2}</td>
<td>1s passwd shadow fstab echo passwd shadow</td>
<td></td>
</tr>
<tr>
<td>Insert the total number of arguments</td>
<td>echo $#</td>
<td>1s passwd shadow fstab echo 3</td>
<td></td>
</tr>
<tr>
<td>Insert contents of argument $#</td>
<td>echo ${#$}</td>
<td>1s passwd shadow fstab echo fstab</td>
<td></td>
</tr>
</tbody>
</table>

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 247). 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
   - Web RDP users
   - 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.
If you want to change the order in which the commands are listed, use the arrow buttons.

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 **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 4-6 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

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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-b</td>
<td>Do not break lines to column width when displaying output.</td>
</tr>
<tr>
<td>-c</td>
<td>Do not remove the host from the list if the command fails.</td>
</tr>
<tr>
<td>-d</td>
<td>Add a time stamp to the displayed output.</td>
</tr>
<tr>
<td>-f &lt;num&gt;</td>
<td>Specify the maximum number of concurrent processes to run.</td>
</tr>
<tr>
<td>-g &lt;hostgrp&gt;, &lt;hostgrp wildcard&gt;</td>
<td>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/*</td>
</tr>
<tr>
<td>-l &lt;user&gt;</td>
<td>Specify the user to run the command as.</td>
</tr>
<tr>
<td>-q</td>
<td>Quiet. Do not display output.</td>
</tr>
<tr>
<td>-t &lt;timeout&gt;</td>
<td>Specify the timeout in seconds for the command to complete on each host.</td>
</tr>
<tr>
<td>-v</td>
<td>Verbose output.</td>
</tr>
<tr>
<td>-w &lt;host&gt;, &lt;host wildcard&gt;</td>
<td>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/*</td>
</tr>
</tbody>
</table>

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 6-3  udsh Keywords

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${uid}$</td>
<td>Calling user’s UID</td>
</tr>
<tr>
<td>${gid}$</td>
<td>Calling user’s primary group ID</td>
</tr>
<tr>
<td>${gecos}$</td>
<td>Calling user’s gecos</td>
</tr>
<tr>
<td>${home}$</td>
<td>Calling user’s home directory</td>
</tr>
<tr>
<td>${shell}$</td>
<td>Calling user’s shell</td>
</tr>
<tr>
<td>${cwd}$</td>
<td>Calling user’s current working directory</td>
</tr>
<tr>
<td>${lhost}$</td>
<td>Local hostname</td>
</tr>
<tr>
<td>${rhost}$</td>
<td>Remote hostname</td>
</tr>
<tr>
<td>${pid}$</td>
<td>PID of the individual udsh call</td>
</tr>
<tr>
<td>${ppid}$</td>
<td>PID of the udsh</td>
</tr>
</tbody>
</table>

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 187. 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 187.

**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 permissions. You can use these scripts only if a script is associated and evaluated as part of permission. Privileged Account Manager contains the embedded Perl interpreter which you can use for 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**

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 184 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 188.

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.
5. For some sample scripts, see “Sample Scripts” on page 189.
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 188.
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 189
- “pcksh Illegal Commands Script” on page 191

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.
Working With Access Policies

Sample Environment Script

```perl
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" && $a->value() =~ /^(.*)\s*=(.*)$/) {
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clearenv=1</td>
<td>Clears all environment variables (unless specifically kept using keepenv)</td>
</tr>
<tr>
<td>keepenv=VAR</td>
<td>Specifically keeps environment variables. As soon as this is set, all other</td>
</tr>
<tr>
<td></td>
<td>environment variables are deleted.</td>
</tr>
<tr>
<td>setenv=VAR=val</td>
<td>Sets up a specific environment variable.</td>
</tr>
<tr>
<td>unsetenv=VAR</td>
<td>Deletes a specific environment variable.</td>
</tr>
<tr>
<td>defaultenv=#</td>
<td>Sets the default environment:</td>
</tr>
<tr>
<td></td>
<td>0: Sets up no default environment variables.</td>
</tr>
<tr>
<td></td>
<td>1: Sets up all default environment variables.</td>
</tr>
<tr>
<td></td>
<td>2: Sets up default environment variables that do not already exist in the</td>
</tr>
<tr>
<td></td>
<td>environment.</td>
</tr>
</tbody>
</table>
```

Sample Environment Script

```perl
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" && $a->value() =~ /^(.*)\s*=(.*)$/) {
```
$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.

```sh
# 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

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 192.

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 192.

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.

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 194.

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 194.

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.

6.3.5 Command Control Options

Section contains all the 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

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 Section 10.2.1, “Importing and Exporting Command Control Settings,” on page 341.

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 Section 10.2.1, “Importing and Exporting Command Control Settings,” on page 341.

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 197
- “Making Command Control Configuration Changes with Transactions Enabled” on page 198
- “Committing a Transaction” on page 198
- “Backing Up and Restoring” on page 198
- “Defining Audit Settings” on page 199

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
equivalent, 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.

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.

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 Section 10.2.2, “Backing Up and Restoring a Command Control Configuration,” on page 341.

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.

### 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.
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.

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 Reports console to decrypt the password data.

Specify the password again in the Confirm password text box.

(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.

Click Finish.

**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**

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 201 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 165.)

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:
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:

```xml
<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 202.

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.
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 Section 10.2.3, “Running Test Suites,” on page 343.

**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.
   You can now run the test suite as explained in “Running a Test Suite” on page 202.

**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 restore 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.
6.3.6 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.

6.3.7 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 Reports 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 User Manager, refer Chapter 3, “Managing Users and Groups,” on page 39.
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 Reports console. To disconnect a user from the session on which an unauthorized command is used, perform the following steps in the Reports 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.

For information on setting the command risk refer “Setting the Command Risk” on page 182. 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 Section 6.4.1, “Configuring Emergency Access Settings,” on page 209.

**Viewing the Disconnect fields in the Reports Console**

In the Reports 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 Reports.
2. Click Command Control Reports then, click the required report.
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.

**SSH Relay Allow Commands**

The SSH Relay feature is enhanced to support allow commands. With this enhancement, on a privileged SSH session, the end user is allowed to run only the allowed commands and for all the other commands, the user would be denied command execution with a 'Permission Denied' message. This implementation is applicable from Privileged Account Manager 3.7 onwards.

The SSH Relay policy configuration remains as it is today. For the allow commands support, the same or similar policy can be enhanced by attaching a command control script to the Policy or Rule and by defining the allowed commands as Script Arguments to the Policy or Rule. Only one instance of the script must be created manually and the same can be attached to the Rule where the allow commands are to be applied. The particular Rule’s Script Arguments determines the commands that are allowed for the session authorized by that Rule.
When the user connects to Privileged Account Manager and establishes a privileged SSH session, if the authorizing Rule/Policy is associated with an allowed script and arguments, the user is presented with a list of allowed commands.

If the SSH Relay Rule is not associated with the particular script and its arguments then the policy behavior would be like a normal ssh-relay policy where the user would be given the privileged ssh session with no command restriction/control by SSH Relay server. The target server can be an SSH server or Telnet server.

**NOTE:** With this feature, the user is restricted or allowed to run only the commands that are allowed and the runUser (user on target) would be as per the Policy or Rule configuration. The target OS may also restrict the allowed command based on the runUser set on the Rule or Policy. For example, if `/sbin/fdisk` is a allowed command as per SSH Relay Policy or Rule and the runUser set on the Rule or Policy is a normal non-root user, then the user would still be denied access by the target Operating System permission as the command can be executed by a root-user only.

You can set up these permissions using the following procedure:

1. Click Administration Console > Command Control, create an SSH-Relay policy. You could also use the SSH Relay template to create this policy.
2. Create a new Command Control Script, name it as allow command. The contents of the script should be as below:
   ```perl
   my $cmds = $args->arg("Commands");
   if ($cmds) {
     $cmds =~ s//
/g;
     $meta->child("Command")->arg("CmdList", $cmds);
   }
   return 1;
   
   return 1;
   
3. Associate the script with the SSH policy by dragging the script and dropping it on to the SSH-Relay Rule.
4. The Commands are taken from ScriptArgs set on the SSH-Relay Rule. The name of the ScriptArgs should be Commands and the list of commands are delimited by new-line as shown in the below example. The command can also be a regex.

   ```
   ssh -t -p 2222 john@rhel8din
   Warning: Permanently added 'rhel8din:2222' (RSA) to the list of known hosts.
   john@rhel8din's password:
   0) Exit
   1) ssh relay - root@ssh
   Enter option (1-1): 1

