Securden

Endpoint Privilege Manager (EPM)

Best Practices for a Smooth Rollout

Best Practices for a Smooth Rollout

Endpoint Privilege Management (EPM) is an essential security initiative; however, its implementation often faces internal resistance and friction. Users frequently feel that their rights are being taken away, leading to concerns that they will need to rely heavily on the help desk and that their productivity will suffer.

It's important to note that the EPM initiative is not a one-time deployment, such as installing antivirus software. Instead, it is a comprehensive program that requires ongoing effort, adjustments, and buy-in from stakeholders. Engaging all stakeholders at the appropriate times and adequately preparing end users for the changes are critical factors that contribute to the successful implementation of EPM and broader security objectives.

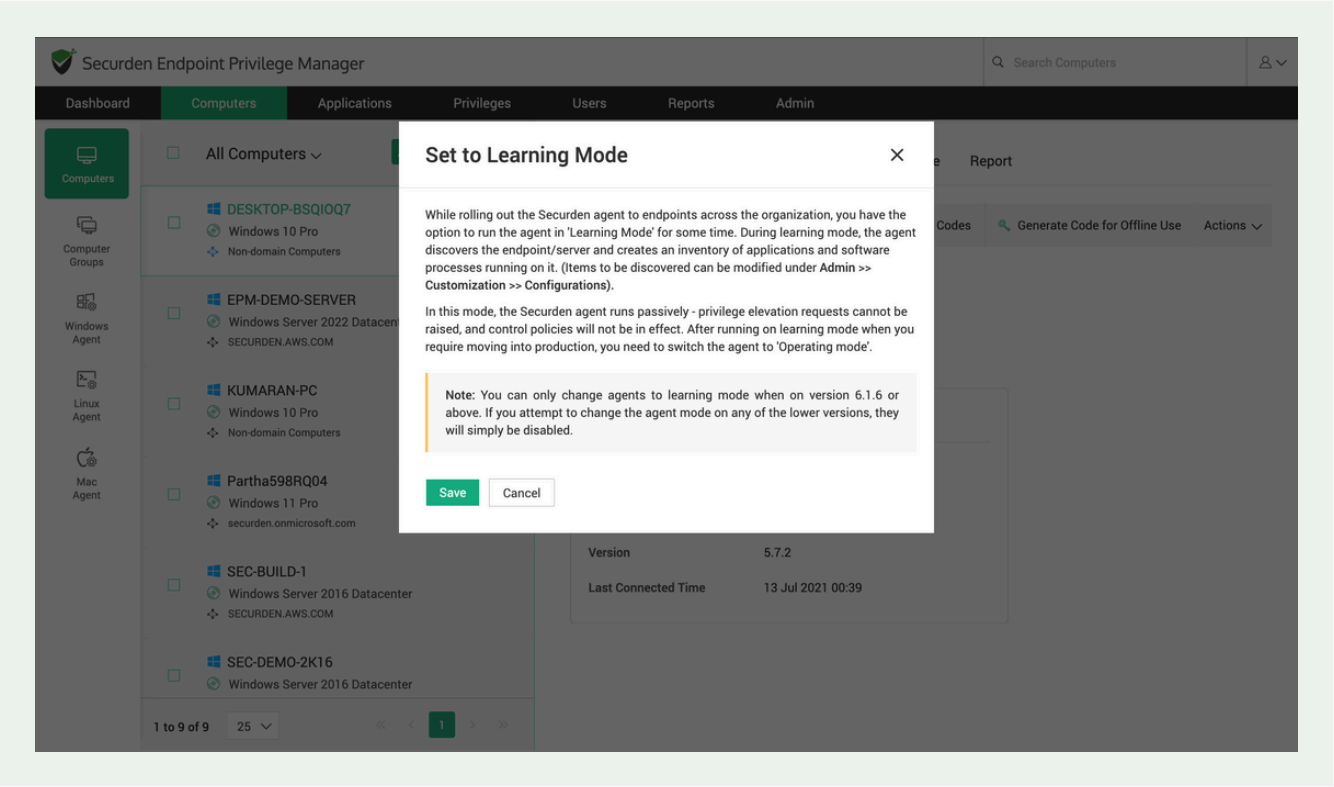
To ensure a smooth implementation and rollout, here is a compilation of best practices. Successful implementation can be divided into three phases:

- **Preparatory Phase**
- **Involving Key Stakeholders**
- **Rollout in Phases**

Preparatory Phase

Run Securden EPM in learning mode

After signing up for **Securden EPM**, run it in learning mode for a couple of weeks. During this learning phase, Securden EPM will discover all applications and processes that are currently in use in your environment. By the end of this period, you will have a complete inventory of all applications.

