

Endpoint Privilege Manager (EPM) Use Case Walkthrough

01 0 1 00 011



011

0101

00

1 101



This document explores the different use cases Securden Endpoint Privilege Manager addresses. The privilege elevation mechanism along with the steps required to test the functionality is explained in detail.

What are the different use cases that the Securden Endpoint Privilege Manager helps address?

Securden EPM helps address various privilege management requirements an organization could face in day-to-day operation. Securden EPM helps the workforce function without having local administrator rights through provisions that grant the minimum level of privileges required for each user to complete their tasks seamlessly.

The different use cases that are addressed are listed below:

Case 1: Users regularly run a set of applications with admin rights to fulfill their responsibilities

Case 2: Users who need to run new apps with admin rights that are not covered under policies.

Case 3: Users who need to elevate multiple applications within a short span of time.

Case 4: Controlling application usage by users in the organization through allowlists and blocklists.

Case 5: Granting temporary application access to users when allowlist/blocklist is enforced

Pre-requisites:

 Before testing privilege elevation using Securden EPM Cloud Edition, ensure that the Securden Privilege Management agent is installed on an endpoint. **Note**: If the endpoint is an AD domain computer, then you need to deploy a lightweight remote connector. Refer to the EPM SaaS quick start guide.

- 2) Ensure there is internet connectivity at the endpoint.
- 3) Ensure that the user account on the endpoint is a standard user account without admin rights. You can remove the admin rights by navigating to **Privileges >> Remove Admin Rights** on the EPM web-interface.
- 4) In the web-interface, navigate to the application tab and ensure that the required applications (for testing purposes) are available in the repository.

Note: A comprehensive list of applications is added to the repository by default and can be used for privilege management and application control. Apart from these applications, once the agent is deployed, the applications that are run with admin rights will be automatically added to the repository.

a. If the required application is unavailable, then add the application manually. You need to specify the attribute using which Securden identifies the application during privilege management.

Case 1: Users regularly run a set of applications with admin rights to fulfill their responsibilities

To grant the required permissions to users who might regularly need to run a specific set of applications with admin rights, Securden EPM Cloud Edition provides a policy-based privilege elevation provision. To test policy-based privilege elevation, follow the steps below

Step 1: Create a privilege-elevation policy

1. In the Securden EPM web interface, navigate to **Privileges** >> **Application Policies** >> **Add Policy**.

💙 End	[†] Endpoint Privilege Manager				Contact Technical Support Get Quote					Q Search Computers		
ę	බ Dashboard Requests Computers			Applications	Privileges	Users	Reports	Admin				
Application Policies		Арр	lication Con	trol Policies	?							
Remove		Q	C Add Policy	Delete Policies							Showing 1 to 21 of 21	25 🗸
Privileges			Name ‡		Description		Privilege Ele	evation	Statu	s	Actions	
Request Privil	lege		1				E Blockliste	d	😑 Dis	sabled [Enable) 🛯 🖉 📋	
			Advanced Configura	ations Built-in	This policy governs the	application privilege f	or 背 Local Adn	ninistrator Privilege	😑 Dis	abled [Enable) 🛯 🖉 🗇	
			allowlist		Added through privilege	e elevation request	F Allowliste	d	 Ac 	tive [Disable]	A / 📋	
			allow list for notepad	d			Allowlister	d	😑 Dis	abled [Enable) 🗇 🗇	
			allowlist test				F Allowlister	d	😑 Dis	abled [Enable) 🛯 🖉 📋	
			blocklist				FBIOCKIISte	d	😑 Dis	abled [Enable) 🛯 🖉 📋	
			block policy				Blockliste	d	😑 Dis	abled [Enable) 🕅 🦉 📋	
			Cloud Storage Serv	ices Built-in	This policy governs the	application privilege f	or 🚦 Local Adn	ninistrator Privilege	😑 Dis	abled [Enable) 🛯 🖉 🗇	
			Command Line Inte	rface Built-in	This policy governs the	application privilege f	or 🚦 Local Adn	ninistrator Privilege	😑 Dis	sabled [Enable) 🛯 🖉 🗇	
			Configurations Buil	It-in	This policy governs the	application privilege f	or 🚦 Local Adn	ninistrator Privilege	😑 Dis	abled [Enable) 🛯 🖉 🗇	

2. Select the policy type in accordance with the operating system on the endpoint. For explaining the process, we will assume that the endpoint is running on **Windows**.

