netwrix

White Paper

Protecting Local and Domain Admin Rights Efficiently, Securely, and Easily

While also Increasing Productivity and Lowering Total Cost of Ownership

Table of contents

Netwrix SbPAM and Netwrix PolicyPak deliver just-in-time identity and privilege orchestration that overcomes the challenges of traditional Privileged Access Management Solutions, including weak security, opportunistic lateral movement, and high cost of ownership.

If local admin accounts are the keys to the kingdom, then domain admin accounts are the golden tickets. A compromised domain admin account can give threat actors and malware executables free reign over all your machines, including domain controllers and DNS servers. In fact, it's never been easier for bad actors to cause destruction. Attackers with access to your environment can easily find tools on the internet that provide the means to take over accounts and gain domain admin privileges. Once your domain is compromised, it's game over.

So what can you do about it? No matter how often you change the passwords for these high-privilege accounts, they still have an attack surface. Even if you retain privileged credentials in a vault, the attack surface still exists, which means those credentials can be compromised by adversaries or misused at any time by their owners. The simple truth is that any AD account with persistent privilege is vulnerable to attack; this type of account is said to have "standing privilege."

If such an attack surface is present, instead of having privileged accounts hanging around, maybe they simply shouldn't exist, or at least not exist until you need them.

That's where Privileged Access Management (PAM) comes in. Netwrix SbPAM can remove privileges from your accounts until the exact point at which you need to use them; it can even orchestrate privileged accounts on-demand to reduce your exploitable attack surfaces and remove them at the end of your session.

Elite Security with All Necessary PAM functionality

Netwrix SbPAM is the only Zero Standing Privilege (ZSP) solution to also offer all necessary PAM functionality, including discovery, session management and secrets/credential management. Its endpoint component allows users to run applications that require privileged access directly from their desktops, removing the need for RDP. Furthermore, the product removes the RDP attack surface when it is not in active use.Because Netwrix SbPAM is built around a ZSP approach and the principle of Zero Standing Privilege applied in every aspect of the product's feature set.

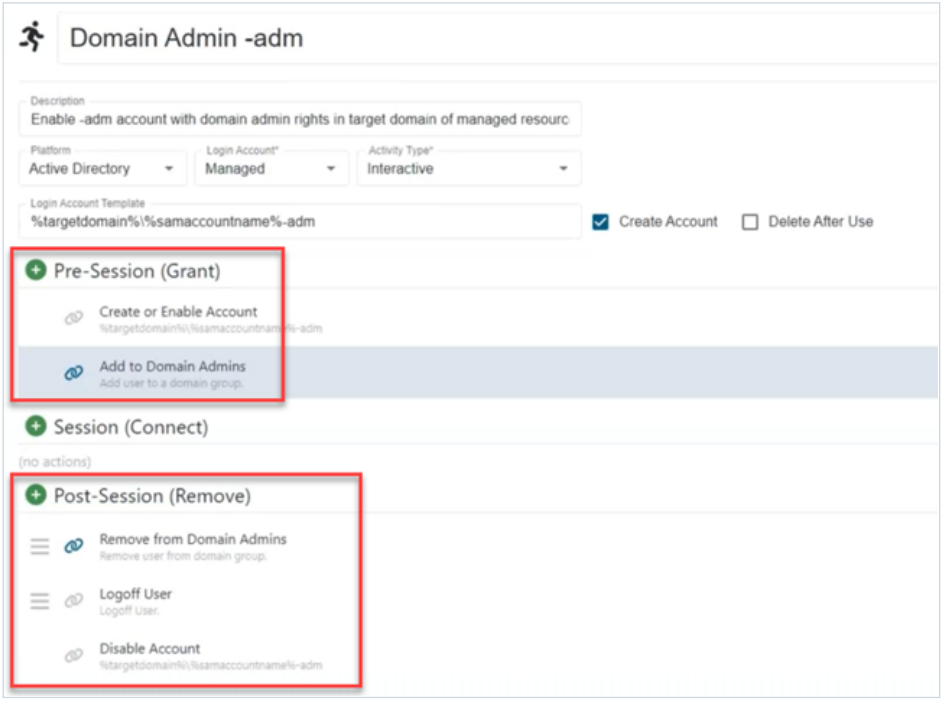
Netwrix SbPAM Utilizes On-Demand Domain Admin Accounts

Need to modify AD group membership for an employee? Now your domain admin can do so from their own laptop while remaining logged on as their standard user account. This isn't your typical "right click: run as administrator."

