# Password Safe 22.4 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

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.

2

### **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.

Λ

### 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.

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

### **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</u> at <u>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
- 6. Click Create Smart Rule.

Servers: D	iscover Wi	indows Servers	5			
Details 🖯						
Category						
Servers			•			
Name						
Discover Wind	dows Servers		0	Active		
Description						
Discover Wind	dows Servers		0			
Reprocessing limi						
Default			•	0		
Selection Crit	_					
Include Items	s that match	ALL	▼ of the	e following		
Directo	ory Query				•	0
Inc	lude assets fro	om query			•	
Wir	ndows Servers				•	
Def	fault Workgrou	up			•	
Re-r	un the query e	every X hours	0	Đ		
	Use to discov	ver new assets during	g scans			
Add another	r condition Ad	id a new group				
Actions 🖯						
Show asset as	s Smart Group				· (3)	
View asset	ts in a standar	d asset grid			•	
Add another act	tion					
SAVE CHANC	GES DISC	ARD CHANGES				

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 <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 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.

# BeyondTrust

- 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.

Server	rs: Add Windows Servers To Password Safe	
Details		
Category		
Servers	<b>▼</b>	
Name		
Add Win	ndows Servers to Password Safe 🛛 🖉 Active	
Description		
Add Win Function	ndows Servers to Password Safe using AD On al Account	
Reprocessi		
Default	- O	
Selection	n Criteria 😑	
Include	e Items that match ALL	
C	Operating System 🔹	8
	contains •	
	windows	0
	Limit to most recent OS detected	•
	Asset fields 🔹	8
	Domain Name 👻	
and	contains -	
	domain	0
Add ar	nother condition Add a new group	
·		
Actions		
Show as	sset as Smart Group 👻 🔇	
View	v assets in a standard asset grid 🔹	
Manage	e Assets using Password Safe 🔹 😵	
Platfo	Vindows	•
Chang	ge Agent Password Safe	•
Accou	unt Name Format Domain\Username	
Funct	tional Account Windows FA (windows\windows)	
Enabl	le Automatic Password Management yes	
Enabl	le Accounts For AD Queries no	
Passw	word Rule Default Password Policy	•
Conne	aection Timeout 🗖 30 💽	
Add anoth	heraction	
CREATE	E 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.

©2003-2023 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: 3/22/2023 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.

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.

Create New Managed System Based Sm	art Rule
Details 🕀	
Category	
Managed Systems	•
Name	
Add Windows Servers to All Managed Systems Smart Gr	c 🛛 🗹 Active
Description	
Smart Group for adding Windows servers to the All Managed Systems Smart Group.	Ø
Reprocessing limit	
Default	<b>→</b> 0
Selection Criteria 🖯	of the following
Platforms	· 8
Windows	•
Add another condition Add a new group	
Actions 🕀	
Show managed system as Smart Group	- O
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 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
  - 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.

	Account Na	me															
	equals (=)																
												0					
	Administrat											0					
	Discover acc	ounts for Pa	sword 9	iafe Man	ageme	nt	yes										
	Discover acc	ounts from	Add W	Vindows 9	ervers	to P	asswo	rd Safe						•			
	Include disal	oled account	; no												•		
Add a	another conditio	n Add a nev	group														
ctions	A																
	nanaged accou		roup							•	0						
Aanag	e Account Setti	ngs								•	0						
Pass	word Rule D	efault Passv	ord Poli	cy									٠				
Enat	ole Automatic P	assword Ma	lageme	nt yes		•											
Char	nge Password T	ime 23	•	30	•												
Char	nge Password F	requency I	VERY 30	D DAYS													
Defa	ult Release Du	ration DAY	: 0 HOL	IRS: 2 MI	UTES:	0											
Max	imum Release I	Duration D	NYS: 0 H	OURS: 2	MINUT	ES: 0											
ISA P	Release Duratio	n DAYS: 01	IOURS:	2 MINUTI	ES: 0												
Max	Concurrent Re	quest 🗖	1	6	3												
Acco	ount Options	Change Pas	sword a	fter Relea	se. Ch	eck P	asswo	rd					•				
	Change Passw	ord on Mism	atch														
Ema	il release notifi	ations to															
d ano	ther 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 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.