Findpoint 🗸	t Privilege Manager	Contact Technical Supp	ort Get Quote				Q Search Computers	8~
🕞 Dash	board Requests	Computers Applications	Privileges	Users	Reports	Admin		
Request Privilege	board Requests Add Application Cor Policy type Windows Control Policy Name* I Application Elevation Prefet Elevate with local administrato Elevate with domain administrato Elevate with system privilege	Computers Applications Acc Clinux Description erence r privilege ator privilege	Privileges	Users	Reports	Admin Help C Please rr Application Privilege Application Spec Spec All us Vou can s grant diffe requireme privileges, If two diffe will be base	fer to the section below for help with c n Control Policies. Elevation Precedence n control policies can be created and associated fic users fic groups ers ers except 'Excluded' ones elect the required application elevation preferer ernt levels of privileges to the users based o ths. These include, system level privileges, o local admin privileges, allowiists and blocklists. rent policies affect the same user, the policy in ed on the following order of user/group precede	d with ance to on their domain n effect ence.
	Allowlist Blocklist Select Applications/Groups Search applications	3				Specific L Users Note: By prioritized However, users car section to Excluded If the tw precedenc on the foll Local Adn	sers >> Specific Groups >> All Users / Ex default policies associated with all users i over the policy created by excluding specific this order of priority between All users and Ex be interchanged. Navigate to the configu- set the order of priority between All user users. o policies assigned have the same user e, the application control policy in effect will be wing order of privilege precedence: in Privilege >> Domain Admin Privilege >> 5	cluded users. ccluded irations rs and r/group based System

3. Give a suitable name for the policy for identification purposes.

- 4. Select the application elevation preferences. For testing purposes, we can select **Elevate with local administrator privilege**.
- 5. Select the required application(s) by searching the field.



6. Select the devices on which this control policy should be enforced. You have the option to associate the policy with all the devices available in Securden. You can also associate the policy with specific devices.

💙 Endpoi	nt Privilege Manager		Contact Technical Suppor	t Get Quote				Q Search Computers	2~		
Ę⊚ Da	shboard Requests	Computers	Applications	Privileges	Users	Reports	Admin				
Application Policies	Application Elevation F Elevate with local administ 	Preference strator privilege					You can grant diff requireme privileges	select the required application elevation prefer arent levels of privileges to the users based ints. These include, system level privileges, local admin privileges, allowlists and blocklists	ence to on their domain		
Remove Privileges	 Elevate with domain adm Elevate with system privil 	inistrator privilege (j) ege					If two diff will be ba Specific	If two different policies affect the same user, the policy in effe will be based on the following order of user/group precedence. Specific Users >> Specific Groups >> All Users / Exclude			
Request Privilege	 Allowlist Blocklist 		Users Note: By prioritized However,	default policies associated with all users over the policy created by excluding specific this order of priority between All users and E	will be susers. xcluded						
	Select Applications/Gro	oups	users can be interchanged. Navigate to the contigural section to set the order of priority between All users Excluded users.								
	🔚 7-Zip File Manager (7z	FM.exe) 🗙 🔚 Adobe F	If the the preceden on the fol	vo policies assigned have the same use ce, the application control policy in effect will be owing order of privilege precedence:	er/group e based						
	Associate Policy with V	Vindows Computer	Local Ad	System							
	All Windows Computers	 Specific Windows 	For exampolicy (Perevented and elevate and	ple, User A and User B have an application blicy 1) associated to them. Policy 1 allows t specific application with domain admin privilege	control them to es.						
	DESKTOP-E3PHE3H	X Search computer/gr	A differen same app	t control policy (Policy 2) allows User B to elevilication with local admin privilege.	/ate the						
	Associate Policy with U	Associate Policy with Users/User Groups in Securden						se, User B will only be able to elevate with loca However, User A will still be able to eleva dmin privileges. Policy 1 is prioritized over F the order of precedence.	I admin ate with Policy 2		
	 All users	pecific users/user group	es O Exclude specific e	 Exclude specific users/user groups 			You can Blocklist	change this priority order with a configural rivilege to take precedence over Allowlist privile	tion for ege.		