Consider this more secure workflow using Netwrix SbPAM:

- The admin selects a privileged tool they need to use; e.g., active directory users & computers.
- Netwrix SbPAM prompts them for login credentials and MFA
- Once authenticated, a brand new, "never existed before" domain admin account is automatically generated for the session
- Active directory users & computers is automatically launched under the context of the new domain admin account
- Once the task is performed, the admin closes active directory users & computers, and the privileged domain admin account is destroyed
- The session activity can also be recorded and archived

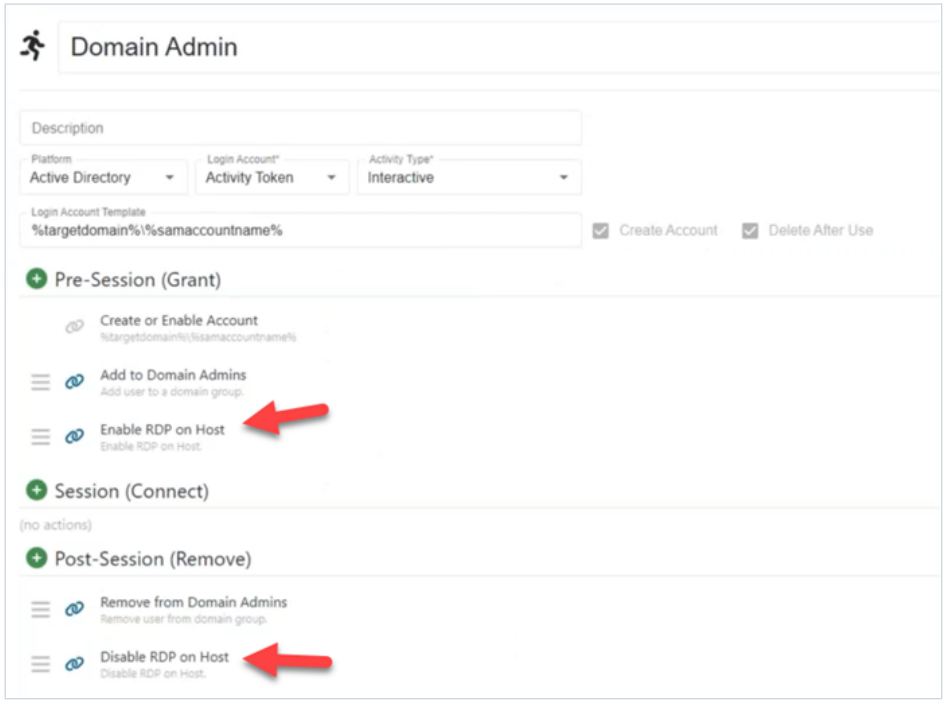
Netwrix SbPAM does this by assigning pre- and post-session actions. The screenshot below shows some options to create on-demand admin privileges in real time.



It's not just domain admins that can benefit from privileged access management. Software developers are ideal targets, as are backup operators, database operators, and server admins. Anyone with access to critical resources within your organization should have their elevated access reduced to a least-privileged state, which is easy to do with Netwrix SbPAM.

Netrix SbPAM Reduces Your Attack Surface

In addition to the attack surface exposed by standing privilege, Windows services that run 24/7 on your endpoints, such as RDP, are commonly exploited and should only be enabled when actively used. Netwrix SbPAM can dynamically turn endpoint services on and off such that they only run when required. The screenshot below outlines the process of enabling and disabling RDP.



Attack surfaces are often augmented by administrative activities that leave behind artifacts commonly exploited by adversaries; this includes malware propagation. While your enterprise depends on privileged activity for basic functionality, that privilege puts your organization at risk. This is why you must end the practice of retaining standing privileges within the enterprise; the shelf life of an escalated account or privilege should be as brief as possible to reduce the attack surface of your IT estate.

