Securden

Endpoint Privilege Manager (EPM)

Deployment Guide

Recommended Measures and Configurations for Deploying Securden Endpoint Privilege Manager

Securden Endpoint Privilege Manager provides foundational endpoint security for organizations working with Windows, Mac, and Linux endpoints. Enforcing security best practices at the time of installation, deployment, and operation of the endpoint privilege manager can help secure the endpoint and network.

This guide is split into three sections. The sections are.

1. **Recommendations for Installing Securden EPM**
2. **Recommendations for Rolling Out the EPM Solution**
3. **Recommendations for Efficient Privilege Management**

Recommendations for Installing Securden Endpoint Privilege Manager

Securden Endpoint Privilege Manager is delivered as a binary package when you purchase an on-prem license. You can install the EPM server on any Windows server that satisfies the minimum requirements. Optionally, you can host the server on any virtual machine or your private cloud instance. The installation is simple and can be completed in less than 5 minutes. The recommended server specifications are listed below.

Recommended Server Configurations

Server Operating System	**Minimum:** Windows Server 2008 R2 and later. **Recommended:** Windows Server 2019 or later.
Memory and Storage	8 GB RAM and 50 GB Free Hard Disk Space in each machine.
Backend Database	PostgreSQL by default. **Recommended:** MS SQL Server 2019 or later.
Web-Interface	Chrome, Firefox, Edge, Safari, Internet Explorer 10 and above in endpoints.

Deployment Pre-Requisites

1. **SMTP Server:** Securden EPM uses the email service for sending out alerts, reports, etc. You need to create a dedicated SMTP server for Securden or configure API based email service integration with Gmail or Outlook.

2. **DNS:** A public DNS must be created for Securden EPM to register the server's name with the IP address.

3. **SSL Certificate:** A public SSL certificate needs to be installed on the application server to authenticate and encrypt connections between user devices and the EPM server.

4. **Ports Used:** The list of all firewall port settings that must be configured is available in the table below.

Port Name	Port Used	Source	Destination
PostgreSQL Database Port	5252 (TCP)	Primary, Secondary, and all Application Servers	PostgreSQL Server
MS SQL Database Port	1433	Primary and Application Servers	MS SQL Server
Securden Server Port	5151	To all Users (End Machines), Agents, and Secondary Servers	Primary
SMTP Sever Port (Mail Server Port)	587 (TLS) 465 (SSL)	–	–
AD Domain Controller	636 (TLS/SSL) 389 (No SSL)	Primary Server	Active Directory Domain Controller
RADIUS Server Port	1812	–	–

Recommendations for Rolling Out Securden EPM to End Users

Once Securden Endpoint Privilege Manager is installed, you need to deploy the agents on the endpoints that need to be governed using the EPM solution. Rolling out the endpoint privilege manager includes installing the agent on endpoints, discovering the applications being used, understanding the use of admin rights by users, and creating policies to support the workforce while fully enforcing the security measures. While rolling out the Securden Agent on endpoints in your network, adhere to the following recommendations for a smooth experience.

1. Create a Plan for Installing the Securden Agent

The Securden agent must be installed on all endpoints that need to be managed using the EPM. These might run on Windows, Mac, and Linux. Securden provides the installation package for each operating system separately.

The Securden Agent can be pushed to domain joined Windows machines from the central server through integration with Active Directory and Azure AD. Securden also supports installation of the agent through GPOs and SCCM for large deployments.

However, for non-domain Windows devices, and devices running on Mac and Linux, the agent must be manually installed or deployed through a patch management solution.

Given the options, it is important to have a plan of action to cover all the required devices in your deployment plan.

2. Ensuring Connectivity from Endpoints to EPM

Once the agents are deployed on the endpoints, they connect with the EPM server to fetch policies, manage requests, report application usage data, among other critical functions. The agents can work with the latest information if connectivity with the server is severed. However, it is advisable to ensure that the agent on the endpoint is able to reach the server at the set time interval for critical functions such as request based admin access to work seamlessly.

3. Permissions for Connecting to Active Directory and Azure AD

If you are using Active Directory or Azure AD (Entra ID), you would have to grant Securden EPM the permissions required for importing users and devices. In Active Directory environments, you need to provide the username and password of a user account with the delegated permissions to read the entire directory. You can also enforce Active Directory port verification before connecting to the AD.

Navigate to **Admin >> Configurations** and find **AD Port Check** under **Miscellaneous**. You can enforce this option to enforce AD port verification before initiating connection.

If you are using Azure AD for this purpose, you need to grant the following API permissions to the enterprise application you create for Securden. You can refer to the detailed steps in the administrator's guide.

- **User.Read.All**
- **Group.Read.All**
- **Domain.Read.All**

Once the required domain devices are onboarded, you can install the Securden Agent on these endpoints.

4. Enforcing Device Validation

When importing and synchronizing computers from AD, you have the option to validate the device being imported. Sometimes, the active directory might retain the computer details of devices that have been removed and devices that don't physically exist.