GROUP: EXAMPLE.LOCAL	REQUESTORS					2 ø	Û
Has 2 users Active (last synced of	m Oct 27, 2020, 6:21 P	MQ					
Group Details	<	Smart Groups Permissions					
Details & Attributes		Show Enabled Smart Groups - T Alter by					
Features		Assign Permissions					0
Smart Groups (1)		1 item (1 selected)					
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	:
					+ Assign	Permissions Full Co	ntrol
					O Disable	Permissions	
					C Edit Par	ssword Safe Roles	
		H 4 Page 1 of 1 H 100 V It	ems per page				·

11

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

©2003-2023 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: 3/22/2023 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.



>

- 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

A

Access Policy for Requestor	
24x7 - No Approval	-

Approver

Credentials Manager

Recorded session reviewer

Active session reviewer

SAVE ROLES DISCARD CHANGES

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

©2003-2023 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: 3/22/2023 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 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.
- 2. Click Create Smart Rule.
- 3. Select the Category and enter a meaningful Name and Description for the Smart Rule.

<sup>©2003-2023</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: 3/22 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.



- 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 Ø
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 <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.

- 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.

Category		
Servers	•	
Name		
Add Lin	ux Servers to Password Safe 🛛 💿 🗹 Active	
Descriptio	n	
Add Lin	ux Servers to Password Safe 🔹	
Reprocess	ine limit	
Default	· 0	
Coloctio	n Criteria 🖯	
Include	Items that match ALL   of the following	
0	Operating System 🔹 🔇	
	contains 🗸	
	linux Ø	
	✓ Limit to most recent OS detected	
Add a	nother condition Add a new group	
Actions		
	set as Smart Group	
Show a		
Show as	set as Smart Group  assets in a standard asset grid	
Show as View Manage	set as Smart Group     assets in a standard asset grid	
Show as	set as Smart Group	
Show as View Manage Platfe	set as Smart Group     assets in a standard asset grid	
Show as View Manage Platfe Chan	set as Smart Group  assets in a standard asset grid  Assets using Password Safe  (Dirux	
Show as View Manage Platfi Chan Allow	set as Smart Group	
Show as Viev Manage Platfe Chan Allow Acco	set as Smart Group	
Show as View Manage Platfi Chan Allow Acco Func	set as Smart Group	
Show a Viev Manage Platfi Chan Allow Acco Func Enab	set as Smart Group	·
Show a Viev Manage Platfi Chan Allow Acco Func Enab	set as Smart Group	
Viev Manage Platfi Chan Allow Acco Func Enab	set as Smart Group	
Show a: View Manage Platfi Char Allow Acco Func Enab	set as Smart Group	
Show a: View Manage Platfi Char Allow Acco Func Enab	set as Smart Group	
Show as View Manage Platfi Char Allow Acco Enab Enab Enab Enab Esab	set as Smart Group	
Show ar View Manage Platfi Char Allow Acco Func Enab Enab Passi Eleva Key E	set as Smart Group	
Show as View Manage Platfr Chan Allow Enab Enab Enab Enab Enab Enab Enab Conr	set as Smart Group	

## 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.

- 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
Managed Systems
Name
Add Linux Servers to All Managed Systems Smart Group 🐵 🔽 Active
Description
Add Linux Servers to All Managed Systems Smart Group
Reprocessing limit
Default 🗸 🥑
Selection Criteria  Include Items that match ALL
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
  - 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.