   Allowed commands in this session are:
   1) id 2) /sbin/ifconfig*
   Password:
   Last failed login: Thu Dec 10 10:21:51 MST 2020 from 10.71.130.191 on ssh:notty
   There were 3 failed login attempts since the last successful login.
   vlab031509:~ # id
   ```
uid=0(root) gid=0(root) groups=0(root)
vlab031509:~ # /etc/passwd
Permission denied!
vlab031509:~ # /sbin/ifconfig
eth0    Link encap:Ethernet  HWaddr 00:50:56:86:F2:A2
        inet addr:10.204.101.237  Bcast:10.204.103.255
        Mask:255.255.252.0
        UP  BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:51746838 errors:0 dropped:245080 overruns:0
        frame:0
        TX packets:18860334 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:55836832085 (53250.1 Mb)  TX bytes:12912375114
       (12314.2 Mb)
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:17818674 errors:0 dropped:0 overruns:0 frame:0
        TX packets:17818674 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:8788789816 (8381.6 Mb)  TX bytes:8788789816 (8381.6 Mb)

6.4 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.

6.4.1 Configuring Emergency Access Settings

To configure emergency access settings, perform the following:

1. On the home page of the console click **Settings > Server Settings > Access Requests**.
2. 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.

**IMPORTANT:** All the resources of emergency access must be present in Credential Vault.

### 6.4.2 Managing Emergency Access Requests

You can analyze a user’s requests to access applications and then either grant access for a specific duration or deny the request.

If you detect any malicious activity on a resource after you grant access, you can revoke a user’s access to the resource. If you revoke a request while a user is accessing a resource, the user can continue to use the resource until the session is disconnected. However, the user will not be able to start a new session to the resource.

Settings such as the email ID to which requests are sent to, the duration after which a request must be deleted, and so on are configured by default. To change the default settings, see Configuring Emergency Access Settings.

**NOTE:** You cannot approve a request if a user is in the Blocked Users user group. For more information about removing a user from the Blocked Users user group, see “Blocked Users” on page 187.

**To approve a request:**

1. Select a pending request from **Dashboard > Requests. All or PENDING.**
2. Click Approve.
3. Perform the following based on the type of privileged access:
   - For more information on the completing the prerequisites in Credential Vault, see Section 5.1, “Credential Vault,” on page 73.
<table>
<thead>
<tr>
<th>Request Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td><strong>Connection Type:</strong> Select SSO when you need privileged single sign on access to Windows agent. When you select this option you get single sign on access through Privileged Account Manager proxy as well as Privileged Account Manager credential provider. Select <strong>Direct Access</strong> when you want to access the Windows directly using the server credentials.</td>
</tr>
<tr>
<td>Windows Web Access</td>
<td><strong>Connection Type:</strong> Select the application or computer you want to access such as, Windows RDP and Windows Web RDP. Select <strong>Web Access</strong> when you want to access the Windows agent directly using the server credentials. Select <strong>&gt; Active Sessions</strong> to view the active sessions.</td>
</tr>
<tr>
<td>SSH/Telnet</td>
<td><strong>Connection Type:</strong> Select SSH or Telnet based on the connection method the target system supports. <strong>Enable X11:</strong> Select this option to get X11 application access through SSH.</td>
</tr>
<tr>
<td>SSH Web Access</td>
<td><strong>Connection Type:</strong> Select SSH or Telnet based on the connection method the target system supports. Select <strong>&gt; Active Sessions</strong> to view the active session.</td>
</tr>
</tbody>
</table>
| Privileged Shell  | 1. In **Credential Vault:**
  a. Register the target machine for which the request is sent, as an agent.
  b. Set up the user’s account on the target machine.
  2. Specify the required **Run User**. Specify the name of the user as whom a requesting user can start the session. For example, if the requesting user wants to run the session as root, specify **Run User** as **root**. |
| Database          | **Database:** Select the database you want to access. **Password Checkout:** Select this option to check out credentials to access the database. **Database Access:** Select this option when you know the credentials to access the database but you need access to the database through Privileged Account Manager proxy. |
| Applications      | 1. In **Credential Vault**, configure the **Resources** for the required application. 2. To share the application’s host details with the user as a part of the approval comment, select the **Send Run Host ID to the User** check box. |
6.4.3 Creating Emergency Access Requests

To create an emergency access request:

1. From > Requests > New Request.
2. Select the required target.
3. Configure the following based on the selected target:

<table>
<thead>
<tr>
<th>Request Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application SSO</td>
<td>In Credential Vault, add the application credential for application SSO using RemoteApp mode or direct access mode.</td>
</tr>
</tbody>
</table>

Based on the type of application SSO modes, do one of the following:

- **RemoteApp Mode**
  1. Select RemoteApp and select the required credential.
  2. Select the domain user created for SSO. For more information about creating users, see Creating an Active Directory User.
  3. Select the application credential for SSO.
  4. (Conditional) Select Video Offload to convert session images to video in a video off-load server.

- **Direct Access Mode**
  2. Select the application credential for SSO.
  3. Select Video Offload to convert session images to videos in a video off-load server.
  4. Create direct RDP and run as privileged user rules. For more information on creating these rules, see Adding a Direct RDP Rule and Adding a Rule to Run Application as a Privileged User.

**Application SSO Web Access**

- **Connection Type**: Select the application or computer you want to access.
  - Select Web Access when you want to access the Windows directly using the server credentials.
  - Select > Active Sessions to access the active session.

**Application Credential**

- **Application**: Select the application for which you want to get the credentials.

4. Click Approve.
### Target Actions

<table>
<thead>
<tr>
<th>Target</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Select the <strong>Connection Type</strong> as follows:</td>
</tr>
<tr>
<td></td>
<td>- Select the <strong>SSO</strong> when you need privileged single sign on access to Windows. When you select this option you get single sign on access through PAM proxy as well as PAM credential provider.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>Direct Access</strong> to access Windows directly using the server credentials.</td>
</tr>
<tr>
<td>SSH/Telnet</td>
<td>Select the <strong>Connection Type</strong> as <strong>SSH</strong> or <strong>Telnet</strong> based on the connection method the target system supports.</td>
</tr>
<tr>
<td>Database</td>
<td>1. Select the required database.</td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>Credential Checkout</strong> to check out credentials to access the database.</td>
</tr>
<tr>
<td></td>
<td>3. Select <strong>Database Access</strong> when you know the credentials to access the database but you need access to the database through PAM proxy.</td>
</tr>
<tr>
<td>Privileged Shell</td>
<td>Choose this option to get elevated access to the UNIX/Linux workstation using your local credentials.</td>
</tr>
<tr>
<td>Application SSO</td>
<td>Select this option if you need SSO access to an application or a Windows machine.</td>
</tr>
<tr>
<td>Application Credential</td>
<td>Select this option if you need credentials to access an application.</td>
</tr>
</tbody>
</table>

4 Specify the following details for all the target resources:

4a Specify the hostname or IP address of the target resource which you want to access, wherever applicable.

4b Select **Normal User** to access the resource without any privileges or select **Super User** when you want privileged access to the resource.

4c Specify the duration for which you want access to the resource.

4d Specify the email address for receiving notification about the status of the request.

5 Click **Create**.

You will receive an email notification after a request is created. Whenever the status of the request changes, you will receive a notification and an email.

6 From **Requests** to view emergency requests.
7 Configuring Privileged Access

7.1 Agent and Agentless Capability

Agent is an installable component that resides on a machine and helps to manage and monitor privileged access to the machine. It creates comprehensive session audits and video recordings of the privileged sessions of the machine beyond the limits of the Agentless approach. This approach requires regular maintenance and is not suitable for a sophisticated environment.

Agentless enables you to secure, manage and monitor privileged access to remote machines through the PAM User Portal. This approach provides monitoring of computers without agents by using a proxy agent and applying those management packs that support agentless monitoring. The ability to capture session audits and create video recordings of the privileged sessions varies from one agentless module to another. This approach is easy to manage as new updates to the agent need not be applied.

Clientless enables users to connect through a web browser and use HTTPS connections. Clientless solutions provides access to the web-based resources without any client. On demand client - Users connect through a web browser and a client is installed when necessary. The client supplies access to most types of corporate resources according to the access privileges of the user.

Privileged Account Manager provides both these capabilities. Refer to “Remote Desktop Protocol Web Relay” on page 234 and Section 7.3.3, “Agentless Session Management in Unix and Linux,” on page 253 to use SSH and RDP on Linux/Unix and Windows machines respectively to reap agentless as well as clientless benefits. Browser refresh disconnects the active sessions for both SSH Web and RDP Web.

Figure 7-1  Agentless Capability

The following tabular overview illustrates the agent and agentless features available in the product.
<table>
<thead>
<tr>
<th>Methods</th>
<th>Key Stroke Audit</th>
<th>Command Audits</th>
<th>Video Capture</th>
<th>High level Session Audits (Who got access to what and how)</th>
<th>Session Level Elevation</th>
<th>Command Risks</th>
<th>Automatic Disconnect</th>
<th>Manual Disconnect</th>
<th>Live Video Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux/Unix/Network Devices/SSH Servers</td>
<td>Agent</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Agentless (SSH Relay)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agentless (SSH Web Relay)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>Agent-Direct/CP Connection</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agent-Proxy Connection (RDP Relay)</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agentless-Proxy Connection (RDP Web Agent Relay)</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agent (appss o)</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
7.1.1 Sample Use Cases for Agentless Capability

This section describes different requirements and configurations required to achieve the requirement using the following sample use cases:

- Securing and Monitoring Web Based RDP Sessions without Installing Privileged Account Manager Agent
- Examining the Elevated SSH Session without the Thick Client

Securing and Monitoring Web Based RDP Sessions without Installing Privileged Account Manager Agent

Let us assume, an organization Intech Data, Inc. wants to secure and monitor employees’ action during the privileged access to Windows Server that is located in the network lab. This Windows Server contains confidential data.

Employees can access this server without using the remote desktop client. A few employees can access it remotely only during the business hours (9 AM to 6 PM) on business days (Monday to Friday).

This example refers to the following user profiles:

- Markus: An administrator of Intech Data, Inc.
- Albert Jones: An employee of Intech Data, Inc.

Markus wants to enforce Windows Agentless Web RDP to secure the Windows server. With this implementation, designated employees can access the Windows server through PAM User console for privileged access, and each action is recorded and monitored for auditing purposes. If employees perform any action that poses potential risk, such as deleting, copying data, and so on, the actions are recorded. Markus can suspend the just-in-time session if he is monitoring the active session.

The following diagram depicts the requirement of this use case:
This section explains the prerequisites, flow of actions, and step-by-step configuration details to achieve this requirement.

**Flow Diagram**

The following diagram illustrates the sequential flow of configuration required for implementing the Windows Agentless Web RDP:

1. **Add Active Directory Services as the LDAP Server**
2. **Create resource for Windows Server in Credential Vault**
3. **Define a User Role for the LDAP users or group**
4. **Create a Resource pool with Windows vault for Agentless Windows Servers**
5. **Create an Assignment for RDP Web and grant required permission**
6. **Administration Console > Reports**
7. **Windows Server**
8. **Privileged Access via User Console**
9. **Recorded actions and video capture are stored in Reports**

End-user (Albert Jones)
To achieve this requirement, Markus performs the following tasks:

1. Configure the LDAP Repository
2. Add a Resource
3. Defining a User Role
4. Create a Resource Pool
5. Create an Assignment and Grant Permission

Prerequisites

- Privileged Account Manager is installed with the required Agentless module.

**NOTE:** The agentless component of Privileged Account Manager (agentless) is supported on SLES 12 (64-bit), SLES 15 (64-bit), Oracle Linux 8 (64-bit), and RHEL 8(64-bit).

- Enable the Access Control Engine option in Server Settings > Policy Engine.
- Import the CA certificate on the system where Privileged Account Manager is installed to enable communication over Secure Sockets Layer (SSL).
  
  For more information, see Exporting the Certificate From the Active Directory Server.

Configure the LDAP Repository

1. Click Settings on the Administration Console.
2. Click LDAP Servers on the left pane and click Add New.
3. Perform the following actions:
   
   3a Specify Domain Name of the LDAP Server.
   
   3b Type is set to Active Directory Services, by default.
   
   3c Specify Host Name/IP Address of the LDAP Server.
   
   **NOTE:** Port is set to 636, by default.
   
   3d Select SSL and Verify Certificate to secure the connection via SSL by using the CA certificate.
   
   3e Click GetBaseDN to fetch the appropriate details.
   
   3f Set Scope to Subtree.
   
   3g Specify User DN, User Name, and Password that are required for retrieving the user details and domain details for authentication.

4. Click Save.

Add a Resource

A resource is a network device, application, repository, or data storage device to which users can get privileged access.

1. Click Credential Vault on the Administration Console.
2. Click +Add > Windows > Windows Host.
3. In Name, specify a name for Windows Server.
   
   For this example, the resource name is set to winsrv16.intech.com.
4 Click Next.
5 Perform the following actions to configure the Connection details:
   5a In Host Name/IP Address, specify the host name or IP address of Windows Server.
      
      **NOTE:** Port is set to 3389, by default.

   5b Select Active Directory Domain displays the list of domains if the specified host name is associated to a domain.
      In this example, Windows Server is a standalone device and does not need to be associated to any Active Directory Domain.

6 Click Next.
7 Click Finish.
8 Click the resource that you have added and click Credentials tab.
9 Click Add.
10 Specify the User Name, Password, and Privilege Type required to access Windows Server.

**Defining a User Role**

1 Click Access Control > User Roles > Create.
2 Specify the role name in Name and additional information about the role in Description.
3 Click Next.
4 Click +Add > LDAP Users and Groups.
5 Select the domain and select the preferred user or group.
   In this example, the user **AlbertJ** is selected.
6 Click Add > Create.

**Create a Resource Pool**

1 Click Access Control > Resource Pools > Create.
2 Specify Name and Description for this resource pool.
   For this example, the resource pool name is set to **Windows Server with AD Users**.
3 Select Type as Windows Servers under Agentless.
4 Click Next.
5 Click Add and select the resource that you added in Add a Resource.
6 Click Add.
7 Select Default Credentials that is required to allow users to access the resource.
8 Click Create.

**Create an Assignment and Grant Permission**

1 Click Access Control > Assignments > Create.
2 Select the Resource Pool that you created in Create a Resource Pool.
3 Select the User Role that you defined in Defining a User Role.
The Description gets generated with the name that you have provided for Resource Pool and User Role.

4 Click Add and select Web RDP permission in the Privilege Elevation window.

**NOTE:** By default, Credential is set to Default to allow users to access Windows Server with the default credentials that is configure for the resource.

5 Click Next.

6 Select Custom Days and set the days and time frame as follows:
   6a Select Mon to Fri as the days.
   6b Specify 9 to 6 as time frame for the selected days.

7 Click Next.

8 Disable Secondary Authentication.

9 In User Message, specify a message that is displayed to users on connecting to the resource.

10 Click Next > Finish > Create.

After Markus implements Windows Agentless Web RDP, the following are possible scenarios:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albert logs in to the User Console and accesses the Windows Server. Later, he installs software and configures it.</td>
<td>Each action is recorded, the live session video is captured, and stored in Reports. No malicious activity is detected.</td>
</tr>
<tr>
<td>Albert wants to access Windows Server on Thursday at 8 PM.</td>
<td>The Windows Server resource is not available on the User Console for Albert. As Windows Server is accessible from 9 AM to 6 PM.</td>
</tr>
<tr>
<td>Albert installs a malware on Windows Server unintentionally.</td>
<td>The install procedure is recorded. When Markus checks the report and notices malware installation, he notifies Albert to uninstall the identified malware.</td>
</tr>
<tr>
<td>Markus is monitoring the live session and Albert attempts to delete the server configuration.</td>
<td>Markus terminates the session. Later, he drafts a mail with the reason and sends it to Albert.</td>
</tr>
</tbody>
</table>

**Examining the Elevated SSH Session without the Thick Client**

Let us assume an organization, Intech Data, Inc. wants to assess the user actions during the elevated session to the Linux system that functions as the Web Server of the organization. The Linux system is accessed without the thick clients, such as PuTTY, MobaXterm, and so on. In the elevated session, an employee can access Linux system with the root permissions.

This example refers to the following user profiles:

- Markus: An administrator of Intech Data, Inc.
- Silvia Pereria: An employee of Intech Data, Inc.

Markus wants to implement Linux Agentless Web SSH to secure the elevated session from internal misuse. With this implementation, authorized employees can access Linux system through the User Console for elevated access and each Keystore is captured and recorded for auditing purposes. Also,
Markus has the authority to inspect the live session and perform the following upon noticing any suspicious activity, such as changing the system configuration, installing an unauthorized application, and so on:

- Terminate the active session and send a notice to the user
- Block access to the elevated session

The following diagram depicts the requirement of this use case:

This section explains the prerequisites, flow of actions, and step-by-step configuration details to achieve this requirement.
Flow Diagram

The following diagram illustrates the sequential flow of configuration required for implementing the Linux Agentless Web SSH:

1. Add LDAP Repository
2. Add Linux System as a Resource
3. Define User Role
4. Create a Resource Pool
5. Create an Assignment and Grant Permission

Prerequisites

- The Privileged Account Manager is installed with the required Agentless module.

**NOTE:** The agentless component of Privileged Account Manager (agentless) is supported only on SLES 12 (64-bit), SLES 15 (64-bit), Oracle Linux 8 (64-bit), and RHEL 8(64-bit).

- Ensure to enable the Access Control Engine option in Server Settings > Policy Engine.
- Import the CA certificate on the system where you have installed Privileged Account Manager to enable communication over Secure Sockets Layer (SSL).
  For more information, see Exporting the Certificate From the Active Directory Server.

Add LDAP Repository

1. Click Settings on the Administration Console.
2. Click LDAP Servers on the left pane and click Add New.
3. Perform the following actions:
   a. Specify Domain Name of the LDAP Server.
   b. Specify Host Name/IP Address of the LDAP Server.

   NOTE: By default, Type is set to Active Directory Services and Port is set to 636.

   c. Select SSL and Verify Certificate to secure the connection via SSL by using the CA certificate.
   d. Click GetBaseDN to fetch the appropriate details.
   e. Set Scope to Subtree.
   f. Specify User DN, User Name, and Password that are required for retrieving the user details and domain details for authentication.
4. Click Save.

Add Linux System as a Resource

1. Click Credential Vault on the Administration Console.
2. Click +Add > Linux/Unix/Network Device > SSH.
3. In Name, specify a name for the Linux system.
   For this example, the resource name is set to lnx-mchs.intech.com.
4. Click Next.
5. Perform the following to configure the Connection details:
   a. In Host Name/IP Address, specify the host name or IP address of the Linux system.

   NOTE: Port is set to 22 by default.
   b. Click Get Host Key to get the key of the specified machine.
6. Click Next.
7. Click Finish.
8. Click Count of the resource that you have added.
9. Click Add in the Credentials tab.

   NOTE: Credential Type is set to Password by default, this grants elevated access to the resource using the specified Password.
10. Specify the User Name, Password, and Privilege Type required to access Linux system.
11. Click Add.
Defining a User Role

1. Click Access Control > User Roles > Create.
2. Specify the role name in Name and additional information about the role in Description.
3. Click Next.
4. Click +Add > LDAP Users and Groups.
5. Select the domain and select the preferred user or group.
   In this example, the user Silvia is selected.
6. Click Add > Create.

Create a Resource Pool

2. Specify Name and Description for this resource pool.
   For this example, the resource pool name is set to inx-ssh-pool.
3. Select Type as SSH Servers under Agentless.
4. Click Next.
5. Click Add and select the resource that you added in Add Linux System as a Resource.
6. Click Add.
7. Select Default Credentials that is required to allow users to access the resource.
8. Click Create.

Create an Assignment and Grant Permission

1. Click Access Control > Assignments > Create.
2. Select the Resource Pool that you created in Create a Resource Pool.
3. Select the User Role that you defined in Defining a User Role.
   The Description gets generated with the name that you have provided for Resource Pool and User Role.
4. Click Add and select Web SSH permission.

**NOTE:** By default, the Credential is set to Default in the Privilege Elevation window.
5. Click Next.

**NOTE:** Time Restriction is set to All Days (24 hours) by default, allowing Linux system to be accessible for 24 hours without any restriction.
6. Click Next.
8. In User Message, specify a message that is displayed to users on connecting to the resource.
9. Click Next > Finish > Create.
After Markus implements **Linux Agentless Web SSH**, the following are possible scenarios:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silvia logs in to the User Console and accesses the elevated session on Linux. Later, she executes some commands.</td>
<td>Each command is recorded and the live session video is captured. No malicious activity is detected.</td>
</tr>
<tr>
<td>Silvia installs malware on Linux SSH unintentionally.</td>
<td>The install procedure is recorded. When Markus goes through the recorded session and notices malware installation, he notifies Silvia to uninstall the identified malware.</td>
</tr>
<tr>
<td>Markus is monitoring the live session and Silvia attempts to modify the security controls.</td>
<td>Markus terminates the session and blocks access to Linux SSH. Later, he drafts a mail with the reason and sends it to Silvia.</td>
</tr>
<tr>
<td>Silvia deletes a configuration file.</td>
<td>The action is recorded and saved in the <strong>Reports</strong>. Markus can take relevant actions while auditing the report.</td>
</tr>
</tbody>
</table>

## 7.2 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](#).

- **Remote Desktop Protocol Web Relay (RDP relay)**: Using this method, you can create a policy for a windows RDP web relay which can be accessed by the user from the User Console.

  For information about configuring RDP Web Relay, see [Remote Desktop Protocol Web 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 Privileged Account Manager 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 administrator 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 Privileged Account Manager agent.

  For information about configuring application SSO, see Configuring RemoteApp Mode Using Command Control.

Based on the information in the following table, you can choose the appropriate method to establish privileged session in windows system:

<table>
<thead>
<tr>
<th>Method</th>
<th>Keystroke Audit</th>
<th>Video Capture</th>
<th>Privileged Access</th>
<th>Live Session View</th>
<th>Command &amp; Automatic Session Disconnect</th>
<th>Access Through</th>
<th>Authentication Through</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDP Relay</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>(Agent based)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RDP Web Relay (Agentless)</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credential Provider</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>(Agent based)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct RDP</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>(Agent based)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 7.2.1 Work Flow to Configure Privileged Access for Windows

This is the generic work flow that must be followed to configure privileged access for Windows:

1. **Register the agent (Conditional)**
   - For steps to register the agent, refer to [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 to “Adding a User Group” on page 172.

4. **Add a Command**
   - You can use the commands that are preloaded by Privileged Account Manager that is loaded with 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 to “Adding a Command” on page 178.
     - For detailed information on modifying a command, refer to “Modifying a Command” on page 178.

5. **Add and Modify a Rule**

### Table: Privileged Access Methods

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Run as Privileged User</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>(Agent based)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Audits only privileged application access)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application SSO</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>(Agentless)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Privileged access to specific application)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Keystrokes are not audited in the Windows Command Prompt.
For steps to add a rule, refer “Adding a Rule” on page 164

**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 165

**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.

7.2.2 Agent-Based Session Management In Windows

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 229
- “Remote Desktop Protocol Web Relay” on page 230
- “Credential Provider” on page 231
- “Direct Remote Desktop Protocol” on page 232

**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 230
- “Accessing the RDP Relay” on page 230
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 “Work Flow to Configure Privileged Access for Windows” on page 228

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.

Accessing the RDP Relay

After a RDP relay is configured by an administrator, the user can access the privileged session as follows:

1. Click on home icon on the new Administration console.
2. Specify the username and password to log in to Privileged Account Manager and click Login.
3. Click > My Access and click the launch icon before the appropriate resource name.
4. You can administer the active Remote Desktop Protocol Web Relay session as it opens in > Active Sessions. The administrator audits the user actions in this privileged session and views these reports in the administration console.
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.

Remote Desktop Protocol Web Relay

Privileged session monitoring and management is important for achieving the compliance and security requirements, but can be complex and time-consuming to achieve. Privileged account Manager 4.0 onwards you can monitor and manage RDP sessions with agent-based web relay capability.
Usage Scenario for Agent-based Windows Web RDP Relay

Consider a scenario where the administrator has to provide privileged access to Windows Agent and the Privileged Account Manager user can access the session from the browser. For this scenario, the administrator must perform the following configuration in Access Control:

1. Create a Windows or LDAP type Credential Vault resource for the Windows agent and add the respective credentials.
2. Go to Hosts console (Old Administration Console) and double click Windows Agent and add the vault created in the previous step to the vault label.
3. Go to new administration console and click Users and add the users (LDAP or Local) who will be using the resource.
4. Click Access Control > Users and create a user group and add the users who can access the resource. For more information, see “Configuring a User Role” on page 146.
5. Click Access Control > Resource Pools and create a resource group and add the Windows Vault for Agent-based Windows Servers. For more information, see “Configuring Access Control” on page 144.
6. Click Access Control > Assignments and create a Web Agent RDP and add the user group and resource pool that you created in steps 2 and 3 to it.
7. Assign the permissions as relevant.
8. Click Finish. After the administrator configures the authorization rule in Privileged Account Manager, the Privileged Account Manager user can get access to privileged session using steps 9, 10, and 11.
9. Log in using the Privileged Account Manager user credentials and click Login.
10. Click > My Access and click the launch icon before the appropriate resource name.
11. You can administer the live Remote Desktop Protocol Web Relay session as it opens in > Active Sessions. The administrator audits the user actions in this privileged session and views these reports in the administration console.

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, “Prerequisites for Disconnecting a Session” on page 205.

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 Reports 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 Using Command Control

You can create a rule to allow/deny access to specific users on a Windows server or desktop to connect to the required server.

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 an 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 are not monitored but in the Reports console you can view the users who are connecting to the server or desktop, and the time when they started the session.
7.2.3 **Agentless Session Management in Windows**

Privileged session monitoring and management is important for achieving the compliance and security requirements, but can be complex and time-consuming to achieve. Privileged account Manager 4.0 onwards you can monitor and manage RDP sessions with agentless capability.

**Prerequisites for Agentless Session Management in Windows**

Ensure that the agentless module is installed.

- The agentless component of Privileged Account Manager (agentless) is supported only on SLES 12 (64-bit), SLES 15 (64-bit), Oracle Linux 8 (64-bit), or RHEL 8 (64-bit).

**NOTE:**
- For Oracle Linux 8 (64-bit) and RHEL 8 (64 bit), install the redhat-lsb-core package.
- For SLES 12 (64-bit) and SLES 15 (64-bit), install the lsb-release package.
- You must install libpango and libcairo, and the dependent packages for both SLES and RHEL. Additionally for RHEL alone install dejavu-sans-fonts.

**Remote Desktop Protocol Web Relay**

This method has agent less access benefits. This feature works without any agent installed in the target machine. Using this method, you can provide access to the target RDP machine through a standard RDP client. This feature provides the ability to access Privileged Account Manager functionality without an agent for Privileged Account Manager on the target host. RDP Relay allows users to connect to a remote host without knowing the privileged account credentials such as password or identity certificate of the user. RDP Relay session videos can be captured only if the Privileged Account Manager is in Linux environment.

The functionality also provides clientless benefits. It is called "clientless" because no plugins or client software is required. Remote desktop gateway supports standard protocols like VNC, RDP, and SSH. Once the agentless module is installed all you need to access your desktops is a web browser.

**NOTE:** You cannot add scripts when you are using RDP Web Relay.

**Advantages of Configuring the Remote Desktop Protocol Web Relay**

- You can configure a RDP Web Relay for Windows machines to allow users to remotely access these machine without the privileged account credentials
- This method is beneficial if you do not want any operating system installed software or client.
- Resolves issues with Network level Authentication users as they do not have to do any additional configurations.
- No requirement of MSTC-RDP file to be downloaded. System from which you launched the RDP session can be lightweight in terms of space and memory.
Accessing the Remote Desktop Protocol Web Relay

After a RDP Web relay is configured by an administrator, the user can access the privileged session as follows:

1. Log in using the Privileged Account Manager user credentials and click Login.
2. Click > My Access and click the Start Session icon adjacent to the preferred resource name.
3. You can administer the active Remote Desktop Protocol Web Relay session as it opens in > Active Sessions. The administrator audits the user actions in this privileged session and views these reports in the administration console.

Usage Scenarios for Agentless Windows RDP Relay

Consider a scenario where the administrator has to provide privileged access to Windows system and the Privileged Account Manager user can access the session from the browser. For this scenario, the administrator must perform the following configuration in Access Control:

1. Create a Windows or LDAP type Credential Vault resource for the Windows system and add the respective credentials.
2. Click Users and add the users (LDAP or Local) which will be using the resource.
3. Click Access Control User Roles and create a user group and add the users who can access the resource.
4. Click Access Control Resource Pools and create a resource group and add the Windows Vault for Agentless Windows Servers
5. Click Access Control Assignments and create an RDP Web and add the user group and resource pool that you created in steps 2 and 3 to it.
6. Assign the permissions as relevant.
7. Click Finish.

After the administrator configures the authorization rule in Privileged Account Manager, the Privileged Account Manager user can gain privileged session as follows:

1. Log in using the Privileged Account Manager user credentials and click Login.
2. Click > My Access and click the launch icon before the appropriate resource name.
3. You can administer the live Remote Desktop Protocol Web Relay session as it opens in > Active Sessions. The administrator audits the user actions in this privileged session and views these reports in the administration console.

The administrator audits the user actions in this privileged session and views these reports in the administration console.

7.2.4 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 Privileged Account Manager agent.

For information about configuring application SSO, see Configuring RemoteApp Mode Using Command Control.

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 236
- “Accessing Windows System to Run as privileged user” on page 236

Configuration to Run as Privileged user

For configuring the windows machine to Run as Privileged, see “Work Flow to Configure Privileged Access for Windows” on page 228

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.
7.2.5 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 237
- “Defining the User Group” on page 237
- “Creating a Rule for the LDAP Group” on page 238
- “Modifying a Rule for the LDAP Group” on page 238
- “Enabling Virtual List View” on page 239

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 172.

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**: Includes the users you have added in this 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.
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 164.

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>

**Enabling Virtual List View**

Virtual List View (VLV) allows you as the LDAP application developer to query a very large directory container in efficient and bite-sized chunks. Virtual List View is enabled by default on eDirectory.

**Enabling Virtual List View on Active Directory:**

1. Click **Start > Run** type `Adsiedit.msc` and **ENTER**.
2. In the **ADSI Edit** tool, expand the `Configuration[DomainController]` node.
3. Expand the `CN=Configuration,DC=DomainName` container.
4. Expand the `CN=Services` object.
5. Expand the `CN=Windows NT` object.
6. Right-click the `CN=Directory Service` object.
7. Click **Properties**.
8. In the **Attributes** list, click `msds-Other-Settings > Edit`.
9. In the **Values** list, click any instance of `DisableVLVSupport=x` where `x` is not equal to 0, and click **Remove**.
10. Click **OK** twice. Close the **ADSI Edit** tool.

**Installing schema and sort control:**

1. Open a command prompt and type `regsvr32 schmmgmt.dll` command, and then press **ENTER**.
2. Click **Start Run**.
3. Type `mmc` and then click **OK**.
4. On the **File** menu, click **Add/Remove Snap-in**.
5. In the **Available snap-ins** field, click **Active Directory Schema Add OK**.
6. Click on the created schema search for `cn → properties → enable`. Index this attribute for containerized searches.

**Enabling Virtual List View on OpenLDAP:**

1. Bind to the server that you want to perform the search on using `ldap_bind` or `ldap_bind_s`.
2. Set the members for `LDAPVLVInfo` and create the control using `ldap_create_vlv_control`.
3. Create a sort control using `ldap_create_sort_control` and add it to an array with the VLV control.
4. Perform a search on the server using `ldap_search_ext_s` or `ldap_search_ext`. 
5. Parse the results from the server using `ldap_parse_result`, then parse the vlv results received from the response control (LDAP_CONTROL_VLVRESPONSE) using `ldap_parse_vlv_control`.

6. Free the control using `ldap_control_free`.

### 7.3 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 provide privileged access to specific UNIX or Linux command. This package is installed as part of the Command Control Agent.

- **Secure Shell Relay (SSH Relay)**: Using this method, you can provide access to the target SSH machine through a standard SSH client.

- **SSH Web Relay**: The functionality provides the benefit of achieving SSH relay to target servers without a requirement of installation of a client or an agent as the SSH session can be achieved in the web browser itself. This functionality requires an "Agentless module" to be installed on Privileged Account Manager Linux manager. For more information, see “Secure Shell Web Relay” on page 253.

- **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 Configuring RemoteApp Mode Using Command Control.

Based on the information in the following table, you can choose the method to establish privileged session in Unix or Linux system:
### Session Replay

Session replay is replay of the SSH user’s terminal input and output.

<table>
<thead>
<tr>
<th>Methods</th>
<th>Audit</th>
<th>Video Capture</th>
<th>Privileged Access</th>
<th>Live Session View</th>
<th>Command Risk &amp; Automatic Session Disconnect</th>
<th>Access Through SSH Client</th>
<th>User Console</th>
<th>System Account</th>
<th>Privileged Account Manager Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>pcksh (Agent-based)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cpcksh (Agent-based)</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>usrun (Agent-based)</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>SSH Relay (Agentless)</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>SSH Web Relay (Clientless)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

(Audits all the user actions in the privileged shell)

(Audits only the commands that has usrun as a prefix)

(Session replay* of SSH session along with video capture of X11 window.)
7.3.1 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**
   
   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 172.

4 **Add and Modify the Command**
   
   For steps to add a command, see “Adding a Command” on page 178. 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 178.

5 **Add a Rule**
   
   For steps to add a rule, see “Adding a Rule” on page 164.

   **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.

7.3.2 Agent-Based Session Management in Unix and Linux

Privileged session and session capture can be achieved through the following methods:

- “pcksh” on page 243
- “cpcksh” on page 247
- “Secure Shell Relay” on page 248
**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.

**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 243**
- **“Accessing pcksh for a Privileged Session” on page 243**
- **“Usage Scenario” on page 244**

**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 **“Work Flow to Configure Privileged Access for Windows” on page 228**

**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.

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 187**.

You can also define illegal commands, including built-in shell commands, in a script assigned to the rule.
**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 245
- “Accessing pcksh for Complete Session Capture” on page 245

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 “Work Flow to Configure Privileged Access for Windows” on page 228

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set -o host &lt;hostname&gt;</td>
<td>Specifies that all authorized commands are executed on the defined host, if permitted.</td>
</tr>
<tr>
<td>set -o user &lt;username&gt;</td>
<td>Specifies that all authorized commands are executed as the defined user if permitted.</td>
</tr>
</tbody>
</table>
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 167), 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:

```bash
#!/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**

To get complete session capture using *cpcksh*, the administrator must make appropriate configurations in Privileged Account Manager.

**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.

**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:**
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 Privileged Account Manager is in Linux environment.

- “Configuring an SSH Relay Session” on page 249
- “Accessing an SSH Relay Session” on page 249
- “Usage Scenarios for Agent-Bases Secure Shell Relay” on page 249
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.

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 249
- “Accessing an SSH Relay Session from SSH Client” on page 249

Accessing an SSH Relay Session from My access console

1. Click on home icon on the new Administration console.
2. Specify the username and password to log in to Privileged Account Manager and click Login.
3. Click > My Access and click the launch icon before the appropriate resource name.
4. You can administer the SSH Relay session as it opens in > Active Sessions. The administrator audits the user actions in this privileged session and views these reports in the administration console.

Accessing an SSH Relay Session from SSH Client

1. You can initialize an SSH relay session by using the following command:
   
   ssh -t -p 2222 <PUMframeworkuser@sshrelayhost> <root@hostname>
   
   To initialize an SSH relay session with X11 forwarding, use the following command:
   
   ssh -X -t -p 2222 <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 for Agent-Bases Secure Shell Relay

Scenario 1:

Consider a scenario where the administrator has to provide privileged access to a Privileged Account Manager 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 Privileged Account Manager, the Privileged Account Manager user can gain privileged session as follows:

1. Click on home icon on the new Administration console.
2. Specify the username and password to log in to Privileged Account Manager and click Login.
3. Click  > My Access and click the launch icon before the appropriate resource name.
4. You can administer the SSH Relay session as it opens in  > Active Sessions. 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 Privileged Account Manager 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.
   - **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 Privileged Account Manager, the non-privileged Linux or UNIX user can gain privileged session as follows:

1 Log in using the Privileged Account Manager user credentials and click **Login**.
2 Click ➩ > *My Access* and click the launch icon before the appropriate resource name.
3 You can administer the SSH Relay session as it opens in *Home > Active Sessions*. 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 Privileged Account Manager 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 Privileged Account Manager 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 Privileged Account Manager, the Privileged Account Manager user can gain access to the session as follows:

1 Log in using the Privileged Account Manager user credentials and click **Login**.

2 Click **> My Access** and click the launch icon before the appropriate resource name.

3 You can administer the SSH Relay session as it opens in **> Active Sessions**. 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 Privileged Account Manager 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 Privileged Account Manager user can gain access to the session as follows:

1. Log in using the Privileged Account Manager user credentials and click **Login**.
2. Click **My Access** and click the launch icon before the appropriate resource name.
3. You can administer the active Remote Desktop Protocol Web Relay session as it opens in **Active Sessions**. The administrator audits the user actions in this privileged session and views these reports in the administration console.

### 7.3.3 Agentless Session Management in Unix and Linux

Infrastructure and application monitoring is shifting from an agent-based approach to an agentless one. Agentless monitoring holds the promise of cheaper and easier-to-maintain monitoring technology. Non-Windows systems is to use Virtual Agents to collect state and performance data from those resources. When using Virtual Agents, there is no necessity to deploy any software on the managed systems. Instead, REST API calls are made to the systems to capture data or invoke an action are made using common interfaces supported by the managed systems.

**Secure Shell Web Relay**

The functionality provides the benefit of achieving SSH relay to target servers without a requirement of installation of a client or an agent as the SSH session can be achieved in the web browser. This functionality requires an Agentless module to be installed on Privileged Account Manager Linux manager.

**NOTE:** You cannot add scripts when you are using SSH Web Relay.

**Prerequisite**

Ensure that the **agentless** module is installed.

- The agentless component of Privileged Account Manager (**agentless**) is supported only on Windows, SLES 12 (64-bit), SLES 15 (64-bit), Oracle Linux 8 (64-bit), or RHEL 8 (64-bit).

**NOTE:**
- For **Oracle Linux 8** (64-bit) and **RHEL 8** (64-bit), install the **redhat-lsb-core** package.
- For **SLES 12** (64-bit) and **SLES 15** (64-bit), install the **lsb-release** package.
- You must install **libpango** and **libcairo**, and the dependent packages for both SLES and RHEL. Additionally for RHEL alone install **dejavu-sans-fonts**.

Advantages of configuring the secure shell web relay are:

- You can configure SSH Web Relay for Linux and Unix machines to allow users to remotely access these machines without the privileged account credentials.
- This method is beneficial if you do not want any operating system installed software or client.
Removes the requirement of JMobaxTerm to help application to be launched on a client desktop by using resources that are hosted remotely.

You can administer the active SSH Web Relay session in real time as it opens in the My Access page.

Configuring the Secure Shell Web Relay

You can configure a SSH Web Relay for Unix and Linux machines to allow users to remotely access these machine without the privileged account credentials. After a SSH Web relay is configured by an administrator, the user gets an elevated access to target Linux and Unix machines over SSH using a web console and can access the privileged session as follows:

1. Log in using the Privileged Account Manager user credentials and click Login.
2. Click My Access and click the launch icon before the appropriate resource name.
3. You can administer the active SSH Web Relay session as it opens in Home > Active Sessions. The administrator audits the user actions in this privileged session and views these reports in the administration console.

Usage Scenario for Agentless Secure Shell Web Relay

Scenario 1

Consider a scenario where the administrator has to provide privileged access to Linux or UNIX system and the Privileged Account Manager user can access the session from the same browser itself. For this scenario, the administrator must perform the following configuration in the Access Control.

1. Create an SSH type Credential Vault resource for the Linux or UNIX system and add the respective credentials.
2. Click Users, add the users (LDAP or Local) which will be using the resource.
3. Click Access Control > User Roles and create a user group and all the users which will use the resource.
5. Click Access Control > Assignment and create SSH Web and add the user group and resource pool you created in the 2 and 3 step to it.
6. Select the permissions you want to give.
7. Click Finish.

After the administrator configures the authorization rule in Privileged Account Manager, the user can gain privileged session as follows:

1. Log in using the Privileged Account Manager user credentials and click Login.
2. Click My Access and click the launch icon before the appropriate resource name.
3. You can administer the active SSH Web Relay session as it opens in Home > Active Sessions. The administrator audits the user actions in this privileged session and views these reports in the administration console.
The administrator audits the user actions in this privileged session and views these reports in the administration console.

