Securden

Help Document

How to Onboard Computers?

Endpoint Privilege Manager (Cloud Edition)

About the Product

Securden Endpoint Privilege Manager (SaaS) is a solution that helps organizations remove local admin rights and enforce application control on endpoints that are present in the corporate network as well as remote devices. Hosted on the cloud, the solution works by communicating with the endpoints through a lightweight agent over the internet. You may deploy the agent on the endpoints you want to manage using the solution.

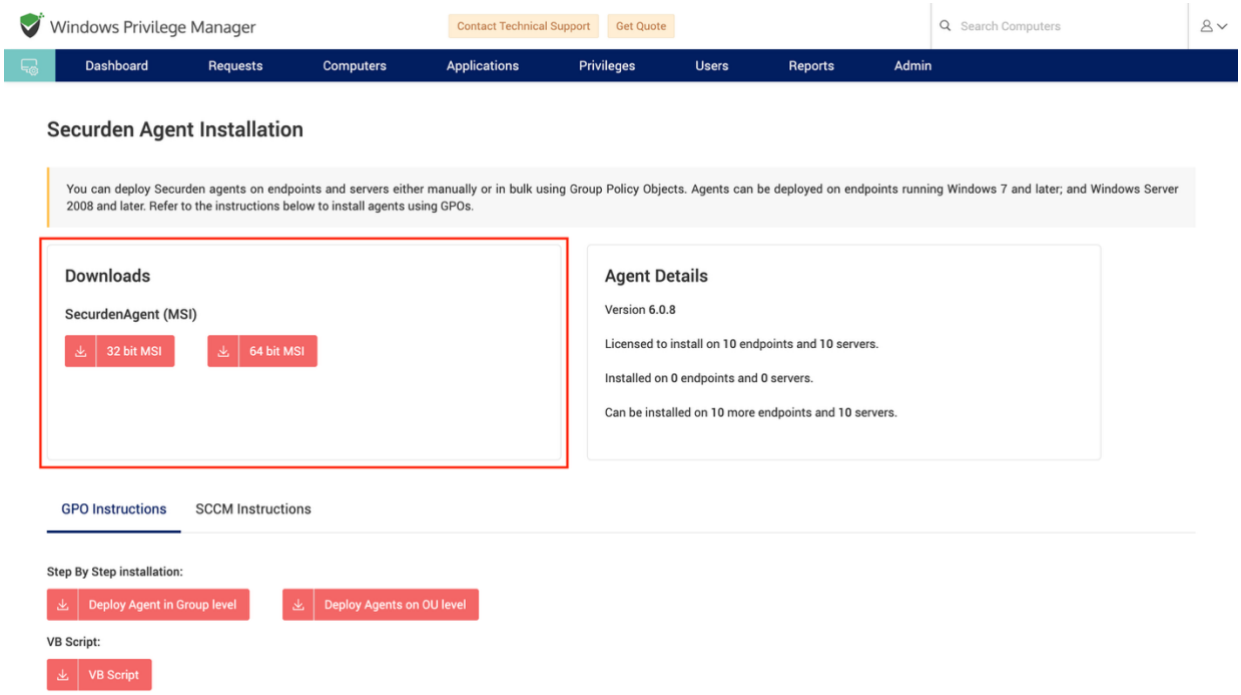
What is covered in this guide?

This guide covers in detail the steps required to onboard endpoints into Securden Endpoint Privilege Manager (SaaS). This guide covers topics including

1. How to onboard non-domain computers?
2. How to onboard domain computers?
    a. How to configure the Remote Connector?
    b. How to add an Active Directory Domain?
    c. How to deploy Agents on domain computers?

Onboarding Non-Domain Computers

To add computers to Securden, you need to deploy the agent on the required device. To deploy the agent on devices outside the Active Directory or Entra ID domain, you need to download the agent and install them on the required device manually. Navigate to the **Securden Agents** section to download the agent.



Once the agent is installed on a device, the computer will automatically be added to Securden. You may view the device by navigating to the **Computers** section.

Discovering Domain Computers from Active Directory (On-Prem)

To start managing privileges on AD domain computers, Securden needs to connect to your AD domain. Since Securden is hosted on cloud and cannot directly reach the AD domain running in your network, you need to deploy a lightweight remote connector on a device in your domain. Securden will connect to the AD domain through this lightweight remote connector.