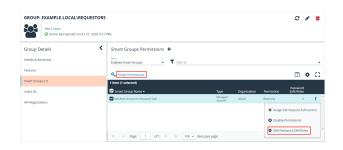
Category Manag	ed Accounts	•				
Name						
Add Lir	nux Root Account to Password Safe	e 🗹 Act	ive			
Descriptio	on					
Add Lir	nux Root Account to Password Safe	•				
Reproces	ising limit					
Default		• 0				
Selectio	on Criteria 😑					
		of the following				
		or the following		•		
	User Account Attribute			- O		
	Account Name			•		
	equals (=)			•		
	root			0		
	Discover accounts for Password Safe Manager	ment yes				
	Discover accounts from Add Linux Servers	to Password Saf	e		•	
	to deale disabilitate constanting					
	Include disabled accounts no				•	
Actions	another condition Add a new scoup			S	•	
Actions Show n	another condition Add a new group		•	8		
Actions Show n Manag	another condition Add a new group 5  managed account as Smart Group e Account Settings			0		
Actions Show n Manag Pass	another condition Add a new groun S  B managed account as Smart Group re Account Settings word Rule Default Password Policy			0	•	
Actions Show n Manag Pass Enat	another condition Add a new prouse is E managed account as Smart Group er Account Settings word Rule Default Password Policy ble Automatic Password Management yes	•		0		
Actions Show n Manag Pass Enat	another condition Add a new groun S  B managed account as Smart Group re Account Settings word Rule Default Password Policy	•		0		
Actions Show n Manag Pass Enat Char	another condition Add a new prouse is E managed account as Smart Group er Account Settings word Rule Default Password Policy ble Automatic Password Management yes	• ]		0		
Actions Show n Manag Pass Enat Char Char	another condition Add a new proun is B managed account as Smart Group et Account Settings word Rule [Default Password Policy] ble Automatic Password Management [yes] nge Password Time [23] • [30] •			0		
Actions Show n Manag Pass Enat Char Char Defa	another condition Add a new groun managed account as Smart Group re Account Settings word Rule Default Password Policy ble Automatic Password Management yes rige Password Time 23 • 30 • nge Password Time 23 • 30 • nge Password Frequency EVERY 30 DAYS built Release Duration DAYS: 0 HOURS: 2 MINUT	] TES: 0		0		
Actions Show n Manag Pass Enat Char Char Defa	another condition Add a new groun another condition Add a new groun anaged account as Smart Group re Account Settings word Rule Default Password Policy bie Automatic Password Policy bie Automatic Password Policy bie Automatic Password Time 23 • 30 • nge Password Time 23 • 30 •	] TES: 0		0		
Actions Show n Manag Pass Enat Char Char Defa Max	another condition Add a new groun managed account as Smart Group re Account Settings word Rule Default Password Policy ble Automatic Password Management yes rige Password Time 23 • 30 • nge Password Time 23 • 30 • nge Password Frequency EVERY 30 DAYS built Release Duration DAYS: 0 HOURS: 2 MINUT	ES: 0		0		
Actions Show n Manag Pass Enat Chai Chai Defa Max	another condition Add a new provid and a set of the second secon	ES: 0		0		
Actions Show n Manag Pass Enat Chan Defa Max	another condition Add a new provid another condition Add a new provid managed account as Smart Group re Account Settings word Rule Default Password Policy bite Automatic Password Management yes nge Password Time 23 • 30 • nge Password Time 23 • 30 • nge Password Frequency EVERY 30 EAYS ault Release Duration DAYS: 0 HOURS: 2 MINUTES Release Duration DAYS: 0 HOURS: 2 MINUTES	TES: 0		0		
Actions Show n Manag Pass Enat Chan Defa Max Acco	Another condition Add a new groun another condition Add a new groun an anaged account as Smart Group re Account Settings aword Rule Default Password Policy ble Automatic Password Management yes nge Password Time 23 • 30 • 10 •	TES: 0		0		
Actions Show n Manag Pass Enat Chas Chas Chas Chas SA R Max Acccc	Another condition Add a new groun managed account as Smart Group re Account Settings word Rule Default Password Policy bie Automatic Password Management yes nge Password Time 23 So Password Time 23 So	TES: 0		0		

#### **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

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

©2003-2023 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 To 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 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 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.

Details 😑	
Category	
Assets and Devices	•
Name	
Discover Cisco Devices	Active
Description	
Discover Cisco Devices	0
Reprocessing limit	
Default	• 0
Selection Criteria 😑	
Include Items that match ALL -	of the following
	of the following
Address Group	· 8
Cisco Network Devices	•
Use to discover new assets during scan	5
Add another condition Add a new group	
Actions 🕀	
Show asset as Smart Group	· 8
View assets in a standard asset grid	•
Add another action	

Create New Asset Based Smart Rule

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

©2003-2023 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: 3/22/2023 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.