7. Select the users to which this control policy should be associated.

8. When associating the policy with specific devices and specific users, you can associate the policy with local user accounts.

💙 Endpoint	Privilege Manager		Contact Technical Suppo	Get Quote				Q Search Computers	2~	
न् _छ Dasht	ooard Requests	Computers	Applications	Privileges	Users	Reports	Admin			
	Select Applications/Gro	oups				Reset	users can section to Excluded	 be interchanged. Navigate to the co set the order of priority between All users. 	nfigurations users and	
Policies	37-Zip File Manager (7zł	FM.exe) 🗙 🔚 Adobe	Reader × Search applica	ations			If the two policies assigned have the same user/group precedence, the application control policy in effect will be based on the following order of privilege precedence:			
Remove Privileges	Associate Policy with V	Vindows Compute	rs/Groups in Securd	en			Local Adr Privilege 3	nin Privilege >> Domain Admin Privilege >> Allowlist >> Blocklist	>> System	
Request Privilege	All Windows Computers	 Specific Window 	Reset	For example, User A and User B have an application cont policy (Policy 1) associated to them. Policy 1 allows them elevate a specific application with domain admin privileges.						
	DESKTOP-QKG8PQV	Search computer/	A differen same app	control policy (Policy 2) allows User B to ication with local admin privilege.	elevate the					
	Associate Policy with L	Jsers/User Groups	In this case, User B will only be able to elevate with local admin privileges. However, User A will still be able to elevate with domain admin privileges. Policy 1 is prioritized over Policy 2 based on the order of precedence.							
	 All users Include s 	pecific users/user grou	You can change this priority order with a configuratic Blocklist privilege to take precedence over Allowlist privileg							
	A 2 (2@veeravelazoonou	tlook.onmicrosoft.com)	× Search user/group				Allowlist A	pplication(s)		
	Associate with Local U	sers					The allow access th application allowlist p	list option allows the selected users/use e applications that form the policy and blo ns from being run. For this to be in effect, plicy must be configured.	r groups to ock all other at least one	
	User@DESKTOP-QKG8P	QV × Search User				Reset	For exam User A of cannot be precedent application	ple: If a policy has allowlisted 'Google n Computer A, all other applications on accessed by User A. (Unless a policy ce is configured allowing the user to).	Chrome' for Computer A with higher access an	
	Save Cancel						Note: File will not be	s under default windows folder (typically of blocked from running even when an allow	2:\Windows)	

Note: Users added to Securden from Azure (Entra ID) and AD will be available under **Associate Policy with Users/User Groups in Securden**. If you want to associate the policy with local users on the selected endpoints, then you need to search and them in the field **Associate with Local Users**.

9. Click **Save**.

Note: If only one user in Securden has the role of **Administrator**, then the policy will be enforced right after you click **Save**. However, if more than one user has the administrator user role, the policy must be approved by the other administrator before it is enforced.

Step 2: Elevating the application on the endpoint

Once the policy is enforced, we can test running the associated application with admin rights on the endpoint associated with the policy.

In the endpoint, right click on the app and click **Run with Securden Privilege** to run the app with admin rights.

	Open
V	Delete with Securden privilege
	Open file location
V	Run with Securden privilege
•	Run as administrator
2	Edit with Notepad++
V	Edit with Securden privilege
	Troubleshoot compatibility
	Pin to Start
	7-Zip >
	Unpin from taskbar
	Restore previous versions
	Send to >
	Cut
	Сору
	Create shortcut
	Delete
	Rename
	Properties

2. Alternatively, you can use the command prompt to run the app with admin rights. Open command prompt and prefix **secudo** with the exact command that you need to run to start the application from the command prompt.