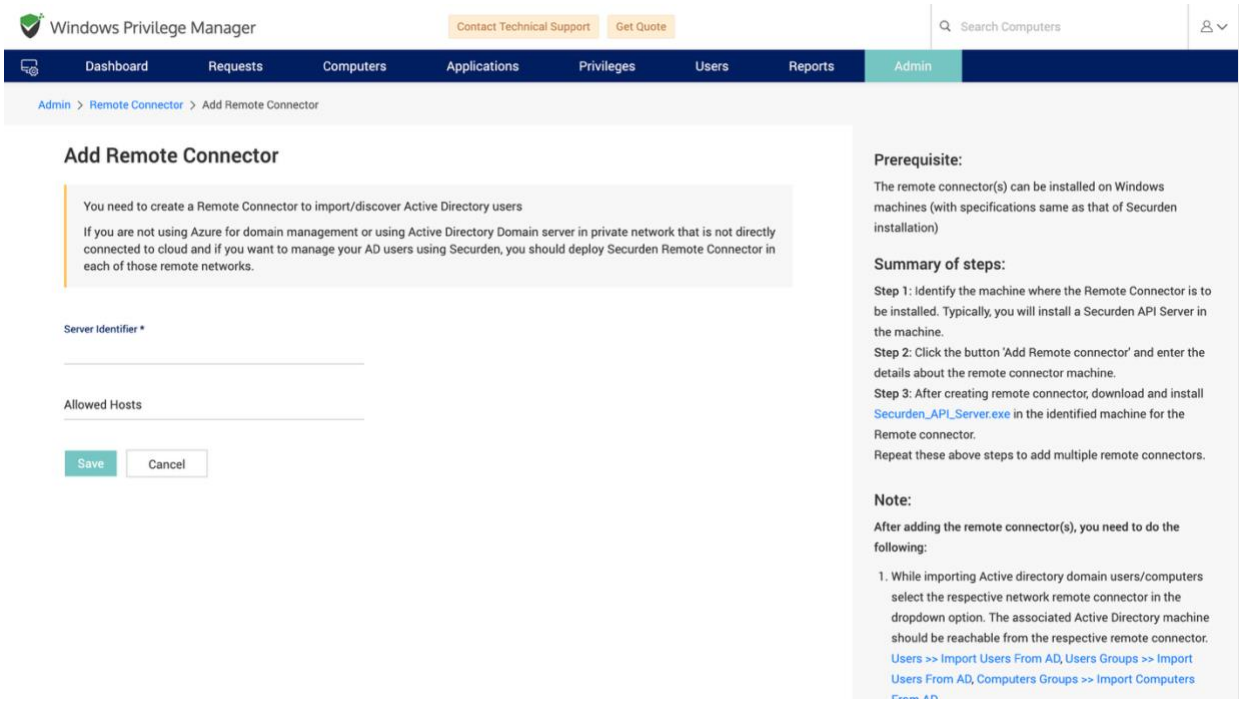
How to Configure the Remote Connector?

To configure this gateway device and deploy the remote connector, navigate to **Admin >> Remote Connector**.

Note:
The remote connector(s) should be installed on Windows machines (with specifications same as that of Securden EPM Primary Server).

In the Remote Connector section, the list of all available remote connectors along with their status will be displayed. You may click **Add Remote Connector** and create a new remote connector to be deployed on the required device.