7.3.4 **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 255
- “Configuring usrun Command for Privileged Access” on page 256
- “Accessing usrun for Privileged Access” on page 256
- “Usage Scenario” on page 256

**usrun Command Syntax**

The *usrun* function can be used with the following options:

```
usrun [-b] [-p] [-t] [-x] [-u <user>] [-h <host>] <command>
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-b</td>
<td>Puts the execution of the command into the background.</td>
</tr>
<tr>
<td>-p</td>
<td>Provides a pipe compatibility option for competitive products. It is only used for a competitive swap-out.</td>
</tr>
<tr>
<td>-t</td>
<td>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.</td>
</tr>
<tr>
<td>-x</td>
<td>Enables the X11 forwarding option.</td>
</tr>
<tr>
<td>-u &lt;user&gt;</td>
<td>Specifies the user you want the command to run as, although this can be overwritten by the Command Control rules.</td>
</tr>
<tr>
<td>-h &lt;host&gt;</td>
<td>Specifies the host you want the command run on, although this can be overwritten by the Command Control rules. For &lt;host&gt; you can use either the hostname of the server or the agent name specified in the Hosts console.</td>
</tr>
<tr>
<td>&lt;command&gt;</td>
<td>Specifies the command to pass to the Command Control Manager.</td>
</tr>
</tbody>
</table>
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.

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.

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.

### 7.3.5 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**

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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/dir/file</code></td>
<td>Specifies the file that the application can access in the <code>/dir/</code> directory.</td>
</tr>
<tr>
<td><code>/dir/</code></td>
<td>Specifies the directory that the application can access.</td>
</tr>
</tbody>
</table>
Configuring Privileged Access

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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>privperms</td>
<td>Enables the application with the read, write, and ownership permissions for the specified directory or file. The privperms command limits two areas of functionality:</td>
</tr>
<tr>
<td></td>
<td>1. Using the chmod command to set a file to setuid or setgid.</td>
</tr>
<tr>
<td></td>
<td>2. Using the chown or chgrp command to change the ownership of a file.</td>
</tr>
<tr>
<td>perms</td>
<td>Enables the application to assign the permissions of a specified directory or file.</td>
</tr>
<tr>
<td>read</td>
<td>Enables the application to assign the read permission for a specified directory or file.</td>
</tr>
<tr>
<td>write</td>
<td>Gives the application the create and write permissions for the specified directory or file.</td>
</tr>
<tr>
<td>unlink</td>
<td>Gives the application the deletion rights for the specified directory or file.</td>
</tr>
<tr>
<td>mknod</td>
<td>Enables the application to create system files in the specified directory.</td>
</tr>
<tr>
<td>exec</td>
<td>Enables the application to execute the shared files and files for which the application does not have read and write permission.</td>
</tr>
<tr>
<td>unsafe</td>
<td>Enables the application to execute any file that does not inherit the policy.</td>
</tr>
<tr>
<td>link</td>
<td>Enables the application to create a symbolic link or hard link to another file.</td>
</tr>
</tbody>
</table>

Table 7-2 Capability Options
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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log[=&lt;0-9&gt;]</td>
<td>Enables the application to audit system calls, with an optional risk value of 0-9.</td>
</tr>
<tr>
<td>all</td>
<td>Enables the application to have all permissions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Read / Write Permission</th>
<th>Read Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>/tmp/</td>
<td>/etc/resolv.conf</td>
</tr>
<tr>
<td>/dev/zero</td>
<td>/etc/hosts</td>
</tr>
<tr>
<td>/dev/null</td>
<td>/etc/passwd</td>
</tr>
<tr>
<td>/dev/tty</td>
<td>/etc/groups</td>
</tr>
<tr>
<td>/devices/**</td>
<td>/dev/random</td>
</tr>
<tr>
<td>/proc/&lt;pid&gt;/**</td>
<td>/dev/urandom</td>
</tr>
<tr>
<td>/tmp/**</td>
<td>/etc/utmp</td>
</tr>
<tr>
<td>/var/tmp/**</td>
<td>/etc/utmpx</td>
</tr>
<tr>
<td></td>
<td>/usr/share/**</td>
</tr>
<tr>
<td></td>
<td>/usr/lib/**</td>
</tr>
<tr>
<td></td>
<td>/lib/**</td>
</tr>
<tr>
<td></td>
<td>/usr/lib64/**</td>
</tr>
<tr>
<td></td>
<td>/lib64/**</td>
</tr>
</tbody>
</table>

**NOTE:** Solaris 9/sbin/sh is a static binary and therefore cannot enforce EAC.

### 7.4 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.

  **NOTE:** Credential check out is not supported when Privileged Account Manager is installed on a Windows server as a manager.

- **Database Access Through Privileged Account Manager Proxy:**

  Using this method, you can allow users to access the database through Privileged Account Manager proxy where Privileged Account Manager monitors the activities performed on the database.

- **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 Configuring RemoteApp Mode Using Command Control.

Based on the information in the following table, you can choose the appropriate database access method:

<table>
<thead>
<tr>
<th>Method</th>
<th>Keystroke Audit</th>
<th>Command Audit</th>
<th>Video Capture</th>
<th>Command Risk &amp; Automatic Session Disconnect</th>
<th>Manual Disconnect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Access Through Privileged Account Manager Proxy</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Database Credential Checkout</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Privileged SSO to Database</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

### 7.4.1 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.
7.4.2 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](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 Privileged Account Manager:
   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 You can either create database permissions using Access Control. For more information, see “Create Database Monitoring Permissions Using Access Control” on page 262. OR

5 You can also create a database rule using Command Control:
   5a On the home page of the console, click **Command Control**.
   5b In the Command control pane, click **Rules**.
   5c In the details pane, click **Add Rule**.
   5d Specify a name for the database rule, then click **Finish**.
   5e 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.

   5f Click **Finish**. The settings you have defined for the rule are displayed in the console.
6 Add database password check out command to the rule:

6a On the middle pane, click the Commands icon.

6b 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.

7.4.3 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.
- 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.

7.4.4 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:

Create Database Monitoring Permissions Using Access Control

Create a database monitoring permissions using Access Control:

1 On the home page of the console, click Access Control.
2 In the Access Control pane, create resource pool for database users by clicking Create.
   2a In the General page enter the name, description and select the Database type for which you want to create the resource pool. Example: Microsoft SQL.
   2b Click Next
   2c Click +Add to select Microsoft SQL database. The resources are populated from the resources configured in the Credential Vault. If you have not done configure it at this point to view and select the appropriate resources.
   2d Click Create. You can view the newly created resource pool using Access Control > Resource Pools.
3 Create user role of database users for database monitoring.
   3a To create this role, go to Access Control > User Roles > Create > General – specify the fields name and description. Click Next.
   3b In the Included Members page, click Add and select Database users. Click Add to select the users you want to add.
4 Create an assignment.

4a To configure the assignment, select the Access Control > Assignment, click Create Assignment.

4b From the Resource Pools page, select the database you want to create the assignment for. Example: My SQL.

4c Click Select.

4d Select the User Role. Example: DB Users.

4e Add a Description.

4f Add Permissions. Example: My SQL Database Access and set the following fields

- **Time Restrictions**: All Days (24 hours), Specify time range starting and ending. If you want custom setting use custom days.

- **Access and Monitoring Options** page: Move the slider to the right if you want to disable Session Capture, by default this option is set to enable.

- **Customization** page: add the customized scripts.

4g Click Finish.

5 You are redirected to the Assignments page, Click Create. Assignment created successfully message is displayed.

For more information about creating Resource Pools, User Roles, and Assignments, see “Access Control” on page 133. For more information about Database connectors, see “Adding Database Connectors Using Access Control” on page 266.

### Create Database Monitoring Permissions Using Command Control

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.
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. 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.

### 7.4.5 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” on page 127.

- 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.

### 7.4.6 Database Access Through Privileged Account Manager 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 Privileged Account Manager proxy IP address and port number must be communicated to the user to whom you are providing access.

*Figure 7-2  Database Connector*

<table>
<thead>
<tr>
<th>Type</th>
<th>Port</th>
<th>Database Address</th>
<th>Database Port</th>
<th>Database Instance Name</th>
<th>Database Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>11521</td>
<td>Oracle Database</td>
<td>1521</td>
<td>---</td>
<td>TCP</td>
</tr>
<tr>
<td>Oracle</td>
<td>11522</td>
<td>Oracle Database</td>
<td>2484</td>
<td>---</td>
<td>TCPS</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>11523</td>
<td>Microsoft SQL Server 1</td>
<td>1433</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>11524</td>
<td>Microsoft SQL Server 2</td>
<td>1433</td>
<td>MSSQLSERVER2008</td>
<td>---</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>11525</td>
<td>Microsoft SQL Server 2</td>
<td>---</td>
<td>MSSQLSERVER2012</td>
<td>---</td>
</tr>
</tbody>
</table>

After you provide database access through Privileged Account Manager proxy, you can allow the user to log into the database using:

- Their own database credentials.
- Credentials checked out from Privileged Account Manager.

In this method, you are enhancing the database security by allowing Privileged Account Manager to manage database credentials.
For configuring the database access through Privileged Account Manager proxy to monitor the database activities, perform the following:

- “Prerequisite” on page 266
- “Adding Database Connectors Using Access Control” on page 266
- “Adding Database Connectors Using Command Control” on page 267
- “Managing Database Connectors” on page 271
- “Database Monitoring Using Access Control” on page 272
- “Adding Rules for Database using Command Control” on page 273

**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 Using Access Control**

You can add the database connections which creating resource.

1. Click Credential Vault > Database > Add New.
2. Click + next to Resources.
3. Specify the following information:

**General Setting**

- **Name:** Specify the name of the database. This name is used along with the Credential to authenticate. If you do not provide the correct domain name, user authentication fails.

**Connection Details**

- **Connect String:** You can specify the string that will reset the password in the database and check in the password.
- **Connect As:** Select SYSDBA. If you want Privileged Account Manager to perform the password check in process then, to check the connection to the database server, click Test Connection or select Default.
- **Password Change on Check In:**
Based on the following selection the password of the application will be changed automatically every time a credential is checked in.

- **Never**: You can use this option if you do not want to change the password after every credential check-in.

- **Delegate to Identity Manager**: If you want to delegate the password check-in process to Identity Manager, select Delegate to Identity Manager. On selecting this option, the IDM (Identity Manager) driver for Privileged Account Manager takes care of generating random password and synchronizing the password to IDM. The PAM IDM driver checks in the new password to PAM. IDM takes care of synchronizing password on the database through the respective database driver. For more information, refer the Driver Implementation guide on the PAM documentation page. Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

**NOTE**: Before you delegate password check-in to Identity Manager ensure that both the Privileged Account Manager IDM driver and database driver are operational.

- **Internal**: Use this option, if you want Privileged Account Manager to manage password change.

Select the appropriate Password Policy that must be used when Privileged Account Manager generates a new password. By default Default Password Policy is selected. You can either modify the default password policy or create a new password policy.

**Proxy Connector Setting**

- **Database IP Address**: Specify the IP address or the Host Name of the Database.
- **Database Port**: Specify the Database port number.
- **Connection Protocol**: Select TCP or TCPS.
- **Database SSL Version**: In case you have selected TCPS, specify if it is Any Database SSL version, or the specific one from the dropdown list.
- **DBAudit Servers**: You can either select All or Selected server. Specify the proxy port.

**Adding Database Connectors Using Command Control**

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 Using Port Number**
- **Adding Microsoft SQL Server Connector Using Named Instance**
- **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 the 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, Privileged Account Manager supports only the TLS1V0 SSL version.
- If you are using Oracle 12.x, Privileged Account Manager 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 the 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 Server 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 Server** 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.
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.

### 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.

<table>
<thead>
<tr>
<th>Databases</th>
<th>Connection Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sybase</td>
<td>You can choose TCP or TLS (SSL Connection) connection protocol.</td>
</tr>
<tr>
<td>MySQL and MariaDB</td>
<td>Privileged Account Manager dynamically selects the protocol based on the database client and database server configuration.</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>Privileged Account Manager supports only TCP protocol in this release.</td>
</tr>
<tr>
<td>IBM Db2</td>
<td>Privileged Account Manager supports only TCP protocol in this release.</td>
</tr>
</tbody>
</table>
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 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 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.

Database Monitoring Using Access Control

Create a database monitoring permissions using Access Control:

1. On the home page of the console, click Access Control.
2. In the Access Control pane, create resource pool for database users by clicking Create.
   - 2a In the General page enter the name, description and select the Database type for which you want to create the resource pool. Example: Microsoft SQL.
   - 2b Click Next
   - 2c Click +Add to select Microsoft SQL database. The resources are populated from the resources configured in the Credential Vault. If you have not done configure it at this point to view and select the appropriate resources.
   - 2d Click Create. You can view the newly created resource pool using Access Control > Resource Pools.
3 Create user role of database users for database monitoring.
   3a To create this role, go to Access Control > User Roles > Create > General – specify the fields name and description. Click Next.
   3b In the Included Members page, click Add and select Database users. Click Add to select the users you want to add.

4 Create an assignment.
   4a To configure the assignment, select the Access Control > Assignment, click Create Assignment.
   4b From the Resource Pools page, select the database you want to create the assignment for. Example: My SQL.
   4c Click Select.
   4d Select the User Role. Example: DB Users.
   4e Add a Description.
   4f Add Permissions. Example: My SQL Database Access and set the following fields
      • Time Restrictions: All Days (24 hours), Specify time range starting and ending. If you want custom setting use custom days.
      • Access and Monitoring Options page: Move the slider to the right if you want to disable Session Capture, by default this option is set to enable.
      • Customization page: add the customized scripts.
   4g Click Finish.

5 You are redirected to the Assignments page, Click Create. Assignment created successfully message is displayed.

For more information about creating Resource Pools, User Roles, and Assignments, see “Access Control” on page 133.

Adding Rules for Database using Command Control

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.

### 7.4.7 Viewing Database Activity

To view the activities of a database user, perform the following:

1 In the Reports 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.

**NOTE:** 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.

7.5 Privileged Access to Applications and Cloud Services

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:

<table>
<thead>
<tr>
<th>Target</th>
<th>Application SSO Based Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Application SSO (<a href="#">Configuring RemoteApp Mode Using Command Control</a>)</td>
</tr>
<tr>
<td></td>
<td>For example, you can enable SSO to any Windows server by granting access to the Remote Desktop Connection application.</td>
</tr>
<tr>
<td></td>
<td>• RDP Relay (&quot;Remote Desktop Protocol Relay&quot; on page 229)</td>
</tr>
<tr>
<td></td>
<td>• Credential Provider (&quot;Credential Checkout&quot; on page 82)</td>
</tr>
<tr>
<td>UNIX, Linux, Mainframes, and Network Devices</td>
<td>• SSH Relay (&quot;Secure Shell Relay&quot; on page 248)</td>
</tr>
<tr>
<td></td>
<td>• Application SSO (<a href="#">Configuring RemoteApp Mode Using Command Control</a>)</td>
</tr>
<tr>
<td></td>
<td>For example, you can enable SSO to any UNIX or Linux server by granting access to PuTTY.</td>
</tr>
<tr>
<td>Database</td>
<td>Application SSO (<a href="#">Configuring RemoteApp Mode Using Command Control</a>)</td>
</tr>
<tr>
<td></td>
<td>For example, you can enable SSO to any database by granting access to appropriate database clients.</td>
</tr>
<tr>
<td>Enterprise Applications</td>
<td>Application SSO (<a href="#">Configuring RemoteApp Mode Using Command Control</a>)</td>
</tr>
<tr>
<td></td>
<td>For example, you can enable SSO to any application by granting access to appropriate application clients.</td>
</tr>
<tr>
<td>Web Applications</td>
<td>Application SSO (<a href="#">Configuring RemoteApp Mode Using Command Control</a>)</td>
</tr>
<tr>
<td></td>
<td>For example, you can enable SSO to any web application by granting access to appropriate web browsers.</td>
</tr>
</tbody>
</table>

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” on page 82.

- **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 Configuring RemoteApp Mode Using Command Control.

Based on the information in the following table, you can choose the appropriate method:

<table>
<thead>
<tr>
<th>Method</th>
<th>Keystroke Audit</th>
<th>Command Audit</th>
<th>Video Audit</th>
<th>Command Risk &amp; Automatic Session Disconnect</th>
<th>Manual Disconnect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Checkout</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>(Agentless)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileged SSO</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>(Agentless)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 7.6 Configuring Just-in-Time Access

You can grant privileged access to an application or system to users in real-time using the just-in-time (JIT) access methodology to complete a particular task.

#### 7.6.1 Configuring Just-in-Time Access For AWS Resource

The user fetches the AWS token from the Privileged Account Manager to log into the AWS workspace to access the dynamic secret for a specific resource delegated by the Administrator. Follow the procedure to configure.

1. On the home page of Privileged Account Manager, click **Credential Vault**
2. Click **Add +**
3. Select **Cloud > Amazon Web Services**
4. In the **General** page, add the **Domain** name as AWS Resource
5 In the **Connection Details** page, add the following:
   - Sign-In URL for IAM users
   - Region
   - Password Policy
   - Vault Host: AWS IP
   - Vault Region: Ex: Mumbai

6 In the **Password Management** page, select the **Reconcile Account Credential**.

7 Optionally add the extended attributes and the Reconcile Credential.

8 In **Template** page add the credential required for dynamic secret configuration.
   
   Checkbox or UI string with the following information:
   ```json
   account": "aws-user5",
   "type": "dyn_ephemeral",
   "privilege_type": "shift-leader",
   "ttl": 30
   ```

   The Administrator assigns delegated policies using Access control.

9 Log into Privileged Account Manager.

10 Click on **My Access**.

11 Retrieve username and password.

12 This secret is used to log into the AWS console and access a specific resource along with details such as AWS account Active, password Age, and Active key information.

### 7.6.2 Configuring Just-in-Time Access For PKI Resource

Dynamic certificates for X.509 are produced by the PKI secrets engine. With this secrets engine, services can obtain certificates without going through the typical manual procedure of generating a private key and CSR, submitting to a Certificate Authority, and waiting for a verification and signing process to finish. The functionality for verification is provided by the internal authentication in Privileged Account Manager.

1 On the home page of Privileged Account Manager console, click **Credential Vault**.

2 Click **Add +**

3 Select **Certificate Issuer PKI**.

4 In the **General** page, add the Domain name as PKI Resource. Click **Next**.

5 In the Certificate Authority page, enter the following details:
   - Select **Import** to import the certificate
   - Enter the **CA Certificate Name**
   - Enter the **Passphrase**

6 Optionally add the **Extended Attributes** and the **Reconcile Credential**.

7 Add the attributes.

The certificate and the key are generated. User uses it from Privileged Account Manager user console by clicking **My Access > Read Secret**.
7.6.3 Configuring Just-in-Time Access for SSH Certificate User

To achieve this requirement, perform the following tasks:

1. On the home page of Privileged Account Manager console, click Credential Vault.
2. Click Add +
3. Select Certificate Issuer SSH.
4. In the General page, add the Domain name as SSH Resource. Click Next.
5. In the Certificate Authority page, enter the following details to import the Certificate:
   - Select Import to import the certificate
   - Enter the CA Certificate Name
   - Enter the Passphrase
6. To create a new Certificate Authority, enter the following details:
   - Key Type: Type of key, ex: ed25519
   - Key Size: Size of the key, ex: 256
7. Optionally add the Extended Attributes.
8. Add the attributes.
9. Click Finish.
10. Go to Credential Vault > Resources > Resource Details, export the certificate from CA Certificate field.
11. Configure the exported certificate in the target server.

7.7 Configuring RemoteApp Mode Using Command Control

Using application SSO, you can achieve the following:

- Privileged SSO to any target resource using the appropriate application.
- Privileged access without the Privileged Account Manager 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 Using Access Control
- Direct Access Mode Using Command Control
Prerequisites

- Ensure that you have completed all the steps mentioned in the section Configuring Application Single Sign-On in the Privileged Account Manager Installation Guide.
- Whether you are using Access Control or Command Control, 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 > Add New > Application SSO and click + next to Resources in the new administration console.

7.7.1 RemoteApp Mode

In RemoteApp mode, the user launches the application from the user console and Privileged Account Manager 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.

Points to Remember for Configuring Application SSO in RemoteApp Mode

Ensure to perform the following for a seamless Application SSO configuration to work:

- Specify Remote Desktop Services licensing per user
- Change the Registry key single session per user from 1 to 0 in (HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer \fSingleSessionPerUser
- Navigate to Local Computer Policy Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections and specify the Limit Number of Connections to 999999.
- On your computer, navigate to Group Policy Editor Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host and set time limit for disconnected sessions.
- Click Remote Desktop Service > Session Collection properties > Configure Session Settings and specify End a disconnected session as 1 minute.

The following sections explain how to configure application SSO using RemoteApp mode and how to view application SSO reports:

- “Configuring RemoteApp Mode Using Access Control” on page 280
- “Configuring RemoteApp Mode Using Command Control” on page 281
- “Configuring Application SSO Agents for Load Balancing” on page 282
- “Viewing Reports” on page 282
Configuring RemoteApp Mode Using Access Control

You can use RemoteApp mode for Application SSO using Access Control. For more information, see Section 7.7, “Configuring RemoteApp Mode Using Command Control,” on page 278.

- “Add a Permission” on page 280

Add a Permission

After you have created resource in the Credential Vault, follow the procedure:

**Add an Application SSO Role:**

1. On the home page of the console, click Access Control.
2. In the navigation pane, click User Roles.
3. In the details pane, click Create. A Create User Role page with General, Included Members, and Excluded Members setting is displayed.