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 <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.

- 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.

etails ⊟	
tegory	
Assets and Devices	•
ame	
Add Cisco Network Devices to Password Safe	Active
escription	
Add Cisco Network Devices to Password Safe	0
eprocessing limit	
Default	- O
election Criteria 😑	
Include Items that match	of the following
Operating System	- 0
contains	•
cisco	٥
Limit to most recent OS detected  Add another condition Add a new group	
Add another condition Add a new group	- 0
_	- 0 -
Add another condition Add a new group ctions  Show asset as Smart Group	, ~
Add another condition Add a new proup ctions show asset as Smart Group Wew assets in a standard asset grid	· · · · · · · · · · · · · · · · · · ·
Add another condition Add a new proue ctions	· · ·
Add another scondition Add a new proup ctions	· · ·
Add another condition Add a new proup ctions	v Ø
Add another condition Add a new group ctions    thow asset as Smart Group  Wew assets in a standard asset grid  Wew assets using Password Safe  platform Cisco  Allow Managed System to be an Application Hic Account Name Format	x x
Add another condition Add a new erous ctions	x x
Add another condition Add a new erouse ctions	st Ino
Add another condition Add a new erouse ctions	• • • • • • • • • • • • • • • • • • •
Add another condition Add a new erouse ctions	• • • • • • • • • • • • • • • • • • •
Add another condition Add a new erouse ctions	• • • • • • • • • • • • • • • • • • •

### 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 Managed System	า Based Smart	Rule	
Details 🖂			
Category			
Managed Systems	•		
Name			
Add Cisco Network Devices to All Manag	ged Systems 🛛 🕲	Active	
Description			
Add Cisco Network Devices to All Manag Smart Group	ged Systems 🛛 🕲		
Reprocessing limit			
Default	•	0	
Selection Criteria 😑			
Include Items that match ALL	▼ of the	following	
Platforms			· 8
Cisco			•
Add another condition Add a new grou	<u>p</u>		
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.

# BeyondTrust

- 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
  - 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.