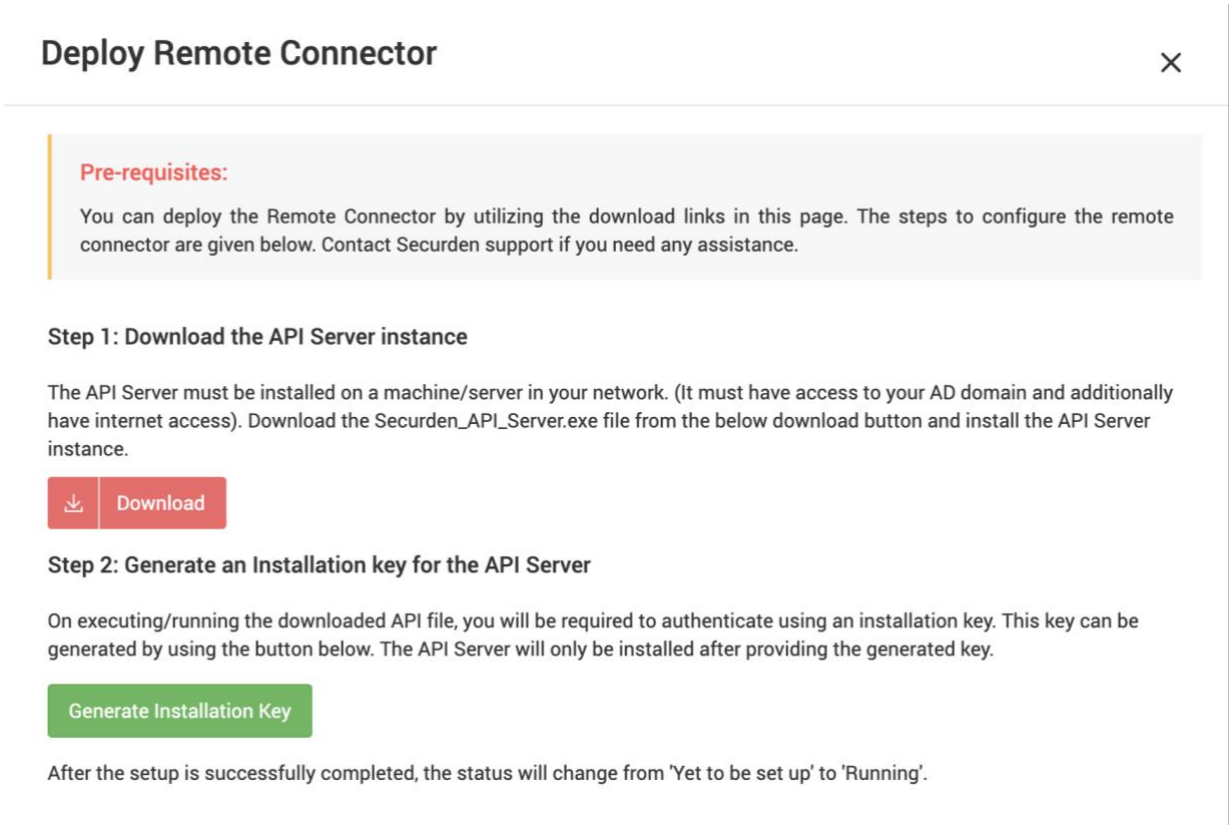
In the UI, you need to provide a unique server identifier for the device on which the remote connector will be deployed. The identifier will be used by the administrator for identifying the remote connector when configuring an Active Directory Domain.



Additionally, you have the option to restrict the remote connector to running from the designated server(s) alone. You can specify the IP addresses of the devices on which you want the remote connector to run. Once the required details are furnished, you may click **Save.**

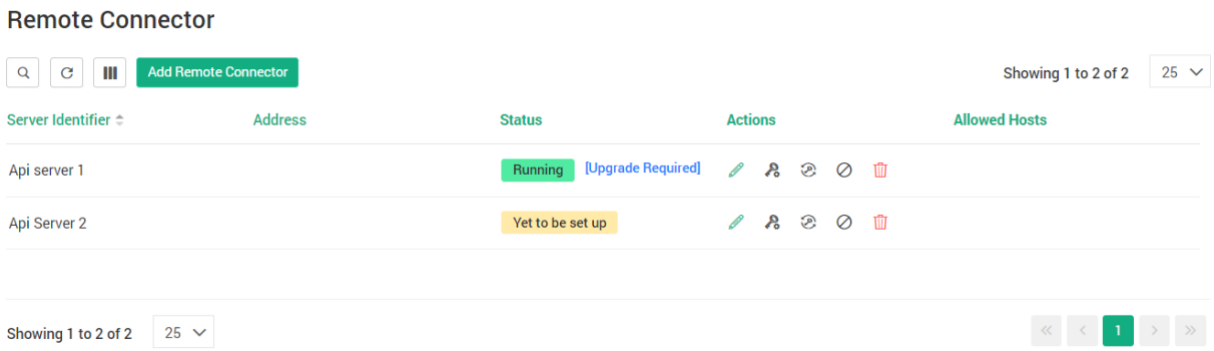
How to Deploy the Remote Connector?

Once the remote connector details are configured, you need to download the Remote connector (called *API Server*) package and deploy it on the required device.



