



BeyondTrust

Password Safe 23.3 Getting Started Guide

Table of Contents

Password Safe Getting Started Guide	3
Workflow to Add Systems and Accounts to Password Safe Management	4
Use Case Preparation	5
Required Service Accounts	5
Preparation for Smart Groups	5
Use Case 1: Add Local Admin Accounts for Windows Servers	7
Use Case 2: Add Local Root Accounts for Linux Servers	13
Use Case 3: Add Local Admin Accounts for Network Devices	19
Use Case 4: Add Directory Admin Accounts for Windows Servers	25
Use Case 5: Add Directory Admin Accounts for Linux Servers	28
Use Case 6: Add Directory Admin Accounts for Network Devices	31
Use Case 7: Add Dedicated Directory Accounts for Windows Servers	34
Use Case 8: Dedicated Directory Accounts for Entra ID	38
Use Case 9: Define Just in Time Access Policies	41
Configure Password Safe Access Policies	41

Password Safe Getting Started Guide

This document is designed to help you understand the flow of a typical Password Safe implementation and to get you started with using Password Safe by walking you through common use case examples.

Password Safe is your privileged access management solution to ensure your resources are protected from insider threats. It combines privileged password and session management to discover, manage, and audit all privileged credential activity.

Password Safe creates and secures privileged accounts through automated password management, encryption, secure storage of credentials, and a sealed operating system. This is designed to save you time and reduce the risk of human error.

Password Safe's random password generator algorithm does not use any common phrases or dictionary words as inputs or in its generation. It selects each password character randomly from the list of allowable characters, numerals, and symbols to build the password.

More specifically, you can use Password Safe to accomplish the following:

1. Scan, identify, and profile all assets for automated Password Safe management, ensuring no credentials are left unmanaged.
2. Control privileged user accounts, applications, SSH keys, cloud admin accounts, RPA accounts, and more.
3. Use adaptive access control for automated evaluation of just-in-time context for authorization access requests.
4. Monitor and record live sessions in real time and pause or terminate suspicious sessions.
5. Enable a searchable audit trail for compliance and forensics, and achieve complete control and accountability over privileged accounts.
6. Restrict access to critical systems, including assets and applications, keeping them safe from potential inside threat risks.

Workflow to Add Systems and Accounts to Password Safe Management

There are three ways to add systems and accounts to Password Safe:

- Add the asset manually.
- Run a Discovery Scan and then import the assets using an address group or directory query.
- Use API scripts.

The following is a high-level overview of the steps required to add systems and accounts to be managed in Password Safe.

1. **Add the functional account:** A functional account is one that can access the system with the privileges required to manage and change passwords for shared accounts on the system.
2. **Add the managed system:** A managed system is a computer or device where one or more account passwords are to be maintained by Password Safe. Managed systems can be Windows machines, Unix/Linux machines, network devices, databases, firewalls, routers, iLO machines, and LDAP or Active Directory domains.
3. **Add the managed account:** A managed account is an account on the managed system whose password is being stored and maintained through Password Safe. Typically, managed accounts are privileged accounts that can perform administrative tasks on the managed system.
4. **Configure managed system settings:** After a system is added to Password Safe, configure settings that apply to the managed system.
5. **Set up role based access:** Create user groups that permit users to:
 - Log in to the Password Safe web portal.
 - Assign Password Safe roles, such as **Requester** or **Approver**.
 - Create access policies to permit accounts to access the systems, applications, and sessions, and to request password releases.

Use Case Preparation

The use cases provided in this document use Smart Groups to accomplish the following:

- Discover assets and accounts using a Discovery Scan.
- Add assets and accounts into Password Safe management.
- Assign permissions and roles to user groups.

Required Service Accounts

Password Safe uses the following three types of service accounts that you must create in BeyondInsight prior to implementing the use cases in this guide:

Credentials for Discovery Scans: Detailed and advanced Discovery Scans require a credential that has privileges to discover the details for services, tasks, systems, devices, users, and databases from Active Directory or LDAP. To implement the use cases in this guide, you must create a credential that has sufficient privileges to retrieve this information from your directory. You can create credentials from the BeyondInsight Console, by navigating to **Configuration > Discovery and Vulnerability Management > Credentials**.

Functional Accounts: Smart Groups for adding assets into Password Safe management require a functional account that can access the assets with the privileges required to manage and change passwords on the accounts associated with those assets. To implement the use cases in this guide, you must create a functional account for each of the following:

- Windows servers
- Linux servers
- Network devices

Directory Credentials: Smart Groups for discovering Windows servers and directory accounts use a directory query for the Discovery Scan to pull details from Active Directory or LDAP and populate the Smart Group. A directory query requires a directory credential that has privileges to access the directory and request this information. To implement the use cases in this guide, you must create a directory credential for each of the following:

- Windows servers
- Windows directory accounts
- Linux directory accounts



For more information, please see:

- [Add Credentials for Use in Scans in the BeyondInsight User Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm)
- [Create a Functional Account in the Password Safe Admin Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/index.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/index.htm)
- [Create and Edit Directory Credentials in the BeyondInsight User Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm)

Preparation for Smart Groups

A Smart Group provides a way of grouping systems and accounts using filter conditions and actions called *Smart Rules*. The following items must be configured in BeyondInsight prior to creating the smart groups for each use case:

Directory Query: Smart Groups for discovering Windows servers and directory accounts use a directory query for the Discovery Scan to pull details from Active Directory or LDAP and populate the Smart Group. You must create a directory query for each of the following:

- Windows servers
- Windows directory accounts
- Linux directory accounts

Address Group: Smart Groups for discovering Linux servers and network devices use address groups for the Discovery Scan to discover and pull details for these assets from Active Directory or LDAP and populate the Smart Group. You need to create an address group for each of the following:

- Linux servers
- Network devices

Access Policy: An access policy to allow approved RDP and SSH sessions must be configured so it can be assigned to user groups when assigning roles and permissions for each of the use cases.



For more information, please see:

- [Use Smart Rules to Organize Assets in the BeyondInsight User Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm)
- [Work with Smart Rules in the Password Safe Admin Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/index.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/index.htm)
- [Create a Directory Query in the BeyondInsight User Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm)
- [Create an Address Group in the BeyondInsight User Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm)
- [Configure Access Policies in the Password Safe Admin Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/index.htm](https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/index.htm)

Use Case 1: Add Local Admin Accounts for Windows Servers

This use case walks through configuring the Smart Groups and user group roles and permissions required to enable automatic password rotation for local admin accounts on Windows servers with auto-approval for RDP sessions enabled.

The shared local administrative account that exists on all Windows servers needs to be controlled, audited, and rotated on a regular schedule. For this use case, you will bring in all Windows domain joined servers and manage the local built-in administrator account. You will also grant permissions to a specific set of users who need access to all Windows servers. As you do not know if there are additional local administrator accounts, you will configure a Smart Group to find them. You will also configure a Smart Group to ensure new servers are added dynamically as they are joined to the domain on a recurring basis.

To accomplish all of the above, you must create the following Smart Groups in the BeyondInsight Console:

- An asset Smart Group for discovering the Windows servers
- An asset Smart Group for adding the Windows servers to Password Safe management
- A managed system Smart Group for granting system access to user groups
- A managed account Smart Group to add the local admin accounts to Password Safe management

You must also associate the managed account Smart Group to user groups, and then assign roles and permissions to the associated managed account Smart Group.

Create Asset Based Smart Group to Discover Windows Servers

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Click **Create Smart Rule**.
3. Select the **Category** and enter a meaningful **Name** and **Description** for the Smart Rule.

4. Set **Selection Criteria** as:


- **Directory Query, Include assets from query, <query name>, Use to discover new assets during scans (enabled)**
- Enter the interval in hours to rerun the query to ensure new servers that have joined the domain are automatically captured

5. Set **Actions** as:

- **Show asset as Smart Group, View assets in a standard asset grid**

6. Click **Create Smart Rule**.

Servers: Discover Windows Servers


Details 

Category


Name Active


Description

Reprocessing limit

Selection Criteria 


Include items that match of the following


- 
-
-
-

Re-run the query every X hours 

Use to discover new assets during scans

[Add another condition](#) [Add a new group](#)


Actions 

- 
-

[Add another action](#)

You can now run a Discovery Scan against this Smart Group. In order to pull details, including local accounts, from each asset into BeyondInsight, execute a scan with appropriate credentials.

You can initiate a scan from the vertical ellipsis menu for the Smart Group on the **Smart Rules** page in BeyondInsight. You can also schedule a recurring scan to discover new assets and confirm the local accounts and services have not changed on the existing assets. This is key to a dynamic onboarding process.


