# BeyondTrust

### Password Safe 21.3 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
Use Case 1: Add Local Admin Accounts for Windows Servers	. 6
Use Case 2: Add Local Root Accounts for Linux Servers	10
Use Case 3: Add Local Admin Accounts for Network Devices	. 14
Use Case 4: Add Directory Admin Accounts for Windows Servers	.19
Use Case 5: Add Directory Admin Accounts for Linux Servers	.21
Use Case 6: Add Directory Admin Accounts for Network Devices	.23
Use Case 7: Add Dedicated Directory Accounts for Windows Servers	.25

2

### **Password Safe Getting Started Guide**

This document is designed to help you with understanding 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.

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.
- 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.
- 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

#### **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 on creating credentials, Smart Rules, functional accounts, address groups, access policies, directory credentials, and directory queries, please see the following:* 
  - "Add Credentials for Use in Scans, Use Smart Rules to Organize Assets, Create and Edit Directory Credentials, Create a Directory Query" in the <u>BeyondInsight User Guide</u> at <u>https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm</u>
  - "Work with Smart Rules, Create a Functional Account, Create an Address Group, Configure Access Policies" in the
     <u>Password Safe Admin Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/index.htm</u>

#### 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 the BeyondInsight Console, 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

Create New Asset Based Smart Rule	:
Details 🗄	
ingoy Servers •	
Gene Active (yes)	
becroson Discover Windows Servers	
Aerotoming line. Default v O	
bedude teems that match. ALL — of the following Directory Query — include assers from query — Windows Servers QU — Re-run the query every X hours  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	ns C
Actions E	
now asset as siniart Group 👻 Wew assets in a standard asset grid 👻	
Add another action	

6. Click Create Smart Rule.

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 **More Options** (ellipsis) menu for the Smart Group on the **Smart Rules** page in BeyondInsight. You can also schedule a recurring scan to pull in 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 <u>BeyondInsight User Guide</u> at <u>https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/discovery.htm</u>.

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

- 1. From the left menu in the BeyondInsight Console, 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.

- 4. 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>
- 5. Click Create Smart Rule.



7

<sup>©2003-2021</sup> BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 11/30/2021 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.



**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 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 the BeyondInsight Console, 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.

Details 🖯		
Category Managed Systems	•	
<sub>Name</sub> Add Windows Servers to A	Il Managed Systems Active (yes)	
Description Smart Group to Add Wind	ows Servers to All Managed Systems Smart Group for delegating ass	et level permissions to user groups
Reprocessing limit Default	- 0	
Selection Criteria 🖯		
Include Items that match	ALL  v of the following	
Include Items that match	n <u>ALL</u> ▼ of the following Idows ▼	
Include Items that match	ALL  of the following idows Control Co	
Include Items that match <u>Platforms</u> <u>Wir</u> <u>Add another condition</u> Actions	n ALL  of the following idows	
Include Items that match <u>Platforms</u> <u>Wir</u> <u>Add another condition</u> Actions Show managed system as	n ALL  of the following idows  Control  Add a new group  Smart Group  Control  Contro  Control  Control  Control  Control  Control  Control  Contro	

#### 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 the BeyondInsight Console, 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
- With the second seco
- 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 Windows servers to Password Safe, and then click **Assign Permissions** above the grid.
- 7. Select Assign Permissions Read Only.
- 8. Click the **More Options** (ellipsis) button for the Smart Group, and then select **Edit Password Safe Roles**.

GROUP: EXAMPLE.LOCAL	\REQUESTORS				ς,	1	Û
Has 2 users Q Active (last synced)	on Oct 27, 2020, 6:21 PM)						
Group Details	Smart Groups Permissions						
Details & Attributes	Show Enabled Smart Groups - T Riter by						
Features	A Arrian Demokrister					~	,
Smart Groups (1)	1 item (1 selected)						Ì
Users (2)	Smart Group Name +		Organization	Permission	Password Safe Roles		
API Registrations	Add Local Admin Account to Password Safe	Managed Account	Global	Read only	0		1
				+ Assign	Permissions Full	Conto	rol
				O Disable	Permissions		
				😨 Edit Pa	ssword Safe Role	s	
	H 4 Page 1 of 1 H 10	0 👻 Items per page				-	

q



>

- 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 the BeyondInsight Console, click Smart Rules.