   - General: Specify the name and description of the user role. Click Next.
   - Included Members: Click Add to select users from the dropdown list which should be included in the user role.
   - Browse to users or groups and select a source.
   - Click Next.
4. Click Create.

**Add an Application SSO Resource Pool:**

1. On the home page of the console, click Access Control.
2. In the navigation pane, click Resource Pools.
3. In the details pane, click Create. A left pane with Create Resource pool is displayed with General and Resources settings.
4. In the General settings, specify the following:
   - Name: Name of the resource pool. Example: appsso-rp3
   - Description: Add a description. This is not a mandatory field.
   - Type: Select the type as Applications > Application SSO
5. Click Next. Resources page is displayed for configuration.
6. Click Add. Select the resources.
7. Select or enter the Default Credential. For more information, see “Default Credential” on page 145.
8. Click Create.

**Add an application SSO Permission**

1. On the home page of the console, click Access Control.
2. In the access control pane, click Assignments.
3. In the details pane, click Create.
To create an assignment, you must select a User Role, Resource Pool, and provide a Description. This Description is shown to the users while listing their permissions.

Click Add and select Application SSO as the permission. For more information, see “Configuring Permissions” on page 148.

Click Create to add the new assignment.

**NOTE:** After creating the assignment or permissions, you cannot modify the User Role and Resource Pool.

**NOTE:** Secondary authentication is present in the permission which performs second factor authentication for the application SSO Web session and not the application.

### Configuring RemoteApp Mode Using Command Control

- Adding a Rule

**Adding a Rule**

You must add a rule using Command Control or permission using Access Control for every application to which Privileged Account Manager 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**.

For more information about all the rule configuration fields, see “Modifying a Rule” on page 165.

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 Privileged Account Manager 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 172.

**Configuring Application SSO Agents for Load Balancing**

In RemoteApp mode, Privileged Account Manager load balances the application SSO requests. For Privileged Account Manager 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 **applss** 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**

Privileged Account Manager 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 **Reports > Command Control Reports.**

2 All report instances are displayed. You can interpret the SSO report columns as follows:
   - **User:** Privileged Account Manager 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.

7.7.2 Direct Access Mode Using Access Control

You can now access a direct RDP session using Access Control.

Prerequisites:
Ensure that you have configured resources for Application SSO, with the following permissions:

- Direct RDP
- Privileged Application. These are applications that are used for Application SSO
- Application SSO

After these permissions are created, log in as the user configured for the assignment and perform a direct RDP to the session you want to access. The credentials are injected and you have accessed the session successfully.

To monitor the session, click Reports All Sessions and view Direct RDP, Application SSO sessions.

7.7.3 Direct Access Mode Using Command Control

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 Privileged Account Manager 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 Privileged Account Manager agent.
   - For information about other rule configuration fields, see “Modifying a Rule” on page 165.
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 165.
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.

- **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.

For more information about the rule fields, see “Modifying a Rule” on page 165.

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**

Privileged Account Manager audits all the activities performed in the application SSO session. Based on the rule configuration, the report can show keystroke and video audits.

Privileged Account Manager 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 **Reports > 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.
Managing Reports

Privileged Account Manager enables auditing for the following events:

- Keystroke logging
- Command authorization
- Login success
- Login failure

In the Reports console, you can perform the following tasks:

- View and manage the logs for events
- Modify built-in reports
- Customize reports

8.1 Creating Reports

Privileged Account Manager provides built-in reports for the following data:

- All Sessions
- Disconnected Sessions
- Change Logs
- Credential Checkouts
- Shared Key Checkouts

You can create reports for the following data:

- Sessions
- Administrator Activities
- Credential Checkouts
- Shared Key Checkouts

For more information, see the following sections:

- Section 8.1.1, “Creating Reports for Sessions,” on page 290
- Section 8.1.2, “Creating Reports for Administrator Activities,” on page 291
- Section 8.1.3, “Creating Reports for Credential Checkouts,” on page 292
- Section 8.1.4, “Creating Reports for Shared Key Checkouts,” on page 293
- Section 8.1.5, “Customizing Reports,” on page 294
8.1.1 Creating Reports for Sessions

This page displays audit logs of privileged sessions in the form of keystrokes, screenshots, and videos. To create a report for sessions, perform the following steps:

1. On the home page of the console, click Reports > Create Report.
2. Select Sessions.
3. Click Next.
4. Specify the following details:
   - **Report Name**: Specify a name for the report.
   - **Description**: (Optional) Describe the purpose of the report.
5. Click Next.
6. (Optional) Add the required permission in Read and Update fields.

**NOTE**: To add these permissions:

- Define them using Users > + Create Group > Permissions > Custom Permissions pane with Module and Role.
- Add the user to whom these permissions apply, using the following procedure:
  1. On the home page of the console, click Users > Users & Groups. Select the group from the left pane, click the edit icon.
  2. In the General pane, select the details you want to modify. You cannot modify the Group Name field.
  3. In the Members section, select to add or remove the users you want to be members of this group.

You can also create a separate user group with these permissions.

To assign these roles to a group, see “Audit Reports Permissions” on page 43.

7. Click Next.
8. In the Filters tab, specify the following details:

- **Duration**: Select the Duration. The default duration that is displayed is the Last 3 Months. When you click the Last 3 Months, a calendar is displayed for you to select the exact duration.
- **Databases**: Select the database for which you want to create the report. By default all the databases are selected. You can view the rollover time for each database based on the audit settings you have specified in Reports > Settings. In this setting you have specified the time interval for rolling over the audit file against each Audit DB Name. 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.
- **Filters**: Filters vary based on the report type. You can combine filters with AND logic or OR logic.
  - **AND** combines two criteria and displays the matching report data only if both the criteria are matched.
OR combines two criteria and finds a matching if either of the criterion is matched. Select Criteria from the list. You can also Add Criteria or Add Group, if necessary. For more information, see “Filtering the Viewable Records” on page 299.

9 Click Preview to confirm if the information is correct. Preview takes you to the Session details page.

10 Click Save. You can export the details using Export to CSV.

8.1.2 Creating Reports for Administrator Activities

This report displays audit logs of all administration console activities performed using the Privileged Account Manager user interface, command line, and the API.

To create a report for administrator activities, perform the following steps:

1 On the home page of the console, click Reports > Create Report.
2 Select Administrator Activities.
3 Click Next.
4 Specify the following details:
   - Report Name: Specify a name for the report.
   - Description: (Optional) Describe the purpose of the report.
5 Click Next.
6 (Optional) Add the required permission in Read and Update fields.

NOTE: To add these permissions:

- Define them using Users > + Create Group > Permissions > Custom Permissions pane with Module and Role.
- Add the user to whom these permissions apply, using the following procedure:
  1. On the home page of the console, click Users > Users & Groups. Select the group from the left pane, click the edit icon.
  2. In the General pane, select the details you want to modify. You cannot modify the Group Name field.
  3. In the Members section, select to add or remove the users you want to be members of this group.

You can also create a separate user group with these permissions.

To assign these roles to a group, see “Audit Reports Permissions” on page 43.

7 Click Next.
8 In the Filters tab, specify the following details:
   - Duration: Select the Duration. The default duration that is displayed is the Last 3 Months. When you click the Last 3 Months, a calendar is displayed for you to select the exact duration.
   - Databases: Select the database for which you want to create the report. By default all the databases are selected. You can view the rollover time for each database based on the audit settings you have specified in Reports > Settings. In this setting you have specified the...
time interval for rolling over the audit file against each Audit DB Name. 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.

- **Filters**: Filters vary based on the report type. You can combine filters with AND logic or OR logic.
  - **AND** combines two criteria and displays the matching report data only if both the criteria are matched.
  - **OR** combines two criteria and finds a matching if either of the criterion is matched.

Select Criteria from the list. You can also Add Criteria or Add Group, if necessary. For more information, see “Filtering the Viewable Records” on page 299.

9. Click **Preview** to confirm if the information is correct. Preview takes you to the Administrator Activities details page.

10. Click **Save**. You can export the details using **Export to CSV**.

### 8.1.3 Creating Reports for Credential Checkouts

This report displays audit logs of all credential check-in and checkout operations.

1. On the home page of the console, click **Reports > Create Report**.
2. Select **Credential Checkouts**.
3. Click **Next**.
4. Specify the following details:
   - **Report Name**: Specify a name for the report.
   - **Description**: (Optional) Describe the purpose of the report.
5. Click **Next**.
6. (Optional) Add the required permission in **Read** and **Update** fields.

---

**NOTE:** To add these permissions:

- Define them using **Users > + Create Group > Permissions > Custom Permissions** pane with Module and Role.
- Add the user to whom these permissions apply, using the following procedure:
  1. On the home page of the console, click **Users > Users & Groups**. Select the group from the left pane, click the edit icon.
  2. In the **General** pane, select the details you want to modify. You cannot modify the **Group Name** field.
  3. In the **Members** section, select to add or remove the users you want to be members of this group.

You can also create a separate user group with these permissions.

To assign these roles to a group, see “Audit Reports Permissions” on page 43.

7. Click **Next**.
8 In the Filters tab, specify the following details:

- **Duration**: Select the Duration. The default duration that is displayed is the Last 3 Months. When you click the Last 3 Months, a calendar is displayed for you to select the exact duration.

- **Databases**: Select the database for which you want to create the report. By default all the databases are selected. You can view the rollover time for each database based on the audit settings you have specified in Reports > Settings. In this setting you have specified the time interval for rolling over the audit file against each Audit DB Name. 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.

- **Filters**: Filters vary based on the report type. You can combine filters with AND logic or OR logic.
  
  - **AND** combines two criteria and displays the matching report data only if both the criteria are matched.
  
  - **OR** combines two criteria and finds a matching if either of the criterion is matched.

  Select Criteria from the list. You can also Add Criteria or Add Group, if necessary. For more information, see “Filtering the Viewable Records” on page 299.

9 Click Preview to confirm if the information is correct. Preview takes you to the Credential Checkouts details page.

10 Click Save. You can export the details using Export to CSV.

### 8.1.4 Creating Reports for Shared Key Checkouts

This report displays audit logs of all Shared key check-in and checkout operations.

1 On the home page of the console, click Reports > Create Report.

2 Select Shared Key Checkouts.

3 Click Next.

4 Specify the following details:

   - **Report Name**: Specify a name for the report.
   - **Description**: (Optional) Describe the purpose of the report.

5 (Optional) Add the required permission in Read and Update fields.

**NOTE**: To add these permissions:

- Define them using Users > + Create Group > Permissions > Custom Permissions pane with Module and Role.

- Add the user to whom these permissions apply, using the following procedure:
  
  1. On the home page of the console, click Users > Users & Groups. Select the group from the left pane, click the edit icon.
  
  2. In the General pane, select the details you want to modify. You cannot modify the Group Name field.
  
  3. In the Members section, select to add or remove the users you want to be members of this group.

You can also create a separate user group with these permissions.
To assign these roles to a group, see “Audit Reports Permissions” on page 43.

6 Click Next.

7 In the Filters tab, specify the following details:
   - **Duration**: Select the Duration. The default duration that is displayed is the Last 3 Months. When you click the Last 3 Months, a calendar is displayed for you to select the exact duration.
   - **Databases**: Select the database for which you want to create the report. By default all the databases are selected. You can view the rollover time for each database based on the audit settings you have specified in Reports > Settings. In this setting you have specified the time interval for rolling over the audit file against each Audit DB Name. 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.
   - **Filters**: Filters vary based on the report type. You can combine filters with AND logic or OR logic.
     - **AND** combines two criteria and displays the matching report data only if both the criteria are matched.
     - **OR** combines two criteria and finds a matching if either of the criterion is matched.
       Select Criteria from the list. You can also Add Criteria or Add Group, if necessary. For more information, see “Filtering the Viewable Records” on page 299.

8 Click Preview to confirm if the information is correct. Preview takes you to the Shared Key Checkouts details page.

9 Click Save. You can export the details using Export to CSV.

### 8.1.5 Customizing Reports

You can customize reports using the following procedure:

1 On the home page of the console, click Reports > Create Report.
2 Select either Sessions, Administrator Activities, Credential Checkout, or Shared Key Checkouts.
3 Click Next.
4 Specify the following details:
   - **Report Name**: Specify a name for the report.
   - **Description**: (Optional) Describe the purpose of the report.
5 (Optional) Add the required permission in Read and Update fields.

**NOTE**: To add these permissions:
   - Define them using Users > + Create Group > Permissions > Custom Permissions pane with Module and Role.
   - Add the user to whom these permissions apply, using the following procedure:
     1. On the home page of the console, click Users > Users & Groups. Select the group from the left pane, click the edit icon.
2. In the General pane, select the details you want to modify. You cannot modify the Group Name field.

3. In the Members section, select to add or remove the users you want to be members of this group.

You can also create a separate user group with these permissions.

To assign these roles to a group, see “Audit Reports Permissions” on page 43.

6 Click Next.

7 Select the Duration. The default duration that is displayed is Last 3 Months. When you click the Last 3 Months, a calendar is displayed for you to select the exact duration.

8 Click Apply.

9 Select Criteria from the list. You can also Add Criteria or Add Group, if necessary. For more information, see “Filtering the Viewable Records” on page 299.

10 Click Preview to confirm if the information is correct. Preview takes you to the Sessions, Administrator Activities, Credential Checkout, or Shared Key Checkouts respective details page.

11 Click Save. You can export the details using Export to CSV.

12 Preview the report data. You can view the Details page. You can perform the following actions:

• Time Filter: This is the time filter selected by default.

• Save: Click this to save the changes you made to the report. A Edit View Info dialog box is displayed for you to end Name, Description, Read, and Update fields. Specifying Name is mandatory. Click Save.

• Cancel: Click this to cancel changes you made to the report.

• Show Filter: A fly-out is displayed when you click Show Filter, displaying the filter criteria you have configured. You can add additional criteria or group if you require. The fly-out also provides a Databases tab, which displays the databases you have selected. You can modify the databases using select or deselect the check-box as necessary.

If you want to refine the data, modify the filters as required. Click Save

12a Click Apply

12b Click Reset to restore the previous filter setting.

12c Click Cancel to discard the changes.

NOTE: To view this saved report under My Reports. Click Reports from the home page of the Privileged Account Manager console. If you click on the saved report you have the Details which have options for you to save the report with additional changes. You can click + to save the report as with a different name with additional changes.

NOTE: You can create custom report using the Built-in Reports.
8.2 Using Reports Settings

Use this page to control the rollover of the audit database files, encryption, and video report settings.

- Section 8.2.1, “Using Audit Settings,” on page 296
- Section 8.2.2, “Using Encryption Settings,” on page 297
- Section 8.2.3, “Using Video Report Filter Settings,” on page 297
- Section 8.2.4, “Configuring Video Capture,” on page 303
- Section 8.2.5, “Viewing the Videos,” on page 306
- Section 8.2.6, “Video Off-Load,” on page 307
- Section 8.2.7, “Change Log Reports,” on page 310
- Section 8.2.8, “Password Management,” on page 311
- Section 8.2.9, “Enabling Password Management,” on page 311
- Section 8.2.10, “Viewing Report Data,” on page 311
- Section 8.2.11, “Shared Key Management,” on page 312
- Section 8.2.12, “Enabling Shared Key Management,” on page 312

8.2.1 Using Audit Settings

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 Reports > Settings > Audit Settings on the home page of the Privileged Account Manager console.

2. In Audit Log Settings page, for each audit database file, set the rollover parameters. Rolled-over databases are kept as SQLite databases.

   **Audit DB Name:** This column lists the configured audit database names. Except for Change Management `chngmgnt` database name which is present by default, all other database names are populated only when you configure them.

   **Rollover 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.

   **Rollover 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 Reports Settings > Encryption Settings.

Encrypting the file can impact the performance of your audit managers. Also, the encrypted file can be decrypted by the Privileged Account Manager, but it cannot be displayed on new systems that do not detect the encryption keys.
To configure the encryption keys, click Reports > Settings > Encryption settings.

3 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.

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

4 Click Finish.

8.2.2 Using Encryption Settings

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

1 Click Reports > Settings on the home page of the console.

2 Click Encryption Settings in the task pane.

3 The NULL Cipher (clear text) key is enabled at Reports Settings > Encryption Settings by default.

   If the you want to encrypt the databases then you must first disable the null cipher and then change the database to encryption and save, Privileged Account Manager encrypts all the databases, which has the Protection set to Encrypted in Reports Settings > Audit Settings, with the latest key. This can be very time-intensive and can affect performance until it is completed.

4 To specify how frequently the key is changed, move the Key Rollover slider to the right and specify a Key Rollover interval by selecting the type of interval (years, months, weeks, or days).

5 (Optional) In the Encryption Keys list, disable or enable keys by moving the slider to the right or left against the respective Key ID.

   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 databases 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 Reports Settings > Audit Settings, with the latest key. This can be very time-intensive and can affect performance until it is completed.

6 Click Finish.

8.2.3 Using Video Report Filter Settings

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 Reports > Settings on the home page of the console.
2. Click Video Report Settings.

By default, Video Report Filter Settings has the following filters:

- Type: click | Checked | Close window | Terminate | msc | user | group | start | stop | Log Off

You can use any filter from the above mentioned options. Example: Terminate

4. Click Reports > All Sessions.
5. Select a Windows session and click Capture. The video Details page is displayed. Click Videos > Filtered Events and enter Terminate in the search box. Only the Terminate filtered events are listed.
6. Click Update.

**NOTE:** After editing the filter configuration, if you want the initial filter configuration, then click Reset > Update.

### Viewing Report Data

1. Click Reports on the home page of the console.
2. Select the report from Built-In Reports.
3. The navigation pane displays the following information about each instance of the report.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>Displays the date and time when the report started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Displays the date and time when the report ended.</td>
</tr>
<tr>
<td>User</td>
<td>Displays the name of the user who issued the command.</td>
</tr>
<tr>
<td>Host</td>
<td>Displays the name of the host from which the command was issued.</td>
</tr>
<tr>
<td>Run As</td>
<td>Displays the name of the user who issued the command.</td>
</tr>
<tr>
<td>Run Host</td>
<td>Displays the name of the host who issued the command.</td>
</tr>
<tr>
<td>Audit ID</td>
<td>Displays the unique ID of the audit record.</td>
</tr>
<tr>
<td>Command</td>
<td>Displays the command that was executed.</td>
</tr>
<tr>
<td>Authorized</td>
<td>Displays whether the rule for this command is authorized.</td>
</tr>
<tr>
<td>Capture</td>
<td>Displays whether the rule for this command was captured as video or as keystrokes.</td>
</tr>
<tr>
<td>Audits</td>
<td>Displays Audit ID and the respective capture details.</td>
</tr>
</tbody>
</table>
NOTE: When second factor authentication is enabled through Advanced Authentication in Privileged Account Manager, a user requests some session and is prompted to select second factor authentication Chain (Example: Access Control permission has 'Secondary Authentication:yes') and successfully completes. Two duplicate Access Control sessions are audited in the Reporting Console with the same Audit ID. Authorized: No, Capture: Yes and Authorized: yes, Capture: yes. This is because of the time it takes to sync with the Advanced Authentication data.

Filtering the Viewable Records

Use the Filters 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 Reports on the home page of the console.
2. Click any of the four types of reports namely, Sessions, Administrator Activities, Credential Checkouts, and Shared Key Checkouts for which you want to view in the navigation pane.
3. Click Filters.
4. 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.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Domain</td>
<td>Displays the user domain of the user who issued the command.</td>
</tr>
<tr>
<td>Disconnect Type</td>
<td>Displays the date, time, and disconnect type: Manual or Automatic.</td>
</tr>
</tbody>
</table>
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.

Session Start: 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.

5 Click Apply.

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 “Audit Reports Permissions” on page 43.

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

### Selecting Log Files

The Audit Manager indexes any rolled-over audit database. 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 Reports 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 have 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 specific 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 Reports 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 sessions 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 to 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 Privileged Account Manager 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, Section 10.8, “sreplay Command Line Options,” on page 351.
8.2.4 Configuring Video Capture

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 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 contain appropriate video configuration.

For example, if the Framework Manager has 2 hosts with the 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 on 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 subfolders 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 the 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 Video Archival (Optional)**

To archive the videos:

1 Click **Reports > Settings** on the home page of the console.
2 Click **Audit Settings**.
3 Add the following sample script under **Rollover Script**:

```plaintext
\nuse warnings;\nuse File::Copy; \n$ctx->log_info("=========================================================");\nif ($DBGRP eq 'cmdctrl') {
    my $srcdir = ($^O eq 'MSWin32') ? 'C:/Program Files/Netiq/npum/service/local/audit/video/capture/' : '/opt/netiq/npum/service/local/audit/video/capture/'; \n    my $dest = ($^O eq 'MSWin32') ? 'C:/Program Files/Netiq/npum/service/local/audit/videobk/' : '/opt/netiq/npum/service/local/audit/videobk/'; \n    my $fileage = 1; \n    opendir(DIR, $srcdir) or die $ctx->log_error("Can't open $srcdir: $!"); \n    my @files = grep {!/^\. $/} readdir(DIR); \n    foreach my $file (@files) {
        my $old = "$srcdir/$file";
        if ( (-f $old) && ($fileage< -M $old) ) {
            unlink glob "*.*"; \n            move($old, $dest) or die $ctx->log_error("Move $old -> $dest failed: $!"); \n        } 
    }  \n    close(DIR);
    $ctx->log_info("Backup Complete");\n}
```

4 Click **Update**.

**Configuring the Video Conversion Settings**

Using the video conversion settings, you can optimize the videos conversion process based on quality, size, and CPU utilization.

The video conversion settings are 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**.
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 the 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 the video duration is more, the number of video files are less.

**Video Conversion Priority:** This option determines the video conversion process priority in the CPU. By setting the priority, you can ensure that other operations of the CPU are uninterrupted.

Set this option to Low when the video conversion is not of high priority.

Set this option to Normal when the video conversion process is of moderate or high priority.

5 Click Save.

**Enabling Video Capture**

To enable video capture:

1 Add a 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 the 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:
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.exe -i <input_file_name>.flv -c:v libvpx-vp9 -speed 8 -deadline realtime <output_file_name>.webm
```

8.2.5 Viewing the Videos

To view the videos:

1. Click Reports on the home page of the console, and click Built-In Reports > All Sessions, Disconnected Sessions, Change Logs, Credential Checkouts, or Shared Key Checkouts.
2. Select the session report you want to view, the Details page is displayed.
3. In the Capture column, click on the video icon.
   
   The video icon 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 305.
   • 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.

4. The following information about the session is displayed.
   • Overview
   • Keystrokes
   • Screenshots
   • Videos

5. In the Video 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.
   **Find:** Searches the events based on the options provided by you.
### 8.2.6 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 the 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, Privileged Account Manager 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 resources. When the video off-load agent is down, the conversion operation is performed on the Privileged Account Manager agent where the session is running.

*Figure 8-1 The following illustrations explains the flow of the video generation process in an agent environment:*
**Figure 8-2** The following illustrations explains the flow of the video generation process with multiple audit managers:

- 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 Privileged Account Manager agent, where the session images are converted to videos. For the system requirements of the video off-load server, see the System Requirements in Privileged Account Manager Documentation website.

**To setup and configure a video off-load agent:**

1. Install and register the Privileged Account Manager 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 Privileged Account Manager 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:
   1. Click Hosts.
   2. Select the host, which is a video off-load server, then click Packages.
   3. Click Install Packages.
   4. 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, Privileged Account Manager 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 the 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 the 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 the 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 Privileged Account Manager 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 off-load.
   - 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 off-load.
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.

8.2.7 Change Log Reports

Any GUI-specific operation performed by you is audited by the Change Logs reports. Each operation is tracked, and the log is maintained in the Change Logs report. The default Sample Report displays all of the collected audit records and any associated keystroke capture.

Viewing Report Data

1. Click Reports > Change Logs on the home page of the console.

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

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Time</td>
<td>Displays the date and time when the GUI operation was performed.</td>
</tr>
</tbody>
</table>
8.2.8 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, “Privileged Access to Applications and Cloud Services” on page 275.

8.2.9 Enabling Password Management

A console package named report_pwdcheckout needs to be installed to enable the Password Management feature.

8.2.10 Viewing Report Data

1. Click Reports > Built-In Reports on the home page of the console.
2. Click Credential Checkouts.
3. The Details pane displays the following information about each instance of the report.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checkout Time</td>
<td>Displays the date and time when the password was checked-out.</td>
</tr>
<tr>
<td>Checkin Time</td>
<td>Displays the date and time when the password was checked-in.</td>
</tr>
<tr>
<td>User</td>
<td>Displays the name of the user who checked-out the password</td>
</tr>
<tr>
<td>Run As</td>
<td>Displays the name of the user who checked-out the password</td>
</tr>
<tr>
<td>Run Host</td>
<td>Displays the name of the host from which the password was issued</td>
</tr>
<tr>
<td>Request ID</td>
<td>Displays the request ID of the password checkout</td>
</tr>
<tr>
<td>Checked-in By</td>
<td>Displays the user who check-in the password</td>
</tr>
</tbody>
</table>
8.2.11 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 5, “Working with Credentials,” on page 73.

8.2.12 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 Reports > Built-In Reports > Shared Key Checkouts.
2. The Details pane displays the following information about each instance of the report.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checkout Time</td>
<td>Displays the date and time when the key was checked-out.</td>
</tr>
<tr>
<td>Check-in Time</td>
<td>Displays the check-in time of the shared key</td>
</tr>
<tr>
<td>User</td>
<td>Displays the name of the user who checked-out the key</td>
</tr>
<tr>
<td>Key</td>
<td>Displays the name of the checked out key under the shared key domain</td>
</tr>
<tr>
<td>Key Domain</td>
<td>Displays the shared key domain from which the key was checked-out</td>
</tr>
<tr>
<td>Used</td>
<td>Displays the number of keys which have been used</td>
</tr>
<tr>
<td>Total Allowed</td>
<td>Displays the total number of keys available under the shared key domain</td>
</tr>
<tr>
<td>Request ID</td>
<td>Displays the request ID of the key checkout</td>
</tr>
</tbody>
</table>
8.3 Using 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 playback 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 Reports 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 314.
- Create one or more rules to pull the required events into the Compliance Auditor. See “Adding or Modifying an Audit Rule” on page 315.
- Define ACLs for individual user.
- View event records and authorize them, or mark them as unauthorized and define further action. See “Compliance Auditor Records” on page 322.
- Configure auditing reports to be automatically e-mailed to the appropriate personnel. See “Adding, Copying and Modifying an Audit Report” on page 316.
- Provide failover and load balancing by installing the Compliance Auditor on multiple hosts. See “Deploying the Compliance Auditor” on page 327.
- Export and import compliance auditing settings. See Section 10.7.1, “Exporting and Importing Compliance Auditor Settings,” on page 349.
8.3.1 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 the use of 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:

<table>
<thead>
<tr>
<th>Module</th>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>secaudit</td>
<td>console</td>
<td>View the Compliance Auditor console.</td>
</tr>
<tr>
<td>secaudit</td>
<td>audit</td>
<td>View and edit records.</td>
</tr>
<tr>
<td>secaudit</td>
<td>&lt;audit role name&gt;</td>
<td>(Optional) Custom role. Allows the users to access records retrieved by the Audit Rules configured to use this Audit Role.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you do not add the &lt;audit role name&gt; role, the users can only access records generated by rules with no Audit Role defined.</td>
</tr>
<tr>
<td>audit</td>
<td>read</td>
<td>View a keystroke replay.</td>
</tr>
</tbody>
</table>

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 “Audit Reports Permissions” on page 43.

6. Click Update.
7. To continue setting up the Compliance Auditor, see “Adding, Copying and Modifying an Audit Report” on page 316.

8.3.2 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, Copying and Modifying an Audit Report” on page 316.

### 8.3.3 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 314.
   - **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**.
8.3.4 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. Based on time and available capacity, Privileged Account Manager automatically archives session recording data to external storage or media.

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

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.

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 Section 3.2.2, “Modifying User,” on page 51.

• **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 318.

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) {
  my $style1 { color: #000000;
                font-family: Arial, Helvetica, sans-serif;
                font-size: 12px; }
  my $style2 { color: #000000;
                font-family: Arial, Helvetica, sans-serif;
                font-size: 12px;
                font-weight:bold; }
  
  <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; }
</style>
}</%>
Hello $User.ACT_FULL_NAME.value$,

This is an automated event notification email from the Compliance Auditor.

It is the responsibility of management to log into the Compliance Auditor each day and review their team's keystroke logs.

Please log on to the Compliance Auditor at your earliest convenience using this link: https://admin.company.com

Events &lt; 5 days old ( gt0 )

<table>
<thead>
<tr>
<th>Time</th>
<th>User</th>
<th>Run As</th>
<th>Host</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>tme</td>
<td>usr</td>
<td>ras</td>
<td>hst</td>
<td>cmd</td>
</tr>
</tbody>
</table>

Events &gt; 5 days old ( 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><%= "$tme" %></td>
<td><%= "$usr" %></td>
<td><%= "$ras" %></td>
<td><%= "$hst" %></td>
<td><%= "$cmd" %></td>
</tr>
<% 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>
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.

### 8.3.5 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:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>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 182.</td>
</tr>
<tr>
<td>Level</td>
<td>The escalation level set by the auditor editing the event record.</td>
</tr>
<tr>
<td>Status</td>
<td>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.</td>
</tr>
<tr>
<td>Time</td>
<td>The date and time the event occurred.</td>
</tr>
<tr>
<td>Event</td>
<td>A description of what the record contains.</td>
</tr>
<tr>
<td>Note</td>
<td>Any notes made by the auditor when editing the event record.</td>
</tr>
<tr>
<td>Assigned</td>
<td>The user the event has been assigned to by the auditor of the event record.</td>
</tr>
<tr>
<td>Rule</td>
<td>The audit rule that is pulled in the event.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of event.</td>
</tr>
<tr>
<td>Size</td>
<td>The size of the keystroke capture with the total time of the session displayed between parentheses.</td>
</tr>
<tr>
<td>Event ID</td>
<td>The unique event ID.</td>
</tr>
</tbody>
</table>

From this page, you can perform the following tasks:
8.3.6 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 323 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 182 and “Modifying a Rule” on page 165.

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 325.

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 325.

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.

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 316.
   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 Section 10.7.2, “Managing Compliance Auditor Records,” on page 349.

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 Section 10.7.2, “Managing Compliance Auditor Records,” on page 349.

**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**.

Deployment Dashboard: 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.

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.

For more information about Deployment Dashboard, see Deployment Dashboard.

Modifying 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.

8.3.7 Deploying the Compliance Auditor

You can provide failover and load balancing by installing the Compliance Auditor on multiple hosts.
Fully automatic failover from a single active instance to a backup/standby instance with a fully
replicated repository is possible using compliance auditor. 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.
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 Section 2.6.6, “Installing Packages
   on a Host,” on page 32 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.
Privileged Account Manager provides capability to integrate with ArcSight Intelligence, ticketing tool, ServiceNow, Identity Manager, and other external services.

### 9.1 Integrating with ArcSight Intelligence

Privileged Account Manager assesses the risk associated with an access attempt based on the contextual information. For example, the contextual information can be IP address and device information.

Some threats are very complex and difficult to trace through rule-based computation. These unknown threats are unpredictable and do not leave any evidence behind. The evidence might be hidden within your data. These threats require a more sophisticated approach to anomaly detection using machine learning.

To enable the unknown threat or anomaly detection, Privileged Account Manager integrates with ArcSight Intelligence and leverages its User and Entity Behavioral Analytics (UEBA) capability. Using the organization's data, ArcSight Intelligence establishes the normal behavior for the organizational entities and then, using advanced analytics and machine learning, identifies the anomalous behaviors that constitute potential risks such as compromised accounts, insider threats, or other unknown cyber threats.

The following are a few examples of anomalies in behavioral access control:

- A large number of session authentication successes and failures
- A large number of application access events
- A large number of distinct applications accessed
- Unusual application access events
- Unusual browser used during authentication
- Unusual working hours or working days

This integration enables Privileged Account Manager to perform the following actions by using behavioral analytics:

- Detect compromised account and bots
- Detect insider threats
- Detect compromised network, host, and devices
- Detect unknown threats

### 9.1.1 Example Scenarios

The following are a few common scenarios where enabling behavioral analytics helps accelerate threat detection:
Scenario: Compromised Account Detection

Albert works in a Healthcare organization. He browses news sites from his corporate computer. One day, he inadvertently clicks a malicious URL that injects the spyware script in his browser. The script starts accessing numerous sensitive applications and downloading the data.

ArcSight Intelligence identifies a sudden increase in the number of access attempts and network lateral movements from Albert’s system. ArcSight Intelligence classifies this as high risk and shares his risk score, and Privileged Account Manager blocks Albert from accessing any application.