Category									
Manage	ed Accounts		•						
Name				_					
	ico Admin Account to	Password Safe	٥	Active					
Descriptio	co Admin Account to	Descured Cafe	0						
Add Cis	co Admin Account to	Password Sate	0						
Reprocess	sing limit								
Default			•	Θ					
Selectio	on Criteria 😑								
Include	e Items that match	ALL 👻	of the fo	ollowing					
6	User Account Attribu	e				· 0	,		
	Account Name					•			
	equals (=)					•			
	admin					٥			
	Discover accounts	for Password Safe Mana	gement	yes					
I									
	Discover accounts	from Add Cisco Netw	ork Device:	s to Password Safe					
		from Add Cisco Netw	ork Device	s to Password Safe					
	Discover accounts		ork Device	s to Password Safe				•	
Add a		counts no	ork Device	s to Password Safe				•	
	Include disabled a	counts no	ork Device:	s to Password Safe				•	
Actions	Include disabled a another condition Ac	La new group	ork Device:	s to Password Safe				•	
Actions Show n	Include disabled a another condition Ac :	La new group	ork Device:	s to Password Safe	·	8		•	
Actions Show n	Include disabled a another condition Ac	La new group	ork Device:	s to Password Safe		8		•	
Actions Show n Manage	Include disabled a another condition Ac :	no la new group mart Group	ork Device:	s to Password Safe	•	8	Ţ	<b>·</b>	
Actions Show m Manage Pass	Include disabled a another condition Ac : managed account as : e Account Settings	a new group mart Group Password Policy	vrk Device:	s to Password Safe	•	0	Ţ	•	
Actions Show m Manage Pass Enab	Include disabled a another condition Ac another condition Ac	a new group mart Group Password Policy rd Management	•	s to Password Safe	•	0	Ţ	- -	
Actions Show n Manage Pass Enab Char	Include disabled a another condition Ac C Account Settings word Rule Defaul ble Automatic Passwi rige Password Time	I a new group mart Group Password Policy rd Management yes 23 v 30 v	•	s to Password Safe	•	8	¥	- -	
Actions Show n Manage Pass Enab Char	Include disabled a another condition Ac C Account Settings word Rule Defaul ble Automatic Passwi rige Password Time	a new group mart Group Password Policy rd Management	•	s to Password Safe	•	0	¥	•	
Actions Show m Manage Pass Enab Char Char	Include disabled a another condition Ac a another condition Ac a another condition Ac a another condition Ac a Account Settings word Rule Defaul word Rule Defaul another condition Account are Password Time ange Password Freque	I a new group mart Group Password Policy rd Management yes 23 v 30 v	•	s to Password Safe	•	0	·	- -	
Actions Show m Manage Pass Enab Char Char Defa	Include disabled a include condition Ac include disabled a include disabled a include disabled a e Account Settings word Rule Default lek Automatic Passaw rege Password Time inge Password Time uit Release Duration	I a new group       Password Policy       rd Management     yes       23     30       construction	• •		•	0	¥	•	
Actions Show n Manage Pass Enab Char Char Defa Maxi	Include disabled a monther condition Act in thanaged account as: e Account Settings: word Rule: Defaul word Rule: Defaul iele Automatic Passowich Time inge Password Time inge Password Time inge Password Frequi uut Release Duration mum Release Duration	I a new prove mart Group Password Policy rd Management yes 23 v 30 v ncy EVERY 30 DAYS DAYS: 0 HOURS: 2 MIN	· IUTES: 0		•	0	¥	•	
Actions Show m Manage Pass Enat Char Char Defa Maxi ISA R	Include disabled a monther condition Act in thanaged account as: e Account Settings: word Rule: Defaul word Rule: Defaul ine Automatic Passowich Time inge Password Time inge Password Time inge Password Frequi uut Release Duration mum Release Duration	no i a nex group mart Group Password Policy rd Management yes 23 v 30 v 23 v 30 v 23 v 30 v 23 v 30 v 30 v 23 v 30 v 30 v 24 v 25 v 26 v 26 v 27 v 30 v 28 v 30 v 28 v 30 v 30 v 30 v 30 v 30 v 30 v 30 v 30	V V V V V V V V V V V V V V V V V V V		•	0	•	•	
Actions Show m Manage Pass Enat Char Char Defa Maxi ISA R Max	Include disabled a monther condition Act ananaged account as: a Account Settings word Rule Defaul word Rule Defaul word Rule Defaul assword Trequi uit Release Duration imum Release Duration belease Duration D Concurrent Request	no i a nex group mart Group Password Policy rd Management yes 23 v 30 v 23 v 30 v 23 v 30 v 23 v 30 v 30 v 23 v 30 v 30 v 24 v 25 v 26 v 26 v 27 v 30 v 28 v 30 v 28 v 30 v 30 v 30 v 30 v 30 v 30 v 30 v 30	• • • • • • • • • • • • •		•	0	•	•	
Actions Show m Manage Pass Enab Char Char Char Defa Maxi ISA R Max Acco	Include disabled a monther condition Act ananaged account as: a Account Settings word Rule Defaul word Rule Defaul word Rule Defaul assword Trequi uit Release Duration imum Release Duration belease Duration D Concurrent Request	I a nex group mart Group mart Group Password Policy rd Management yes 23 v 30 v roy EVERV 30 DAYS DAYS: 0 HOURS: 2 MINUTE DAYS: 0 HOURS: 2 MINUTE 1 1 1 2 Password after Release	• • • • • • • • • • • • •		•	0		- -	
Actions Show m Manage Pass Enab Char Char Char Defa Maxi ISA R Max	Include disabled an encoder condition of a conditio	no i a nex group mart Group Password Policy rd Management yes 23 v 30 v 10 v EVERY 30 DAYS DAYS: 0 HOURS: 2 MINUTE DAYS: 0 HOURS: 2 MINUTE 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	• • • • • • • • • • • • •		•	0		-	

#### **Assign User Group Permissions and Roles for Account Access**

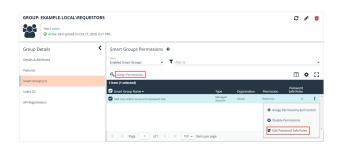
Associate a user group with the Smart Group that you created for adding accounts to Password Safe management, and then assign permissions, roles, and an access policy to the Smart Group. In this use case, the Password Safe users are **Requestors** with an access policy to allow auto-approved RDP sessions.