 For more information on configuring a Discovery Scan, please see *Run Discovery Scans in the [BeyondInsight User Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/discovery.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/discovery.htm>.*

Create Asset Based Smart Group to Add Windows Servers to Password Safe Management

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Click **Create Smart Rule**.
3. Select the **Category** and enter a meaningful **Name** and **Description** for the Smart Rule.

4. Set **Selection Criteria** as:


- **Operating System, contains, windows**
- **Asset fields, Domain Name, contains, domain**

 **Note:** The **Operating System** criteria is used to query servers that have the same functional account. The action associates the functional account with the system.


5. Set **Actions** as:

- **Show asset as Smart Group, View assets in a standard asset grid**
- **Manage Assets using Password Safe, Platform: Windows, Account Name Format: Domain\Username, Functional Account: <functional account name>**

6. Click **Create Smart Rule**.

 **Note:** To ensure new servers are automatically added to Password Safe management, this Smart Group must be repeatedly processed, especially after the last scan completes.

Servers: Add Windows Servers To Password Safe


Details 

Category
Servers

Name
Add Windows Servers to Password Safe Active

Description
Add Windows Servers to Password Safe using AD Functional Account

Reprocessing limit
Default


Selection Criteria 

Include Items that match ALL of the following

Operating System
contains
windows
 Limit to most recent OS detected

Asset fields
Domain Name
and
contains
domain

[Add another condition](#) [Add a new group](#)

Actions 

Show asset as Smart Group

View assets in a standard asset grid

Manage Assets using Password Safe

Platform Windows

Change Agent Password Safe

Account Name Format Domain\Username

Functional Account Windows FA (windows\windows)

Enable Automatic Password Management yes

Enable Accounts For AD Queries no

Password Rule Default Password Policy

Connection Timeout 30

[Add another action](#)

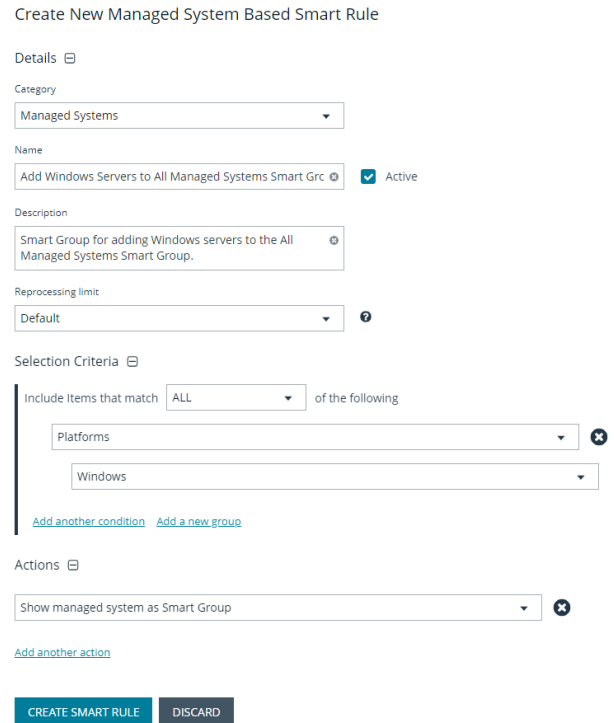
CREATE SMART RULE **DISCARD**

Create Managed System Smart Group for Granting System Access to User Groups

Creating this managed system Smart Group is not always required but it helps you to group systems that have specific managed accounts associated with them and to assign asset level permissions to user groups. As the assets are added to Password Safe management, they automatically populate within the **All Managed Systems** Smart Group.

This smart group specifically looks for all Windows servers that are managed by Password Safe.

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select **Managed System** from the **Smart Rule Type filter** list.
3. Click **Create Smart Rule**.
4. Select **Managed Systems** from the **Category** list.
5. Enter a meaningful **Name** and **Description** for the Smart Rule.
6. Set **Selection Criteria** as:
 - **Platforms, Windows**
7. Set **Actions** as:
 - **Show managed system as Smart Group**
8. Click **Create Smart Rule**.



Create New Managed System Based Smart Rule

Details ▾

Category
Managed Systems ▾

Name
Add Windows Servers to All Managed Systems Smart Gr... Active

Description
Smart Group for adding Windows servers to the All Managed Systems Smart Group.

Reprocessing limit
Default ⓘ

Selection Criteria ▾

Include Items that match ALL ▾ of the following

Platforms ▾

Windows ▾

[Add another condition](#) [Add a new group](#)

Actions ▾

Show managed system as Smart Group ▾

[Add another action](#)


CREATE SMART RULE **DISCARD**

Create Managed Account Smart Group to Add Accounts to Password Safe Management

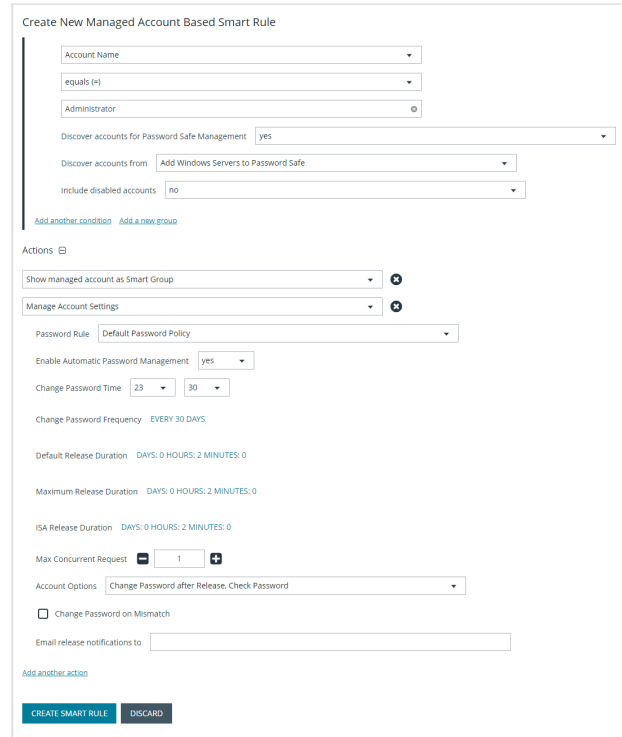
The initial creation of this Smart Group only has the one account name of the built-in Administrator account. After researching and reviewing reports, additional privileged account names may be added to this Smart Group.

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule Type filter** list.
3. Click **Create Smart Rule**.

4. Select **Managed Accounts** from the **Category** list.
5. Enter a meaningful **Name** and **Description** for the Smart Rule.
6. Set **Selection Criteria** as:
 - **User Account Attribute, Account Name, equals, <Administrator>, Discover Accounts for Password Safe Management: yes, Discover accounts from: <Smart Group for adding Windows servers>**
7. Set **Actions** as:
 - **Show managed account as Smart Group**
 - **Manage Account Settings, Password Rule: <password policy>, Enable Automatic Password Management: yes, Change Password Time: <desired time>, Change Password Frequency: <desired frequency>**

 **Note:** The **Manage Account Settings** action onboards the specific account, if found in the system's scan results. This action also dictates whether the account is rotated immediately or not.

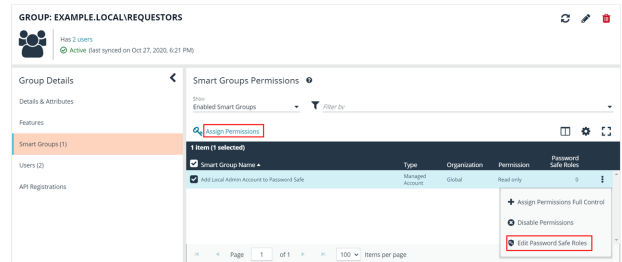
8. Click **Create Smart Rule**.



Assign User Group Permissions and Roles for Account Access

Associate a user group to the Smart Group that you created for adding accounts to Password Safe management, and then assign permissions, roles, and an access policy to the Smart Group. In this use case, the Password Safe users are **Requestors** with an access policy to allow auto-approved RDP sessions.

1. From the left navigation in the BeyondInsight Console, click **Configuration**.
2. Under **Role Based Access**, click **User Management**.
3. Locate the user group in the grid, and then click the **More Options** (ellipsis) button for that group.
4. Select **View Group Details**.
5. From the **Group Details** pane, select **Smart Groups**.
6. In the **Smart Groups Permissions** grid, select the Smart Group you created for adding the local Windows admin account to Password Safe, and then click **Assign Permissions** above the grid.
7. Select **Assign Permissions Read Only**.
8. Click the vertical ellipsis button for the Smart Group, and then select **Edit Password Safe Roles**.



9. Select the **Requestor** role, and then select the **Access Policy**.
10. Click **Save Roles**.

Add Local Admin Account To Password Safe Password Safe Roles

A role is the connection between a Password Safe user account and a managed system. A role defines what the user or group can do with respect to that managed system.