Note: The Remote Connector must be installed on a machine/server in your network. (It must have access to your AD domain and additionally have internet access) Download the **Securden_API_Server.exe** file using the **Download** button and install it on the required device.

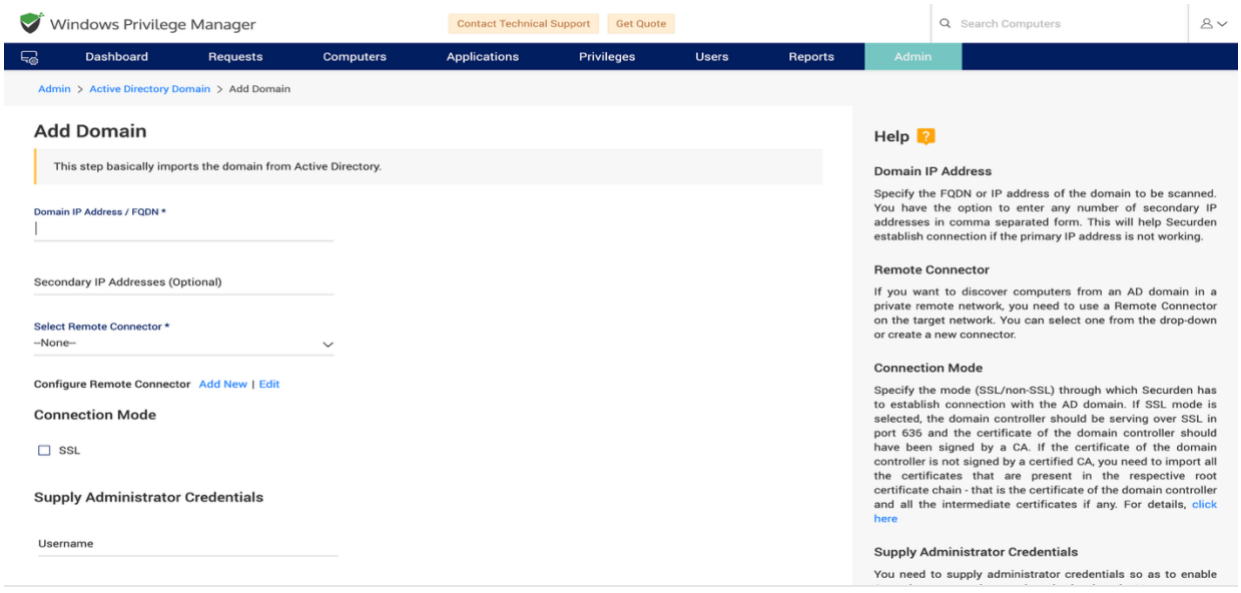
To install the Remote Connector (API Server), an installation key is required. You need to generate the installation key in this pop up and store it securely. The installation can be completed only if you provide the required installation key.



After the Remote Connector is installed, it will connect to the EPM server and become operational. You can verify that the remote connector is operational by checking the status of the remote connector. Make sure the status is displayed as **Running**.

How to add an Active Directory Domain?

Once the remote connector is up and running, you may add an Active Directory domain to Securden. Navigate to **Admin >> Integrations >> Active Directory Domain** and click on **Add Domain**.



In this interface, you need to provide all the required credentials to connect to the domain.

1. **Domain IP address/FQDN**

Specify the FQDN or IP address of the domain to be scanned. You have the option to enter any number of secondary IP addresses in comma separated form. This will help Securden establish connection if the primary IP address is not working.

2. **Select Remote Connector**

If you want to discover computers from an AD domain in a private network, you need to use a Remote Connector on that target network. You can select one from the drop-down or create a new connector. The device on which the selected remote connector is deployed should be part of the domain added.

Note: If the remote connector is not available in the list, you may add a new one by clicking **Add New**. If you want to modify an existing remote connector, you may click **Edit**.

3. **Connection Mode**

Specify the mode (SSL/non-SSL) through which Securden has to establish connection with the AD domain.

