# Password Safe 24.1 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	
Use Case 5: Add Directory Admin Accounts for Linux Servers	
Use Case 6: Add Directory Admin Accounts for Network Devices	31
Use Case 7: Add Dedicated Directory Accounts for Windows Servers	34
Use Case 8: Dedicated Directory Accounts for Entra ID	38
Use Case 9: Define Just in Time Access Policies	41
Configure Password Safe Access Policies	41

# **Password Safe Getting Started Guide**

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

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

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

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

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

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

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

For more information, please see:

- Add Credentials for Use in Scans in the BeyondInsight User Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm.
- Create a Functional Account in the Password Safe Admin Guide at <a href="https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/index.htm">https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/index.htm</a>.
- <u>Create and Edit Directory Credentials</u> in the <u>BeyondInsight User Guide</u> at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/index.htm.

# **Preparation for Smart Groups**

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

6

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

- Windows servers
- · Windows directory accounts
- · Linux directory accounts

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

- Linux servers
- Network devices

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

#### For more information, please see:

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

## Use Case 1: Add Local Admin Accounts for Windows Servers

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

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

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

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

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

### **Create Asset Based Smart Group to Discover Windows Servers**

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



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

Servers: Discover Windows Servers	
Details 😑	
Category	
Servers	•
Name	
Discover Windows Servers	Active
Description	
Discover Windows Servers	ø
Reprocessing limit	
Default	- O
Solaction Critaria	
Selection Criteria 🖻	
Include Items that match ALL -	of the following
Directory Query	· O
Include assets from query	•
Windows Servers	•
Default Workgroup	•
Re-run the query every X hours	0
Use to discover new assets during scar	15
Add another condition Add a new group	
Actions 🖯	
Show asset as Smart Group	× 8
View assets in a standard asset grid	▼
Add another action	
SAVE CHANGES DISCARD 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 BeyondInsight, click Smart Rules.
- 2. Click Create Smart Rule.
- 3. Select the **Category** and enter a meaningful **Name** and **Description** for the Smart Rule.

- 4. Set Selection Criteria as:
  - · Operating System, contains, windows
  - · Asset fields, Domain Name, contains, domain

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

- 5. Set Actions as:
  - Show asset as Smart Group, View assets in a standard asset grid
  - Manage Assets using Password Safe, Platform: Windows, Account Name Format: Domain\Username, Functional Account: <functional account name>
- 6. Click Create Smart Rule.

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

Server	s: Add Windows Servers To Password Safe	
Details (	Θ	
Category		
Servers	•	
Name		
Add Win	dows Servers to Password Safe 🛛 🛛 🗸 Active	
Description	1	
Add Win Function	dows Servers to Password Safe using AD O	
Reprocessi	ng limit	
Default	- 0	
Selectior	n Criteria 😑	
Include	Items that match ALL • of the following	
0	perating System 🔹	0
	contains	•
	windows	0
	Limit to most recent OS detected	
A	sset fields 🗸 🗸	8
	Domain Name	,
and		
	contains	r
	domain	0
Add an	nother condition Add a new group	
Actions	Θ	
-		
Show as	set as Smart Group 👻 🖏	
View	assets in a standard asset grid 🔹	
Manage	Assets using Password Safe 🔹 😵	
Platfo	rm Windows	•
Chang	ge Agent Password Safe	•
Accou	Int Name Format Domain\Username	
Functi	ional Account Windows FA (windows\windows)	
Enable	e Automatic Password Management yes	
Enabl	e Accounts For AD Queries no	
Passw	vord Rule Default Password Policy	•
Conne	ection Timeout 📮 30 💽	
Add anoth	ier action	
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.

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

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

Create New Managed System Based Smart Rule	
Details 🕀	
Category	
Managed Systems	
Name	
Add Windows Servers to All Managed Systems Smart Grc 🛽 🖌 Active	
Description	
Smart Group for adding Windows servers to the All O Managed Systems Smart Group.	
Reprocessing limit	
Default 🗸 🗸	
Selection Criteria	8
Add another condition Add a new group Actions	
Show managed system as Smart Group	•
Add another action	
CREATE SMART RULE DISCARD	

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

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

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

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

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

8. Click Create Smart Rule.

	Account Name 👻	
	equals (=)	
	Administrator	
L	Vierovar arrounte for Daenword Cafa Mananamant Vies	_
	Judice accounts for a safe management	
L	ISCOVER ACCOUNTS FROM AND VIEWED S TO Password Sale	
I	no •	
Add anot	her condition Add a new group	
tions E	1	
how man	aged account as Smart Group 👻 😵	
Aanage Ad	ccount Settings 🗸 🗴	
Passwor	rd Rule Default Password Policy	
Enable A	Automatic Password Management	
Channel		
Change	Password lime 23 • 30 •	
Change	Password Frequency EVERY 30 DAYS	
Default	Release Duration DAVS: 0 HOURS: 2 MINUTES: 0	
Maximu	m Release Duration DAYS: 0 HOURS: 2 MINUTES: 0	
ISA Rele	ase Duration DAYS: 0 HOURS: 2 MINUTES: 0	
Max Cor	ocurrent Request	
Account	College Channe Darrunged after Delease Chark Darrunged	
Account	Change rassing o and needed Check rassing o	
L) Ch	ange Password on Mismatch	
Email re	lease notifications to	
id another	action	