Scenario: Insider Threats Detection

Daniel, a helpdesk engineer, accesses the sensitive data and explores various corporate resources from home at night. ArcSight Intelligence detects the anomalous behavior and classifies Daniel as a high-risk user. ArcSight Intelligence shares the risk score with Privileged Account Manager and it blocks access for Daniel before anything too malicious happens.

Olga, an engineer, is erroneously given access to a privileged application. She decides to browse that application from home on a weekend. ArcSight Intelligence detects this privileged access abuse and increases her risk. Privileged Account Manager blocks Olga’s access to the application.

Lucio, a system admin, has access to a service account with higher privileges. He uses that account’s credentials to access the restricted data. ArcSight Intelligence detects the account misuse as high risk and shares this information with Privileged Account Manager and it locks down this service account.

Scenario: Accidental Insider Threats Detection

Amrita, an HR professional, forgets to lock her computer. This allows a colleague to probe the sensitive data. ArcSight Intelligence detects this account compromise with medium risk and results in the Privileged Account Manager multi-factor authentication requirement the next day. This stops the colleague from the subsequent attempt to steal the data.

Scenario: Compromised Network, Host, or Device Detection

ArcSight Intelligence detects an unusual number of access requests from similar IPs or similar devices. The overall risk is high as the organization might be under a stealth attack or at risk of a DDOS attack.

ArcSight Intelligence detects an increase in the number of identities. It also detects an unusual number of access requests from these identities. ArcSight Intelligence increases the overall risk of this B2C organization as the attackers might be creating an excessive number of identities by using social login. Attackers could also launch a DDOS attack with these valid identities.

Thomas, an engineer, has malware running on his laptop. This malware uses his account to snoop the resources on the network. ArcSight Intelligence detects the infected host by considering unusual access patterns and endpoint threat patterns. ArcSight Intelligence determines the user as high risk. Privileged Account Manager blocks his access.

9.1.2 Configuring ArcSight Intelligence Details

The following information helps you to configure the ArcSight Intelligence details.
Integration with External Services

NOTE: You should synchronize time in the Manager, where Primary Command Control module is running. Otherwise, Risk scores would not be refreshed.

### 9.2 Integrating 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 Privileged Account Manager. For more information about Identity Manager, see Identity Manager documentation page.

NOTE: Although the latest IDM driver version is 4.8.x, ensure that you use 4.5.x version of the IDM driver package, as 4.5.x version is currently supported with Privileged Account Manager.

The Privileged Account Manager driver is a Java program running in Identity Manager. This driver communicates with the Privileged Account Manager application using Java JSON API library provided by Privileged Account Manager. This communication happens over HTTPS channel.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Use the slider to set the ArcSight Intelligence status to enable or disable. Setting this option to enable implies that you want to consider risk score for allowing access to the user and for refreshing the risk data.</td>
</tr>
<tr>
<td>AWS Access Key ID</td>
<td>The AWS access key ID to access the ArcSight Intelligence URL.</td>
</tr>
<tr>
<td>AWS Secret Access Key</td>
<td>The AWS secret access key to access the ArcSight Intelligence URL.</td>
</tr>
<tr>
<td>AWS Region</td>
<td>The AWS region where ArcSight Intelligence is deployed.</td>
</tr>
<tr>
<td>AWS Bucket</td>
<td>Amazon S3 buckets, which are similar to file folders, store objects, which consist of data and its descriptive metadata.</td>
</tr>
<tr>
<td>AWS Path/Base Folder</td>
<td>Path/folder containing the risk files.</td>
</tr>
<tr>
<td>Risk Threshold</td>
<td>Maximum risk score allowed.</td>
</tr>
<tr>
<td>Allow Emergency Access</td>
<td>Set it to on or off using the slider, if you want to allow emergency access for users with the above risk threshold</td>
</tr>
<tr>
<td>Allow Access on Unknown Risk</td>
<td>Allow access to the user because risk score is unavailable.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Set the daily frequency at which you want to refresh in hours and minutes.</td>
</tr>
<tr>
<td>Next Refresh Time</td>
<td>Displays the upcoming scheduled refresh time.</td>
</tr>
<tr>
<td>Last Refreshed Time</td>
<td>Displays the last time when data was refreshed.</td>
</tr>
<tr>
<td>Refresh Now</td>
<td>Allows you to refresh in real time to get the most current data.</td>
</tr>
</tbody>
</table>
To view the high level architecture diagram of how Privileged Account Manager is integrated with the Identity Manager, see Figure 9-1 on page 332. For more information about the driver, see NetIQ Identity Manager® Driver for NetIQ Privileged Account Manager Implementation Guide.

**Figure 9-1  Integrating Privileged Account Manager with Identity manager**

From Privileged Account Manager 3.0.1 onwards, the Privileged Account Manager driver creates a channel from Identity Manager to Privileged Account Manager to synchronize the password that is changed through the password check-in process. The Privileged Account Manager driver checks for any changes performed on the Privileged Account Manager 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.

### 9.2.1 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 Privileged Account Manager, the UserGroup objects are made available as Entitlements in Identity manager through the Driver. The UserGroup object is used in the Privileged Account Manager policy for authorizing privileged access to a server or an application. A user could login to UserApp and request for a Privileged Account Manager 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 Privileged Account Manager Account Domains:** The driver for Privileged Account Manager can synchronize Privileged Account Manager’s Credential Vault objects from Identity Manager to Privileged Account Manager. 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:** Privileged Account Manager allows emergency access and credential checkout/check in to any applications. During the password check in process, Privileged Account Manager generates a random password and the script that is set on the resource takes care of resetting the new password on the target application. Privileged Account Manager 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 “Privileged Access to Applications and Cloud Services” on page 275.

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 Privileged Account Manager 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 Privileged Account Manager. Also with Identity Manager integration, the number of applications that Privileged Account Manager 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.

9.3 Integrating with Syslog Server

For auditing the password check in event details, the Privileged Account Manager audit report can be used and these events can also be logged in the SIEM system like Sentinel.

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:

9.3.1 Configuring Syslog Server 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.

1. Click Setting > External Services on the home page of the console.
2. Click Syslog Server.
3. Configure the following details:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname/IP Address</td>
<td>Specify the DNS name or IP address of the syslog server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port the syslog server is listening on for syslog events.</td>
</tr>
<tr>
<td></td>
<td>The default port is 514. The default port for a Sentinel server or a</td>
</tr>
<tr>
<td></td>
<td>Sentinel Log Manager is 1468.</td>
</tr>
<tr>
<td>SSL</td>
<td>Move the slider to the right to enable SSL communication with a Sentinel</td>
</tr>
<tr>
<td></td>
<td>server. For a syslog server, do not select this option.</td>
</tr>
</tbody>
</table>
NOTE: To use this, ensure that Audit Zone is configured and at least one Syslog emitter is present in each Audit Zone.

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

4 The category and events are listed, and are in the enabled status. You can however disable the status of a specific event by moving the slider to the left.

**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 “Using the Command Rewrite Functionality for Command Arguments” on page 181.
- For information on using a .profile file to enable session auditing, see “Complete Session Control Using pcksh” on page 245.

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

4a To remove an event, highlight it, move the Status slider to left. By default all the events’ status is set to enabled.

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 **Update**. The sample output looks similar to the following string:

(sev:[0 TO 5]) AND pn:("NetIQ Privileged Account Manager")
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 Plugins 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.

9.4 Integration with Ticketing Systems

This integration allows you to create privileged access request for Linux Machines through ServiceNow instead of using Emergency Access Request of Privileged Account Manager. In addition, Privileged Account Manager allows the user to create a ServiceNow access request 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 Privileged Account Manager. Users are able to reset or retrieve a target system password only with an approved approver’s electronic consent. Any combination of target account, group, or system, end-user identity, group, or role, as well as contextual data like day of the week or time of day, can be used to determine approval criteria.

The following sections explain the configuration that must be done to provide access to the user using ServiceNow incident:

9.4.1 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.

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 Privileged Account Manager. If you set this to true, the access to the machine is granted only when the following conditions are matched:
- 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.

### 9.4.2 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.

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.
9.5 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 4.4 Installation Guide (https://www.netiq.com/documentation/access-manager-44/install_upgrade/data/bookinfo.html).

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.Privileged Account Manager.com) and a policy for injecting headers X_PUM_ADMIN and X_PUM_PASSWD. For more information, see the NetIQ Access Manager 4.4 Administration Console Guide.

2. Specify the following values in the policy:
   - Specify any Privileged Account Manager user for X_PUM_ADMIN.
   - Specify the Privileged Account Manager user password for X_PUM_PASSWD.

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

https://<NAM IP address:port>/pam/?sso=1
Privileged Account Manager supports the following command line options:

- Section 10.1, “The unifi Options,” on page 340
- Section 10.2, “Command Control Options,” on page 340
- Section 10.3, “Package Distribution Options,” on page 343
- Section 10.4, “Package Manager Options,” on page 344
- Section 10.5, “Registry Agent Options,” on page 346
- Section 10.6, “Registry Manager Options,” on page 348
- Section 10.7, “Compliance Auditor Options,” on page 348
- Section 10.8, “sreplay Command Line Options,” on page 351

You can run the command line options from either a Linux/UNIX Framework Manager, Windows Framework Manager, or agent machine.

To use the command line options, change to the unifi directory:

The following sections assume that you are running the commands from the unifi directory:

- Linux/UNIX: /opt/netiq/npum/sbin/unifi
- Windows: \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 . \ in the command. If you, remove . / 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.

This section includes the following topics:

- Section 10.1, “The unifi Options,” on page 340
- Section 10.2, “Command Control Options,” on page 340
- Section 10.3, “Package Distribution Options,” on page 343
- Section 10.4, “Package Manager Options,” on page 344
- Section 10.5, “Registry Agent Options,” on page 346
- Section 10.6, “Registry Manager Options,” on page 348
- Section 10.7, “Compliance Auditor Options,” on page 348
- Section 10.8, “sreplay Command Line Options,” on page 351
10.1 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-v</code></td>
<td>Displays the version of the Framework patch.</td>
</tr>
<tr>
<td><code>-s</code></td>
<td>Displays the service name if you have changed it by modifying the <code>unifi.xml</code> file.</td>
</tr>
<tr>
<td><code>-u &lt;username&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-p &lt;pwd&gt;</code></td>
<td>Specifies the password of the user.</td>
</tr>
<tr>
<td><code>-n</code></td>
<td>Indicates that the user’s native account can be used for credentials. This option replaces the <code>-u &lt;username&gt; -p &lt;pwd&gt;</code> options.</td>
</tr>
</tbody>
</table>

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 release.

For example:

```
/opt/netiq/npum/sbin/unifi -v
```

This command displays the version of the Framework patch.

10.2 Command Control Options

The command line options for the Command Control module allow you to perform the following tasks:

- Section 10.2.1, “Importing and Exporting Command Control Settings,” on page 341
- Section 10.2.2, “Backing Up and Restoring a Command Control Configuration,” on page 341
- Section 10.2.3, “Running Test Suites,” on page 343
10.2.1 Importing and Exporting Command Control Settings

The following commands allow you to export a current command control configuration and import one. Importing a configuration overwrites any existing rule set; therefore before importing a configuration, you should back up the current configuration (see Section 10.2.2, “Backing Up and Restoring a Command Control Configuration,” on page 341).

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, 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:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f &lt;arg&gt;</td>
<td>Specifies where to export the configuration to. Replace &lt;arg&gt; with a filename or a path and filename.</td>
</tr>
<tr>
<td>-c</td>
<td>Specifies that the configuration should be exported in clear text. This option cannot be used with the -p option.</td>
</tr>
<tr>
<td>-p &lt;pwd&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

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, 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:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f &lt;arg&gt;</td>
<td>Specifies the file to import. Replace &lt;arg&gt; with a filename or a path and filename.</td>
</tr>
<tr>
<td>-p &lt;pwd&gt;</td>
<td>Specifies the password that was used to encrypt the configuration when it was exported.</td>
</tr>
</tbody>
</table>

10.2.2 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, 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup -t &quot;&lt;reason&gt;&quot;</td>
<td>Backs up the current command control database. The -t &quot;&lt;reason&gt;&quot; parameter allows you to supply a reason for the backup, and is optional but recommended. Enclose the reason text in double quotes.</td>
</tr>
</tbody>
</table>
| 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 197).  
| 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.                             |
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
```

10.2.3 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, 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-t &lt;arg&gt;</code></td>
<td>Specifies a specific test suite to run. Replace <code>&lt;arg&gt;</code> with the name of the test suite. This option cannot be used with the <code>-A</code> option</td>
</tr>
<tr>
<td><code>-A</code></td>
<td>Runs all the test suites. This option cannot be used with the <code>-t</code> option.</td>
</tr>
<tr>
<td><code>-v</code></td>
<td>Outputs the full debug information to the screen.</td>
</tr>
<tr>
<td><code>-V &lt;file&gt;</code></td>
<td>Outputs the full debug information to the specified file or the specified path and file.</td>
</tr>
<tr>
<td><code>-o &lt;file&gt;</code></td>
<td>Outputs the test results to the specified file or the specified path and file.</td>
</tr>
</tbody>
</table>

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.

10.3 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, 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d &lt;directory&gt;</td>
<td>Imports the packages from the specified directory, for example:</td>
</tr>
<tr>
<td></td>
<td>-d /tmp/framework</td>
</tr>
<tr>
<td>-f &lt;package&gt;</td>
<td>Imports the specified package, for example:</td>
</tr>
<tr>
<td></td>
<td>-f /tmp/framework/xxx.pak</td>
</tr>
</tbody>
</table>

### 10.4 Package Manager Options

- Section 10.4.1, “Install and Uninstall Packages,” on page 344
- Section 10.4.2, “Upgrade and Rollback Packages,” on page 345

#### 10.4.1 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 344
- “Install and Uninstall Packages From Agent Machine” on page 345

**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>
```

```
./unifi -n pkgman uninstall <agent> <package>
```

If you have not mapped your local account to a Framework Manager user, 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, 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.

10.4.2 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.
- 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 344

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, 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.

### 10.5 Registry Agent Options

The Registry Agent module allows you to perform the following tasks from the command line:

- Section 10.5.1, “Registering an Agent,” on page 346
- Section 10.5.2, “Finding a Primary Manager Package,” on page 347
- Section 10.5.3, “Agent Status,” on page 347
- Section 10.5.4, “Adding Hosts and Domains,” on page 348

#### 10.5.1 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:

```sh
./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:

```sh
./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:

```sh
./unifi regclnt register manager1 29120 agent1.domain.com agent1 admin netiq
```
10.5.2 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, 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`

10.5.3 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, 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-s &lt;server&gt;</code></td>
<td>Displays status of the specified host. This option can be repeated on the command line for more than one host.</td>
</tr>
<tr>
<td><code>-o &lt;domain&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-S &lt;server&gt;</code></td>
<td>Confirms whether the host can communicate with the specified agent.</td>
</tr>
<tr>
<td><code>-M &lt;module&gt;</code></td>
<td>Confirms whether the agent can communicate with the specified module.</td>
</tr>
<tr>
<td><code>-a</code></td>
<td>Displays the status for all defined hosts.</td>
</tr>
<tr>
<td><code>-c</code></td>
<td>Provides output in CSV format.</td>
</tr>
<tr>
<td><code>-h</code></td>
<td>Prevents the display of the CVS header.</td>
</tr>
<tr>
<td><code>-?</code></td>
<td>Displays the usage message.</td>
</tr>
</tbody>
</table>
10.5.4 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.

10.6 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, 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.

10.7 Compliance Auditor Options

The command line options for the Compliance Auditor allow you to perform the following tasks:

- Section 10.7.1, “Exporting and Importing Compliance Auditor Settings,” on page 349
- Section 10.7.2, “Managing Compliance Auditor Records,” on page 349
10.7.1 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, 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.