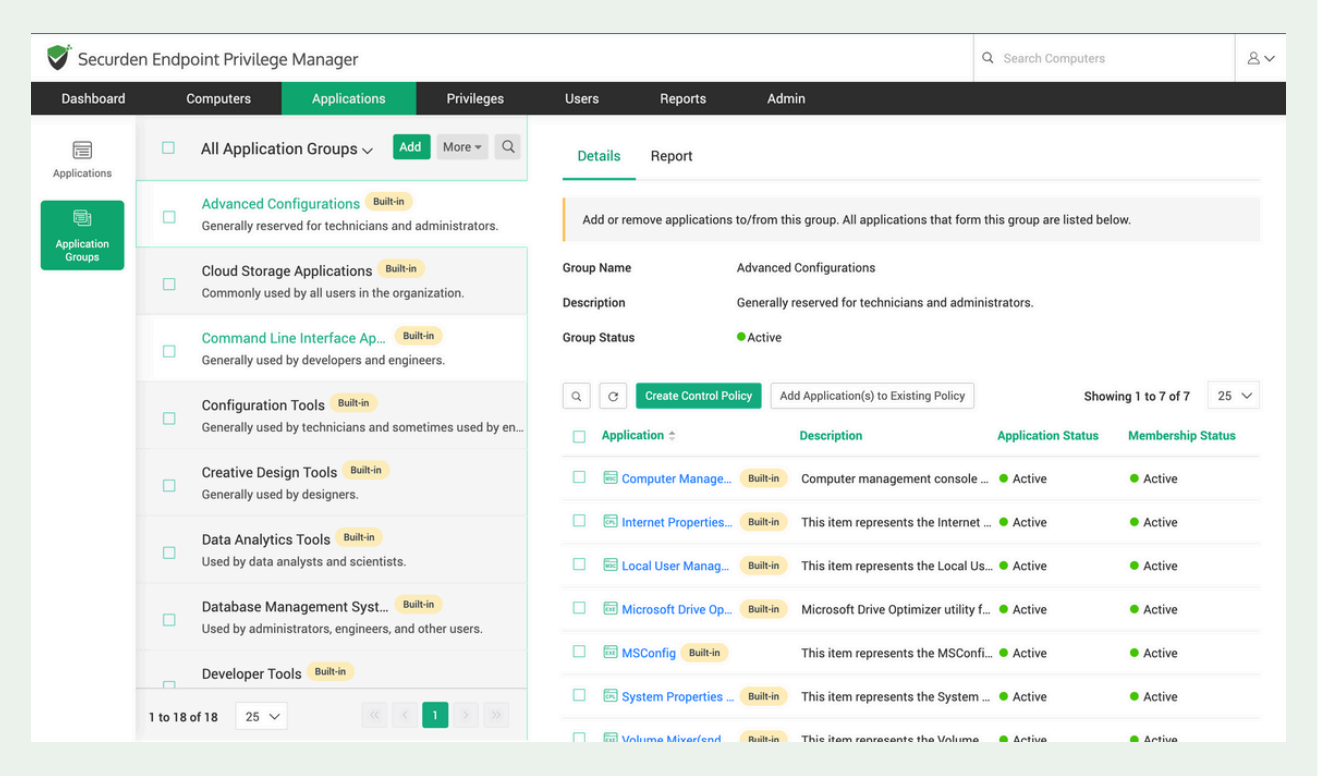


Review the applications

You can conduct a thorough review of the discovered applications and flag any unwanted ones.