- 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.

>

# BeyondTrust

- 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

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

©2003-2023 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 T 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 7.

#### 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 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: 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.

Details 🕀
Category
Managed Accounts
Name
Add Directory Accounts for Windows Servers 🔹 🖉 Active
Description
Add Directory Accounts for Windows Servers
Reprocessing limit
Default 👻 🛛
Selection Criteria 😑
Include Items that match ALL
Directory Query 🗸 😵
Include accounts from Directory Query
Created Directory Query Windows Servers
Re-run the query every X hours 📄 0 🖶
Discover accounts for Password Safe Management
Domain example.com 🔹
Add another condition Add a new group
- Actions 🕀
Link domain accounts to Managed Systems
Asset or Managed System Smart Group WIN - (Asset group)
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
Change Password Frequency EVERY 30 DAYS Default Release Duration DAYS: 0 HOURS: 2 MINUTES: 0
Default Release Duration DAYS: 0 HOURS: 2 MINUTES: 0
Default Release Duration DAYS: 0 HOURS: 2 MINUTES: 0 Maximum Release Duration DAYS: 0 HOURS: 2 MINUTES: 0
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
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 1 1
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 <ul> <li>1</li> <li>2</li> <li>Account Options</li> <li>Change Password after Release. Check Password</li> <li> </li></ul>
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 1 1 Account Options Change Password after Release. Check Password Change Password on Mismatch

#### Assign User Group Permissions and Roles for Account Access

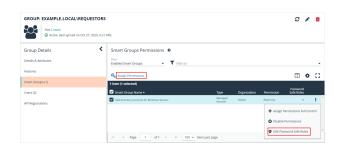
Associate a user group to the Smart Group that you created for adding accounts to Password Safe management, and then assign permissions, roles, and an access policy to the Smart Group. In this use case, the Password Safe users are Requestors with an access policy to allow auto-approved RDP sessions.

- 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.

>

# BeyondTrust

- 5. From the Group Details pane, select Smart Groups.
- 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.

Access Policy for Requestor 24x7 - No Approval	
Approver	

Credentials Manager

Recorded session reviewer

Active session reviewer

SAVE ROLES DISCARD CHANGES

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

©2003-2023 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 T(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 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 the BeyondInsight console, click Smart Rules.
- 2. Select Managed Account 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

- 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 Rules 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	
Add Directory Accounts for Linux Servers 🔹 🖉 Active	
Description	
Add Directory Accounts for Linux Servers	
Reprocessing limit	
Default 🗸 🕡	
Selection Criteria 🕀	
Include Items that match ALL   of the following	
Directory Query	· O
Include accounts from Directory Query	•
Created Directory Query Linux	•
Re-run the query every X hours 🗧 0 🕒	
Discover accounts for Password Safe Management	
Domain example.com	•
Add another condition Add a new group	
1	
Actions 🖯	
Show managed account as Smart Group 👻	0
Manage Account Settings 🔹	0
Password Rule Default Password Policy	•
Enable Automatic Password Management	
Change Password Time 23	
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	
Account Options Change Password after Release, Check Password	•
Change Password on Mismatch	
Email release notifications to	
Link domain accounts to Managed Systems	0
	•
Asset or Managed System Smart Group All Linux Systems - (Asset group)	
Add another action	
CREATE SMART RULE DISCARD	

#### **Assign User Group Permissions and Roles for Account Access**

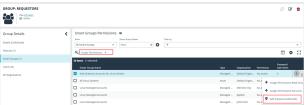
Associate a user group with the Smart Group that you created for adding accounts to Password Safe management, and then assign permissions, roles, and an access policy to the Smart Group. In this use case, the Password Safe users are **Requestors** with an access policy to allow auto-approved RDP sessions.