Note: If SSL mode is selected, the domain controller should be serving over SSL in port 636 and the certificate of the domain controller should have been signed by a CA. If the certificate of the domain controller is not signed by a certified CA, you need to import all the certificates that are present in the respective root certificate chain to establish trust between the browser and the self-signed certificates - that is the certificate of the domain controller and all the intermediate certificates if any. Follow the example below to import the domain controller certificate into the certificate store of the Securden server machine

The procedure explained below is just an example. However, you may use any procedure that you would normally use to import the SSL certificates to the machine's certificate store:

- In the Securden server machine, launch Internet Explorer and navigate to **Tools >> Internet Options >> Content >> Certificates**.
- In the GUI that pops-up, click **Install Certificate** and then choose **Local Machine** in the next step.
- Browse and locate the root certificate issued by the CA.
- Click **Next** and choose the option **Automatically select the certificate store based on the type of certificate** and **install.**
- Click **Import** again.
- Browse and locate the domain controller certificate.
- Click **Next** and choose the option **Automatically select the certificate store based on the type of certificate** and **install.**
- Apply the changes and close the wizard.
- Repeat the procedure to install other certificates in the root chain.

4. **Supply Administrator Credentials**

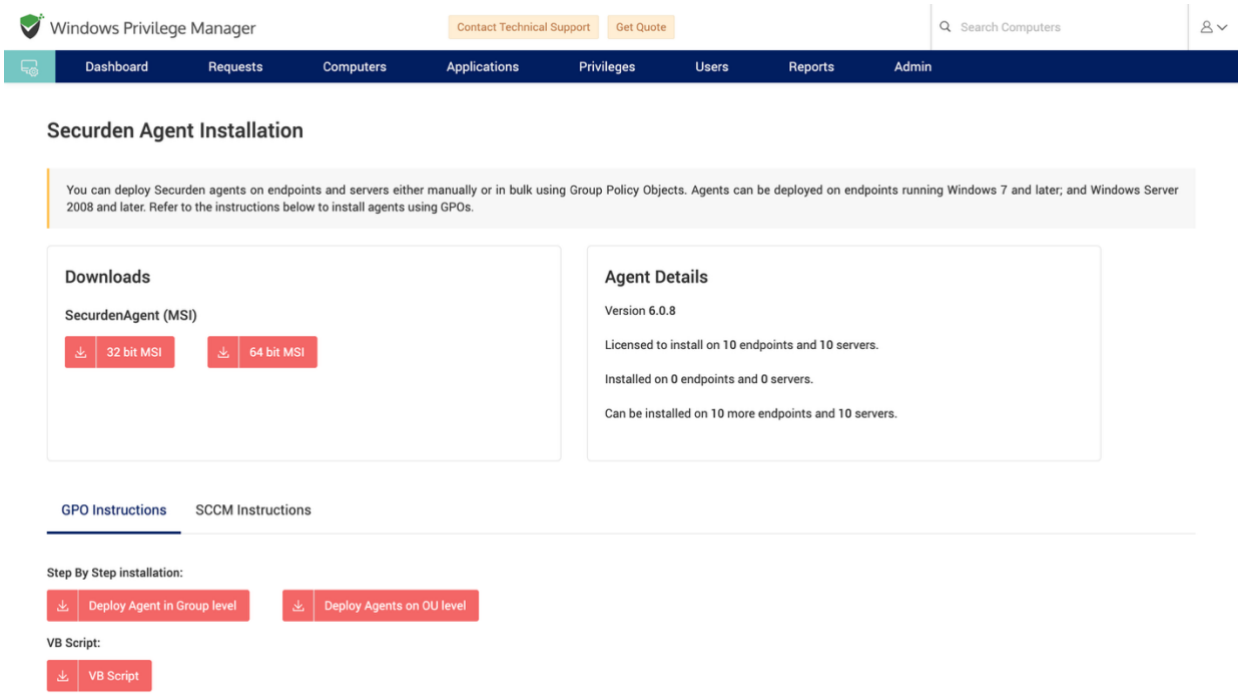
   You need to supply domain administrator credentials of the AD domain so as to enable Securden to import users in the domain. You may enter the domain controller credentials manually once and this will be stored in Securden for use during subsequent import attempts.

Once all the required details are added, click **Add Domain**.

Deploying agent on domain computers

Once the domain is added, you need to deploy the Securden agent on devices in the domain. You have the option to push the agent via GPO, SCCM, or manually install the agent on each device.

Navigate to the **Securden Agents** tab for additional information on deploying agents on endpoints.



After the agents are installed on the endpoints, the devices will automatically be enumerated in Securden. You may view them by navigating to **Computers** section.