Requestor

Access Policy for Requestor
24x7 - No Approval 

Approver

Credentials Manager

Recorded session reviewer

Active session reviewer

SAVE ROLES

DISCARD CHANGES

Use Case 2: Add Local Root Accounts for Linux Servers

This use case walks through configuring automatic password rotation for local admin accounts on Linux servers with auto-approval for SSH sessions enabled.

Root level accounts on all Linux servers should be controlled, audited, and rotated on a regular schedule. For this use case, you will bring in all Linux and Unix servers and manage the local root account. You will also grant permissions to a specific set of users who need access to all Linux servers.

To accomplish all of the above, you must create the following smart groups in the BeyondInsight Console:

- An asset Smart Group for discovering the Linux servers
- An asset Smart Group for adding the Linux servers to Password Safe management
- A managed system Smart Group for granting system access to user groups
- A managed account Smart Group to add the local admin accounts to Password Safe management


You must also associate the managed account Smart Group to user groups, and then assign roles and permissions to the associated managed account Smart Group.


Create Asset Based Smart Group to Discover Linux Servers


1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Click **Create Smart Rule**.
3. Select the **Category** and enter a meaningful **Name** and **Description** for the Smart Rule.


4. Set **Selection Criteria** as:
 - **Address Group**, <address group name>, **Use to discover new assets during scans (enabled)**
 - Enter the interval in hours to rerun the query to ensure new servers that have joined the domain are automatically captured
5. Set **Actions** as:
 - **Show asset as Smart Group, View assets in a standard asset grid**
6. Click **Create Smart Rule**.



Create New Asset Based Smart Rule


Details 


Category
Servers 



Name
Discover Linux Servers  Active


Description
Discover Linux Servers 

Reprocessing limit
Default  

Selection Criteria 


Include items that match ALL  of the following



Address Group  


Linux Servers 

Use to discover new assets during scans

[Add another condition](#) [Add a new group](#)

Actions 

Show asset as Smart Group  

View assets in a standard asset grid 

[Add another action](#)

CREATE SMART RULE **DISCARD**

You can now run a Discovery Scan against this Smart Group. In order to pull details, including local accounts, from each asset into BeyondInsight, execute a scan with appropriate credentials.

You can initiate a scan from the vertical ellipsis menu for the Smart Group on the **Smart Rules** page in BeyondInsight. You can also schedule a recurring scan to discover new assets and confirm the local accounts and services have not changed on the existing assets. This is key to a dynamic onboarding process.



Note: Since an address group is a static list of hosts, this Smart Group doesn't need to reprocess often -- only when known changes to the address group have been made.




For more information on configuring a Discovery Scan, please see *Run Discovery Scans in the [BeyondInsight User Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/discovery.htm) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/discovery.htm>.*

Create Asset Based Smart Group to Add Linux Servers to Password Safe Management

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Click **Create Smart Rule**.
3. Select the **Category** and enter a meaningful **Name** and **Description** for the Smart Rule.

4. Set **Selection Criteria** as:


- **Operating System, contains, linux**

 **Note:** The **Operating System** criteria is used to query servers that have the same functional account. The action associates the functional account with the system.


5. Set **Actions** as:

- **Show asset as Smart Group, View assets in a standard asset grid**
- **Manage Assets using Password Safe, Platform: Linux, Account Name Format: SAM, Functional Account: <functional account name>**

6. Click **Create Smart Rule**.

 **Note:** To ensure new servers are automatically added to Password Safe management, this Smart Group must be repeatedly processed, especially after the last scan completes.

Create New Asset Based Smart Rule


Details 

Category: Servers

Name: Add Linux Servers to Password Safe Active


Description: Add Linux Servers to Password Safe

Reprocessing limit: Default

Selection Criteria 

Include items that match ALL of the following

- Operating System: contains linux Limit to most recent OS detected

Actions 

Show asset as Smart Group

View assets in a standard asset grid

Manage Assets using Password Safe

Platform: Linux

Change Agent: Password Safe

Allow Managed System to be an Application Host: no

Account Name Format: SAM

Functional Account: fa_linux_test

Enable Automatic Password Management: yes

Enable Login Account For SSH Sessions: no

Enable Accounts For AD Queries: no

Password Rule: Default Password Policy

Elevation: None

Key Enforcement Mode: None

Connection Timeout: 30

Port: 22

[Add another action](#)

CREATE SMART RULE **DISCARD**

Create Managed System Smart Group for Granting System Access to User Groups

Creating this managed system Smart Group is not always required but it helps you to group systems that have specific managed accounts associated with them and to assign asset level permissions to user groups. As the assets are added to Password Safe management, they automatically populate within the **All Managed Systems** Smart Group.

This smart group specifically looks for all Linux servers that are managed by Password Safe.

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select **Managed System** from the **Smart Rule Type** filter list.
3. Click **Create Smart Rule**.

4. Select **Managed Systems** from the **Category** list.
5. Enter a meaningful **Name** and **Description** for the Smart Rule.
6. Set **Selection Criteria** as:
 - **Platforms, Linux**
7. Set **Actions** as:
 - **Show managed system as Smart Group**
8. Click **Create Smart Rule**.

Create New Managed System Based Smart Rule

Details ☰

Category

Name
 Active

Description

Reprocessing limit

Selection Criteria ☰

Include items that match of the following

[Add another condition](#) [Add a new group](#)

Actions ☰


[Add another action](#)

Create Managed Account Smart Group to Add Accounts to Password Safe Management

The initial creation of this Smart Group only has the one account name of the root account. After researching and reviewing reports, additional privileged account names may be added to this Smart Group.

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule Type** filter list.
3. Click **Create Smart Rule**.

4. Select **Managed Accounts** from the **Category** list.
5. Enter a meaningful **Name** and **Description** for the Smart Rule.
6. Set **Selection Criteria** as:
 - **User Account Attribute, Account Name, equals, root, Discover Accounts for Password Safe Management: yes, Discover accounts from: <Smart Group for adding Linux servers>**
7. Set **Actions** as:
 - **Show managed account as Smart Group**
 - **Manage Account Settings, Password Rule: <password policy>, Enable Automatic Password Management: yes, Change Password Time: <desired time>, Change Password Frequency: <desired frequency>**

 **Note:** The **Manage Account Settings** action onboards the specific account, if found in the system's scan results. This action also dictates whether the account is rotated immediately or not.

8. Click **Create Smart Rule**.

Create New Managed Account Based Smart Rule

Details ▾

Category: Managed Accounts

Name: Add Linux Root Account to Password Safe Active

Description: Add Linux Root Account to Password Safe

Reprocessing limit: Default

Selection Criteria ▾

Include items that match ALL of the following

User Account Attribute

Account Name

equals (=)

root

Discover accounts for Password Safe Management: yes

Discover accounts from: Add Linux Servers to Password Safe

Include disabled accounts: no

Actions ▾

Show managed account as Smart Group

Manage Account Settings

Password Rule: Default Password Policy

Enable Automatic Password Management: yes

Change Password Time: 23 30

Change Password Frequency: EVERY 30 DAYS

Default Release Duration: DAYS: 0 HOURS: 2 MINUTES: 0

Maximum Release Duration: DAYS: 0 HOURS: 2 MINUTES: 0

ISA Release Duration: DAYS: 0 HOURS: 2 MINUTES: 0

Max Concurrent Request: 1

Account Options: Change Password after Release. Check Password

Change Password on Mismatch

Email release notifications to:

[Add another action](#)

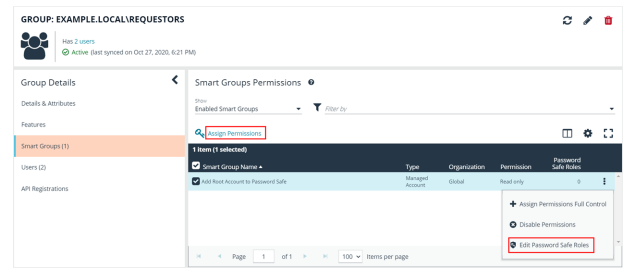
CREATE SMART RULE **DISCARD**

Assign User Group Permissions and Roles for Account Access

Associate a user group to the Smart Group that you created for adding accounts to Password Safe management, and then assign permissions, roles, and an access policy to the Smart Group. In this use case, the Password Safe users are **Requestors** with an access policy to allow auto-approved SSH sessions.

1. From the left navigation in the BeyondInsight console, click **Configuration**.
2. Under **Role Based Access**, click **User Management**.
3. Locate the user group in the grid, and then click the vertical ellipsis button for that group.
4. Select **View Group Details**.