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

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

©2003-2023 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: 3/22/2023 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.

- 5. From the Group Details pane, select Smart Groups.
- 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

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

©2003-2023 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 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 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 the BeyondInsight console, click Smart Rules.
- 2. Select Managed Account 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

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

8. Click Create Smart Rule.

Category				
Managed Acco	ounts	•		
lame				
Linkning AD Ci	sco Accounts	0	Active	
Description				
Linkning AD Ci	isco Accounts	0		
Reprocessing limit	:		0	
Default		•	U	
Selection Crit	eria 🖂			
Include Items	that match ALL	▼ of the	following	
Manage	ed Account Fields			· O
Aco	ount Name			•
equ	ials (=)			•
levi				G
	condition Add a new group			
Add another				
			•	8
Actions 🖯	d account as Smart Group			
Actions 🖂 Show manage	d account as Smart Group ccounts to Managed Systems		•	8
Actions 😑 Show manage Link domain a		Add Cisco Netw	vork Devices to All Managed Systems	•

#### 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.

GROUP: EXAMPLE.LOCAL	\REQUESTORS						C	<b>A</b>	۵
Has 2 users Active (last synced	on Oct 27, 2020, 6:21 P	M							
Group Details	<	Smart Groups Permissions							
Details & Attributes		Stow Enabled Smart Groups - T	Riber by						
Features		Assign Permissions					ш	0	
Smart Groups (1)		1 item (1 selected)						÷	-
Users (2)		Smart Group Name +			Organization	Permission	Password Safe Role		
API Registrations		Linking AD Cisco Accounts		Managed Account	Global	Read only			1
						+ Assign P	ermissions Fi	ull Con	trol
						O Disable	Permissions		
						C Edit Pas	sword Safe R:	oles	
		H 4 Page 1 of 1 + H	100 v Items per pa	6e		-		_	

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.

32 TC: 3/22/2023



- 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

33

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

©2003-2023 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: 3/22/2023 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 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 the BeyondInsight console, click Smart Rules.
- 2. Select Managed Account from the Smart Rule Type filter list.
- 3. Click Create Smart Rule.

©2003-2023 Beyond Trust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. Beyond Trust is not a chartered bank or trust company, or TC: 3/22/2023 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.