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

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

- 1. From the left navigation in the BeyondInsight Console, click **Configuration**.
- 2. Under Role Based Access, click User Management.
- 3. Locate the user group in the grid, and then click the 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		C /	Û				
Has 2 users Active (last synced of	m Oct 27, 2020, 6:21 F	540					
Group Details	<	Smart Groups Permissions 🛛 🛛					
Details & Attributes		Show Enabled Smart Groups - T Alter by					
Features		Assign Permissions				П¢	53
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 F	Permissions Full Co	ntrol
					O Disable	Permissions	
					C Edit Pas	isword Safe Roles	
		H 4 Page 1 of 1 ⊨ H 100 v It	erns per page				

11

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



>

12

- 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

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

# **Use Case 2: Add Local Root Accounts for Linux Servers**

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

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

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

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

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

### **Create Asset Based Smart Group to Discover Linux Servers**

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



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

Create New Asset Based Smart Rule
Details 🕀
Category
Servers 👻
Name
Discover Linux Servers 🛛 🖉 Active
Description
Discover Linux Servers Ø
Reprocessing limit
Default 🗸
Selection Criteria 🖯
Include Items that match ALL
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 BeyondInsight, click Smart Rules.
- 2. Click Create Smart Rule.
- 3. Select the Category and enter a meaningful Name and Description for the Smart Rule.



- 4. Set Selection Criteria as:
  - · Operating System, contains, linux

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

- 5. Set Actions as:
  - Show asset as Smart Group, View assets in a standard asset grid
  - Manage Assets using Password Safe, Platform: Linux, Account Name Format: SAM, Functional Account: <functional account name>
- 6. Click Create Smart Rule.

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

category								
Servers		•						
Name								
Add Lin	ux Servers to Password Safe	٥	<ul> <li>Active</li> </ul>					
Descriptio	in							
Add Lin	ux Servers to Password Safe	0						
Reprocess	sing limit							
Default		•	0					
Selectio	on Criteria 🖯							
Include	e Items that match ALL 👻	of the	following					
	Operating System			•	0			
	contains				<b>-</b>			
	IIIIux				0			
	Limit to most recent OS detected							
Add a	upther condition Add a new group							
Actions	Ξ							
/ (0115								
Show a	sset as Smart Group			- 0				
Show a	sset as Smart Group v assets in a standard asset grid			- O				
Show as View	sset as Smart Group v assets in a standard asset grid • Assets using Password Safe			· 0				
Show as View Manage	sset as Smart Group v assets in a standard asset grid e Assets using Password Safe			- 0 - - 0	_			
Show a: Viev Manage Platfe	sset as Smart Group v assets in a standard asset grid * Assets using Password Safe orm Linux			· 0 · 0	¥			
Show a: Viev Manage Platfi Char	sset as Smart Group v assets in a standard asset grid z Assets using Password Safe I Linux ge Agent Password Safe			· 0 ·	•			
Show as View Manage Platfi Chan Allow	sset as Smart Group v assets in a standard asset grid assets using Password Safe Unrux ge Agent Password Safe V Managed System to be an Application Host	no		· 0 ·	•			
Show a: Viev Manage Platfi Chan Allow	sset as Smart Group v assets in a standard asset grid assets using Password Safe Linux ge Agent Password Safe V Managed System to be an Application Host unt Name Format SAM	no		· 0 ·	•	]		
Show a: Viev Manage Platfi Chan Allow Acco	sset as Smart Group v assets in a standard asset grid t assets using Password Safe UInux ge Agent Password Safe V Managed System to be an Application Host unt Name Format SAM tional Account fg_ulmux_test	no		· 8 · .	•	• •		
Show as View Manage Platfi Chan Allow Acco Func Enab	sset as Smart Group v assets in a standard asset grid assets uning Password Safe orm Linux ge Agent Password Safe v Managed System to be an Application Host unt Name Format SAM tional Account fa_linux_test ke Automatic Password Management yes	no		· 0 · 0	•			•
Show as View Manage Platfi Chan Allow Acco Func Enab	sset as Smart Group v assets in a standard asset grid a sasets uning Password Safe orm Linux ge Agent Password Safe Wanaged System to be an Application Host unit Name Format SAM tional Account fa_linux_test lek Automatic Password Management yes lek Login Account for SSH Sessions mo	no		· 0	•	• •		• •
Show a: Viev Manage Platfi Chan Allow Acco Func Enab Enab	sset as Smart Group v assets in a standard asset grid c assets uning Password Safe orm Linux ge Agent Password Safe v Managed System to be an Application Host unt Name Format SAM tional Account for Jinux_test lek Automatic Password Management yes lek Login Account For S5H Sessions Ino lek Accounts For AD Queries Ino	no		· 8 · 8	·	· )	•	• •
Show a: View Manage Platfr Chan Allow Acco Func Enab Enab Passi	sset as Smart Group v assets in a standard asset grid c assets uning Password Safe orm Linux ge Agent Password Safe Managed System to be an Application Host unit Name Format SAM tional Account fa_linux_test lek Automatic Password Management yes lek Login Account for SSH Sessions no lek Accounts For AD Queries no word Rule Default Password Policy	no		· 0	· ·	· )	•	• .
Show a: View Manage Plath Chan Allow Acco Func Enab Enab Enab Enab	sset as Smart Group v assets in a standard asset grid t assets uning Password Safe orm Linux ge Agent Password Safe v Managed System to be an Application Host unt Name Format SAM tional Account fra_linux_test lei Automatic Password Management yess lei Login Account for SSH Sessions no lei Accounts For AD Queries no word Rule Default Password Policy tion None	no		· 0	· · · · · · · · · · · · · · · · · · ·	] • ] • ]	•	• .
Show a: View Manage Plath Chan Allow Acco Func Enab Enab Enab Enab Seleva Key E	sset as Smart Group v assets in a standard asset grid c assets uning Password Safe orm Linux ge Agent Password Safe v Managed System to be an Application Host unt Name Format SAM tional Account Fr6_linux_test le Automatic Password Management Vyes le Login Account For SSH Sessions no le Accounts For AD Queries no word Rule Default Password Policy tion None Enforcement Mode None	no		· 0	• • •	] • • •	×	* *
Show a: View Manage Platfi Chan Allow Func Enab Enab Enab Enab Enab Eseva Key E Conr	sset as Smart Group v assets in a standard asset grid c assets in a standard asset grid c assets using Password Safe orm Linux ge Agent Password Safe v Managed System to be an Application Host unt Name Format SAM tonal Account For_Jinux_test le Automatic Password Management Vess le Login Account For SSH Sessions no le Accounts For AD Queries no word Rule Default Password Policy tolon None Enforcement Mode None ection Timeout 10 30 10	no		· ©	• • •	· · ·	•	•
Show a: View Manage Platfi Chan Allow Acco Func Enab Enab Enab Enab Enab Enab Conr Port	sset as Smart Group v assets in a standard asset grid c Assets uning Password Safe orm Linux ge Agent Password Safe v Managed System to be an Application Host unt Name Format SAM tonal Account For Jinux_test ele Login Account For SSH Sessions no te Accounts For AD Queries no word Rule Default Password Policy tition None enction Timeout 22	no		· ©	•	· · ·	•	• . •