5. From the **Group Details** pane, select **Smart Groups**.
6. In the **Smart Groups Permissions** grid, select the Smart Group you created for adding the Linux root account to Password Safe, and then click **Assign Permissions** above the grid.
7. Select **Assign Permissions Read Only**.
8. Click the vertical ellipsis button for the Smart Group, and then select **Edit Password Safe Roles**.
9. Select the **Requestor** role, and then select the **Access Policy**.
10. Click **Save Roles**.



Add Root Account To Password Safe Password Safe Roles

A role is the connection between a Password Safe user account and a managed system. A role defines what the user or group can do with respect to that managed system.

Requestor
 Access Policy for Requestor
 24x7 - No Approval

Approver

Credentials Manager

Recorded session reviewer

Active session reviewer

SAVE ROLES **DISCARD CHANGES**

Use Case 3: Add Local Admin Accounts for Network Devices

This use case walks through configuring automatic password rotation for local admin accounts on network devices with auto-approval for SSH sessions enabled.

Admin level accounts exist on all network devices that need to be controlled, audited, and rotated on a regular schedule. For this use case, you will import all Cisco switches (or network devices from other vendors that allow administration via SSH) and manage the local admin account. You will also grant permissions to a specific set of users who need access to all network devices.

To accomplish all of the above, you must create the following Smart Groups in the BeyondInsight console:


- An asset Smart Group for discovering the devices
- An asset Smart Group for adding the devices to Password Safe management
- A managed system Smart Group for granting system access to user groups
- A managed account Smart Group to add the local admin accounts to Password Safe management

You must also associate the managed account Smart Group with user groups, and then assign roles and permissions to the associated managed account Smart Group.

Create Asset Based Smart Group to Discover Network Devices

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Click **Create Smart Rule**.
3. Select the **Category** and enter a meaningful **Name** and **Description** for the Smart Rule.
4. Set **Selection Criteria** as:
 - **Address Group, <address group name>, Use to discover new assets during scans (enabled)**
 - Enter the interval in hours to rerun the query to ensure new servers that have joined the domain are automatically captured
5. Set **Actions** as:
 - **Show asset as Smart Group, View assets in a standard asset grid**
6. Click **Create Smart Rule**.


Create New Asset Based Smart Rule


Details 

Category
Assets and Devices

Name
Discover Cisco Devices Active

Description
Discover Cisco Devices

Reprocessing limit
Default 

Selection Criteria 


Include items that match ALL of the following

Address Group

Cisco Network Devices

Use to discover new assets during scans

[Add another condition](#) [Add a new group](#)

Actions 

Show asset as Smart Group

View assets in a standard asset grid

[Add another action](#)

CREATE SMART RULE **DISCARD**

You can now run a Discovery Scan against this Smart Group. In order to pull details, including local accounts, from each asset into BeyondInsight, execute a scan with appropriate credentials.

You can initiate a scan from the vertical ellipsis menu for the Smart Group on the **Smart Rules** page in BeyondInsight. You can also schedule a recurring scan to discover new assets and confirm the local accounts and services have not changed on the existing assets. This is key to a dynamic onboarding process.



Note: Since an address group is a static list of hosts, this Smart Group doesn't need to reprocess often -- only when known changes to the address group have been made.



For more information on configuring a Discovery Scan, please see *Run Discovery Scans in the [BeyondInsight User Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/discovery.htm)* at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/discovery.htm>.

Create Asset Based Smart Group to Add Network Devices to Password Safe Management

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Click **Create Smart Rule**.
3. Select the **Category** and enter a meaningful **Name** and **Description** for the Smart Rule.

4. Set Selection Criteria as:

- **Operating System, contains, cisco**



Note: The **Operating System** criteria is used to query servers that have the same functional account. The action associates the functional account with the system.

5. Set Actions as:

- **Show asset as Smart Group, View assets in a standard asset grid**
- **Manage Assets using Password Safe, Platform: Cisco, Account Name Format: SAM, Functional Account: <functional account name>**

6. Click **Create Smart Rule**.



Note: To ensure new servers are automatically added to Password Safe management, this Smart Group must be repeatedly processed, especially after the last scan completes.

Create New Asset Based Smart Rule

Details

Category: Assets and Devices

Name: Add Cisco Network Devices to Password Safe Active

Description: Add Cisco Network Devices to Password Safe

Reprocessing limit: Default

Selection Criteria

Include items that match ALL of the following

- Operating System: contains cisco
- Limit to most recent OS detected

Actions

- Show asset as Smart Group
- View assets in a standard asset grid
- Manage Assets using Password Safe
- Platform: Cisco
- Allow Managed System to be an Application Host: no
- Account Name Format: Domain/Username
- Functional Account: cisco
- Enable Automatic Password Management: yes
- Enable Accounts For AD Queries: no
- Password Rule: Default Password Policy
- Key Enforcement Mode: None
- Connection Timeout: 30
- Port: 22

[Add another condition](#) [Add a new group](#)

[CREATE SMART RULE](#) [DISCARD](#)

Create Managed System Smart Group for Granting System Access to User Groups


Creating this managed system Smart Group is not always required but it helps you to group systems that have specific managed accounts associated with them and to assign asset level permissions to user groups. As the assets are added to Password Safe management, they automatically populate within the **All Managed Systems** Smart Group.

This Smart Group specifically looks for all network devices that are managed by Password Safe.

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select **Managed System** from the **Smart Rule Type** filter list.
3. Click **Create Smart Rule**.

4. Select **Managed Systems** from the **Category** list.
5. Enter a meaningful **Name** and **Description** for the Smart Rule.
6. Set **Selection Criteria** as:
 - **Platforms, Cisco**
7. Set **Actions** as:
 - **Show managed system as Smart Group**
8. Click **Create Smart Rule**.


Create New Managed System Based Smart Rule


Details 

Category


Name
 Active

Description


Reprocessing limit
 


Selection Criteria 

Include Items that match of the following



[Add another condition](#) [Add a new group](#)

Actions 



[Add another action](#)

Create Managed Account Smart Group to Add Accounts to Password Safe Management

The initial creation of this Smart Group only has the one account name of the local admin account. After researching and reviewing reports, additional privileged account names may be added to this Smart Group.

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule Type** filter list.
3. Click **Create Smart Rule**.

4. Select **Managed Accounts** from the **Category** list.
5. Enter a meaningful **Name** and **Description** for the Smart Rule.
6. Set **Selection Criteria** as:

- **User Account Attribute, Account Name, equals, <Admin>, Discover Accounts for Password Safe Management: yes, Discover accounts from: <Smart Group for adding network devices>**

7. Set **Actions** as:

- **Show managed account as Smart Group**
- **Manage Account Settings, Password Rule: <password policy>, Enable Automatic Password Management: yes, Change Password Time: <desired time>, Change Password Frequency: <desired frequency>**

Create New Managed Account Based Smart Rule

Details ☰

Category: Managed Accounts

Name: Add Cisco Admin Account to Password Safe Active

Description: Add Cisco Admin Account to Password Safe

Reprocessing limit: Default

Selection Criteria ☰

Include items that match ALL of the following

- User Account Attribute
 - Account Name
 - equals (=)
 - admin
- Discover accounts for Password Safe Management: yes
- Discover accounts from: Add Cisco Network Devices to Password Safe
- Include disabled accounts: no


[Add another condition](#) [Add a new group](#)

Actions ☰

- Show managed account as Smart Group
- Manage Account Settings
 - Password Rule: Default Password Policy
 - Enable Automatic Password Management: yes
 - Change Password Time: 23 30
 - Change Password Frequency: EVERY 30 DAYS
 - Default Release Duration: DAYS: 0 HOURS: 2 MINUTES: 0
 - Maximum Release Duration: DAYS: 0 HOURS: 2 MINUTES: 0
 - ISA Release Duration: DAYS: 0 HOURS: 2 MINUTES: 0
 - Max Concurrent Request: 1
 - Account Options: Change Password after Release, Check Password
 - Change Password on Mismatch
 - Email release notifications to:

[Add another action](#)

CREATE SMART RULE DISCARD

 **Note:** The **Manage Account Settings** action onboards the specific account, if found in the system's scan results. This action also dictates whether the account is rotated immediately or not.

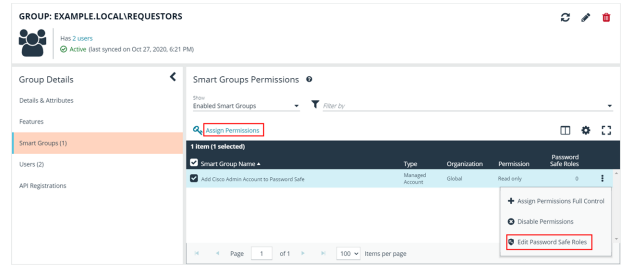
8. Click **Create Smart Rule**.