Faster Time to Value, Lower Total Cost of Ownership (TCO), and Greatest Ease of Use

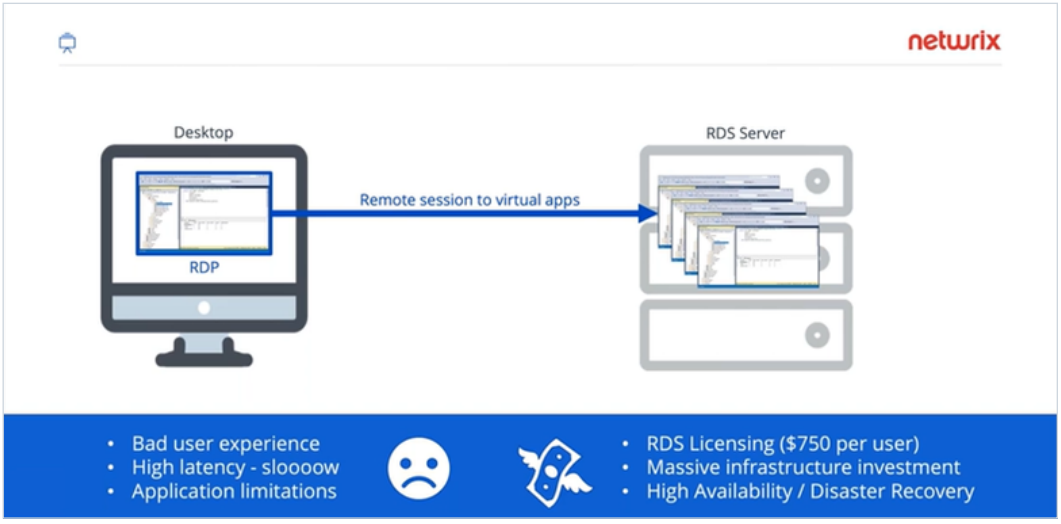
Netwrix SbPAM is built as ZSP from the ground up, meaning it is more reliable, cheaper to deploy, easier to set up, and requires much less infrastructure. Its orchestration capability allows the product to easily manipulate accounts (add, remove, enable, disable) and plug into organization's existing solutions, resulting in implementations that last days, not months. Because Netwrix SbPAM enables customers to run everything from the desktop, it reduces the cost of RDS infrastructure and Microsoft CALs. Furthermore, Netwrix SbPAM facilitates productivity and rapid adoption by utilizing a unique activity-centric card-based display, a single dashboard with all necessary information, and **direct integration** with users' existing desktop toolsets. Its seamless integration with other vault solutions incorporates credentials stored outside of the product and allows for customers and partners to build their own integrations for faster implementation. Lastly, Netwrix SbPAM is more flexible, extensible, and future proof than the competition because it is fully abstracted and designed on a microservices infrastructure.

The Value of Running Applications from the Desktop

With traditional PAM implementations, privileged applications are generally invoked on jumphosts or RDS infrastructure under managed privileged accounts.

Running applications remotely requires costly Microsoft CALs and additional infrastructure investment, as servers must have enough allocated resources to handle multiple personnel's workloads. This all adds considerable cost. The practice also expands the attack surface of a given session and introduces latency that degrades the user experience.

The visual below outlines the weaknesses that plague remote sessions with virtual apps.



Netwrix SbPAM provides administrators with a far easier approach. They continue to operate their privileged tools locally, on their desktop, using a managed account rather than accessing them remotely via RDS remote apps or jumphosts.

With Netwrix SbPAM, a standard user account can click on an app on their local machine and select "Run with Netwrix SbPAM" and get the job done locally without opening an application over a remote RDP session. With Netwrix SbPAM, you can even specificy which machines an admin may operate your most privileged tools from, such as a designated company-assigned laptop. All this takes place with no change in application functionality for the user, while ensuring that the utilized privilege isn't exposed when in use.

The desktop control is introduced when Netwrix PolicyPak is placed on it via its simple installer and managed using existing tools like Group Policy.