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

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

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

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

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

Create New Managed System Based Smart Rule
Details 🖯
Category
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   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 BeyondInsight, click Smart Rules.
- 2. Select Managed Account from the Smart Rule Type filter list.
- 3. Click Create Smart Rule.

- 4. Select Managed Accounts from the Category list.
- 5. Enter a meaningful Name and Description for the Smart Rule.
- 6. Set Selection Criteria as:
  - User Account Attribute, Account Name, equals, root, Discover Accounts for Password Safe Management: yes, Discover accounts from: <Smart Group for adding Linux servers>
- 7. Set 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	ged Accounts	-					
Name							
Add Li	inux Root Account to Password Safe	0	Active				
Descripti	ion						
Add Li	inux Root Account to Password Safe	0					
Reproces	ssing limit						
Defaul	It	- U					
Selecti	ion Criteria 😑						
Includ	de Items that match ALL 👻	of the follo	wing				
1	User Account Attribute			•	0		
	Assessment Manual						
	Account Name			•	-		
	equals (=)				·		
	root				0		
	Discover accounts for Password Safe Man	agement ye	15				
	Discover accounts from Add Linux Serv	vers to Passwo	rd Safe			•	
	Include disabled asseuts DO						
	Include disabled accounts no						
Add	Include disabled accounts no						
Add.	Include disabled accounts no						
Add Action:	Include disabled accounts no no another condition Add a new group						
Add Action: Show I	Include disabled accounts no no another condition Add a new group s managed account as Smart Group			- 0			
Add Action: Show r Manag	Include disabled accounts no no another condition Add a new stoke s managed account as Smart Group ge Account Settings			- 0 - 0			
Add Action: Show r Manag Pas:	Include disabled accounts no another condition Add a new process S E managed account as Smart Group ge Account Settings award Rule Default Password Policy			- 0 - 0	·		
Add Action: Show r Manag Pas: Ena	Include disabled accounts no another condition Add a new power 6 B managed account as Smart Group ge Account Settings secount Rule Default Password Policy bib Automatic Password Management yes			• 0 • 0	·		
Add Action: Show r Manag Pas: Ena	Include disabled accounts no another condition Add a new proce 5 B are Account Smart Group are Account Strang are Account Settings second Rule Default Resound Policy bible Automatic Resound Management Types			- 0 - 0	•		
Add Action: Show I Manag Pas: Ena Cha	Include disabled accounts no another condition Add a new proce 5 E managed account as Smart Group ge Account Settings sevori Rule Default Password Policy bible Automatic Password Management. [745] mge Password Time [23 ] [30]	· · ·		- 0 - 0	·		
Add Action: Show i Manag Pas: Ena Cha Cha	Include disabled accounts no another condition Add a new proce 5 ge Account Settings sword Rule Default Password Policy bile Automatic Password Management yes manage Password Management yes ange Password Management yes approximation of the setting of the setting of the setting ange Password Frequency EVERY 30 DAYS	· · ·		- 0 - 0	Y		
Add Action: Show n Manag Pass Ena Cha Cha Cha	Include disabled accounts no another coordinos ddd a new prova 5 B managed account as Smart Group ge Account Settings sectorunt Settings word Rule Default Password Policy ble Automatic Password Management (res ringe Password Time (23 • ) 30 mige Password Frequency (FKR V3 DAVS audit Release Duration (DAVS: 0 HOURS: 2 MII	× NUTES: 0		· 0 • 0	×		
Add Action: Show I Manag Pas: Ena Cha Cha Cha Def	Include disabled accounts no another condition Add a new zowa 5 B managed account as Smart Group ge Account Settings aword Rule Default Password Policy bile Automatic Password Management yes inge Password Time 23 3 aug Password Frequency EVERY 30 DAYS ault Release Duration DAYS 0 HOURS 2 Mil aimum Release Duration DAYS 0 HOURS 2 Mil	v NUTES: 0 MINUTES: 0		- 0 - 0	·		
Add Action: Show I Manage Pass Ena Cha Cha Cha Cha Def. Mas ISA	Include disabled accounts no another condition dida a new provid 5 B managed account as Smart Group ar Account Settings account Settings account Gefuilt Password Policy bile Automatic Password Management. [Pes mange Password Time [23] + ] 30 mge Password Time [23] + ] 30 automatic Password Time [23] + ] 30 automatic Password Providers (PURK) 20 AVS automatic Password Public Pu	• • • • • • • • • • • • • • • • • • •		· 0 · 0	·		
Add Action: Show I Manag Ena Cha Cha Cha Def Mao ISA Mao	Include disabled accounts no account a Smart Group ger Account as Smart Group ger Account Statings sound Rule Default Password Policy bite Automatic Password Management yes nger Password Time 23  Quit Release Duration DAYS 0 HOURS 2 MINUT autit Release Duration DAYS 0 HOURS 2 MINUT Accounterst Request  Quit Release Time 21  Quit Release Duration DAYS 0 HOURS 2 MINUT	• • • • • • • • • • • • • • • • • • •		· 0	•		
Add Action: Show in Manage Ena Cha Cha Cha Def Mao ISA Mao Acce	Include disabled accounts no account as smart Group ge Account Settings awordh Rule Default Password Policy bite Automatic Password Management yes inge Password Time 23  30 inge Password Time 23  30 inge Password Time 23  30 inge Password Prequency EVER' 30 DAYS auto Release Duration DAYS 0 HOURS 2 MINUT Accountment Request 1 1 Change Password after Request Change Password after Release 1 Change Password Time Request	V V V V V V V V V V V V V V V V V V V	sword	· 0	•		
Add. Action: Show I Managg Pass Ena Cha Cha Cha Cha Cha ISA May Acco	Include disabled accounts no account as smart Group ge Account Somart Group ge Account Sothings aword Rule Default Password Policy bite Automatic Password Management yes age Password Time 23 • 30 inge Password Prequency EVERY 30 DAYS automatice Devision DAYS: 0 HOURS: 2 Milli automatice Duration DAYS: 0 HOURS: 0 HOURS: 2 Milli automatice Duration DAYS: 0 HOURS: 2 Mil	V V V V V V V V V V V V V V V V V V V	sword	· 0	•		
Add Action: Show Manag Pass Ena Cha Cha Cha Cha Cha ISA May Acce Ena	Include disabled accounts no account as smart Group ge Account Settings awordh Rule Default Password Policy ge Account Settings aword Rule Default Password Policy bite Automatic Password Management yes inge Password Time 23	NUTES: 0 MINUTES: 0 ES: 0 ase. Check Pas	sword	· 0	•		
Add Action: Show in Manag Pass Ena Cha Cha Cha Def Cha ISA Mas Acci Enz Add anc	Include disabled accounts no account as smart Group another condition Add a new zowa s B managed account as Smart Group ge Account Settings aword Rule Default Password Polycy bite Automatic Password Management yes mge Password Time 23 • 30 mge Password Time 23 • 30 mge Password Frequency EVERY 30 DAYS auti Release Duration DAYS 0 HOURS 2 MINU minum Release Duration DAYS 0 HOURS 2 MINU accountrett Request Change Password of Mismatch all release notifications to	NUTES 0 MINUTES 0 MINUTES 0	sword	· 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

18

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

# **Use Case 3: Add Local Admin Accounts for Network Devices**

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

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

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

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

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

### **Create Asset Based Smart Group to Discover Network Devices**

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

Details 🖂		
Category		
Assets and Devices	•	
Name		
Discover Cisco Devices	Active	
Description		
Discover Cisco Devices	0	
Reprocessing limit		
belak		
Include Items that match ALL	of the following	8
Cisco Network Devices		
Use to discover new assets during sca	ans	
Actions 🗆		
Show asset as Smart Group	- 8	
	-	
View assets in a standard asset grid	•	

19

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

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 BeyondInsight, click Smart Rules.
- 2. Click Create Smart Rule.
- 3. Select the Category and enter a meaningful Name and Description for the Smart Rule.