If validation is enforced, Securden will not import ghost machines that do not exist outside the Active Directory.

Navigate to **Admin >> Configurations** and find **Validate Devices During Import**.

5. Ensuring that Tamper Proofing Measures are Enforced

The Securden Agent is installed on the endpoints, and it monitors and governs local administrator privileges. Securden provides measures that prevent users from uninstalling the Securden agent. Apart from these measures, you can enforce authentication for uninstalling the Securden agent.

Navigate to the **Admin >> Configurations** in the web interface and find the **Agent Uninstall Workflow** under the **Agent Configuration** tab. Enforce this option and provide a password/passphrase for uninstalling the Securden Agent.

6. Road to Eliminating Admin Rights

Before removing admin rights, you need to enforce measures in place that would take care of end user needs to run certain applications with admin rights.

Agent Learning Mode

To get the most accurate insights on application usage, you need to gather data from the endpoints. The Securden Agent can run in learning mode where the agent simply collects data on admin rights usage and application usage.

Application Repository

Before creating new application control policies ensure that all the applications that are regularly used by employees are added to the application repository. The agent automatically onboards applications when in learning mode. If anything needs to be added, you can add them manually from the **Applications** tab in the web interface.

Creating Policies

You can create policies that would elevate the privileges of certain approved applications or make use of the built-in policies as a quick solution. These built-in policies can help in the short term, but it is advisable to create policies of your own from insights derived from the different reports accessible from the web-interface.

Removing Admin Rights

Once the policies are pushed into effect, you can go ahead and remove admin privileges from the local accounts. When removing admin rights, you can create an exclusion list and demote every other user account across the organization.

This way, you would know for sure which accounts have admin rights.

Recommendations for Efficient and Secure Privilege Management

Once admin rights are removed, users would be able to elevate applications through policies that are in force. If they need to access an application that is not covered through policies, then they might raise a privilege elevation request with the EPM administrator.

To best streamline privilege management, we recommend the following settings and procedures.

1. **Assigning Designated Approvers**

   By default, whenever end users raise requests, the administrators in EPM are alerted through email. Only these users can approve or reject the request. However, in large enterprises a select few people cannot make a decision on these issues for hundreds and thousands of users.

   Securden allows you to designate an approver for individual users and groups. Once designated, these approvers will be alerted and will be able to approve and reject the request.

   This feature can be used to replicate the organizational structure in a team, where managers can manage their team members' requests. You have the option to retain the team hierarchy from AD when importing users. Go to **Configurations** page in the **Admin** tab, locate and enable **Retain Approval Hierarchy.**

2. **Creating Policies from Requests**

Whenever end users raise requests to gain access to an app or run them with admin rights or gain temporary admin rights for themselves, the administrator who approves or rejects the request has the option to create a policy for the request.

What this means is that if gone through with, any future requests would be automatically handled for this application. You can add the app to an existing policy or create a new policy for this application.

This simple step would eliminate the repetitive process of raising a request and approving it. However, from a security standpoint, this measure must only be reserved for applications that have been repeatedly featured in requests.

3. **Restricting Time for Elevated Access**

When raising a request, the end users specify the time parameters providing information on how long they need elevated access. You can restrict the maximum permissible duration that a user can raise a request from the **Configurations** page in the Admin tab.

Whenever the administrator or designated approver is approving the request, they can set a time limit they see fit for the task at hand. If the user needs admin rights for installing a simple tool and has placed a request for five hours, the approver can and is encouraged to limit the time to 30 minutes or an hour accordingly.

4. **Enforcing Multi-factor Authentication for Privilege Elevation**

You have the option to enforce multi-factor authentication for gaining elevated access, starting technician access, and gaining application access. You can configure MFA methods from the admin console and enforce MFA from the configurations page.

It is recommended to enforce MFA for privilege elevation for added security. You need to enforce MFA for request-based privilege elevation and policy-based privilege elevation separately from the configuration page.

5. **Limiting Login Attempts to Web-Interface**

   You can enforce a limit on the maximum number of unsuccessful login attempts a user is allowed to make. You can also enable captcha verification after a certain number of unsuccessful attempts.

   Upon reaching the maximum number of unsuccessful login attempts, you have the option to configure temporary account lockout. It is recommended to enforce this for security reasons.

   This prevents unauthorized access to the endpoint privilege manager interface.

6. **Time Limit for Technician Access**

   To prevent usage of domain admin credentials on endpoints, Securden provides technician access provisions that help technicians gain temporary admin rights when they login using their own standard user account on endpoints.

   You can enforce a time limit of each technician access session by navigating to **Admin >> Configurations** and locating **Restrict Time Limit for Technician Access.**

7. **Remove New Admin Users**

   When users gain temporary local admin rights, they can potentially create a user account and make it a member of the local administrator group. You can configure the Securden Agent to monitor the local admin group and remove new admin user accounts created by end users.

   Navigate to **Admin >> Configurations** and locate **Remove New Admin Users.** Enforce this configuration to automatically delete the newly created account.