- 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

**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.

Details 🖂	
ategory	
Managed Accounts 👻	
ame	
Add Dedicated Account to Password Safe 🛛 🖉 Active	
escription	
Add Dedicated Account to Password Safe Ø	
sprocessing limit	
Default 🔹 🕜	
election Criteria 🖯	
Include Items that match ALL	
Directory Query	- 8
Include accounts from Directory Query	<b>•</b>
Dedicated Account Directory Query	•
	-
Re-run the query every X hours D	
<ul> <li>Discover accounts for Password Safe Management</li> </ul>	
Domain example.com	•
Add another condition Add a new group	
ctions 🖯	
	0
show managed account as Smart Group 👻	0
show managed account as Smart Group 👻	0
show managed account as Smart Group	00
show managed account as Smart Group	000000000000000000000000000000000000000
show managed account as Smart Group	0 0 0
show managed account as Smart Group  ink domain accounts to Managed Systems  Asset or Managed System Smart Group WIN - (Asset group)  Manage Account Settings  Password Rule Default Password Policy Enable Automatic Password Management yes	0 0 0 0
show managed account as Smart Group	0 0 0 
show managed account as Smart Group  ink domain accounts to Managed Systems  Asset or Managed System Smart Group WIN - (Asset group)  Manage Account Settings  Password Rule Default Password Policy Enable Automatic Password Management yes	0 0 0
Show managed account as Smart Group  Link domain accounts to Managed Systems  Asset or Managed System Smart Group WIN - (Asset group)  Manage Account Settings  Password Rule Default Password Policy Enable Automatic Password Policy Enable Automatic Password Management yes  Change Password Time 23  Ghange Password Frequency EVERY 30 DAYS	0 0 0
Show managed account as Smart Group  Link domain accounts to Managed Systems  Asset or Managed System Smart Group WIN - (Asset group)  Manage Account Settings  Password Rule Default Password Policy Enable Automatic Password Management yes  Change Password Time 23  J0	0 0 0 
Show managed account as Smart Group  Link domain accounts to Managed Systems  Asset or Managed System Smart Group WIN - (Asset group)  Manage Account Settings  Password Rule Default Password Policy Enable Automatic Password Policy Enable Automatic Password Management yes  Change Password Time 23  Ghange Password Frequency EVERY 30 DAYS	0 0 0 0
Show managed account as Smart Group  Link domain accounts to Managed Systems  Asset or Managed System Smart Group WIN - (Asset group)  Manage Account Settings  Password Rule Default Password Policy Enable Automatic Password Management yes  Change Password Time 23  Jo  Change Password Frequency EVERV 30 DAYS Default Release Duration DAYS: 0 HOURS: 2 MINUTES: 0  Maximum Release Duration DAYS: 0 HOURS: 2 MINUTES: 0	0 0 0 
show managed account as Smart Group  ink domain accounts to Managed Systems  Asset or Managed System Smart Group WIN - (Asset group)  Anage Account Settings  Password Rule Default Password Policy Enable Automatic Password Management yes  Change Password Frequency EVERY 30 DAYS Default Release Duration DAYS: 0 HOURS: 2 MINUTES: 0	0 0 0 
show managed account as Smart Group  ink domain accounts to Managed Systems  Asset or Managed System Smart Group WIN - (Asset group)  Anage Account Settings  Password Rule Default Password Policy  Enable Automatic Password Management yes  Change Password Frequency EVERY 30 DAYS  Default Release Duration DAYS: 0 HOURS: 2 MINUTES: 0  Maximum Release Duration DAYS: 0 HOURS: 2 MINUTES: 0	0 0 0 
show managed account as Smart Group   Link domain accounts to Managed Systems   Asset or Managed System Smart Group   WIN - (Asset group)   Manage Account Settings   Password Rule   Default Password Policy   Enable Automatic Password Management   Ves   Change Password Time   23   30   Change Password Time   23   So   Change Password Frequency   EVERY 30 DAYS   Default Release Duration   DAYS: 0 HOURS: 2 MINUTES: 0	0 0 0 
show managed account as Smart Group   ink domain accounts to Managed Systems   Asset or Managed System Smart Group   WIN - (Asset group)   Aanage 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	· · · · · · · · · · · · · · · · · · ·
Link domain accounts to Managed Systems Asset or Managed System Smart Group WIN - (Asset group) Manage Account Settings Password Rule Default Password Policy Enable Automatic Password Policy Enable Automatic Password Policy Change Password Time 23  Grange Password Time 23  Grange Password Frequency EVERY 30 DAYS Default Release Duration DAYS: 0 HOURS: 2 MINUTES: 0 ISA Release Duration DAYS: 0 HOURS: 2 MINUTES: 0 ISA 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	· · · · · · · · · · · · · · · · · · ·

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

©2003-2023 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: 3/22/2023 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.

### 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>
- Set Actions
  - Map Dedicated Accounts to, User Group, <user group name>
  - · Show managed account as Smart Group
- 8. Click Create 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 v of the following	
Dedicated Account 🗸 😵	
Account Name 👻	
with suffix	
da Ø	
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	

Create New Managed Account Based Smart Rule

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.

36

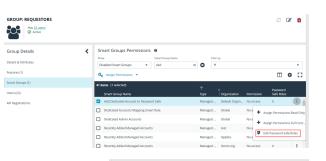
#### **Assign User Group Permissions and Roles for Account Access**

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.

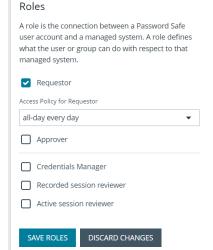
- 1. From the left navigation in the BeyondInsight console, click Configuration.
- 2. Under Role Based Access, click User Management.
- 3. Locate the user group in the grid, and then click the vertical ellipsis button for that group.
- 4. Select View Group Details.
- 5. From the Group Details pane, select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



Add Dedicated Account To

Password Safe Password Safe

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



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

©2003-2023 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: 3/22/2023 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.

>