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



- 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						
ssets and Devices	•					
ame						
Add Cisco Network Devices to Passv	vord Safe 🛛 🖗	Active				
escription						
Add Cisco Network Devices to Passv	vord Safe 🛛 🤅					
eprocessing limit						
Default	•	0				
election Criteria 😑						
Include Items that match ALL	▼ of th	e following				
Operating System				- 0		
contains				•		
circo						
Add another condition Add a new.	group					
Add another condition Add a new ctore of the condition of th	group		•	Ø		
Add another condition Add a new.	SLOND SLIG			C		
Chine do Mosk Federat  Add another condition Add a new  ctions  how asset as Smart Group  View assets in a standard asset g  Annage Assets using Password Safe	grid		• •	8		
Chine do most recent	group grid		•	© ©		
Clinic United Cechnic	proup grid		• •	© ©		
Clinic United Recent Add another condition Intervention Int	grid s upplication Host no.		•	© ©		
Clinic United (Edith Add another condition Add another condition Add another condition Add another condition Intervention	grid s Application Host no nUsername		•	© ©	¥	
Control of floor (Cecher)  Add another condition  Account Name Format  Domail  Functional Account  Cosco	grid grid grid grid grid grid grid grid		•	0 0 -	•	
Common Minos (eccent)  Add another condition  Add another condition  Add another condition  (View asset as Smart Group  View asset as Smart Group  View asset as Smart Group  Allow Managed System to be an  Account Name Format  Denall  Functional Account  Cosco  Enable Automatic Password Mann	grid grid host no host		•	© © -	•	•
Count of Max Cechnic	aroup grid		•	0 0 -	•	· · ·
Clinic United (Edition Add another condition Add another condition Add another condition Add another condition Internation In	grid prid pplication Host no NUsername agement yes no dr Policy		•	© © 	•	
Control Minos (exem)  Add another condition	agement yes no		•	© © 	· ·	· · · · · · · · · · · · · · · · · · ·
Connection Timeout Concetion	agement yes		•	© • •	•	· · · · · · · · · · · · · · · · · · ·
Connection Timeout Connection Connection Connection Connection Connection Connection Connection Connection	agement yes on one of the second seco		•	© • •	•	•

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

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

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

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

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

Create New Managed System Based Smart Rule
Details 😑
Category
Managed Systems 👻
Name
Add Cisco Network Devices to All Managed Systems 🛛 🛛 🖌 Active
Description
Add Cisco Network Devices to All Managed Systems Smart Group
Reprocessing limit
Default 👻 🛛
Selection Criteria 🕀
Include items that match ALL
Platforms 👻 😣
Cisco 💌
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 BeyondInsight, click Smart Rules.
- 2. Select Managed Account from the Smart Rule Type filter list.
- 3. Click Create Smart Rule.