Review application groups

You will have the need to allow applications as groups based on various criteria. The most common scenario is grouping the applications based on the vendor or the publisher - for example, “All Microsoft Applications”. Securden EPM automatically creates application groups to address these common use cases based on the applications discovered in your environment. Please review the application groups

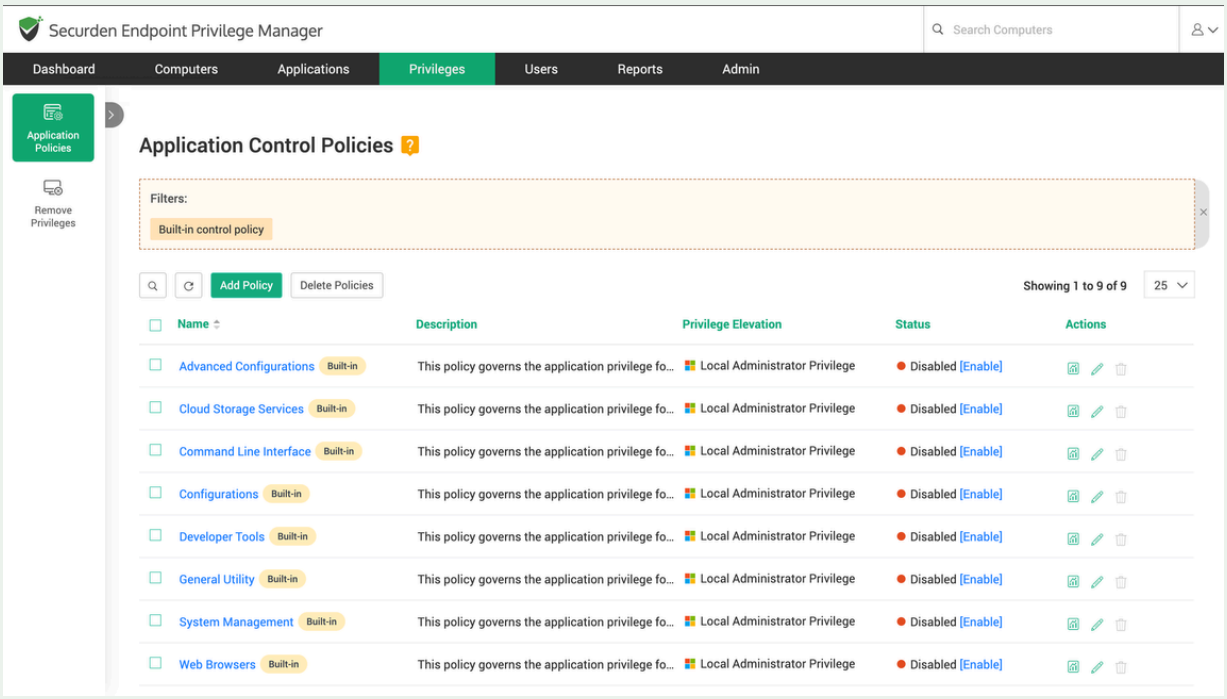


Prepare a list of common operations

Compile a list of common tasks users perform daily, such as installing applications, updating device drivers, running specific diagnostics etc.