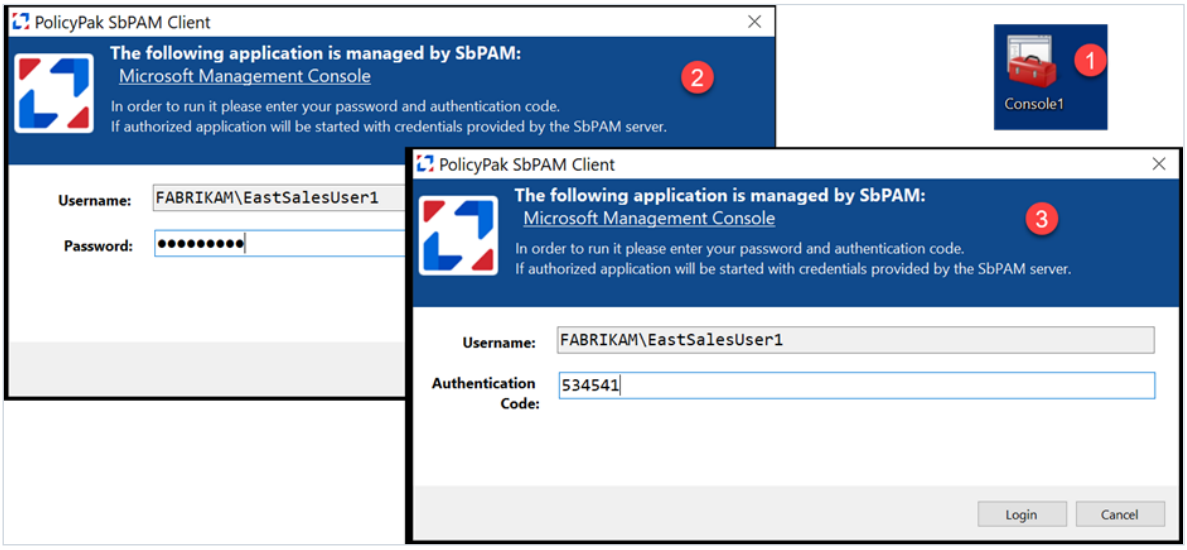
But let's jump to the "end of the story" and show you the final experience and result.

Final Experience and Result

Here you will see what the final experience and result look like when someone wants to run something privileged from their workstation rather than remote control into a server to operate.

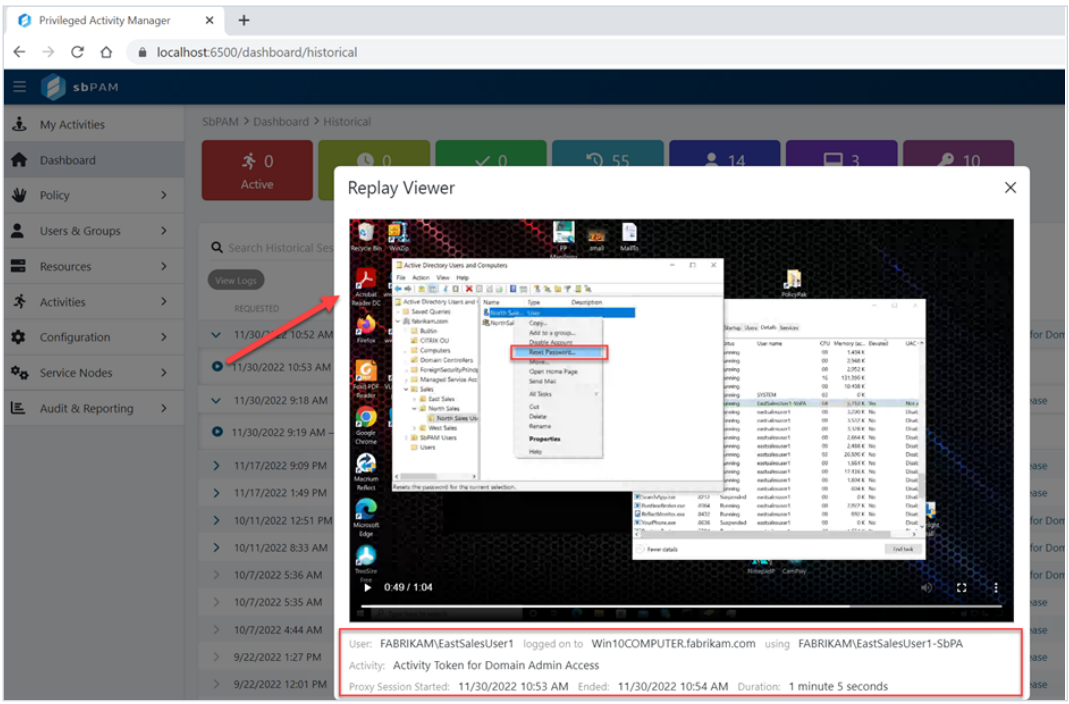
In this example, when users go to use a privileged tool (1), they are prompted to re-enter their login credentials (2), plus an optional 2fa code (3) using the dialog below.