- 4. Select Managed Accounts from the Category list.
- 5. Enter a meaningful Name and Description for the Smart Rule.
- 6. Set Selection Criteria as:
  - User Account Attribute, Account Name, equals, <Admin>, Discover Accounts for Password Safe Management: yes, Discover accounts from: <Smart Group for adding network devices>
- 7. Set 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 Cit	sco Admin Account to Pass	word Safe Ø	Active				
Descripti	on						
Add Ci	sco Admin Account to Pass	word Safe Ø					
Reproces	ising limit		1 -				
Defaul	t	•	U				
Selection	on Criteria 😑						
Includ	le Items that match ALL	▼ of th	e following				
ſ	User Account Attribute			•	0		
	Account Name						
					-		
	equals (=)				•		
	admin				٥		
	Discover accounts for Pa	issword Safe Management	yes				
			ines to Dessword Safe			•	
	Discover accounts from	Add Cisco Network Dev					
	Discover accounts from	Add Cisco Network Dev	ices to Fussiona sale				
	Discover accounts from Include disabled accoun	Add Cisco Network Dev	ices to russilon suice			٠	
Add.	Discover accounts from Include disabled accoun	Add Cisco Network Dev				•	
Add.	Discover accounts from Include disabled accoun another condition Add a ne	Add Cisco Network Dev ts no				•	
Add. Actions	Discover accounts from Include disabled accoun another condition Add a ne s	Add Cisco Network Dev				•	
Add. Actions	Discover accounts from Include disabled accoun another condition Add a ne s managed account as Smart	Add Cisco Network Dev ts no w group Group		• 8		•	
Add. Actions Show r Manag	Discover accounts from Include disabled account another condition Add a ne s managed account as Smart re Account Settings	Add Clsco Network Dev ts no w group		- 0		•	
Add. Actions Show r Manag Pass	Discover accounts from Include disabled account another condition Add a ne s managed account as Smart e Account Settings word Rule Default Passa	Add CISCO Network Dev Is no Group Group word Policy		- C - C		•	
Add Actions Show r Manag Pass Enal	Discover accounts from Include disabled account another condition Add a ne s managed account as Smart te Account Settings aword Rule Default Passy bib Automatic Password Mit	Add Lisco Network Dev ts no or group Group word Policy nagement yes		- 0 - 0	×	•	
Add. Actions Show r Manag Pass Enal	Discover accounts from include disabled account another condition Add a ne s managed account as Smart e Account Settings word Rule Default Passy bile Automatic Password Mu	Lad Cisco Network Dev is no erroup Group word Policy magement yes •		- 0 - 0	-	•	
Add. Actions Show r Manag Pass Enal Cha	Discover accounts from include disabled account another condition Add ane 5 managed account as Smart e Account Settings word Rule Default Passo ble Automatic Password Mi nge Password Time 23	Ladi Cisco Network Dev is no Group vord Policy nagement yes v 30 v		· 0	×	•	
Add. Actions Show r Manag Pass Enal Chai Chai	Discover accounts from include disabled accoun- another condition <u>add ane</u> s <u>G</u> managed account as Smart e Account Settings word Rule <u>Default Pass</u> bel Automatic Password Min nge Password Triem <u>13</u> nge Password Frequency	Ladi Cisco Network Dev Is no Group word Policy nagement yes • 30 • EVERY 30 DAYS		· 0	¥	•	
Add. Actions Show r Manag Pass Enal Chai Chai	Discover accounts from Include disabled account another condition Add ane s e Account Settings world Rule Default Pass world Rule Default Pass world Rule Default Pass more Password Time 23 nge Password Frequency sult Release Duration DRA	Lado Cico Nettion Dev is no estrolia Group Group word Policy word Policy word Policy estrolia Every 30 Jav Every 30 Jav S: 0 HOURS; 2 MINUTES: C		· 0	Ť	v	
Add. Actions Show r Manag Pass Enal Chai Chai Chai Defa Max	Discover accounts from Include disabled account another condition Add a re- s = managed account as Smart er Account Settings word Rule Default Passo ble Automatic Password Mi nge Password Time 23 ange Password Frequency auft Release Duration DA imum Release Duration D	Lad Cisco Vettion R. Dev Is no ensure Group word Policy word Policy word Policy word Policy word Policy word Policy S. 0 HOURS: 2 MINUTES: C MINUTES: C	50	- 0 - 0	•	•	
Add. Actions Show r Manage Pass Enal Chai Chai Chai Defz Max	Discover accounts from Include disabled accoun- another condition <u>6.06 a ne</u> s <u> </u> managed account as Smart e Account Settings word Rule <u>Default Pass</u> bile Automatic Password Minge Password Time <u>13</u> nge Password Time <u>13</u> nge Password Frequency sult Release Duration <u>10</u> Release Duration <u>1075</u> .0	Lad CRO Network Dev           Is         no           extraction         extraction           Group		- 0 - 0	v	Ţ	