10.7.2 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, 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:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list &lt;format&gt;</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>-x: For XML output.</td>
</tr>
<tr>
<td></td>
<td>-D &lt;date&gt;: For modifying the date format. For example, if you replace &lt;date&gt; 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).</td>
</tr>
<tr>
<td></td>
<td>-F &lt;fmt&gt;: For specifying what template information is displayed. By default, the following information is displayed.</td>
</tr>
<tr>
<td></td>
<td>- id: The unique ID of the archive.</td>
</tr>
<tr>
<td></td>
<td>- who: The ID of the user who created the archive.</td>
</tr>
<tr>
<td></td>
<td>- reason: The reason for the archive, if provided by the user.</td>
</tr>
<tr>
<td></td>
<td>- timestamp: The date and time when the archive occurred.</td>
</tr>
<tr>
<td></td>
<td>Replace &lt;fmt&gt; 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:</td>
</tr>
<tr>
<td></td>
<td>-F '${id}$,${reason}$'</td>
</tr>
<tr>
<td>archive -n <a href="">from:to</a> -p &lt;pwd&gt; -r &quot;&lt;reason&gt;&quot;</td>
<td>Creates a database in the /opt/netiq/npum/service/local/secaudit directory with the following format:</td>
</tr>
<tr>
<td></td>
<td>sa-2009-06-05_11-38-43.db</td>
</tr>
<tr>
<td></td>
<td>Each archived database can then be taken offline (moved to another storage area) and put back in place at any point.</td>
</tr>
<tr>
<td></td>
<td>Specify values for the following parameters:</td>
</tr>
<tr>
<td>-n <a href="">from:to</a>:</td>
<td>Specifies the records to archive. To archive one record, specify its ID. To archive a range of records, replace <a href="">from:to</a> 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.</td>
</tr>
<tr>
<td>p &lt;pwd&gt;:</td>
<td>(Optional) Specifies a password. If a password is specified for an archive, the same password must be used to restore the archive.</td>
</tr>
<tr>
<td>-r &quot;&lt;reason&gt;&quot;:</td>
<td>(Optional) Specifies a reason for the archive. The text must be included in double quotes.</td>
</tr>
<tr>
<td>listarchive &lt;format&gt;</td>
<td>Displays each of the archives that have been created. To view a format other than the default, replace &lt;format&gt; with a supported format. See the list option for valid values.</td>
</tr>
</tbody>
</table>
10.8 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-U user</td>
<td>Username</td>
</tr>
<tr>
<td>-P passwd</td>
<td>Password</td>
</tr>
<tr>
<td>-N</td>
<td>Uses native account for authorization</td>
</tr>
<tr>
<td>-l</td>
<td>Lists available logs</td>
</tr>
<tr>
<td>-g &lt;logfile&gt;</td>
<td>Gets available session entries in log</td>
</tr>
<tr>
<td>-u &lt;user&gt;,&lt;logfile&gt;</td>
<td>Gets available session entries for a particular user</td>
</tr>
<tr>
<td>-r &lt;session#&gt;,&lt;logfile&gt;</td>
<td>Replays a particular session</td>
</tr>
<tr>
<td>-f</td>
<td>Date format</td>
</tr>
<tr>
<td>-C</td>
<td>csv output</td>
</tr>
<tr>
<td>-Z</td>
<td>csv separator</td>
</tr>
</tbody>
</table>

Options that can be used with -g and -u

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-F &lt;FMT&gt;</td>
<td>Displays extra info, specified by FMT (comma seperated list)</td>
</tr>
<tr>
<td>groupid[=n]</td>
<td>Display group id of session</td>
</tr>
<tr>
<td>time[=n]</td>
<td>Displays time of start of session</td>
</tr>
</tbody>
</table>

- Options that can be used with -g and -u

- Options that can be used with -r

- Options that can be used with -f

- Options that can be used with -C

- Options that can be used with -Z
## Command Line Options

### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key=[n]</td>
<td>Displays session number</td>
</tr>
<tr>
<td>user=[n]</td>
<td>Displays submit user</td>
</tr>
<tr>
<td>host=[n]</td>
<td>Displays submit host</td>
</tr>
<tr>
<td>runas=[n]</td>
<td>Displays run user</td>
</tr>
<tr>
<td>runhost=[n]</td>
<td>Displays run host</td>
</tr>
<tr>
<td>cmd=[n]</td>
<td>Displays command</td>
</tr>
<tr>
<td>term=[n]</td>
<td>Displays term type</td>
</tr>
<tr>
<td>size=[n]</td>
<td>Displays size of session in Kb</td>
</tr>
</tbody>
</table>

**NOTE:** This can cause high CPU utilization on large files.

| all         | Lists all events                                |

### Option that can be used with `-g` and `-r`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-z</td>
<td>Get using group ID</td>
</tr>
</tbody>
</table>

### Options that can be used with `-r`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i</td>
<td>Displays stdin</td>
</tr>
<tr>
<td>-o</td>
<td>Displays stdout</td>
</tr>
<tr>
<td>-e</td>
<td>Displays stderr</td>
</tr>
<tr>
<td>-s</td>
<td>Displays signals</td>
</tr>
<tr>
<td>-p</td>
<td>Displays passwords</td>
</tr>
<tr>
<td>-d &lt;# ms&gt;</td>
<td>Sets display delay</td>
</tr>
<tr>
<td>-c &lt;charset&gt;</td>
<td>Enables character set conversion</td>
</tr>
<tr>
<td>-a</td>
<td>Displays all data</td>
</tr>
<tr>
<td>-l</td>
<td>Displays character by character, waiting for keypress</td>
</tr>
<tr>
<td>-m</td>
<td>Displays line by line, waiting for keypress</td>
</tr>
<tr>
<td>-x</td>
<td>Displays x11 capture</td>
</tr>
</tbody>
</table>

### 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"
11 Troubleshooting

This section contains potential problems and error codes that you may encounter when configuring or using Privileged Account Manager across all features.

- Section 11.1, “General Issues,” on page 355
- Section 11.2, “Troubleshooting Issues Related with Managing Hosts,” on page 360
- Section 11.3, “Issues While Integrating with Advanced Authentication,” on page 365

11.1 General Issues

The following is the list of general issues:

- Section 11.1.1, “The Agent Is In An Offline State,” on page 356
- Section 11.1.2, “The Audit Events Are Not Displayed In The Reports Console Even When the Events Are Generated,” on page 356
- Section 11.1.4, “The RDP Relay Session Does Not Start From The User Console,” on page 357
- Section 11.1.5, “The RDP Relay To a Windows Server 2012 Server Fails,” on page 357
- Section 11.1.6, “The Privileged Session Is Not Established Through The Backup Manager,” on page 357
- Section 11.1.7, “The Changes To The Syslog Settings Do Not Get Applied,” on page 358
- Section 11.1.8, “The Manual Disconnect For a Windows Session Does Not Work,” on page 358
- Section 11.1.10, “Agent Registration Fails In Windows Platform,” on page 358
- Section 11.1.11, “Direct RDP Sessions Are Enabled For All Users By Default,” on page 358
- Section 11.1.12, “Issues When Updating Or Downloading The License Summary,” on page 358
- Section 11.1.13, “Failed To Connect To A Module,” on page 359
- Section 11.1.14, “The System Cannot Process The Details Because One or More Agents With DB Audit Module is in Offline State,” on page 359
- Section 11.1.15, “The System Cannot Process The Details Because Of A Disconnect With The Credential Vault Modules,” on page 359
- Section 11.1.16, “SSL Connection to Microsoft SQL Sever Fails with a Timeout Error,” on page 359
11.1.1 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.

11.1.2 The Audit Events Are Not Displayed In The Reports Console Even When the Events Are Generated

**Issue:** When the audit events are not getting replicated from the Agent to the Manager, the Reports 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.

11.1.3 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 Privileged Account Manager 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.

### 11.1.4 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`.

### 11.1.5 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.

### 11.1.6 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.
11.1.7 The Changes To The Syslog Settings Do Not Get Applied

**Issue:** In the Reports 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.

11.1.8 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.

11.1.9 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.

11.1.10 Agent Registration Fails In 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.

11.1.11 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 11, “Troubleshooting,” on page 355.

11.1.12 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.
11.1.13 Failed To Connect To A 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.

11.1.14 The System Cannot Process The Details Because One or More Agents With 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.

11.1.15 The System Cannot Process The Details Because Of A Disconnect With The Credential Vault Modules

**Issue:** The error gets displayed when there are no credential vault modules in the Privileged Account Manager 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.

11.1.16 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.
11.1.17 **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 Windows 10.

**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.

11.1.18 **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.

11.2 **Troubleshooting Issues Related with Managing Hosts**

- Section 11.2.1, “Promoting Managers When the Primary Manager Fails,” on page 361
- Section 11.2.2, “Viewing Store and Forward Messages,” on page 361
- Section 11.2.3, “Managing Low Disk Space,” on page 362
- Section 11.2.4, “Restarting the Agent,” on page 363
- Section 11.2.5, “Managing the Registry Cache,” on page 363
- Section 11.2.6, “Time Synchronization,” on page 365
- Section 11.2.7, “Direct RDP is Disallowed When Privileged Account Manager Agents are Unable to Reach the Manager,” on page 365
11.2.1 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 Section 10.6, “Registry Manager Options,” on page 348.

11.2.2 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**.

### 11.2.3 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:

```perl
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:

```perl
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.

### 11.2.4 Restoring 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**.

### 11.2.5 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 364.
- 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 364.

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 363 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).
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 364).

11.2.6 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.

11.2.7 Direct RDP is Disallowed When Privileged Account Manager Agents are Unable to Reach the Manager

Issue: After upgrading Privileged Account Manager agents from 4.0 to 4.1 on Windows servers, Direct RDP will be disallowed when agents are unable to reach Privileged Account Manager server.

Workaround: You can configure Windows servers with PAM agents to allow a specific Troubleshoot user to initiate Direct RDP sessions when PAM Manager is not reachable. It is recommended to configure this before you update the agents to 4.1. Note that if you are installing and registering a fresh install of PAM 4.1 agent, you can achieve this automatically as a step during agent registration. Follow the below steps to add this configuration to windows registry:

1. Navigate to Registry Editor > HKEY_LOCAL_MACHINE > SOFTWARE > NetIQ > npum.
2. Right-click npum and add Key named TROUBLESHOOT.
3. Right-click TROUBLESHOOT. Click New > String Value.
4. Specify Value Name as name and Value Data in the hostname\username format.

Sample .reg File

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ]

[HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\npum]
@="C:\Program Files\NetIQ\npum\"

[HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\npum\TROUBLESHOOT]
"name"="dom032100\administrator1"

11.3 Issues While Integrating with Advanced Authentication

Following issue is encountered when integrating with Advanced Authentication server:
11.3.1 Advanced Authentication Server is Inactive 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, “Secondary Authentication Server Setting” on page 63.
This Appendix lists the legacy roles.

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

**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.

<table>
<thead>
<tr>
<th>Module</th>
<th>Role</th>
<th>Allows users to</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmdctrl</td>
<td>console</td>
<td>View the Command Control console.</td>
</tr>
<tr>
<td></td>
<td>read</td>
<td>View the Command Control console content and run test suites.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You must use <strong>console role along with read role</strong> to view the Command Control console and its content.</td>
</tr>
<tr>
<td></td>
<td>write</td>
<td>Modify the command control database. Users with this role cannot cancel other users’ transactions or modify audit or transaction settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Must be used in conjunction with the cmdctrl read role.</td>
</tr>
<tr>
<td></td>
<td>admin</td>
<td>Modify the Command Control database, including canceling other users’ transactions and modifying audit and transaction settings.</td>
</tr>
<tr>
<td></td>
<td>*</td>
<td>Perform all roles.</td>
</tr>
<tr>
<td>auth</td>
<td>read</td>
<td>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.</td>
</tr>
<tr>
<td>prvcrdvlt</td>
<td>read</td>
<td>Configure the resources and credentials in the command control rules.</td>
</tr>
<tr>
<td>unifi</td>
<td>admin</td>
<td>View the listed agents and perform administrative actions.</td>
</tr>
</tbody>
</table>

**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.
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.

<table>
<thead>
<tr>
<th>Module</th>
<th>Role</th>
<th>Allows users to</th>
</tr>
</thead>
<tbody>
<tr>
<td>prvcrdvlt</td>
<td>console</td>
<td>View the Credential Vault console.</td>
</tr>
<tr>
<td></td>
<td>read</td>
<td>View the resources and credentials in Credential Vault.</td>
</tr>
<tr>
<td></td>
<td>write</td>
<td>Add and modify the resources and credentials in Credential Vault.</td>
</tr>
<tr>
<td></td>
<td>admin</td>
<td>View, add, and modify the domains and credentials in Credential Vault.</td>
</tr>
</tbody>
</table>

* Perform all roles.

In conjunction you have to use cmdctrl and admin role.

Must be used in conjunction with userreqdashboard module and admin role.
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.

<table>
<thead>
<tr>
<th>Module</th>
<th>Role</th>
<th>Allows users to</th>
</tr>
</thead>
<tbody>
<tr>
<td>unifi</td>
<td>console</td>
<td>View the Hosts console.</td>
</tr>
<tr>
<td></td>
<td>info</td>
<td>Run the host status check by using the command line interface. You must type the word <code>info</code> because it is not available in the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>admin</td>
<td>View the Hosts console and perform administrative actions.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Module</th>
<th>Role</th>
<th>Allows users to</th>
</tr>
</thead>
<tbody>
<tr>
<td>pkgman</td>
<td>console</td>
<td>View the Package Manager console.</td>
</tr>
<tr>
<td></td>
<td>admin</td>
<td>View, add, update, or remove packages.</td>
</tr>
</tbody>
</table>

Distribution Roles

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

<table>
<thead>
<tr>
<th>Module</th>
<th>Role</th>
<th>Allows users to</th>
</tr>
</thead>
<tbody>
<tr>
<td>distrib</td>
<td>acl</td>
<td>Restricts deployment of packages to specified modules.</td>
</tr>
<tr>
<td></td>
<td>Module:reexec</td>
<td>Install or patch the Command Control Agent (reexec).</td>
</tr>
<tr>
<td></td>
<td>Module:distrib</td>
<td>Install or patch the Distribution Agent (distrib).</td>
</tr>
<tr>
<td></td>
<td>Module:regclnt</td>
<td>Install or patch the Registry Agent (regclnt).</td>
</tr>
<tr>
<td></td>
<td>Module:strfwd</td>
<td>Install or patch the Store and Forward Agent (strfwd).</td>
</tr>
<tr>
<td></td>
<td>Module:syinfo</td>
<td>Install or patch the System Information Agent (syinfo).</td>
</tr>
</tbody>
</table>

NOTE: Any module in the “Package Distribution Permissions” on page 46 can be allowed by using the format `Module:<desired-package-name>` to configure a Module.
Reports Console Roles

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

<table>
<thead>
<tr>
<th>Module</th>
<th>Role</th>
<th>Allows users to</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit</td>
<td>console</td>
<td>View the Reports console.</td>
</tr>
<tr>
<td>read</td>
<td></td>
<td>Read the audit database.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You must use console along with read role to view the Reports console and its content.</td>
</tr>
<tr>
<td>admin</td>
<td></td>
<td>Modify Reports settings.</td>
</tr>
<tr>
<td>command</td>
<td></td>
<td>View Command Control reports.</td>
</tr>
<tr>
<td>logon</td>
<td></td>
<td>View Account Logon reports.</td>
</tr>
<tr>
<td>*</td>
<td></td>
<td>Perform all roles.</td>
</tr>
<tr>
<td>write</td>
<td></td>
<td>Create new audit reports and adjust filter settings.</td>
</tr>
<tr>
<td>report</td>
<td></td>
<td>Access reports with the report defined roles.</td>
</tr>
<tr>
<td>&lt;report defined&gt;</td>
<td></td>
<td>Read and update the reports defined in the General tab of the Reports console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This role is only useful when used in conjunction with the report role.</td>
</tr>
</tbody>
</table>

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 not 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.

Requests Console Roles

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Role</th>
<th>Allows users to</th>
</tr>
</thead>
<tbody>
<tr>
<td>userreqdashboard</td>
<td>console</td>
<td>View the Request console.</td>
</tr>
<tr>
<td>admin</td>
<td></td>
<td>View and update emergency access and credential checkout requests.</td>
</tr>
<tr>
<td>*</td>
<td></td>
<td>Perform all roles.</td>
</tr>
</tbody>
</table>

Also you will require read and write permissions for cmdctrl and prvcrdvlt module.

Task Manager Role

The following roles can be assigned to the task manager module in order to view and modify scripts.

<table>
<thead>
<tr>
<th>Module</th>
<th>Role</th>
<th>Allows users to</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskmanager</td>
<td>role</td>
<td>Used for password management.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See, Section 5.6, “Password Management,” on page 122.</td>
</tr>
</tbody>
</table>

Framework User Manager Roles

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

<table>
<thead>
<tr>
<th>Module</th>
<th>Role</th>
<th>Allows users to</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth</td>
<td>role</td>
<td>View the Framework User Manager console.</td>
</tr>
</tbody>
</table>
## Module Role Allows users to

<table>
<thead>
<tr>
<th>Module</th>
<th>Role</th>
<th>Allows users to</th>
</tr>
</thead>
<tbody>
<tr>
<td>act_settings</td>
<td>Modify account settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>You must use <strong>admin</strong> role to view the Framework User Manager and its content.</td>
</tr>
<tr>
<td>admin</td>
<td>Add or delete users and groups, and assign users to groups.</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>Read the auth database.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You must use <strong>console</strong> role along with <strong>read</strong> role to view the Framework User Manager and its content.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This role must be used with all other auth roles.</td>
<td></td>
</tr>
<tr>
<td>role_admin</td>
<td>Add or remove roles.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You must use <strong>console</strong> role along with <strong>read</strong> and <strong>admin</strong> role to view the Framework User Manager and its content.</td>
<td></td>
</tr>
<tr>
<td>super</td>
<td>View and modify superusers, and view and modify groups with the super role defined. This role should also be able to add or delete users and groups, and assign users to groups.</td>
<td></td>
</tr>
<tr>
<td>api_token</td>
<td>Generate API tokens.</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>Perform all roles.</td>
<td></td>
</tr>
</tbody>
</table>
Appendix: 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 Section B.1, “Understanding Sample Policy template,” on page 373. 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 Section B.2, “Adding a Policy Template,” on page 374.

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.

B.1 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.

**B.1.1 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.

**B.2 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. 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 deseleting the Disable checkbox and then clicking Apply.

- Single sample policy can be imported multiple times at any level in the hierarchy.
This Appendix lists the supported end points for IPv6 for Privileged Account Manager 4.3 release.

<table>
<thead>
<tr>
<th>Resources/ End Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web SSH</td>
</tr>
<tr>
<td>SSH Relay</td>
</tr>
<tr>
<td>Linux Check in Check out (Password Change)</td>
</tr>
<tr>
<td>Web RDP</td>
</tr>
</tbody>
</table>