# BeyondTrust

- 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 (yes)
Description Discover Linux Servers
Reprocessing limit Default
Selection Criteria 🖯
Include Items that match ALL  v 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 **More Options** (ellipsis) menu for the Smart Group on the **Smart Rules** page in BeyondInsight. You can also schedule a recurring scan to pull in 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 <u>BeyondInsight User Guide</u> 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 the BeyondInsight Console, 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.

- 4. 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>
- 5. 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 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 the BeyondInsight Console, click Smart Rules.
- 2. Select Managed System from the Smart Rule Type filter list.
- 3. Click Create Smart Rule.

SALES: www.beyondtrust.com/contact	SUPPORT: www.beyondtrust.com/support	DOCUMENTATION: www.beyondtrust.com/docs
------------------------------------	--------------------------------------	---

betails @	
Caregory Servers	•
Nome Add Linux Servers to Password Safe	Active (yes)
Description Smart Group to Add Linux Servers to Pass	word Safe
Reprocessing limit Default	- Ð
Selection Criteria 😑	
Include Items that match ALL T of th	e following
Operating System   contains	e following
Include Items that match ALL • of th	e following Limit to most recent OS descrited
Include Items that match ALL  or of th Operating System  or contains  Add another condition Add a new g	e following
Include Items that match ALL   of th  Operating System  contains  Add another condition  Add a new g  Artions	e fallowing  limu limit to most recent OS detected
Include Items that match ALL  of th Operating System Contains Add another condition Add a new g Actions O Show asset as Smart Grown View asset	e following  insut insut insut insut to most recent 05 detected  and and and and and and and and and a
Include Items that match ALL • of th <u>Operating System</u> • <u>contains</u> • <u>Add another condition</u> <u>Add a new g</u> Actions Show asset as Smart Group • View ass	e following           insur         Imme to most recent 00 detected         Imme           ets in a standard asset grid         Imme
Include Items that match ALL • of th Operating System • contains • Add another continue Add another continue Add a new p Actions © Show asset as Smart Group. • View ass Manage Assets using Password Safe. •	e fotowng
Include Items that match ALL • of th Operating System • contains • Add another condition Add a new g Actions © Show asset as Smart Group • View ass Manage Assets using Password Safe • Add another action	e following           Imax         Imax

- 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
- Set Actions as:
  - Show managed system as Smart Group
- 8. Click Create Smart Rule.

Details 🖯
Caregory Managed Systems
Name Add Linux Servers to All Managed Systems Sm Active (yes)
Description Smart Rule to Add Linux Servers to All Managed Systems Smart Group for delegating asset level permissions to user groups.
Reprocessing limit Default 0
Selection Criteria 🖯
Include Items that match ALL 💌 of the following
Platforms 👻 Linux 👻 🔇
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 root account. After researching and reviewing reports, additional privileged account names may be added to this Smart Group.

- 1. From the left menu in the BeyondInsight Console, 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 Actionsas:
  - · Show managed account as Smart Group



13

Manage Account Settings, Password Rule: 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.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

#### 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 **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 Linux servers to Password Safe, and then click Assign Permissions above the grid.
- 7. Select Assign Permissions Read Only.
- 8. Click the More Options (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.

GROUP: EXAMPLE.LOCAL	REQUESTORS				C	ø	ť
Has 2 users Active (last synced of	in Oct 27, 2020, 6:21 PM)						
Group Details	Smart Groups Permissions						
Details & Attributes	Enabled Smart Groups - T Allo	r by					
Features	Assign Permissions					¢	5
Smart Groups (1)	1 item (1 selected)						
Users (2)	Smart Group Name +		Organization	Permission	Password Safe Roles		
API Registrations	Add Root Account to Password Safe	Managed Account	Global	Read only	0		1
				+ Assign	Permissions Ful	Cont	rol
				O Disable	Permissions		
				C Edit Par	ssword Safe Rol	es	
	H H Page 1 of 1 H H	100 V Items per page		<u> </u>		_	

#### > 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
Approver
Credentials Manager
Recorded session reviewer
Active session reviewer
SAVE ROLES DISCARD CHANGES

14

#### 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.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

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 the BeyondInsight Console, 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 🖯
Cenagory Assets and Devices
Name Discover Cisco Network Devices Active (yes)
Description Discover Clsco Network Devices
Reprocessing limi Default 🗸 🖉
Selection Criteria 🖯
Include items that match <u>ALL</u> • of the following
Address Group  Clisco 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

15

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 **More Options** (ellipsis) menu for the Smart Group on the **Smart Rules** page in BeyondInsight. You can also schedule a recurring scan to pull in 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.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

# BeyondTrust

For more information on configuring a Discovery Scan, please see Run Discovery Scans in the <u>BeyondInsight User Guide</u> 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 the BeyondInsight Console, 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.