Add. Actions Show r Manag Pass Enal Chai Defa Chai Defa Sh IA	Discover accounts from Include disabled account another condition Add ane s en Account Settings en Account Settings word Rule Default Pass ble Automatic Password Time 3 nge Password Time 3 nge Password Time 3 nge Password Frequency Jult Release Duration DRTs 0 Release Duration DRTs 0	Lad CRO NEWORK Dev a croup croup Group Group Verd Policy Verd Policy Verd Policy Verd Policy Verd Policy Verd Policy St 0 HOURS 2 MINUTES C 1 COMPACT ST 0 HOURS 2 MINUTES C 1 COMPACT ST 0 HOURS 2 MINUTES C		· 0 · 0	•	•	
Add Actions Show r Manag Pass Enal Chai Chai Chai Chai Sh I Max Acco	Discover accounts from Include disabled accoun- another condition <u>odd ane</u> s <u> </u> managed account as Smart ex Account Settings word Rule <u>Default Pass</u> bile Automatic Password Mi arge Password Frequency uit Release Duration <u>DAN</u> uit Release Duration <u>DANS</u> Release Duration <u>DANS</u> outo Concurrent Request <u> </u> Change Password Frequency Unit Dans <u>Dans</u>	Lad CRO Network Dev is no erroue Group Group word Policy word Policy yes v jagement yes v jagement yes v word Policy S: 0 HOURS: 2 MINUTES: C MINUTES: C 1 1 5 0 1 1 5 0 1 5 0	2.0 kPassword	- 0 - 0		•	
Add. Actions Show r Manag Pass Enal Chai Chai Chai Defa Max ISA I Max	Discover accounts from Include disabled accoun- another condition Add ane a G managed account as Smart e Account Settings word Rule Default Passo bite Automatic Password Man nge Password Frequency aut Release Duration DATS 0 Release Duration RATS 0 Chonge Password not Mars Change Password on Mars	Lado Cicko Vestivaria, Dev     s     no     croup     croup     vord Policy     vord     vord Policy     vord     vo	NO APassword	- 0 - 0	•	•	
Add. Actions: Show r Manag Pass Enala Chai Chai Chai Chai Chai SA I Max Accco ISA I Max	Discover accounts from Include disabled accoun- another condition <u>odd ane</u> s <u>a</u> managed account as Smart ex Account Settings word Rule <u>Default Pass</u> bite Automatic Password Min gre Password Frequency aut Release Duration <u>DAN</u> aut Release Duration <u>DANS</u> out Options <u>Change Pa</u> Change Password on Miss Change Password on Miss Change Password on Miss Change Password on Miss	Lad CRO NetWork Dev Is no erroue Group Group Internet yes yes yes yes yes yes yes yes	2.0 k Password	· 0 · 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

24 C: 4/15/2024

## **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 BeyondInsight, 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 <u>"Use Case 6: Add Directory</u> Admin Accounts for Network Devices" on page 31.

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

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

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

8. Click Create Smart Rule.

Details
Antegory Managed Accounts
Varme
Add Directory Accounts for Windows Servers 🛛 🖉 Active
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
Rearing the query X hours
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
manage Account Settings
Password Rule Default Password Policy
Password Rule Default Password Policy   Enable Automatic Password Management yes  Change Password Time 23   Change Password Frequency EVERY 30 DAYS  Default Release Duration DAYS: 0 HOURS: 2 MINUTES: 0
Password Rule Default Password Policy    Enable Automatic Password Management yes   Change Password Time 23   Gaute 23   Change Password Frequency EVERY 30 DAYS  Default Release Duration DAYS: 0 HOURS: 2 MINUTES: 0  Maximum Release Duration DAYS: 0 HOURS: 2 MINUTES: 0
Password Rule Default Password Policy   Enable Automatic Password Management yes  Change Password Time 23   Ghange Password Time 23   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
Password Rule Default Password Policy   Enable Automatic Password Management yes Change Password Time 23   Good State St
Password Rule Default Password Policy   Enable Automatic Password Management yes Change Password Time 23   Good State St
Password Rule Default Password Policy   Enable Automatic Password Management   YES  Change Password Time 23  Change Password Time 23  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  ISA Release Duration DAYS: 0 HOURS: 2 MINUTES: 0  Ax Concurrent Request  1 1 2 Account Options  Change Password after Release. Check Password  Change Password on Mismatch
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  ISA Release Duration DAYS: 0 HOURS: 2 MINUTES: 0  ISA Release Duration DAYS: 0 HOURS: 2 MINUTES: 0  IsA Release Duration DAYS: 0 HOURS
Password Rule Default Password Policy    Enable Automatic Password Management    yes  Change Password Time  23  30  Change Password Frequency EVERY 30 DAYS  Default Release Duration DAYS: 0 HOURS: 2 MINUTES: 0  Maximum Release Duration DAYS: 0 HOURS: 2 MINUTES: 0  ISA Release Duration DAYS: 0 HOURS: 2 MINUTES: 0  Max Concurrent Request  1   Change Password after Release. Check Password  Change Password on Mismatch Email release notifications to