The Netwrix PolicyPak client traps the request and sends the credentials to the sbPAM server for processing.



This one-two combo confirms the identity of the user requesting privileged access, and it assigns accountability. Temporary privileged accounts can be created using the PAM account name of the requesting user so they can be readily identified. This is particularly useful for shared admin accounts because now you know the identity of the person behind each session.

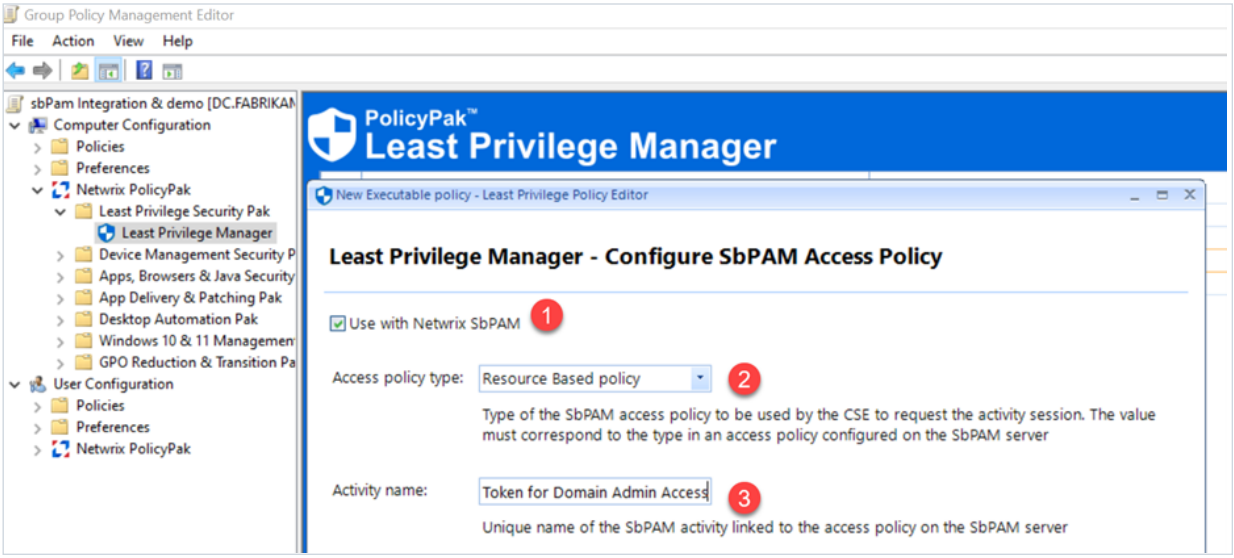
Then, the activity occurs, like running Active Directory Users and Computers and managing DNS and databases. All the while, as seen in the screenshot below, Netwrix sbPAM records the video from all requested sessions. Then, you know exactly who did what with those credentials. This creates easy-to-pull audit trails for auditors and investigators.