- 4. 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>

Create New Asset Based Smart Rule
Details 🖯
Congry Assets and Devices
Name Add Cisco Network Devices to Password Safe
Desirision Smart Group to Add Clico Network Devices to Password Safe
husanun (int Defaut – 0
Selection Criteria B
Include items that match ALL - of the following
Operating System   cisco  Limit to most recent OS detected
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 Cisco 👻 Account Name Format SAM 💌 Functional Account Cisco-FA 💌 Enable Automatic Password Management yes 💌
Add another action
CREATE SMART RILE DISCARD

5. 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 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 the BeyondInsight Console, 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 Mercard Creater Decad Creat Dula
Create New Managed System Based Smart Rule
Details 🕀
Category Managed Systems 👻
Add Clisco Network Devices to All Managed Sys
Description Smart Group to Add Cisco Network Devices to All Managed Systems Smart Group for delegating asset level permissions to user groups.
Beprocessing limit Default - O
Selection Criteria 😑
Include Items that match ALL  of the following
Platforms • Clisco • O
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 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 the BeyondInsight Console, 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 Actionsas:
  - Show managed account as Smart Group

Total     Image: State	Tanga Manga Alaunan	
ange menung menu	A STATE OF	
The Name Market Name of Name And Angle Control of Name And Angle Control of Name Angle Control of Nama Angle C	Attine Uptil Jean Close Antima Account to Patasonid Sele Energine Band Charlo and Close Antimia account from scan details to Patasonid Sele. Improving Joint	
norm mangen må mangen må mangen må mangen må som forman blut, etter bluren bluren bluren versken versken som	neurono multi droup to add Claso Admin account from scan defails to Password Safe.	
	arrossing int	
ear of the set leaders of the set the channel defined in a set of the following the set of the se		
ector Chrise B count term that much Mg, of the following Data term that much Mg, of the following Christian State Sta	1000 · · ·	
lecter Carter B B Contrarter B Auto- of the Manager Decent associated as a second balance associated by a second associated by Managereene <u>Mark</u> B baserer associate from <u>Add Constrained Decent to the</u> Add constrained by Associated by Associated by Associated by Associated by Managereene <u>Mark</u> B baserer associate from <u>Add Constrained Decent to the</u> definition <u>Add Constrained B</u> baserer associated by Associated by Associated B baserer asso		
cola ben ha na k <u>ui -</u> of ta blaneg <u>Bar A mond Alaba + Kuint ben + Kuint ben + Kuint ben + Alaba - Barret annum lo framovi Sub Mangement <u>an +</u> Danner annum hon <u>Alaba Barret hann ben had Constituted Societ hole</u> denotes annung al annung - Romovi han <u>Denot hannon ben had constituted Societ hannon framovi Sub Mangement <u>an +</u> Danner annum hon <u>Alaba Constituted Societ hannon</u> mengad annung - Romovi han <u>Denot hannon ben had hannon ben had constituted Societ hannon framewich hannon framewich</u></u></u>	election Criteria 🖯	
land kan ber Annal Aug - after blange land kan ber Annal Aug - after blange Antanation - Annal - Annal - Annal - Annal - Annal - Annal - Disson assums for hasserd ble blangement - yes - Disson assums for hasserd blangement - yes - Disson assume for hasserd blangement - yes - Disson assume for		
<u>bar Almond Merken 4. Annoch Merken 4. Annoch Merken 4. Annoch 1995</u> <u>Almond Merken Merken 1995</u> <u>Almond Mer</u>	include Items that match ALL   of the following	
All norther mandage All norther mandage tensor is then of the <u>obsection of the power is the tensor of the power is the power is the <u>power is the power is the</u></u>	They become Allebola as a become Manual as another by a second seco	al una 🐱 Discourse accounts from Add Cisco Mathematic Devices to Resource
editarde coltes Mil en page terre B an mangel actues a tear torag • <b>O</b> age <u>konset times</u> • Passed his <u>detartassed his</u> • bale kasmet fassed hisogenet <u>ys</u> • Cange Passed Time <u>3</u> • <u>8</u> • Cange Passed hep-org Eany? Lander actue	DREACOULATIONS · ACCOLLARING ·	
oddorskreadening - Mala van group Smr B wige Associationg • Teasoof Nair - Educit Associativity • Environ Associationegement <u>ym</u> • Owege trassociative <u>33 • 33 • 00 •</u> Owege trassociative genery Landra enam		
tern 8 an mangel actuat a Sear Orașe • O age Accurd State • Praved Nar <u>Orașe Praved Nar</u> <u>Orașe Praved Prave</u>	Add another condition Add a new group	
ten til S menged standet stittet forsa - O Segularizationer i Standet forsa - Objektesserf Margarinet jest - Objektesserf fore 31 + 31 + 00 + Congritesserf frequency Entry Lander ander		
narodnja daniča i stari Osno - <b>O</b> n <u>ago kazarti straje -</u> Prasod Nar <u>Ong Prasod Prioj -</u> balito kazardičkasod Narogenec <u>jes -</u> Ovep Prasod Tine <u>23 - 15 -</u> Ovep Prasod Prejecc (kny) Linema nazo	kctions 🕅	
en mangad konsert Smith Smit	-	
nge <u>konst bling</u> • Passer Mai <u>Sebut Passer Phily</u> • Gale kanner, Passer Hangeren <u>jer.</u> • Gage Passer Tim <u>2</u> • <u>10</u> • Gage Passer Philip Dage (ber) Liveline and	how managed account as Smart Group 👻 🔯	
ugestuurisettiin – rasiona nie leeuviseuvis nieg – boorkuuniuriseuvis niegeneu <u>75 –</u> Goografisiona nie <u>7 – 51 –</u> Goografisiona niegeneu Leeder aster	terre terre failure a former bet finde dimensional data a finde terre at former because the second dimensional and a financial	and Terry All and A
1 another action	vange Account seconds + Password have beaut rassword howy + Enable Account of Password Hanagement yes + Change Passwo	sto line 23 • 50 • Charge Password Requerty Charge Password Requerty
d another action		
	kdd another action	