### **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.

<	Requestor	
Acci 24)	tess Policy for Requestor x7 - 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

ust company, or TC: 4/15/2024

©2003-2024 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.

27

# **Use Case 5: Add Directory Admin Accounts for Linux Servers**

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

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

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

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

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

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

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

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

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

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

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 <u>"Use Case 6: Add Directory</u> Admin Accounts for Network Devices" on page 31.

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

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

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

8. Click Create Smart Rule.

Create New Managed Account Based Smart Rule			
Details 😑			
Category			
Managed Accounts -			
Name			
Add Directory Accounts for Linux Servers 🔹 🖉 Active			
Description			
Add Directory Accounts for Linux Servers			
Reprocessing limit			
Default 👻 0			
Selection Criteria 😑			
Include Items that match ALL			
Directory Query	- 6	Э	
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 appther condition - Add a new group			
LINE REPORT LINE LINE STRAN			
Actions 😑			
Show managed account as Smart Group	- 0		
Manage Account Settings	- <b>B</b>		
Password Rule Default Password Policy		•	
Enable Automatic Password Management			
Change Password Time 23			
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

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



Add Directory Accounts For Linux Servers Password Safe Roles
A role is the connection between a Password Safe user account and a managed system. A role defines what the user or group can do with respect to that managed system.
Requestor
Access Policy for Requestor
24x7 - No Approval
Approver
Credentials Manager
Recorded session reviewer
Active session reviewer
SAVE ROLES DISCARD CHANGES

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

# **Use Case 6: Add Directory Admin Accounts for Network Devices**

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

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

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

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

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

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

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

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

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

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

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 Rule* or other specific criteria for the linking rule action, if desired.

8. Click Create Smart Rule.

Details 🕀	
Eategory	
Managed Accounts	•
Name	
Linkning AD Cisco Accounts	<ul> <li>Active</li> </ul>
Description	
Linkning AD Cisco Accounts	0
Reprocessing limit	- 0
Detault	
Selection Criteria 😑	
Include Items that match ALL	✓ of the following
Managed Account Fields	· 8
Account Name	•
equals (=)	<b>*</b>
levi	Ø
Add another condition Add a new group	
Actions 🖂	
Show managed account as Smart Group	- <b>O</b>
Link domain accounts to Managed System	Q
Asset or Managed System Smart Group	Add Cisco Network Devices to All Managed Systems - (Managed System group)

### **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	540							
Group Details	<	Smart Groups Permissions							
Details & Attributes		Stow Enabled Smart Groups - T /s	lter by						
Features		Assign Permissions					т		
Smart Groups (1)		1 item (1 selected)						÷	-
Users (2)		Smart Group Name +			Organization	Permission	Passwori Safe Role		
API Registrations		Linking AD Cisco Accounts		Managed Account	Global	Read only			1
						+ Assign P	vermissions F	ull Con	trol
						O Disable	Permissions		
						C Edit Pas	sword Safe R	oles	
		H 4 Page 1 of 1 F H	100 v Items per pa	6e		-		_	

<sup>©2003-2024</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: 4/19 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.

#### 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

### **Use Case 7: Add Dedicated Directory Accounts for Windows Servers**

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

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

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

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

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

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

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

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

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

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.

©2003-2024 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

# 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:
  - 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 Rule* or other specific criteria for the linking rule action, if desired.

8. Click Create Smart Rule.

Create New Managed Account Based Smart Rule				
Details 😑				
Category				
Managed Accounts				
Name				
Add Dedicated Account to Password Safe 💿 🗹 Active				
Description				
Add Dedicated Account to Password Safe Ø				
Reprocessing limit				
Default 🗸				
Selection Criteria 🖯				
Include items that match ALL    of the following				
Directory Query				
Include accounts from Directory Query				
Dedicated Account Directory Query				
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 🖯				
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 Pula Default Password Policy				
Enable Automatic Password Management yes 🔹				
Change Password Time 23				
Change Password Frequency EVERY 30 DAYS				
Default Release Duration DAYS: 0 HOURS: 2 MINUTES: 0				
Maximum Release Duration DAVS: 0 HOURS: 2 MINUTES: 0				
ISA Release Duration DAYS: 0 HOURS: 2 MINUTES: 0				
Max Concurrent Request 📮 1				
Account Options Change Password after Release, Check Password				
Change Password on Mismatch				
Email release notifications to				
Add another action				

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 BeyondInsight, click Smart Rules.
- 2. Select Managed Account from the Smart Rule Type filter list.
- 3. Click Create Smart Rule.
- 4. Select Managed Accounts from the Category list.
- 5. Enter a meaningful **Name** and **Description** for the Smart Rule.
- 6. Set Selection Criteria as:
  - Dedicated Account, Account Name, with Suffix, <applicable suffix>
- 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 theme that match All of the following		
Dedicated Account 👻 🕄		
Account Name 👻		
with suffix		
· · · ·		
da 🛛 👳		
Add another condition Add a new group		
-		
Map Dedicated Accounts To		
User Group Requestors 🔹		
Show managed account as Smart Group 🔹 🗴		
Add another action		
CREATE SMART RULE DISCARD		

36

Create New Managed Account Based 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.

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.



Roles

Add Dedicated Account To

Password Safe Password Safe

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



>

37

# **Use Case 8: Dedicated Directory Accounts for Entra ID**

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

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

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

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

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

- For more information, please see the following:
  - Use Case 1: Add Local Admin Accounts for Windows Servers
  - Use Dedicated Account Smart Rule
  - Adding a Managed System Manually

### **Use an Entra ID Smart Rule**

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

Follow the steps below to discover Entra ID accounts.

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

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

*Tip:* To view the contents of a Smart Rule when creating a new rule or editing an existing rule:

- Once the rule is saved, click View Results.
- You are taken to the associated grid, where the contents of the Smart Rule are listed.
- If the rule is actively processing, a banner displays letting you know that.

Create New Managed Account Based Smart Rule				
Details 🖯				
Category				
Managed Accounts -				
Name				
Accounts O Active				
Description				
Reprocessing limit				
Default -				
Selection Criteria 🖯				
Include Items that match ALL   of the following				
Azure Directory Query				
Group Name 🔻				
equals (=) 🗸				
ADQ Group Ø				
Re-run the query every X hours 📃 0 💽				
Discover accounts in Azure synced from on-premise				
Discover accounts for Password sale management				
Domain example.com				
Add another condition Add a new group				
Actions 🖯				
Show managed account as Smart Group 🔹				
Manage Account Settings 🔹 😵				
Password Rule Default Password Policy				
Enable Automatic Password Management yes 👻				
Change Password Time 23				
Change Password Frequency EVery 30 Days				
Default Release Duration Days: 0 Hours: 2 Minutes: 0				
Maximum Release Duration Days: 0 Hours: 2 Minutes: 0				
ISA Default Release Duration Days: 0 Hours: 2 Minutes: 0				
Max Concurrent Request 📮 1 🛨				
Account Options Change Password after Release, Check Password				
Change Password on Mismatch				
Email release notifications to bob@example.com o				
Add another action				
Groute Servet Bule Mounter Discord				
Create sinare rate view results Discort				

#### Note:

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

*Tip:* Because the Smart Rule must process to display the contents in the grid, we recommend viewing the results using only the **Show <entity> as Smart Group** action and before adding additional actions that may make changes to accounts and assets in your network.

Once you have confirmed the rule contains your desired items, you can then add additional actions to the Smart Rule.

# **Use Case 9: Define Just in Time Access Policies**

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

# **Configure Password Safe Access Policies**

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

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

### **Create an Access Policy**

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



#### 4. On the Basic Details tab:

- Enter a description for the policy.
- Optionally, enable the Email Notifications option to send emails when a request is received for the policy.

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

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

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

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

#### 9. Select the type of access to permit: View Password, RDP, SSH, or Application.

10. For each type of access selected, configure the parameters as required. Descriptions for each parameter are as follows:

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

RDP Admin Console	Select this option to show the <b>RDP Admin Console</b> check box on RDP-based requests. This option allows administration of a Remote Desktop Session host server in console mode (mstsc /admin). This can be useful if the number of remote sessions is maxed out on the host.
	Using the RDP Admin Console allows you to use a remote session without requiring other sessions to disconnect. Running a remote session using the RDP Admin Console disables certain services and functionality, such as, but not limited to:
	<ul> <li>Remote Desktop Services client access licensing</li> <li>Time zone redirection</li> <li>Remote Desktop Connection Broker redirection</li> <li>Remote Desktop Easy Print</li> </ul>
Connection Profile	Select a profile from the list or click <b>Manage Connection Profiles</b> to be taken to the <b>Connection Profiles</b> page to create a new profile.

#### 11. Under Policy Options:

- If you want users to provide a reason when making requests in Password Safe, click the toggle for the **Reason is required** for new requests option to enable it.
- If you want users to provide a ticket number for a ticketing system when making requests in Password Safe, click the toggle for the **Require a ticket system and a ticket number for requests** option to enable it.
  - Once enabled, select the Ticket System from the dropdown. If you leave the Ticket System as User Selected, the user can select any ticket system from the list when making their request. If you select a specific ticket system for this option, the user is unable to change the ticket system when making their request.
- 12. Click Create Schedule. If the access policy is not yet marked as available, you are prompted to activate it now.
- 13. Assign the access policy to a user group as follows:
  - Select the Assignees tab.
  - Click Manage Assignees. You are taken to the User Management page.
  - Click the vertical ellipsis for a group, and then select View Group Details.
  - From the Group Details pane, click Smart Groups.
  - Click the vertical ellipsis for a managed account Smart Group, and then select Edit Password Safe Roles.
  - · Check Requestor, and then select the access policy you just created from the dropdown.
  - Click Save Roles.
- 14. Confirm the group is now listed as an assignee on the **Assignees** tab for the access policy you just created.