Assign User Group Permissions and Roles for Account Access

Associate a user group with the Smart Group that you created for adding accounts to Password Safe management, and then assign permissions, roles, and an access policy to the Smart Group. In this use case, the Password Safe users are **Requestors** with an access policy to allow auto-approved RDP sessions.

1. From the left navigation in the BeyondInsight console, click **Configuration**.
2. Under **Role Based Access**, click **User Management**.
3. Locate the user group in the grid, and then click the **More Options** (ellipsis) button for that group.
4. Select **View Group Details**.

5. From the **Group Details** pane, select **Smart Groups**.
6. In the **Smart Groups Permissions** grid, select the Smart Group you created for adding the Cisco Admin account to Password Safe, and then click **Assign Permissions** above the grid.
7. Select **Assign Permissions Read Only**.
8. Click the vertical ellipsis button for the Smart Group, and then select **Edit Password Safe Roles**.
9. Select the **Requestor** role, and then select the **Access Policy**.
10. Click **Save Roles**.



Add Cisco Admin Account To Password Safe Password Safe Roles ➤

A role is the connection between a Password Safe user account and a managed system. A role defines what the user or group can do with respect to that managed system.

Requestor
Access Policy for Requestor
24x7 - No Approval

Approver

Credentials Manager

Recorded session reviewer

Active session reviewer

SAVE ROLES **DISCARD CHANGES**

Use Case 4: Add Directory Admin Accounts for Windows Servers

This use case walks through configuring automatic password rotation for directory admin accounts on Windows servers with auto-approval for RDP sessions enabled.

Directory accounts that have elevated (privileged) access exist within Active Directory. These accounts have permissions to all domain joined Windows servers and should be controlled, audited, and rotated on a regular schedule. For this use case, Password Safe is already managing all Windows domain joined servers by implementing *Use Case 1* and a specific set of users are allowed to use these shared accounts.

Since you have already configured asset Smart Groups for discovering assets, asset Smart Groups for adding systems to Password Safe management, and managed systems Smart Groups for granting system access from previous use cases, you do not need to create any additional Smart Groups for these purposes.

If you need to add additional servers to Password Safe, you can create new Smart Groups using different address groups or directory queries as applicable, and run new scans as applicable, following the steps outlined in previous use cases.

Additionally, if you require only a subset of systems to be allowed to use these directory accounts, you can create a new managed system Smart Group using more specific selection criteria to provide access to a smaller selection of systems.

For this use case, you will create a managed account Smart Group to add the directory accounts to Password Safe and to link the directory accounts to managed systems.

You must also associate the managed account Smart Group with user groups, and then assign roles and permissions to the associated managed account Smart Group.



For more information, please see "[Use Case 1: Add Local Admin Accounts for Windows Servers](#)" on page 7.

Create Managed Account Smart Group to Add Directory Accounts to Password Safe and Configure Account Linking

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule Type** filter list.
3. Click **Create Smart Rule**.

4. Select **Managed Accounts** from the **Category** list.
5. Enter a meaningful **Name** and **Description** for the Smart Rule.
6. Set **Selection Criteria** as:

- **Directory Query, Include Accounts from Directory Query, <query name>, Discover Accounts for Password Safe Management: enabled**



***Tip:** If Password Safe already manages the privileged accounts, you can use criteria of **Managed Account Fields > Account Name** in the Smart Rule instead of using a directory query. For an example of this option, please see ["Use Case 6: Add Directory Admin Accounts for Network Devices"](#) on page 31.*

7. Set Actions

- **Link domain accounts to Managed Systems, Asset or Managed System Smart Group: <Smart Group that contains Windows servers that the accounts will be associated to for session management>**
- **Manage Account Settings, Password Rule: <password policy>, Enable Automatic Password Management: no**
- **Show managed account as Smart Group**



***Note:** The **Manage Account Settings** action onboards the specific account, if found in the system's scan results. This action also dictates whether the account is rotated immediately or not.*



***Tip:** These actions can be separated into multiple managed account Smart Groups with criteria of **Child Smart Rule** or other specific criteria for the linking rule action, if desired.*

8. Click **Create Smart Rule**.

Create New Managed Account Based Smart Rule

Details

Category

Name Active

Description

Reprocessing limit

Selection Criteria

Include items that match of the following

-
-
-

Re-run the query every X hours

Discover accounts for Password Safe Management

Domain

[Add another condition](#) [Add a new group](#)

Actions

-
- Asset or Managed System Smart Group
- Show managed account as Smart Group
- Manage Account Settings
- Password Rule
- Enable Automatic Password Management
- Change Password Time
- Change Password Frequency
- Default Release Duration
- Maximum Release Duration
- ISA Release Duration
- Max Concurrent Request
- Account Options
- Change Password on Mismatch
- Email release notifications to

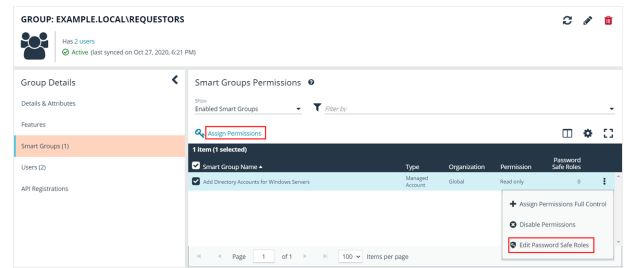
[Add another action](#)

Assign User Group Permissions and Roles for Account Access

Associate a user group to the Smart Group that you created for adding accounts to Password Safe management, and then assign permissions, roles, and an access policy to the Smart Group. In this use case, the Password Safe users are **Requestors** with an access policy to allow auto-approved RDP sessions.

1. From the left navigation in the BeyondInsight Console, click **Configuration**.
2. Under **Role Based Access**, click **User Management**.
3. Locate the user group in the grid, and then click the vertical ellipsis button for that group.
4. Select **View Group Details**.

5. From the **Group Details** pane, select **Smart Groups**.
6. In the **Smart Groups Permissions** grid, select the Smart Group you created for adding Windows directory accounts to Password Safe, and then click **Assign Permissions** above the grid.
7. Select **Assign Permissions Read Only**.
8. Click the vertical ellipsis button for the Smart Group, and then select **Edit Password Safe Roles**.
9. Select the **Requestor** role, and then select the **Access Policy**.
10. Click **Save Roles**.



Add Directory Accounts For Windows Servers Password Safe Roles ➤

A role is the connection between a Password Safe user account and a managed system. A role defines what the user or group can do with respect to that managed system.

Requestor

Access Policy for Requestor
24x7 - No Approval

Approver

Credentials Manager

Recorded session reviewer

Active session reviewer

SAVE ROLES

DISCARD CHANGES

Use Case 5: Add Directory Admin Accounts for Linux Servers

This use case walks through configuring automatic password rotation for directory admin accounts on Linux servers with auto-approval for SSH sessions enabled.

Directory accounts that have elevated (privileged) access exist within Active Directory. These accounts have permissions to all domain joined Windows servers and should be controlled, audited, and rotated on a regular schedule. For this use case, Password Safe is already managing all Linux domain joined servers by implementing *Use Case 2*, and a specific set of users are allowed to use these shared accounts.

Since you have already configured asset Smart Groups for discovering assets, asset Smart Groups for adding systems to Password Safe management, and managed systems Smart Groups for granting system access from previous use cases, you do not need to create any additional Smart Groups for these purposes.

If you need to add additional servers to Password Safe, you can create new Smart Groups using different address groups or directory queries as applicable, and run new scans as applicable, following the steps outlined in previous use cases.

Additionally, if you require only a subset of systems to be allowed to use these directory accounts, you can create a new managed system Smart Group using more specific selection criteria to provide access to a smaller selection of systems.

For this use case, you will create a managed account Smart Group to add the directory accounts to Password Safe and to link the directory accounts to managed systems.

You must also associate the managed account Smart Group with user groups, and then assign roles and permissions to the associated managed account Smart Group.



For more information, please see "[Use Case 2: Add Local Root Accounts for Linux Servers](#)" on page 13.

Create Managed Account Smart Group to Add Directory Accounts to Password Safe and Configure Account Linking

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule Type** filter list.
3. Click **Create Smart Rule**.

4. Select **Managed Accounts** from the **Category** list.
5. Enter a meaningful **Name** and **Description** for the Smart Rule.
6. Set **Selection Criteria** as:

- **Directory Query, Include Accounts from Directory Query, <query name>, Discover Accounts for Password Safe Management: enabled**



Tip: If Password Safe already manages the privileged accounts, you can use criteria of **Managed Account Fields > Account Name** in the Smart Rule instead of using a directory query. For an example of this option, please see ["Use Case 6: Add Directory Admin Accounts for Network Devices" on page 31.](#)

7. Set Actions

- **Link domain accounts to Managed Systems, Asset or Managed System Smart Group: <Smart Group that contains Linux servers that the accounts will be associated to for session management>**
- **Manage Account Settings, Password Rule: <password policy>, Enable Automatic Password Management: no**
- **Show managed account as Smart Group**




Note: The **Manage Account Settings** action onboards the specific account, if found in the system's scan results. This action also dictates whether the account is rotated immediately or not.