3. You can also try right clicking on the application and clicking **Run as Administrator**. The User Account Control prompt will pop up and ask you to provide administrator credentials.

Do you want to allow this app changes to your device?	to make	Securden
Microsoft Edge		Gain admin rights and run the application.
Verified publisher: Microsoft Corporation File origin: Hard drive on this computer Show more details		Proceed
To continue, enter an admin user name and	d password.	
Password		
Yes	No	

 Along with the UAC prompt, the Securden pop-up will also be displayed. You can simply click **Proceed** and the application will be run with admin rights.

Now, you can test running different apps with admin rights that are not covered in the policy. A Securden pop-up will be displayed stating that you do not have the required permissions to run this app with admin rights. Here you can place a request with the EPM administrator to grant the required permissions. The steps are explained in the next use case.

Case 2: Users who need to run new apps with admin rights that are not covered under policies

When the users who need to elevate apps that are not covered in policies, they can use the request-release workflow provided by Securden EPM. Users can raise a request using the agent and once the administrator approves the request, the user can run the app with admin rights. Follow the steps below to test the request-release workflow:

Step 1: Raising a request from the end user machine

1. In the endpoint, right click on an application that is not covered in a policy and click on **Run with Securden Privilege**.



 A Securden dialog box will be displayed stating that you do not have necessary permissions to run the app with admin rights. In this dialog box, you will have the option to raise a request with the administrator. Click **Request Admin Privilege**.



Info

This application has not been marked to run with elevated privileges by your administrator. Contact your administrator

Request Admin Privilege Close

3. In the window that appears, specify details such as the start and end time or the duration of elevated access required.

Securden								
Endpoint Pr	ivilege Mana	ger						
Request admin access View approval status								
You can raise a request to get temporary full administrator access, administrator access only to a specific application on this machine for the currently logged in account, permission to write into a folder and to edit a specific file.								
For a specific	In the specific application O Time-limited full admin access							
Application File Path Publisher <u>Browse a differer</u>	ApplicationMicrosoft EdgeFile PathC:\Program Files (x86)\Microsoft\Edge\AppliPublisherMicrosoft CorporationBrowse a different application							
Specify when you n	eed access							
Till 04:35 PM	Till 04:50 PM	Duration	Custom					
Reason								
Request	Cancel]				

4. Select the check box named **With Admin Rights** if shown.

Note: This checkbox will only be displayed when an allowlist/blocklist policy is enforced.

5. Provide a reason and submit the request.

Step 2: Approving/Rejecting the request

- 1. In the EPM server, go to the **Requests** tab.
- 2. Ensure the **Request Filter** is set to **To Be Approved** and find the request placed from the endpoint.
- 3. Click on **Approve**.
- 4. You will be able to specify the time or duration of elevated access that you as an administrator want to grant the end user.

Approve	e Elevatio	n Requ	lest			×
User Account christus						
Computer Name SEC-SUPPOR	e T-1					
Start Time	📰 29 Jan 20	025 🕓	13 🗸	00	~	
End Time	📰 29 Jan 20	025 🕓	13 🗸	35	\checkmark	
(Current Time Reason	e on Server. iii	24 Jan 20	025 🕒	11:06	hrs)	
Approve	Cancel					

5. Provide a reason and click **Approve**.

Note: Even though the user places a request with a specific time/duration parameters, elevated access will be granted according to the time or duration specified by the administrator while approving the request.

Step 3: Elevating the application

Note: Verify whether the temporary access permission is still valid. i.e The Securden server time must be between the approved start and end time of

the access request. For duration-based privilege elevation, the time of the Securden server doesn't have a bearing on the validity of the request.

- 1. In the end user machine, find the application for which the request was placed.
- Right-click the application and select Run with Securden Privilege.
 Note: You can try any one of the methods discussed in Case
 1>>Step 2 to elevate the application.
- 3. The app will open with admin privileges. You will also be able to see a count-down on the bottom-right corner of the screen. Once the timer runs out, the app will be terminated automatically.

Note: You can also submit your elevated access before time by closing the timer window.