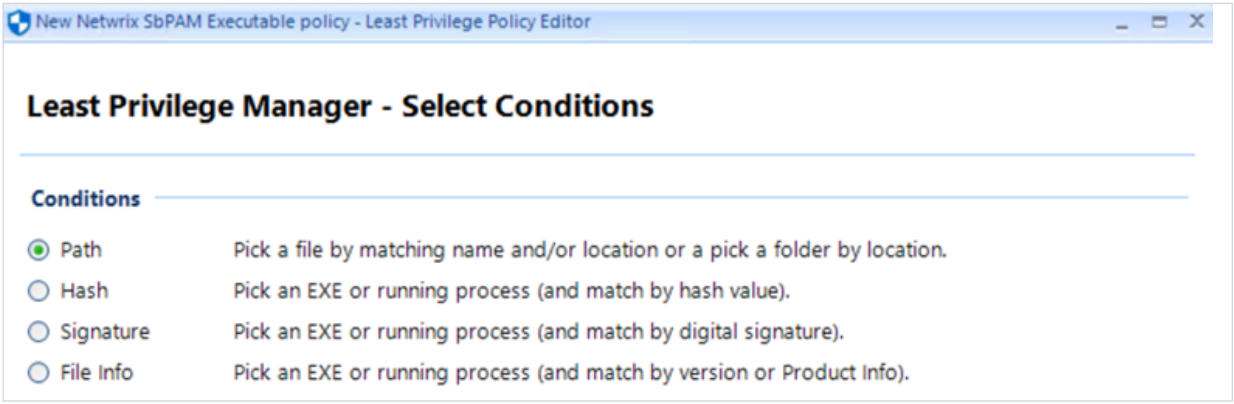
Setting Up sbPAM Example

A big step toward reducing the attack surface of your domain would be terminating where domain admins must remotely manage items directly upon domain controllers. Let's do just that. For this example, we will use "Active Directory Users and Computers."

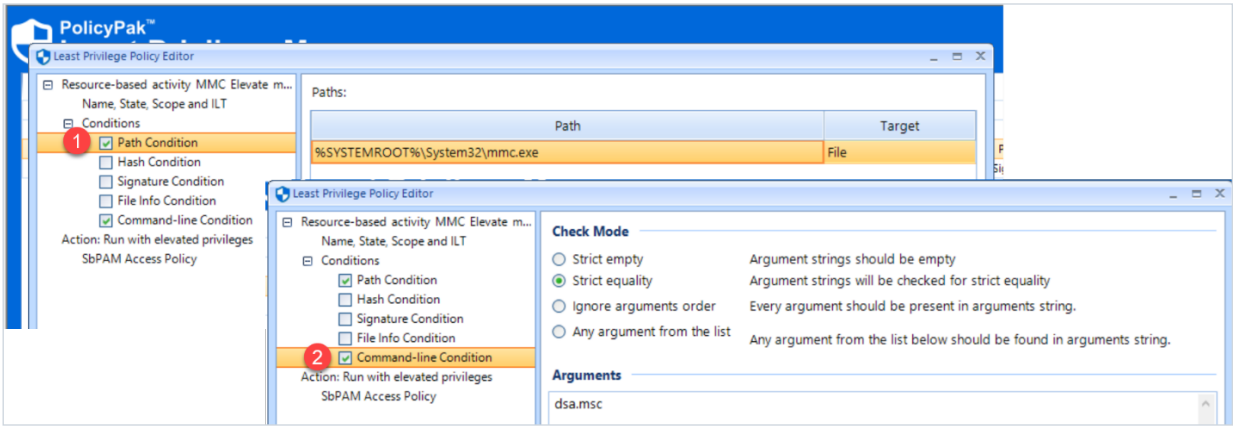
To set up an application like Active Directory Users and Computers to be privileged, you need only configure it using the Netwrix PolicyPak Group Policy UI. Simply (1) state that the rule should be joined with Netwrix sbPAM, (2) specify the policy type, and (3) specify the activity name, which also must exist in Netwrix sbPAM.



Then, choose to create a file path condition.