Tip: These actions can be separated into multiple managed account Smart Groups with criteria of **Child Smart Rule** or other specific criteria for the linking rule action, if desired.

8. Click **Create Smart Rule**.

Create New Managed Account Based Smart Rule


Details 

Category:




Name: Active



Description:

Reprocessing limit:

Selection Criteria 

Include items that match of the following


- 
- 
- 


Re-run the query every X hours:  


Discover accounts for Password Safe Management

Domain:

[Add another condition](#) [Add a new group](#)

Actions 





Password Rule:

Enable Automatic Password Management:



Change Password Time:

Change Password Frequency:

Default Release Duration:

Maximum Release Duration:


ISA Release Duration:

Max Concurrent Request:  

Account Options:

Change Password on Mismatch

Email release notifications to:

Link domain accounts to Managed Systems: 

Asset or Managed System Smart Group:

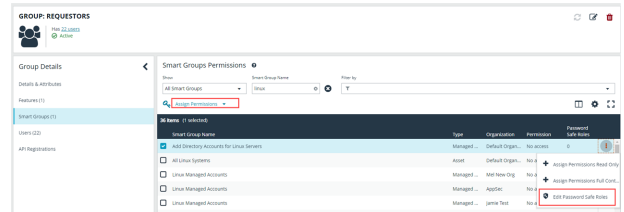
[Add another action](#)

Assign User Group Permissions and Roles for Account Access

Associate a user group with the Smart Group that you created for adding accounts to Password Safe management, and then assign permissions, roles, and an access policy to the Smart Group. In this use case, the Password Safe users are **Requestors** with an access policy to allow auto-approved RDP sessions.

1. From the left navigation in the BeyondInsight console, click **Configuration**.
2. Under **Role Based Access**, click **User Management**.
3. Locate the group in the grid, and then click the vertical ellipsis button for that group.
4. Select **View Group Details**.

5. From the **Group Details** pane, select **Smart Groups**.
6. In the **Smart Groups Permissions** grid, select the Smart Group you created for adding directory accounts for Linux servers to Password Safe, and then click **Assign Permissions** above the grid.
7. Select **Assign Permissions Read Only**.
8. Click the vertical ellipsis button for the Smart Group, and then select **Edit Password Safe Roles**.
9. Select the **Requestor** role, and then select the **Access Policy**.
10. Click **Save Roles**.



Add Directory Accounts For Linux Servers Password Safe Roles ➤

A role is the connection between a Password Safe user account and a managed system. A role defines what the user or group can do with respect to that managed system.

Requestor
Access Policy for Requestor
24x7 - No Approval

Approver

Credentials Manager

Recorded session reviewer

Active session reviewer

SAVE ROLES **DISCARD CHANGES**

Use Case 6: Add Directory Admin Accounts for Network Devices

This use case walks through configuring automatic password rotation for local admin accounts on network devices with auto-approval for RDP sessions enabled.

Directory accounts that have elevated (privileged) access exist within Active Directory. These accounts have permissions to all network devices and need to be controlled, audited, and rotated on a regular schedule. For this use case, Password Safe is already managing network devices by implementing *Use Case 3*, and a specific set of users are allowed to use these shared accounts.

Since you have already configured asset Smart Groups for discovering assets, asset Smart Groups for adding devices to Password Safe management, and managed systems Smart Groups for granting system access from previous use cases, you do not need to create any additional Smart Groups for these purposes.

If you need to add additional devices to Password Safe, you can create new Smart Groups using different address groups and run new scans following the steps outlined in previous use cases.

Additionally, if you require only a subset of systems to be allowed to use these directory accounts, you can create a new managed system Smart Group using more specific selection criteria to provide access to a smaller selection of devices.

For this use case, you will create a managed account Smart Group to link the directory accounts to the managed systems using the **Managed Account Fields > Account Name** criteria.

You must also associate the managed account Smart Group to user groups, and then assign roles and permissions to the associated managed account Smart Group.



For more information, please see "[Use Case 3: Add Local Admin Accounts for Network Devices](#)" on page 19.

Create Managed Account Smart Group to Link Directory Accounts to Managed System

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule Type** filter list.
3. Click **Create Smart Rule**.

4. Select **Managed Accounts** from the **Category** list.
5. Enter a meaningful **Name** and **Description** for the Smart Rule.
6. Set **Selection Criteria** as:

- **Managed Account Fields, Account Name, equals, <name>**

7. Set **Actions**

- **Show managed account as Smart Group**
- **Link domain accounts to Managed Systems, Asset or Managed System Smart Group: <Smart Group that contains network devices that the accounts will be associated to for session management>**



Tip: These actions can be separated into multiple managed account Smart Groups with criteria of **Child Smart Rule** or other specific criteria for the linking rule action, if desired.

8. Click **Create Smart Rule**.

Create New Managed Account Based Smart Rule

Details

Category: Managed Accounts

Name: Linking AD Cisco Accounts Active

Description: Linking AD Cisco Accounts

Reprocessing limit: Default

Selection Criteria

Include items that match ALL of the following

Managed Account Fields

Account Name

equals (=)

levl

Actions

Show managed account as Smart Group

Link domain accounts to Managed Systems

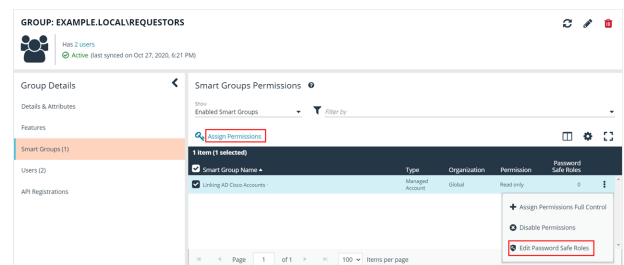
Asset or Managed System Smart Group: Add Cisco Network Devices to All Managed Systems - (Managed System group)

CREATE SMART RULE DISCARD

Assign User Group Permissions and Roles for Account Access

Associate a user group with the Smart Group that you created for adding accounts to Password Safe management, and then assign permissions, roles, and an access policy to the Smart Group. In this use case, the Password Safe users are **Requestors** with an access policy to allow auto-approved RDP sessions.

1. From the left navigation in the BeyondInsight console, click **Configuration**.
2. Under **Role Based Access**, click **User Management**.
3. Locate the user group in the grid, and then click the vertical ellipsis button for that group.
4. Select **View Group Details**.
5. From the **Group Details** pane, select **Smart Groups**.
6. In the **Smart Groups Permissions** grid, select the Smart Group you created for linking AD Cisco accounts to managed systems, and then click **Assign Permissions** above the grid.
7. Select **Assign Permissions Read Only**.
8. Click the vertical ellipsis button for the Smart Group, and then select **Edit Password Safe Roles**.



9. Select the **Requestor** role, and then select the **Access Policy**.
10. Click **Save Roles**.

Linking AD Cisco Accounts Password Safe Roles

A role is the connection between a Password Safe user account and a managed system. A role defines what the user or group can do with respect to that managed system.

Requestor
Access Policy for Requestor
24x7 - No Approval 

Approver

Credentials Manager

Recorded session reviewer

Active session reviewer

SAVE ROLES

DISCARD CHANGES

Use Case 7: Add Dedicated Directory Accounts for Windows Servers

This use case walks through configuring automatic password rotation for dedicated directory accounts on Windows servers.

Individual administrative accounts that exist within Active Directory have permissions to all domain joined Windows servers and should be controlled, audited, and rotated on a regular schedule. For this use case, Password Safe is already managing all Windows domain joined servers by implementing Use Case 1. You have a specific set of user accounts which have a corresponding privileged account within Active Directory that needs to be accessible via Password Safe, but still restricted to only being used by that individual. This is considered to be a dedicated account in Password Safe.

If, in previous use cases, you already implemented asset Smart Groups for discovering assets and adding systems to Password Safe management, as well as managed systems Smart Groups for granting system access to user groups, you do not need to create any additional Smart Groups for these purposes. However, if you want to discover specific domain controllers, you can create a new Smart Group for that purpose. It is the same concept as documented in *Use Case 1*, except you need to create a directory query to pull in domain controllers instead of the Windows OU.

If you need to add additional servers to Password Safe, you can create new Smart Groups, using different address groups and directory queries as applicable, and run new scans as applicable, following the steps outlined in previous use cases.

Additionally, if you require only a subset of systems to be allowed to use these directory accounts, you can create a new managed system Smart Group using more specific selection criteria to provide access to a smaller selection of systems.