Now, you can try elevating a different application to which the user doesn't have permission. The same dialog box will be displayed with the option to raise a request.

Case 3: Users who need to elevate multiple applications within a short span of time

To cater to special needs of developers and technicians who might need to elevate multiple applications simultaneously to test their code or troubleshoot issues on computers, Securden allows users to gain temporary full administrator access.

These administrator sessions are strictly monitored and tracked through text-based audit trails. If the user creates new admin accounts using the permission granted in these sessions, they will be tracked, and their actions can be reversed. To test the request-release workflow for temporary fulladmin access, follow the steps below.

Step 1: Raising a request for time-limited, full-admin privileges

- 1. Go to an endpoint with the Securden agent.
- 2. Open the Securden tray icon and click on **Request Admin Privilege**.



3. In the window that opens, choose **Time-limited full admin access**.

Securd Securd	len		
Endpoint Pr	ivilege Manag	jer	
Request admi	n access View	ı approval stat	tus
You can raise a req access only to a sp account, permission O For a specific	uest to get temporary ecific application on th n to write into a folder a c application I T	full administrator ac is machine for the c ind to edit a specific ime-limited full	ccess, administrator currently logged in c file. admin access
Specify when you n	eed access		
Till 04:35 PM	Till 04:50 PM	Duration	Custom
Select duration Se	lect 🔻		
Reason			
Request	Cancel		

- 4. Provide the start and end time or a duration based on your requirement and submit the request after providing a reason.
- 5. You have successfully placed a time-limited, temporary full admin access request.

Step 2: Approving/rejecting the request for time-limited, full-admin privileges

- 1. In the Securden EPM web-interface, log in as a user with the Administrator role.
- 2. In the **Admin** section, navigate to the **Requests** section.
- 3. Ensure the **Request Filter** is set to **To Be Approved** and find the request placed from the endpoint.
- 4. Click on **Approve**.
- 5. In the window that appears, specify the start and end time or the duration of elevated access you want to grant to the user.

Approv	e Elevation R	eques	t	
User Account christus				
Computer Nam SEC-SUPPOF	ne RT-1			
Start Time	📰 29 Jan 2025	L 13	\sim 0	0 ~
End Time	🛗 29 Jan 2025	I3	√ 3	5 ~
(Current Tim	ne on Server: 📰 24 、	Jan 2025	G 11	:06 hrs)
Reason				
Approve	Cancel			

6. Provide a reason before clicking on **Approve**.

Step 3: Using the elevated access on the endpoint

Note: Verify whether the temporary access permission is still valid. i.e. The Securden server time must be between the approved start and end time of the access request. For duration-based privilege elevation, the time of the Securden server doesn't have a bearing on the validity of the request.

- 1. On the endpoint, open the Securden tray icon and click on **Get Latest Changes from Server**.
- The Securden agent pop-up will be displayed stating that your request was approved. You may start the temporary admin access session by clicking on **Start Admin Access**.



Info

Successfully obtained the changes from the server. You are ready to start elevated access.

Start Admin Access Cancel

3. Once you have temporary full admin access, you can elevate any application by any of the options discussed in Case 1 >> Step 2.

4. The count-down timer will be displayed in the bottom-right corner. Once the timer runs out, all open applications running with admin rights will be terminated automatically. You can surrender the elevated access well before the time runs out by clicking on the close button on the timer.

Case 4: Controlling application usage by users in the organization through application control policies

To allow specific set of users to run a set of trusted applications and blocking malicious applications, Securden provides the provision to create **Allowlists** and **Blocklists**.

Note:

- 1) When accessing an application through allowlists and blocklist, the app will be run according to the privileges of the user account.
- 2) Allowlists and Blocklists do not elevate privileges with which the applications are run.

How does an Allowlist work?

When an allowlist is enforced, the users associated with the allowlist will be able to run the applications associated with the allowlist on their designated endpoints. But the users will not be able to run any application other than the apps included in the allowlist.

How does a Blocklist work?

When a blocklist is enforced, the users associated with the blocklist policy will not be able to run the applications associated with the blocklist. The users are, however, free to run every other application on their endpoints.

You can test application control through allowlists and blocklists by following the steps below.

Step 1: Creating an Allowlist/Blocklist

- 1. In the Securden EPM web-interface, login as an administrator and navigate to the **Privileges** tab and click on **Add Policy**.
- 2. Select the policy type according to the operating system of the endpoint. In this guide we will explain the process for **Windows**.
- 3. Provide a suitable name and a description for the policy.
- 4. Select **Allowlist** or **Blocklist** as the application elevation preference based on the requirement.

Endpoint	t Privilege Manager		Contact Technical Support Get Quote				Q Search Computers		
न् _© Dash	board Requests	Computers	Applications	Privileges	Users	Reports	Admin		
Application Policies Remove Privileges Request Privilege	Add Application (Policy type Windows Control Policy Name* App Control - Web dev Application Elevate on P Elevate with local adminis Elevate with system privik Elevate with system privik Allowlist Blocklist	Computers Control Policy Mac Mac reference trator privilege nistrator privilege () tage	Applications Linux Description Application	Privileges Control for Web Dev	Users	Reports	Admin Help Please re Application Privilege Application Spec All us All us You can s grant differ requireme privileges, If two differ will be bass Specific L Users Note: By prioritized However, users can	Provide the section below for help with a control Policies. Elevation Precedence In control Policies can be created and associated if users file users file users ting groups ters ers compared application elevation preference rent levels of privileges to the users based of this These include, system level privileges, local admin privileges, allowists and blockists. prent policies affect the same user, the policy in ded on the following order of user/group preceded Jaers >> Specific Groups >> All Users / E> default policies associated with all users over the policy created by excluding specific this order of priority between All users and Es to be interchanged. Naviade to the conflour	reating 1 with ance to n their domain n effect ance. ccluded will be : users. kcluded urations
	Select Applications/Gro	oups					section to Excluded	b set the order of priority between All use users.	rs and
	Search applications	ups					Excluded If the tw precedence	vo policies assigned have the same use the application control policy in effect will be	r/group
							on the foll	owing order of privilege precedence: nin Privilege >> Domain Admin Privilege >> 3	System

Note: Refer to the sections How does an Allowlist work? And How does a Blocklist work?

5. Add all the applications that you want to associate with this policy.

💙 Endpo	oint Privilege	Manager		Contact Technical Support Get Quote					Q Search Computers	8~	
E D	ashboard	Requests	Computers	Applications	Privileges	Users	Reports	Admin			
Application Policies Remove Privileges	Add A Policy © V Control PC App Cor Applica Eleva Eleva Eleva © Eleva © Allow © Bloci	Application type /indows licy Name* trol - Web dev ation Elevation ate with local admin ate with local admin ate with system priv fist dist	Control Policy Mac Preference istrator privilege ministrator privilege () ilege	Linux Description Application Co	ux Description Application Control for Web Developers				Help Please refer to the section below for help with creating Application Control Policies. Privilege Elevation Precedence Application control policies can be created and associated with • Specific groups • All users • All users • All users except 'Excluded' ones You can select the required application elevation preference to grant different levels of privileges, to the users based on their requirements. These include, system level privileges, domain privileges, local admin privileges, allowlists and blocklists. If two different levels of user/group precedence. Specific Users >> Specific Groups >> All Users / Excluded Users Note: By default policies associated with all users will be prioritized over the policy created by excluding specific users.		
	Select	Select Applications/Groups T-Zip File Manager (7zFM.exe) × Search applications						However, ' users can section to Excluded u If the tw precedence on the follo Local Adm	this in party determines and the second seco	r/group based	

6. You can associate the policy with specific computers by selecting the required computers in this step. You have the option to associate the policy with all devices for organization wide application control.

Note: To test the policy, ensure that you are associating the device on which you would like to test the application control feature.

💙 Endpoint	Privilege Manager		Contact Technical Supp	ort Get Quote				Q Search Computers	8~		
⊑_ Dashb	oard Requests	Computers	Applications	Privileges	Users	Reports	Admin				
Application Policies	Select Applications/Gr	oups				Reset	However, to users can section to Excluded u	this order of priority between All users and E be interchanged. Navigate to the config set the order of priority between All use users.	xcluded urations ers and		
Remove	7-Zip File Manager (7z	FM.exe) × 🗟 Adobe	Acrobat × Search applic	cations			If the tw precedenc on the follo	o policies assigned have the same use e, the application control policy in effect will be wing order of privilege precedence:	e based		
Privileges	Associate Policy with	Nindows Compute	rs/Groups in Securd	en			Local Adm Privilege >	nin Privilege >> Domain Admin Privilege >> > Allowlist >> Blocklist	System		
Request Privilege	All Windows Computers	Specific Window	vs Computers/Groups			Reset	For examp policy (Po elevate a s	ole, User A and User B have an application licy 1) associated to them. Policy 1 allows specific application with domain admin privilege	control them to es.		
	DESKTOP-113JFQT × Search computer/group						A different same appl	A different control policy (Policy 2) allows User B to elevate the same application with local admin privilege.			
	Associate Policy with	Jsers/User Groups	s in Securden				In this case privileges. domain ac based on t	e, User B will only be able to elevate with loca However, User A will still be able to eleva Imin privileges. Policy 1 is prioritized over f he order of precedence.	al admin ate with Policy 2		
	All users	specific users/user grou	ps () Exclude specific	c users/user groups			You can Blocklist pr	change this priority order with a configura ivilege to take precedence over Allowlist privile	ition for ege.		
								Allowlist Application(s)			
	Save Cancel						The allow access the application allowlist po	ist option allows the selected users/user gr e applications that form the policy and block a s from being run. For this to be in effect, at le licy must be configured.	oups to all other ast one		
							For examp User A on cannot be precedenc application	ble: If a policy has allowlisted 'Google Chrc Computer A, all other applications on Com accessed by User A. (Unless a policy with e is configured allowing the user to acc).	ome' for iputer A i higher cess an		
							Note: Files	under default windows folder (typically C:\W	indows)		

7. Select the users with whom you want to associate the policy. You have the option to associate the policy with all users or select specific users to associate with the policy. You can also create an exclusion list of specific users. In that case, every other user except the selected users will be associated with the policy automatically.

Important: To test the policy, ensure that you are associating the user account on which you would like to test the application control feature.

8. When associating the policy with specific devices and specific users, you have the option to associate the policy with local user accounts.

😴 Endp	oint Privilege Manager		Contact Technical Sup	port Get Quote				Q Search Computers	8~		
E® (ashboard Requests	Computers	Applications	Privileges	Users	Reports	Admin				
	Select Applications	/Groups	Reset	users can be interchanged. Navigate to the configuration section to set the order of priority between All users a Excluded users.							
Policies	m 7-Zip File Manage	r (7zFM.exe) 🗙 🔚 Adobe	Reader × Search appli	ications			If the two policies assigned have the same up precedence, the application control policy in effect will on the following order of privilege precedence:				
Remove Privileges	Associate Policy w	ith Windows Compute	rs/Groups in Secur	den			Local Adr Privilege >	nin Privilege >> Domain Admin Privilege >> > Allowlist >> Blocklist	System		
Request Privileg	All Windows Compute	ters Specific Window 	s Computers/Groups			Reset	For example, User A and User B have an application policy (Policy 1) associated to them. Policy 1 allows the elevate a specific application with domain admin privilege:				
		Search computer/	grout				A different same app	control policy (Policy 2) allows User B to elevication with local admin privilege.	vate the		
	Associate Policy w	Associate Policy with Users/User Groups in Securden						In this case, User B will only be able to elevate with local adn privileges. However, User A will still be able to elevate w domain admin privileges. Policy 1 is prioritized over Policy based on the order of precedence.			
	 All users Incl Incl 	ude specific users/user grou	You can Blocklist p	change this priority order with a configura rivilege to take precedence over Allowlist privile	tion for age.						
	A 2 (2@veeravelazo	onoutlook.onmicrosoft.com	Allowlist A	pplication(s)							
	Associate with Loc	al Users					The allow access the application allowlist p	list option allows the selected users/user gr e applications that form the policy and block a ns from being run. For this to be in effect, at le plicy must be configured.	oups to all other ast one		
	User@DESKTOP-QI	User@DESKTOP-QKG8PQV × Search User						ple: If a policy has allowlisted 'Google Chro n Computer A, all other applications on Com accessed by User A. (Unless a policy with se is configured allowing the user to acc).	me' for puter A higher ess an		
	Save Cancel						Note: File will not be	s under default windows folder (typically C:\W blocked from running even when an allowlist	indows) policy is		

Note: Users added to Securden from Azure (Entra ID) and AD will be available under **Associate Policy with Users/User Groups in Securden**. If you want to associate the policy with local users on the selected endpoints, then you need to search and them in the field **Associate with Local Users**.

Once the preferences are selected, click **Save**.

Similar to privilege elevation policies, the allowlist/blocklist needs to be approved by a second administrator before it is enforced. If there is only one administrator running the EPM, then the policy will be enforced right after creation.

Step 2: Testing application control

- 1. Once the policy is in effect, log in to a device associated with the policy as a user associated with the policy.
- 2. Try to run an application included in the allowlist/blocklist.
 - a. If allowlisted, the app will run.

 b. If blocklisted, the app won't run and a Securden prompt will be displayed.

Note: You can use this prompt to raise a request for temporary access to the application. This is discussed in the next case.

- 3. Now, try running an application that is not associated with the allowlist/blocklist policy.
 - a. For an allowlist policy, the application will not run and the Securden prompt will be displayed.
 - b. For a blocklist policy, then the application will run.

You have successfully tested the application control feature.

Case 5: Granting temporary application access to users when allowlist/blocklist is enforced

When an allowlist or a blocklist is enforced, the user will not be able to run many applications that are installed on the endpoints. To cater to the needs of the users, Securden provides a request-release workflow for obtaining temporary access to applications. You can test this workflow by following the steps below.

Step 1: Raising a temporary access to an application

- 1. On the endpoint, run an application that is not a part of an allowlist or is a part of a blocklist.
- A Securden dialog box will be displayed stating the lack of permissions to run the app and an option to raise a request with the administrator. Click **Request Application Access**.



3. In the window that opens, specify the start and end time of the access or specify the required duration.

Securden							
Endpoint Privilege Manager							
Request app access View approval status							
You (logged in user) can raise requests and get read, write, and access permissions for specific apps or for all apps and files on this device. Select the check box 'Run as Admin' to request elevated access permissions for the same.							
${\ensuremath{}}$ For a specific application \bigcirc For all applications							
ApplicationGoogle ChromeFile PathC:\Program Files\Google\Chrome\ApplicatioPublisherGoogle LLCBrowse a different application							
🗌 With Admin Rig	jhts						
Specify when you ne	eed access			÷			
Till 04:40 PM	Till 04:55 PM	Duration	Custom				
Reason							
]			
Request	Cancel						

4. Ensure that the check box named **With Admin Rights** is unchecked and submit the request after providing a valid reason.

Note: You can also request access to all applications on your device for a limited time. To request access to all applications, select the radio button **For all applications**.

Step 2: Approving the request from the admin console

- Login to the web-interface as an administrator and go to the Requests tab.
- Find the request placed from the endpoint and click on Approve.
 Provide the approved start and end time or the duration of application access.
- 3. Provide a reason and click **Approve**.

Step 3: Running the app on the endpoint

 On the endpoint, open the Securden agent tray icon and click on View Approval Status. Ensure that the agent shows that the request has been approved.



Note: If the request status is not **Approved**, then open the tray icon again and click on **Get Latest Changes from Server** and try again.

- 2. You can now try running the application for which the access request was placed.
- The count-down timer will be displayed in the bottom-right corner of the screen. Once the timer runs out, the application will be terminated automatically.
- 4. After verifying the successful start of the application, try opening a different application to check whether any other application can be

run except those allowed through allowlists/blocklists or the application for which temporary access is granted by the administrator.

You can also repeat Step 1 and try rejecting the request and see if the workflow is working as intended.