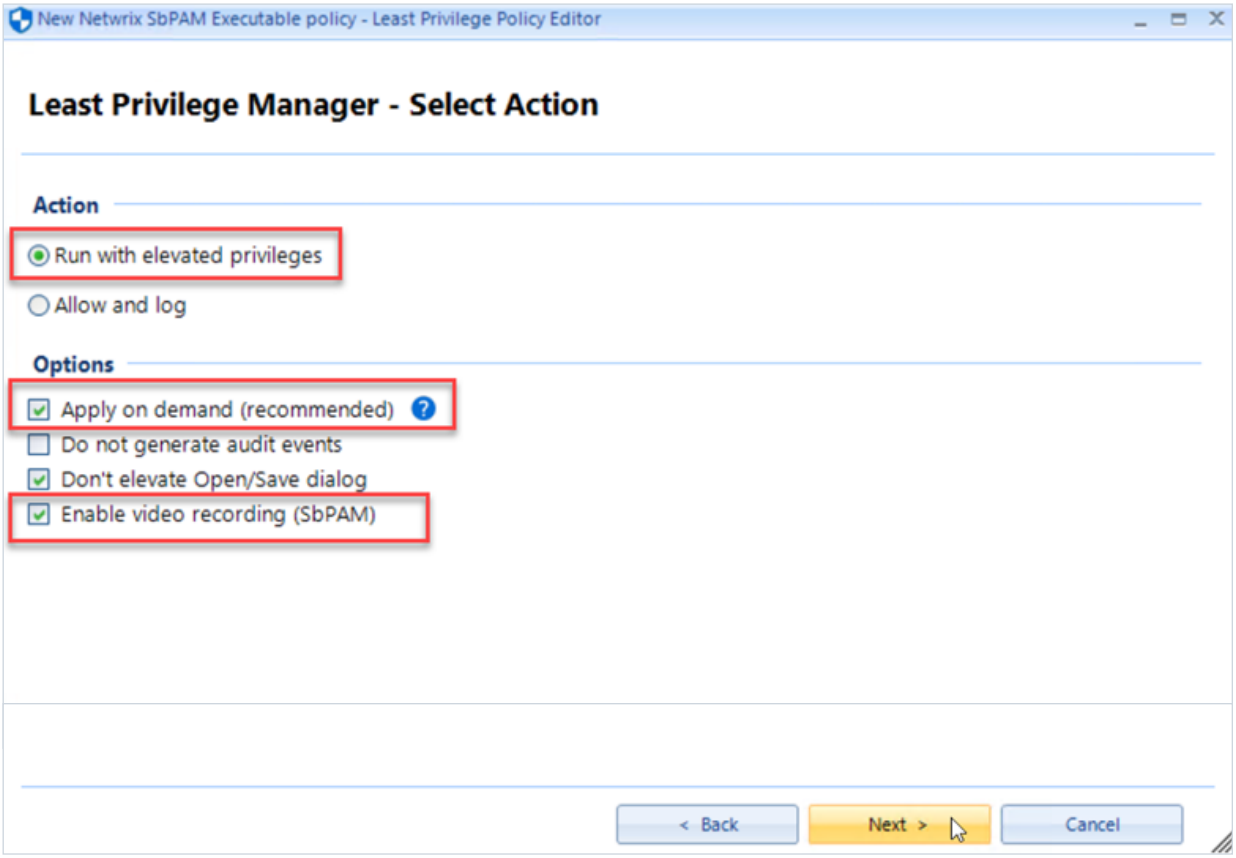


Then, specify the MMC.EXE executable and DSA.MSC arguments.



Then, make your choices on what to do when the application runs.

In this example, the application will be run with elevated privileges (which come from the assigned admin account configured earlier.) The "Apply on demand" selection means that if the user double-clicks on an applicable application, it will run under the standard privileges of the current user. Enabling video recording ensures that Netwrix SbPAM records the entire privileged session.



You can watch a video demonstration of how you can run applications under different active directory credentials by pairing up PolicyPak Least Privilege Manager and SbPAM.

Watch this video demonstration showing how you can create policies using Least Privilege Manager to record privilege sessions with SbPAM video.

Next Steps

If you are a Netwrix SbPAM customer, you will appreciate the simplicity Least Privilege Manager delivers by assigning remote privilege policies to designated users. There is no need to manually approve elevated privileged requests in real time. Create a policy in minutes, automatically deliver it, and it's done. Leverage the power of zero-trust security to ensure that every Windows workstation and server is locked down. If you are a PolicyPak customer, you can expand least privilege security protection to remote resources, not just local machines, thanks to SbPAM integration.

Netwrix SbPAM and Netwrix PolicyPak Least Privilege Manager work in harmony, securing and protecting your enterprise.

Stop leaving privileges available for attackers to compromise and insiders to misuse.

Find out more about how the Netwrix security duo of SbPAM and PolicyPak Least Security Manager can take your enterprise security to the next level with distributable, on-demand privileges.

Schedule a demo

Request quote

Corporate Headquarters:
6160 Warren Parkway, Suite 100 Frisco, TX, US 75034
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

netwrix.com/social