For this use case, you must create two managed account Smart Groups. The first will be the managed account Smart Group for adding accounts to Password Safe management and to link accounts to managed systems. The second Smart Group maps dedicated accounts to users.



For more information, please see "[Use Case 1: Add Local Admin Accounts for Windows Servers](#)" on page 7.

Create Managed Account Smart Group to Add Dedicated Accounts to Password Safe and Configure Account Linking

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule Type** filter list.
3. Click **Create Smart Rule**.


4. Select **Managed Accounts** from the **Category** list.
5. Enter a meaningful **Name** and **Description** for the Smart Rule.
6. Set **Selection Criteria** as:

- **Directory Query, Include Accounts from Directory Query, <query name>, Discover Accounts for Password Safe Management: enabled**

7. Set **Actions**

- **Link domain accounts to Managed Systems, Asset or Managed System Smart Group: <Smart Group that contains Windows servers that the accounts will be associated to for session management>**
- **Manage Account Settings, Password Rule: <password policy>, Enable Automatic Password Management: no**
- **Show managed account as Smart Group**

Create New Managed Account Based Smart Rule


Details 

Category


Name Active



Description

Reprocessing limit

Selection Criteria 

Include items that match of the following





Re-run the query every X hours  


Discover accounts for Password Safe Management

Domain


[Add another condition](#) [Add a new group](#)

Actions 





Asset or Managed System Smart Group



Password Rule

Enable Automatic Password Management



Change Password Time

Change Password Frequency

Default Release Duration

Maximum Release Duration

ISA Release Duration


Max Concurrent Request  


Account Options

Change Password on Mismatch

Email release notifications to

[Add another action](#)

 **Note:** The **Manage Account Settings** action onboards the specific account, if found in the system's scan results. This action also dictates whether the account is rotated immediately or not.

 **Tip:** These actions can be separated into multiple managed account Smart Groups with criteria of **Child Smart Rule** or other specific criteria for the linking rule action, if desired.

8. Click **Create Smart Rule**.

Create Managed Account Smart Group to Map Dedicated Accounts to Password Safe Users


Note: This managed account Smart Group restricts the access to the individual correlating user by filtering the account name with a suffix or prefix, and then mapping the dedicated account to a user group. The user group must exist in BeyondInsight already to complete the rule action for this Smart Group.

IMPORTANT!

The privileged directory account and the unprivileged account you are mapping to must match. You must have a preconfigured naming convention to allow for the match. If the prefix or suffix does not exist, the mapping action in the Smart Rule will not be successful.

1. From the left menu in BeyondInsight, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule Type** filter list.
3. Click **Create Smart Rule**.
4. Select **Managed Accounts** from the **Category** list.
5. Enter a meaningful **Name** and **Description** for the Smart Rule.
6. Set **Selection Criteria** as:
 - **Dedicated Account, Account Name, with Suffix, <applicable suffix>**
7. Set **Actions**
 - **Map Dedicated Accounts to, User Group, <user group name>**
 - **Show managed account as Smart Group**
8. Click **Create Smart Rule**.

Create New Managed Account Based Smart Rule


Details 

Category
Managed Accounts

Name
Map Dedicated Account to User Active

Description
Smart Group for mapping dedicated accounts to users.

Reprocessing limit
Default

Selection Criteria 

Include items that match ALL of the following


Dedicated Account

Account Name

with suffix

da

[Add another condition](#) [Add a new group](#)

Actions 

Map Dedicated Accounts To

User Group Requestors

Show managed account as Smart Group

[Add another action](#)

CREATE SMART RULE **DISCARD**

Assign User Group Permissions and Roles for Account Access

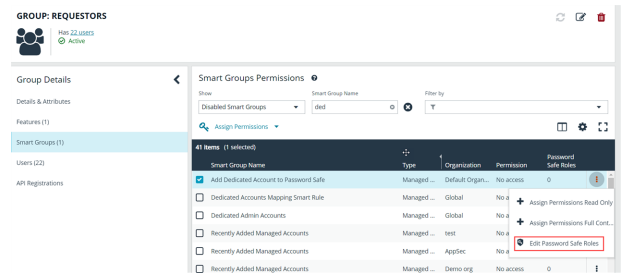
Associate a user group to the Smart Group that you created for adding accounts to Password Safe management, and then assign permissions, roles, and an access policy to the Smart Group. In this use case, the Password Safe users are **Requestors** with an access policy to allow auto-approved RDP sessions.

The user group has a read permission assigned to the Smart Group that was created for mapping the dedicated account. Next you must assign the Password Safe role to it. Even though the entire user group is assigned to the managed account Smart Group because of the dedicated account criteria, only the user with the matching name sees the privileged account within Password Safe.



Note: If there are privileged accounts that do not have a corresponding user to match with, they are treated as shared accounts and seen by all users in that same user group, similar to use cases 1 and 4.

1. From the left navigation in the BeyondInsight console, click **Configuration**.
2. Under **Role Based Access**, click **User Management**.
3. Locate the user group in the grid, and then click the vertical ellipsis button for that group.
4. Select **View Group Details**.
5. From the **Group Details** pane, select **Smart Groups**.
6. In the **Smart Groups Permissions** grid, select the Smart Group you created for adding dedicated accounts to Password Safe, and then click the vertical ellipsis button for that group.
7. Select **Edit Password Safe Roles**.
8. Select the **Requestor** role, and then select the **Access Policy**.
9. Click **Save Roles**.



Add Dedicated Account To Password Safe Password Safe Roles

A role is the connection between a Password Safe user account and a managed system. A role defines what the user or group can do with respect to that managed system.

Requestor

Access Policy for Requestor

all-day every day

Approver

Credentials Manager

Recorded session reviewer

Active session reviewer

SAVE ROLES

DISCARD CHANGES

Use Case 8: Dedicated Directory Accounts for Entra ID

This use case walks through configuring automatic password rotation for dedicated directory accounts for Entra ID.

Individual administrative accounts that exist within Entra ID have permissions to all Entra ID and should be controlled, audited, and rotated on a regular schedule. You have a specific set of user accounts which have a corresponding privileged account within Entra ID that must be accessible via Password Safe, but still restricted to only being used by that individual. This is considered to be a dedicated account in Password Safe.

Previous use cases covered using asset Smart Groups for discovering assets and adding systems to Password Safe management, as well as managed account smart groups for granting access to user groups. To discover and onboard Entra ID accounts, the same concept is documented in Use Case 1, with the exception that you must first create an Entra ID managed system and then use a smart rule to pull in matching accounts from Entra ID.

Additionally, if you require only a subset of users to be allowed to use these directory accounts, you can create a new managed account Smart Group using more specific selection criteria to provide access to a smaller selection of accounts.

Use a dedicated account smart rule to assign a mapping between an Entra ID privileged account and a corresponding Password Safe user to restrict use of that account to that specific user.



For more information, please see the following:

- [Use Case 1: Add Local Admin Accounts for Windows Servers](#)
- [Use Dedicated Account Smart Rule](#)
- [Adding a Managed System Manually](#)

Use an Entra ID Smart Rule

An Entra ID Smart Rule enables Password Safe to automatically discover Entra ID accounts. This allows privileged accounts in Entra ID to be managed, including password rotation and check-in and check-out. RDP sessions, from an Azure-joined VM, can use Entra ID credentials to connect to an Azure-joined VM.

Follow the steps below to discover Entra ID accounts.

1. From the left menu, click **Smart Rules**.
2. Select **Managed Account** from the **Smart Rule type filter** dropdown.
3. Click **+ Create Smart Rule**.

4. Configure the rule as follows:
 - **Category:** Select **Managed Accounts**.
 - **Name:** Provide a meaningful name and description that allows for easy identification of the Smart Rule.
 - **Reprocessing Limit:** If desired, select a reprocessing limit.
 - Under **Selection Criteria:**
 - Select **Azure Directory Query** from the dropdown. There are several filters, and options are dynamic, depending on other selections:
 - Include **ALL** or **ANY** of the selection criteria.
 - There are two matching options available for discovering Entra ID accounts: **Group Name** and **User Principle Name**. Use a **Group Name** match to discover all accounts that are a member of the specified group. Use a **User Principle Name** match to allow a partial name match.
 - If using a **Group Name**, **equals** is the only match option. Enter the **Group Name**.
 - If using a **User Principle Name**, select **starts with** or **ends with** and enter the name.
 - Set the value for how many hours for rerunning the query.
 - Check the **Discover accounts in Azure synced from on-premise** option to include Entra ID accounts synced from on-premises Entra ID, as well as Azure-only accounts.
 - Leave **Discover accounts for Password Safe Management** checked.
 - Select an Azure domain from the dropdown.
 - Add additional selection criteria and groups, as required.
5. Under **Actions**, select **Show managed account as Smart Group**, and then add other actions as required to manage settings or work with the managed account.
6. Click **Create Smart Rule**.