17

 Manage Account Settings, Password Rule: cpassword 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 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 Windows servers to Password Safe, and then click Assign Permissions above the grid.
- 7. Select Assign Permissions Read Only.
- 8. Click the More Options (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.

Smart Groups Permissions						
Enabled Smart Groups						
Assign Permissions					٥	5
1 item (1 selected)						
Smart Group Name +		Organization	Permission	Password Safe Roles		
Add Cisco Admin Account to Password Safe	Managed Account	Global	Read only	0		:
			+ Assign	Permissions Fu	il Cont	trol
	<ul> <li>Smart Groups Permissions</li> <li>Pere Pere Pere Pere Pere Peres Pere</li></ul>	<ul> <li>Smart Groups Permissions ●</li> <li><sup>Dive</sup> Mart Source From Source For Martine Formation Mart Networks Proceeded Info Mart Cole Advances Proceeded Info Martine Formation Formation Formation Formation Martine Formation Formation Formation Formation Formation Martine Formation Formation Formation Formation Formation Martine Formation Formation Formation Formation Formation Formation Formation Martine Formation Formation Formation Formation Formation Martine Formation Formation Formation Formation Formation Formation Formation Formation Martine Formation Formation Formation Formation Formation Formation Formation Formation Martine Formation Formation Formation Formation Formation Formation Formation Formation Formation Formation Martine Formation Formati</li></ul>	Smart Groups Permissions ●     Por     P	Smart Groups Permissions         ●           Switt Switt Auguster Pressions         ●         ● Other International Other Interna	<ul> <li>Smart Groups Permissions ●</li> <li>Proceeding Permissions ●</li> <li>August Premissions</li> <li>There by</li> <li>August Premissions</li> <li>There by</li> <li>August Premissions</li> </ul>	<ul> <li>Smart Groups Permissions ●</li> <li><sup>Pore</sup> <sup>Nore</sup> for <sup>Nore</sup> for</li></ul>

#### 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	

DISCARD CHANGES SAVE ROLES

depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

#### 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 autoapproval 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 6.

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

- 1. From the left menu in the BeyondInsight Console, 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 23.