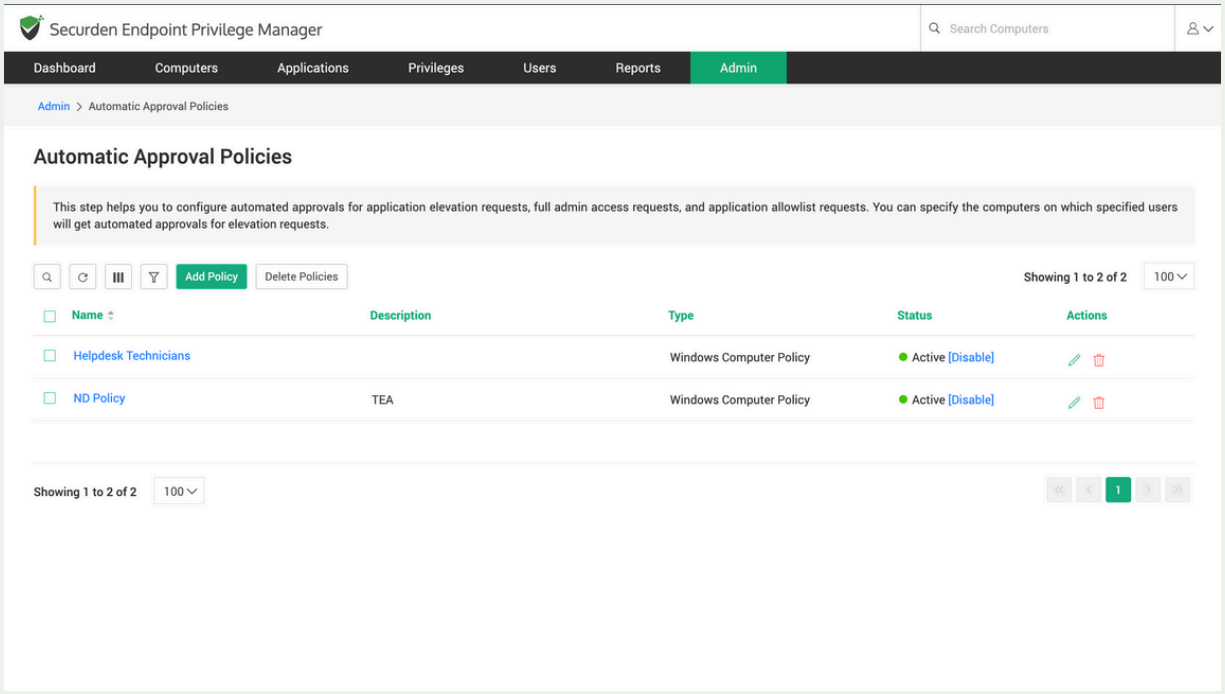
Automatic policy creation

When you deal with a large number of applications, some kind of automation comes in handy in creating control policies. Securden offers a list of automatically created control policies. These policies may help you handle some common elevation scenarios.



Automated approvals

A common concern among stakeholders relates to the approval process for requests. Approvers often dislike taking on additional burdens, while end users expect approvals to happen quickly. To address this challenge, Securden provides options for automated approvals based on various criteria and analytics. Utilize this feature to minimize internal friction.



Carefully consider breakglass scenarios

The primary objective of deploying the EPM is to enforce the principle of least privilege while ensuring productivity remains unaffected. It's essential to have adequate measures in place for emergency situations, such as when an administrator at a customer site needs urgent administrative access. Securden provides features for emergency access. Be sure to evaluate these features and implement them as needed.

Run a pilot

Before engaging a larger group of stakeholders, begin by implementing a pilot program within the IT administration team. Develop policies and start using the product. This approach will help identify potential issues from the end-user perspective and allow for the refinement of the policies.

Involve Key Stakeholders

Once you have a smooth-running pilot, you can involve a larger group of stakeholders, including department heads and end-users. Demonstrating the pilot is the best way to initiate this dialogue.

By showing them a version that operates effectively within your environment and highlighting its ease of use, you can quickly gain their support. Their input will be valuable in shaping the implementation process and ensuring that the solution meets the needs of various teams.

Rollout in Phases

Once you have secured buy-in from stakeholders, plan the rollout of the EPM solution in phases. You can group departments with similar use cases together and create multiple groups. Roll out the EPM solution to one group at a time, allowing for adjustments and refinements based on feedback from each phase. This gradual approach can help reduce feelings of overwhelm and resistance.

Organize an open day

Before starting the rollout phases, host an open day and invite stakeholders from all teams to participate in a trial run of the solution. This event will help identify any potential issues that need to be addressed and prepare the team to embrace the upcoming changes.

Organize short training sessions

Although specialized training is not required for product usage, it is important to conduct short training sessions for end users to help them adapt to the changes.

Support and resources

During the rollout phases, make sure teams have access to sufficient support resources. In addition to help desk assistance, this should include documentation and tutorials.

Securden support is here to help you

During the rollout, Securden support team will be available to address any unexpected issues you may encounter. If you inform us of your schedule in advance, we can assign a dedicated support engineer to assist you.