Create New Managed Account Based Smart Rule

Details ▾

Category: Managed Accounts ▾

Name: AAD Accounts Active

Description:

Reprocessing limit: Default ▾

Selection Criteria ▾

Include items that match ALL ▾ of the following

Azure Directory Query ▾

Group Name: ▾

Match: equals (=) ▾

ADQ Group:

Re-run the query every X hours: 0

Discover accounts in Azure synced from on-premise

Discover accounts for Password Safe Management

Domain: example.com ▾

[Add another condition](#) [Add a new group](#)

Actions ▾

Show managed account as Smart Group ▾

Manage Account Settings ▾

Password Rule: Default Password Policy ▾

Enable Automatic Password Management: yes ▾

Change Password Time: 23 ▾ 30 ▾

Change Password Frequency: Every 30 Days

Default Release Duration: Days: 0 Hours: 2 Minutes: 0

Maximum Release Duration: Days: 0 Hours: 2 Minutes: 0

ISA Default Release Duration: Days: 0 Hours: 2 Minutes: 0

Max Concurrent Request: 1

Account Options: Change Password after Release, Check Password ▾

Change Password on Mismatch

Email release notifications to: bob@example.com

[Add another action](#)

Create Smart Rule View Results Discard



Tip: To view the contents of a new or edited Smart Rule, once it has been saved, click **View Results**. You are taken to the associated grid, where the contents of the Smart Rule are listed. If the Smart Rule is actively processing when **View Results** is clicked, a banner displays letting you know it is still processing.



Note: The **View Results** button displays only if you have permissions to the grid corresponding to the Smart Rule, i.e. Assets, Managed Accounts, Managed Systems. Also, the Smart Rule must be saved with **Show <entity> as Smart Group** selected under **Actions** to view the results.

The Smart Rule must process to display the contents in the grid; therefore, we recommend viewing the results of a Smart Rule before adding additional actions that may make changes to accounts and assets in your network. Once you have viewed the results of the Smart Rule using only the **Show <entity> as Smart Group** action and you have confirmed it contains your desired items, you can add additional actions to the Smart Rule.

Use Case 9: Define Just in Time Access Policies

This use case walks through defining Just in Time Access Policies to include defining the time frame and frequency that users can request passwords, remote access sessions, or access applications within Password Safe management.

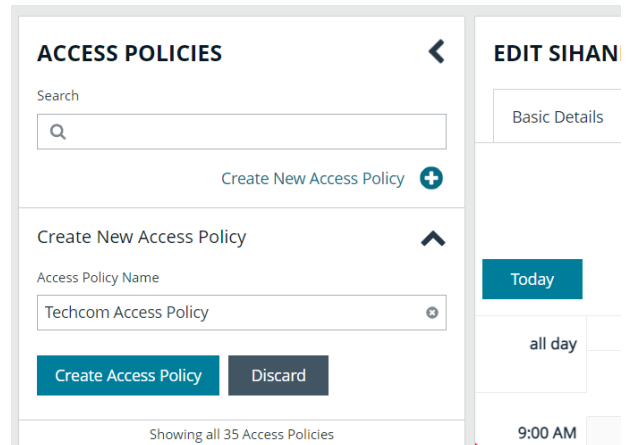
Configure Password Safe Access Policies

An access policy defines the time frame and frequency that users can request passwords, remote access sessions, or access applications under Password Safe management.

An access policy is selected when you are configuring the **Requester** role.

Create an Access Policy

1. Go to **Configuration > Privileged Access Management Policies > Access Policies**.
2. In the **Access Policies** pane, click **Create New Access Policy**.
3. Enter a name for the policy, and then click **Create Access Policy**.



4. On the **Basic Details** tab:
 - Enter a description for the policy.
 - Optionally, enable the **Email Notifications** option to send emails when a request is received for the policy.



Note: Recipients may receive a large number of email notifications. Selective use of this option is strongly advised. Multiple addresses cannot be added at once. Each email address must be added one at a time by clicking **Add Another Email**.

5. Select the **Schedule** tab, and then click **Create Schedule**.
6. Configure the recurrence, time, and date settings for the policy. If you select a daily recurrence, you can optionally select **Allow multi-day check-outs of accounts**. This option allows the user continuous access to a granted request over a span of days.
7. Optionally, enable the **Enable Location Restrictions** option, and then select a location from the list.
8. If applicable, select an address from the **X-Forwarded-For** list. This field is an allowed value of **X-Forwarded-For header**, which was added by an F5 load balancer or proxy. It uses address groups to verify if the IP address is to be in that list. The URL and named host will be ignored. If the **X-Forwarded-For** field has a value of **Any**, then no X-Forwarded-For header is required or verified. In the case where it is configured, the X-Forwarded-For header is required and its value should be in the list of IPs in the address group.



Note: In the case of a new configuration, this error message can be found in the log:

```
CheckLocationAllowed: XForwardedForHeaderValue 1.1.1.1 is not registered/trusted. Add this XForwardedForHeaderValue to the TestGroupName Address group
```

9. Select the type of access to permit: **View Password**, **RDP**, **SSH**, or **Application**.
10. For each type of access selected, configure the parameters as required. Descriptions for each parameter are as follows:

Approvers	Select the number of approvers required to permit access. Check Auto Approve if the requests do not require any approvers.
Allow API Rotation Override	Check this option for View Password access, to allow API callers such as Password Safe Cache to override the Change Password After Any Release managed account setting for view-type requests.
Record	Check the box to record the session.
Keystroke Logging	Keystrokes can be logged during RDP, SSH, and application sessions. Uncheck the boxes for each policy type to disable keystroke logging for that type.
Enhanced Session Auditing	Enhanced session auditing applies to RDP and application sessions and is on by default. Click the toggle to turn off enhanced session auditing.
Concurrent	Set the number of sessions permitted at a time. Check Unlimited to permit the user any number of connections to occur at the same time.
Log off on Disconnect	Check this box to automatically log off the user when the connection to the session disconnects or the session window closes. This option applies only to RDP and RDP application sessions, and is active only when Enhanced Session Auditing is enabled. <div data-bbox="836 1318 885 1375" data-label="Image"> </div> <div data-bbox="901 1329 1487 1421" data-label="Text"> <p>Note: If the session has been terminated by an Active Sessions reviewer, the logoff on disconnect occurs regardless of the access policy setting.</p> </div>
Force Termination	Check this box to close the session when the time period expires. When Log off on Disconnect is also selected, the user is logged off the session. This check box applies to RDP, SSH, and application sessions. When the Requested Duration (as entered by the user on the Requests page in the web portal) is exceeded, the session ends if the Force Termination box is checked for the access policy. The default and maximum release durations are configured on the Managed Accounts page and Managed System Settings page.

RDP Admin Console	<p>Select this option to show the RDP Admin Console check box on RDP-based requests. This option allows administration of a Remote Desktop Session host server in console mode (mstsc /admin). This can be useful if the number of remote sessions is maxed out on the host.</p> <p>Using the RDP Admin Console allows you to use a remote session without requiring other sessions to disconnect. Running a remote session using the RDP Admin Console disables certain services and functionality, such as, but not limited to:</p> <ul style="list-style-type: none"> • Remote Desktop Services client access licensing • Time zone redirection • Remote Desktop Connection Broker redirection • Remote Desktop Easy Print
Connection Profile	<p>Select a profile from the list or click Manage Connection Profiles to be taken to the Connection Profiles page to create a new profile.</p>

11. Under **Policy Options**:

- If you want users to provide a reason when making requests in Password Safe, click the toggle for the **Reason is required for new requests** option to enable it.
- If you want users to provide a ticket number for a ticketing system when making requests in Password Safe, click the toggle for the **Require a ticket system and a ticket number for requests** option to enable it.
 - Once enabled, select the **Ticket System** from the dropdown. If you leave the **Ticket System** as **User Selected**, the user can select any ticket system from the list when making their request. If you select a specific ticket system for this option, the user is unable to change the ticket system when making their request.

12. Click **Create Schedule**. If the access policy is not yet marked as available, you are prompted to activate it now.

13. Assign the access policy to a user group as follows:

- Select the **Assignees** tab.
- Click **Manage Assignees**. You are taken to the **User Management** page.
- Click the vertical ellipsis for a group, and then select **View Group Details**.
- From the **Group Details** pane, click **Smart Groups**.
- Click the vertical ellipsis for a managed account Smart Group, and then select **Edit Password Safe Roles**.
- Check **Requestor**, and then select the access policy you just created from the dropdown.
- Click **Save Roles**.

14. Confirm the group is now listed as an assignee on the **Assignees** tab for the access policy you just created.