Under generation of the second for the large of the second for the	Describe CD	
"" The end percent for windows for windows for windows for the model of the form of the	Crepty Managed Accounts	
Sector Address         •••           Sector Offers 0         •••           Instant and the match state         •••           Sector Offers 0         •••           Instant and match         •••           Detecting Open +         •••           Output         •••           Detecting Open +         •••           Output         •••           Detecting Open +         ••	Name Add Directory Accounts for Wi	ndows Servers Active (yes)
Notions	Description Add Directory Accounts for Wi	ndows Servers
Selection Criters B which frem that white if the though the chart best family from the charter of the though the chart best family from the charter of th	Reprocessing limit Default	- 0
Access 8 (24 domain accession the biological flynom - Access of biological flynom band Group. Add Biological Sprinner 20 and - One Margine Access of Biological Flynom Scholar Sprinner Scholar Accession (24 Sprinner 2 Markets) Markets Data Domanaged Access of Biological Flynom Scholar Accession (24 Sprinner) Markets Data Markets access of Biological Flynom Scholar Accession (24 Sprinner) Markets Data Markets access of Biological Flynom Scholar Accession (24 Sprinner) Markets Data Markets access of Biological Flynom Scholar Accession (24 Sprinner) Markets Data Markets accession (24 Sprinner) Markets Accession (24 Sprinner) Markets Data Markets accession (24 Sprinner) Markets Accession (24 Sprinner) Market	Selection Criteria 🗟 Include Items that match A Directory Query 👻 1 Add another condition	💵 of the following clube accounts from Directory Query 🔹 Windows Administration 🔹 Revus the query every Thours 🖨 O _
Lis damit automas its Managel fysions. New of Wangel Falms Fand Gause Add Wanders Senie to All Managel System Start Grave - Managel Falms prod.	Actions 🖯	
Manga Accord Refing • Pressed Hule <u>Schall Passed Hule</u> • Stable Accords: Passed Mangement <u>no</u> • Schall Resear Duarton <u>Dept 999073 2 Minutes</u> 0 Manuan Relate Duar Book manged accord as front One, • <b>O</b> <u>Millionitor actor</u> <u>ORX 199007 MAL</u> <u>BOCKED</u>	Link domain accounts to Man	ged Systems 🝷 Asset or Managed System Smart Group 🛛 Add Windows Servers to All Managed Systems Smart Group - (Managed System group) 🝷 🔇
Mon manged scame is from force • O	Manage Account Settings 👻	Password Rule Default Password Policy 💌 Enable Automatic Password Management no 💌 Default Release Duration Days: 0 Hours: 2 Minutes: 0 Maximum Release Durat
Alf works wells	Show managed account as Sn	art Group 💌 🖏
CREATE SMANT RULE DISCARD	Add another action	
		ner can

19

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

- 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 Rules or other specific criteria for the linking rule action, if desired.

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 Windows servers to Password Safe, and then click **Assign Permissions** above the grid.
- 7. Select Assign Permissions Read Only.
- 8. Click the **More Options** (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.

SAVE ROLES DISCARD CHANGES
Active session reviewer
Recorded session reviewer
Credentials Manager
Approver
Access Policy for Requestor 24x7 - No Approval
✓ Requestor

#### 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.

depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

### BeyondTrust

22

For more information, please see "Use Case 2: Add Local Root Accounts for Linux Servers" on page 10.

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

- 1. From the left menu in the BeyondInsight Console, 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 23.

take B by the second by the se		in control of the second s	
The second of th	Details 🖯		
The second secon	Crepry Managed Accounts	•	
Note::::::::::::::::::::::::::::::::::::	Name Add Directory Accounts for Line	Servers Active (ves)	
	Description Add Directory Accounts for Link	Servers	
eketon China B Holde Ears Hand ALL - Of the following Dentry George - Mode Ears Hand Protein Operating George - Line Administrations - Reveal the pays remy 1 hours D = 0 D = D = D = D = D = D = D = D = D	Reprocessing limit Defaulit	. 0	
Include tars that much ALL - of the following Description of the following - include accounts then the terrer pays any strengs 1 hours I	Selection Criteria 🕀		
Techny Qeer y Book accounts from Denetry Qeer y   Technologies y  Technologie	Include items that match ALI	<ul> <li>of the following</li> </ul>	
All and the series of All and prove constrained there an experience of a finant from a finance of the series of	Directory Query • In	Je accounts from Directory Query 💌 Linux Administrators 💌 🛛 Re-run the query every X hours 🗧 🚱 🚺 Discover accounts for Password Sa	fe Managen
actions B Theremanded Second Series 1 Annual Annua	Add another condition	d a new group	
tere mangel scored at load forms 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Actions 🖯		
target Account Series • Research Nais <u>Series of Nais</u> • Exolor Advance: Passeod Naisgeneer <u>on</u> • Debut Nesseo Ductors Days Shares 2 Manuelle Naiseon Naisget Sprins <u>Series Series Serie</u>	Show managed account as Smo	:Group 💌 🔇	
ek acman acameta ta Manged System • Asad ar Manged System Smart Group Add Units Servert to al Manged System Smart Group - Managed System proval • • • • • • • • • • • • • • • • • • •	Manage Account Settings 💌	assword Rule Default Password Policy 💌 Enable Automatic Password Management no 💌 Default Release Duration 🛛 Days: O Hours: 2 Minutes: 0 🛛 Maxim	num Release
darante sate	Link domain accounts to Manaj	d Systems 💌 Asset or Managed System Smart Group - Add Linux Servers to All Managed Systems Smart Group - (Managed System group) 👻 🚳	
CERVIT SWIT BALL ESCOND	Add another action		
CREATE SAMPET SHALE DISCARD			
	CREATE SMART RULE	CARD	

- 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: cpassword 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 Rules or other specific criteria for the linking rule action, if desired.

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.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

>

23

- 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 Windows servers to Password Safe, and then click **Assign Permissions** above the grid.
- 7. Select Assign Permissions Read Only.
- 8. Click the **More Options** (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.

# BeyondTrust

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 14.

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

- 1. From the left menu in the BeyondInsight Console, 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>

incate men managed mecount	Sased Smart Rule			
Details 🖂				
aregory Manazed Accounts	•			
inking AD Cisco Accounts	Active (yes)			
escription Jinking AD Cisco Accounts				
leprocessing limit Default	• 0			
Selection Criteria 😑				
Include items that match ALL - of the	ollowing			
Managed Account Fields 💌 Accou	nt Name 💌 equals (=) 💌 levi	0		
Add another condition Add a new gro	up			
Actions 🖯				
ihow managed account as Smart Group 💌	0			
ink domain accounts to Managed Systems	Asset or Managed System Smart Group	Add Cisco Network Devices to All Manage	ed Systems Smart Group - (Managed	System group) 👻
idd another action				

24

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

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.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

>

25

- 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 Windows servers to Password Safe, and then click **Assign Permissions** above the grid.
- 7. Select Assign Permissions Read Only.
- 8. Click the **More Options** (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 users have a corresponding privileged account within Active Directory that need 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 6.

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

- 1. From the left menu in the BeyondInsight Console, 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 Linux servers that the accounts will be associated to for session management>



26

- 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 Rules or other specific criteria for the linking rule action, if desired.

8. Click Create Smart Rule.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

#### 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 the BeyondInsight Console, 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.

Details ⊟	
ategory Aanaged Accounts 🔹	
ame Map Dedicated Account to User Active (yes)	
escription mart Group for mapping dedicated account to users	
eprocessing limit effault T	
election Criteria 🖯	
Include Items that match ALL  of the following	
Dedicated Account  Account Name  with suffix  da	8
Add another condition Add a new group	
Actions 🖯	
Map Dedicated Accounts To     User Group     E     L\Requestors     C	
how managed account as Smart Group 👻 🔞	
idd another action	

27

#### 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.

# BeyondTrust

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 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 dedicated accounts, and then click the **More Options** (ellipsis) button.
- 7. Select Edit Password Safe Roles.

GROUP: EXAMPLE.LOCAL\REQUESTOR Has 2 users C Active (last synced on Oct 27, 2020, 60)	IS 21 PM0				2,	•
Group Details Details & Attributes	Smart Groups Permissions					
Features Smart Groups (1)	Assign Permissions					) (
Users (2) All Resistrations	Smart Group Name  Map Dedicated Account to User	Type Managed Account	Organization Global	Permission Read only	Password Safe Roles	:
не подрайланията	Assign Permissions full Control     Catable Permissions     Lide Reasond Safe Inter					Control
	H 4 Page 1 of 1 + H 100 - Items pe	r page				-

- 8. Select the Requestor role, and then select the Access Policy.
- 9. Click Save Roles.

#### Map Dedicated Account To User 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.



28

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs