Securden

Endpoint Privilege Manager (EPM)

Use Case Walkthrough

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:

1) 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.

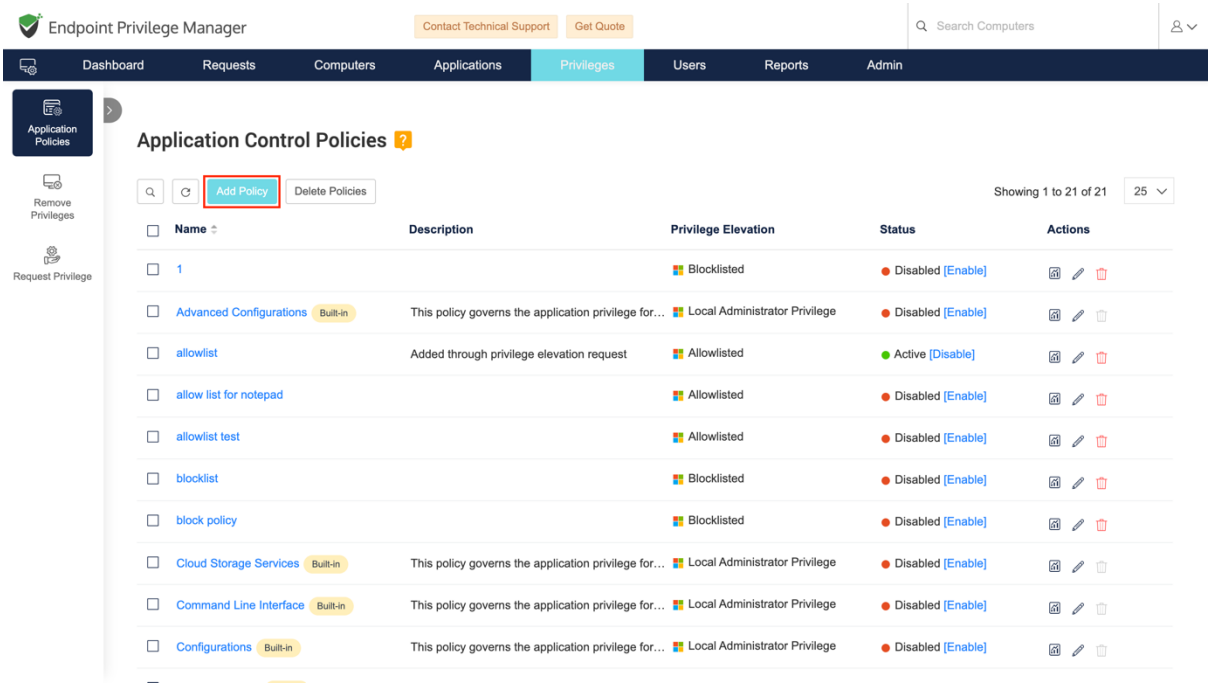
   a. If the required application is unavailable, then add the application manually. You need to specify the attribute using which Securden identifies the application during privilege management.

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

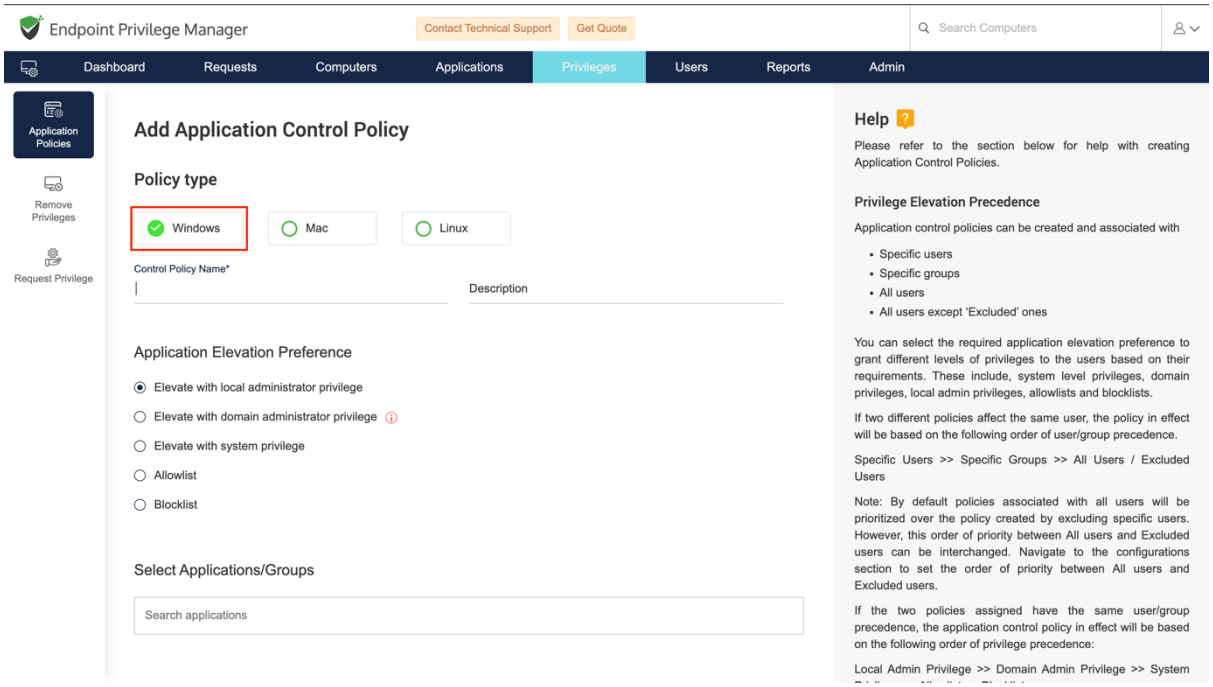
To grant the required permissions to users who might regularly need to run a specific set of applications with admin rights, Securden EPM Cloud Edition provides a policy-based privilege elevation provision. To test policy-based privilege elevation, follow the steps below

Step 1: Create a privilege-elevation policy

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

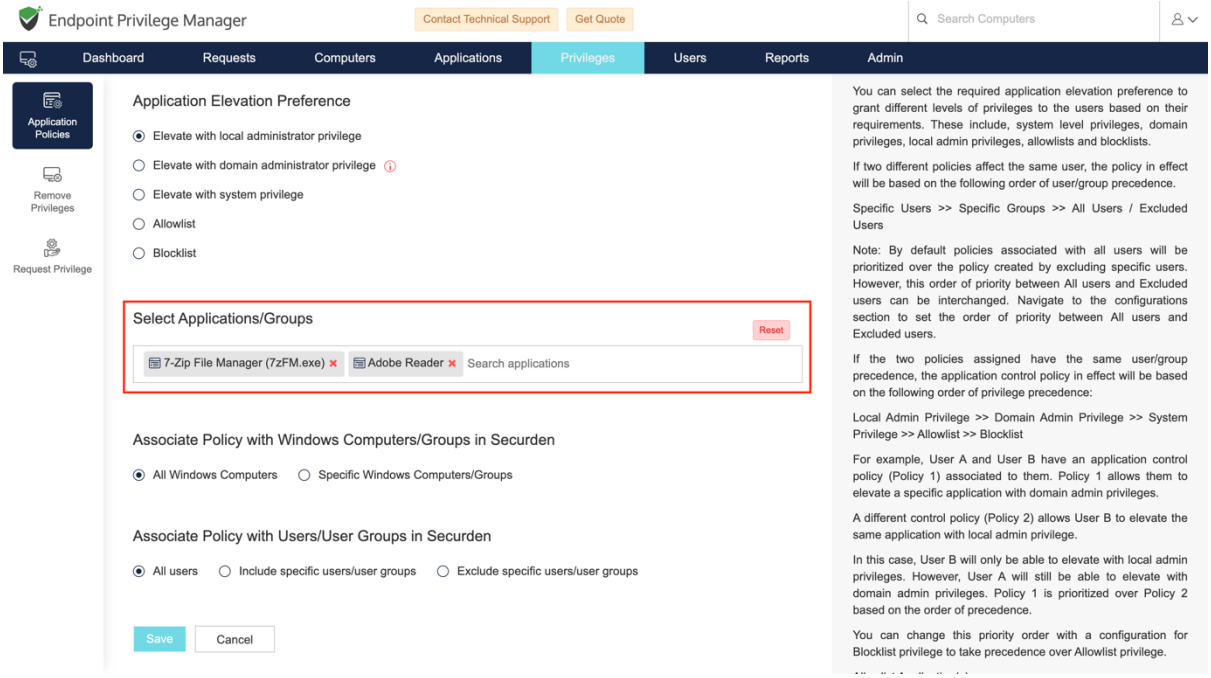


2. Select the policy type in accordance with the operating system on the endpoint. For explaining the process, we will assume that the endpoint is running on **Windows**.

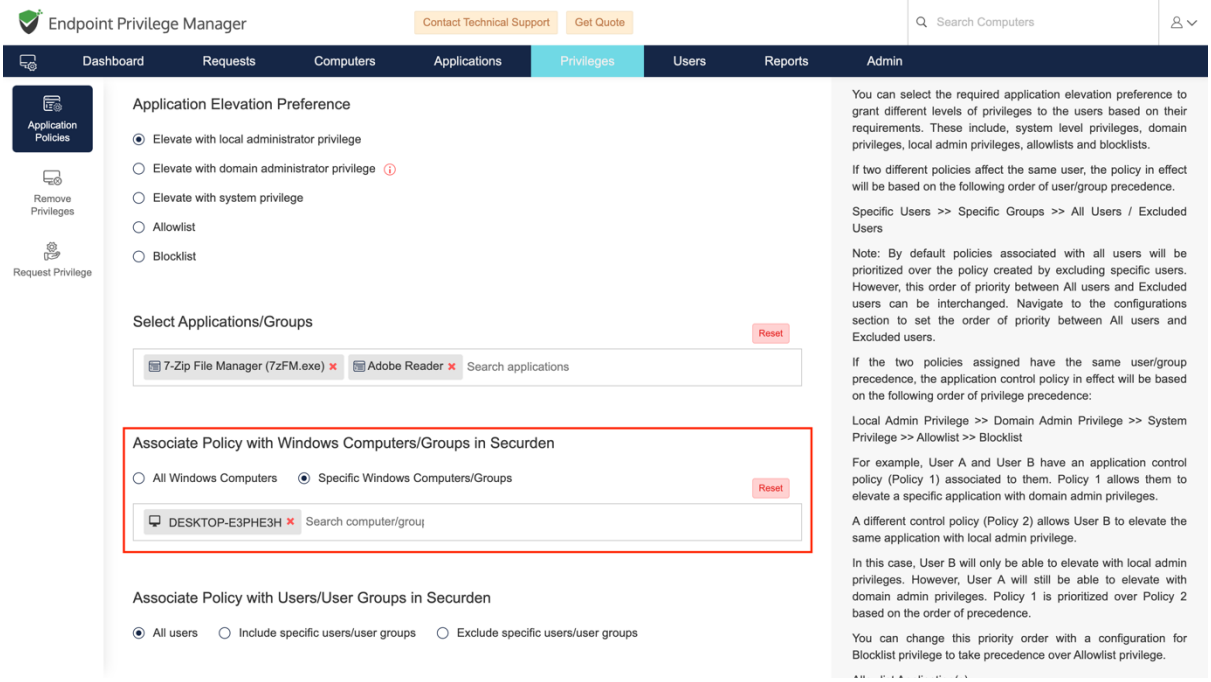


3. Give a suitable name for the policy for identification purposes.

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.

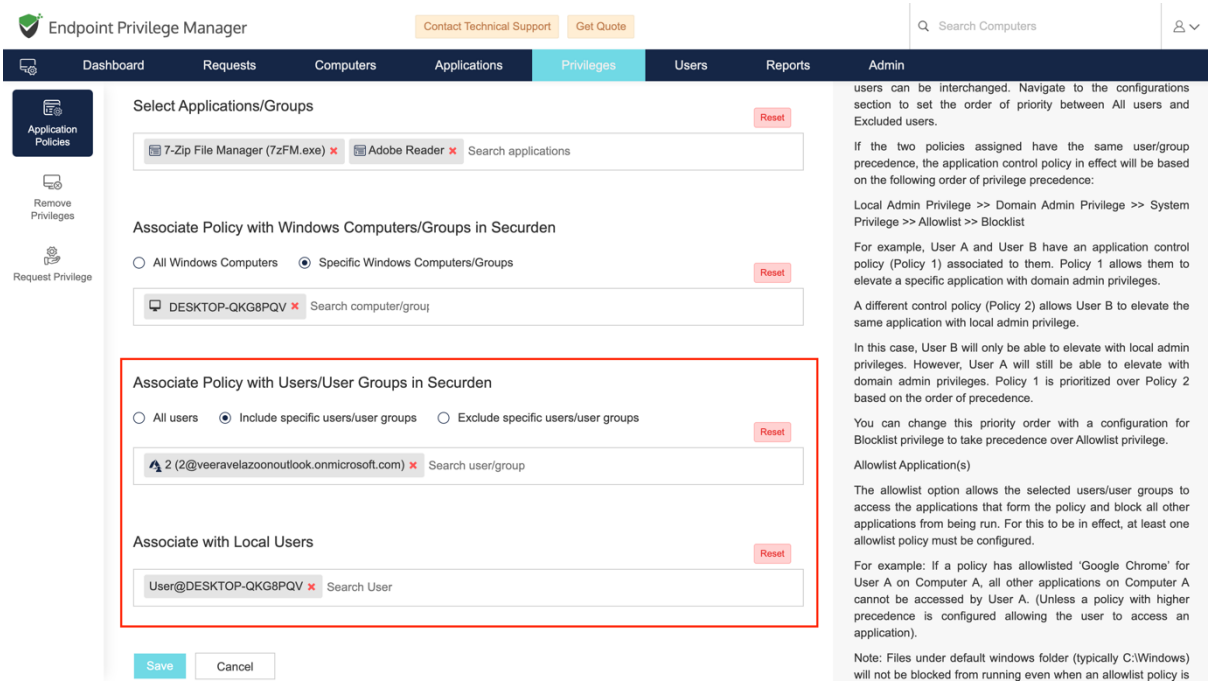


6. Select the devices on which this control policy should be enforced. You have the option to associate the policy with all the devices available in Securden. You can also associate the policy with specific devices.



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.



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**.

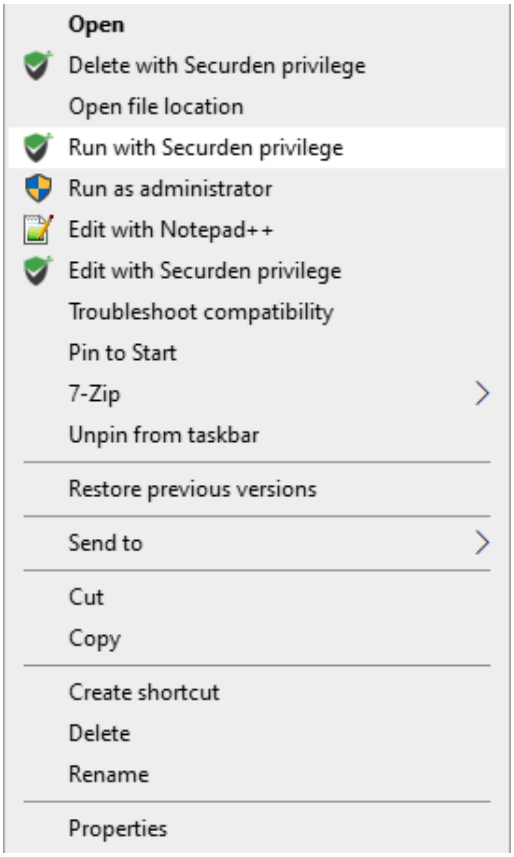
9. Click **Save**.

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.

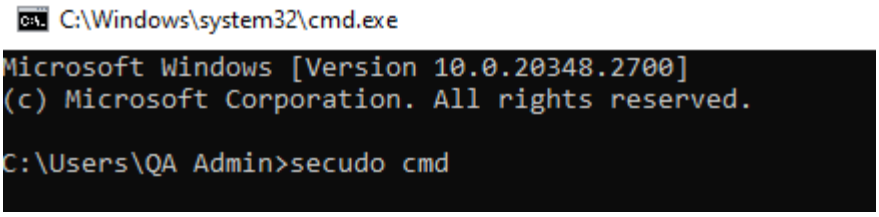
Step 2: Elevating the application on the endpoint

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

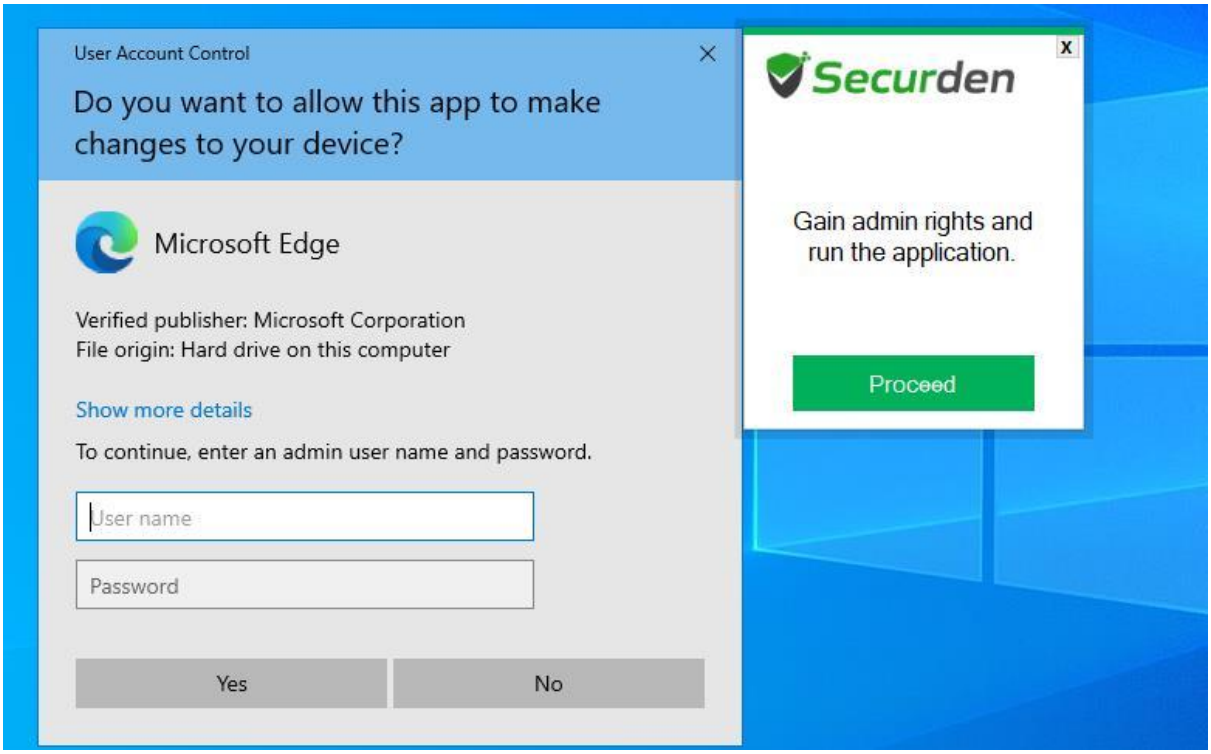
1. In the endpoint, right click on the app and click **Run with Securden Privilege** to run the app with admin rights.



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.



4. 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.

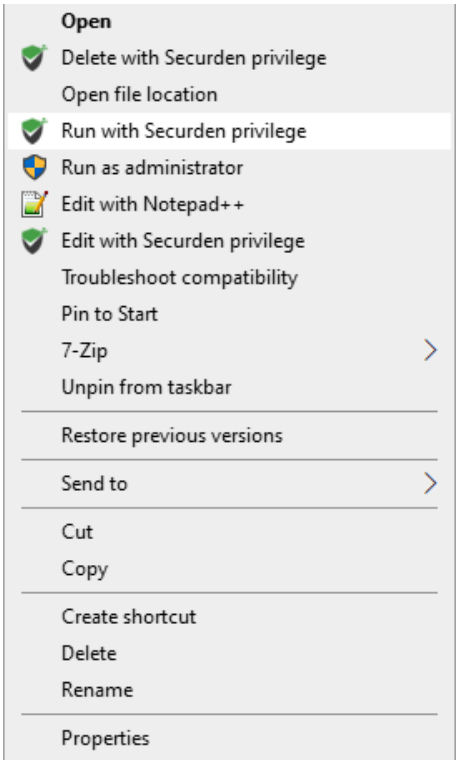
Case 2: Users who need to run new apps with admin rights that are not covered under policies

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.

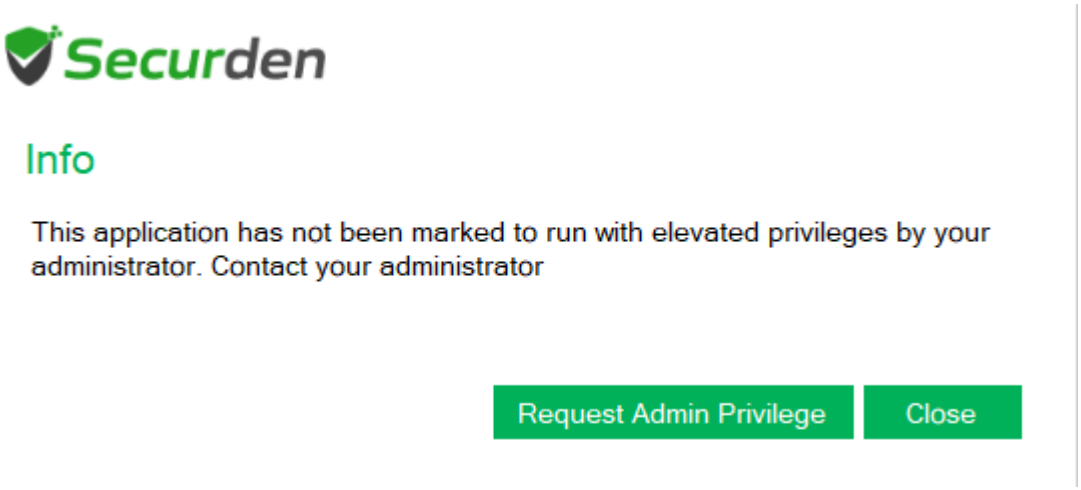
Follow the steps below to test the request-release workflow:

Step 1: Raising a request from the end user machine

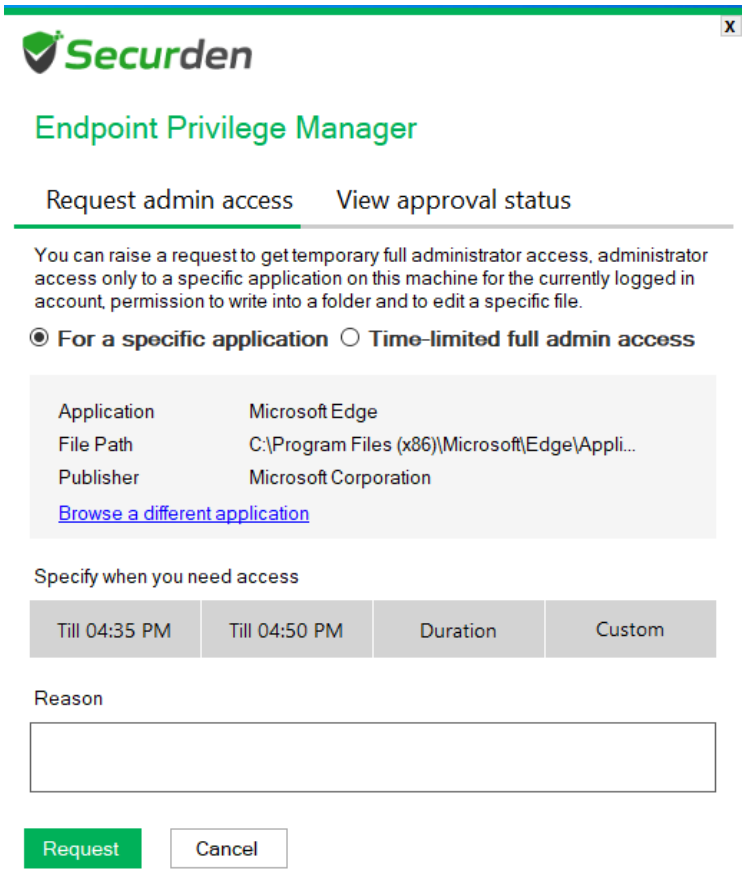
1. In the endpoint, right click on an application that is not covered in a policy and click on **Run with Securden Privilege**.



2. 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**.



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



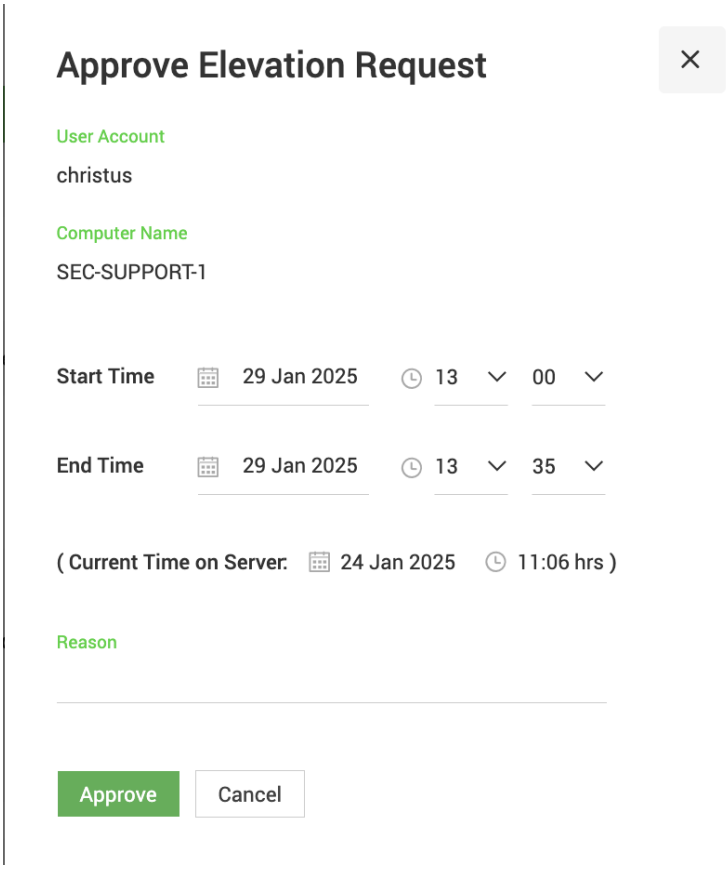
4. Select the check box named **With Admin Rights** if shown.

   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.



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.
2. 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.

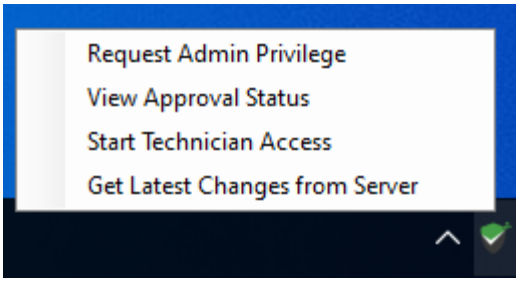
Case 3: Users who need to elevate multiple applications within a short span of time

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.

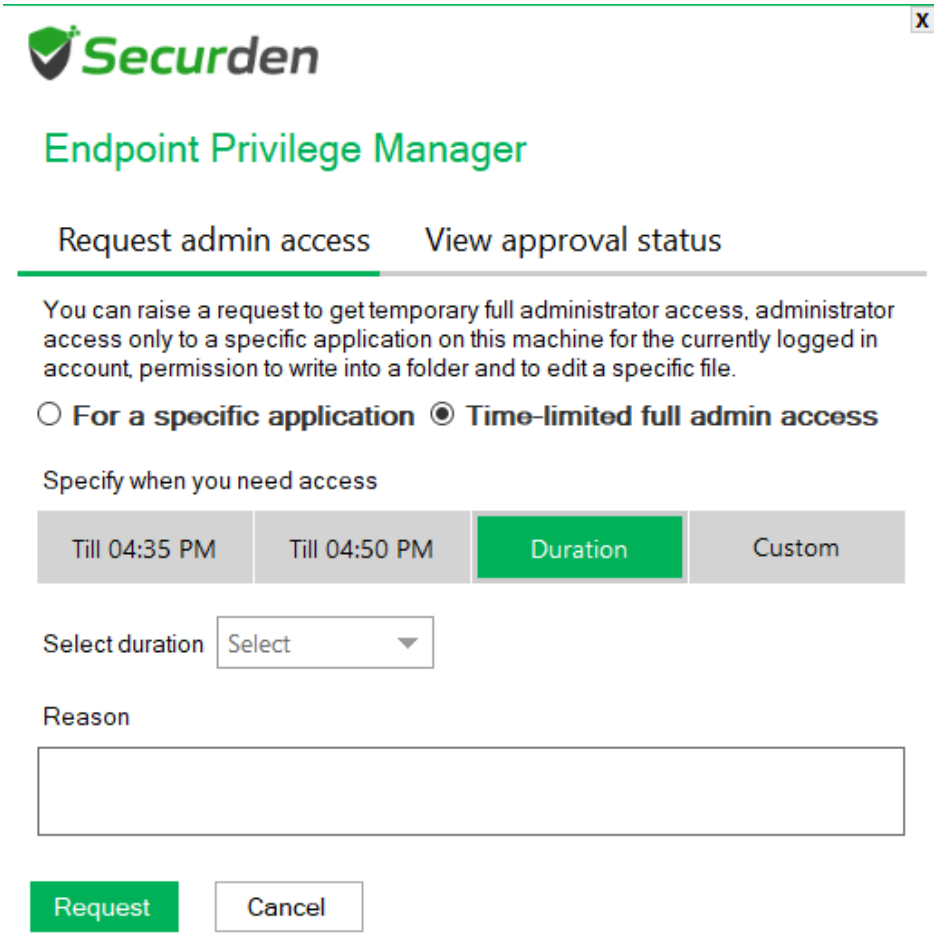
These administrator sessions are strictly monitored and tracked through text-based audit trails. If the user creates new admin accounts using the permission granted in these sessions, they will be tracked, and their actions can be reversed. To test the request-release workflow for temporary full-admin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



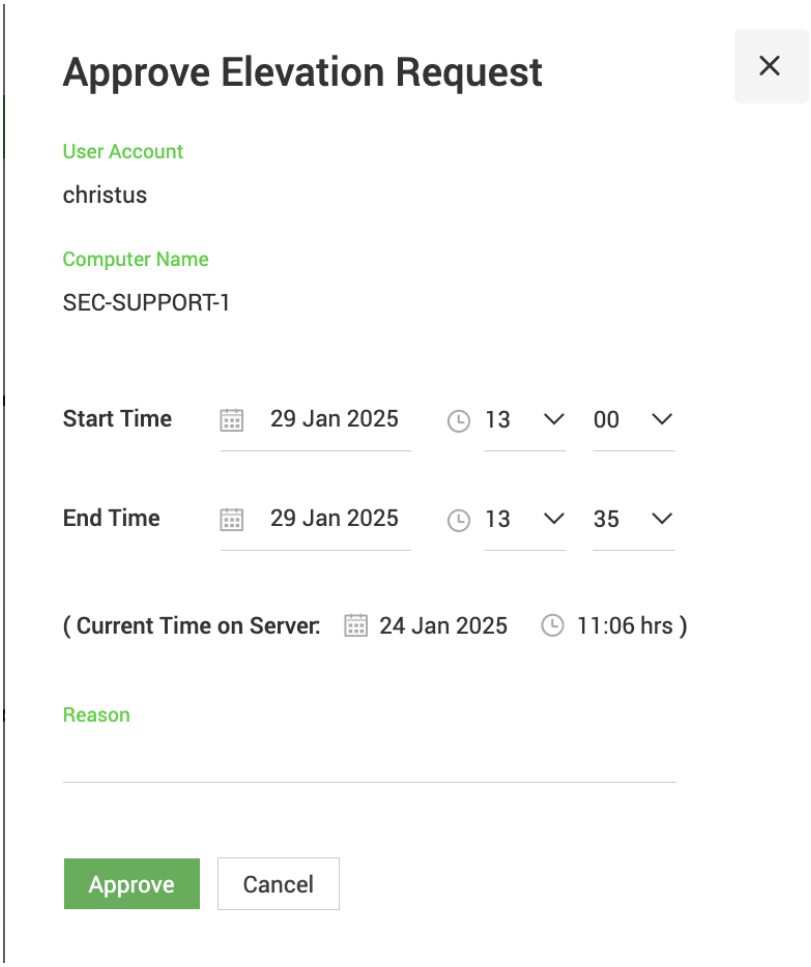
3. In the window that opens, choose **Time-limited full admin access**.



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.

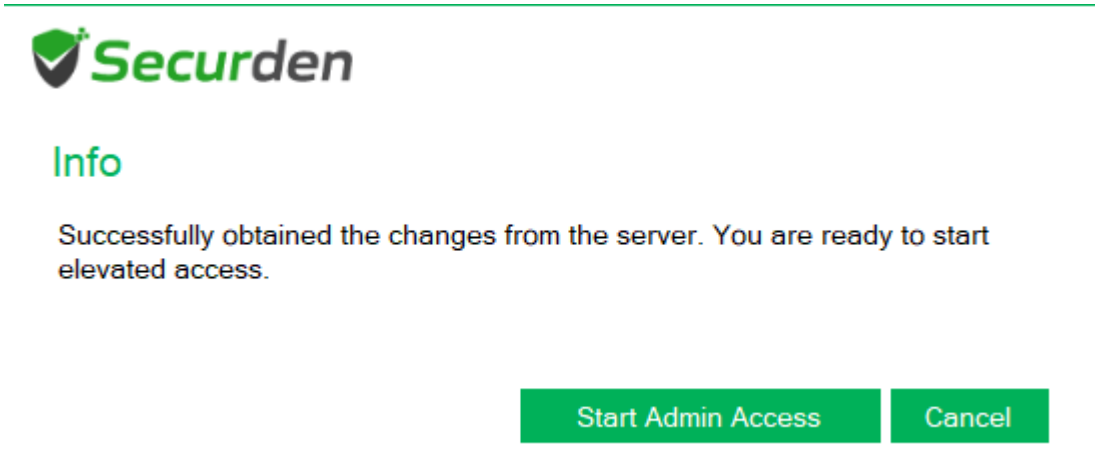


6. Provide a reason before clicking on **Approve**.

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**.
2. 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**.



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.

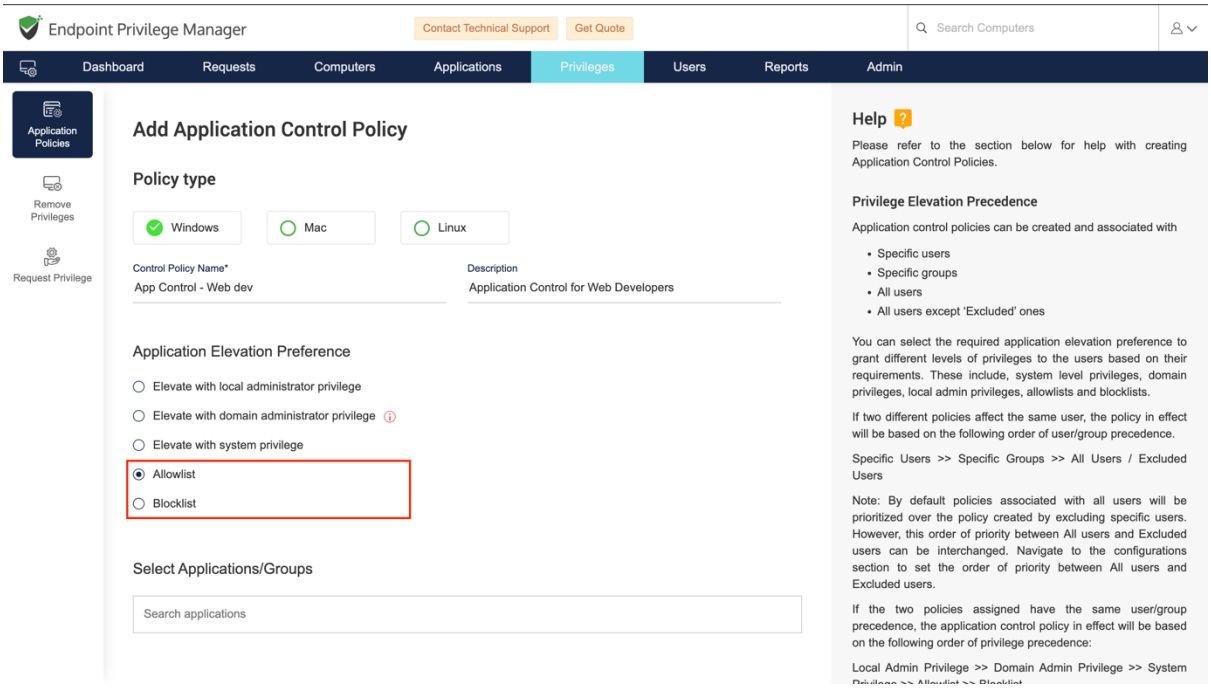
How does a Blocklist work?

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.

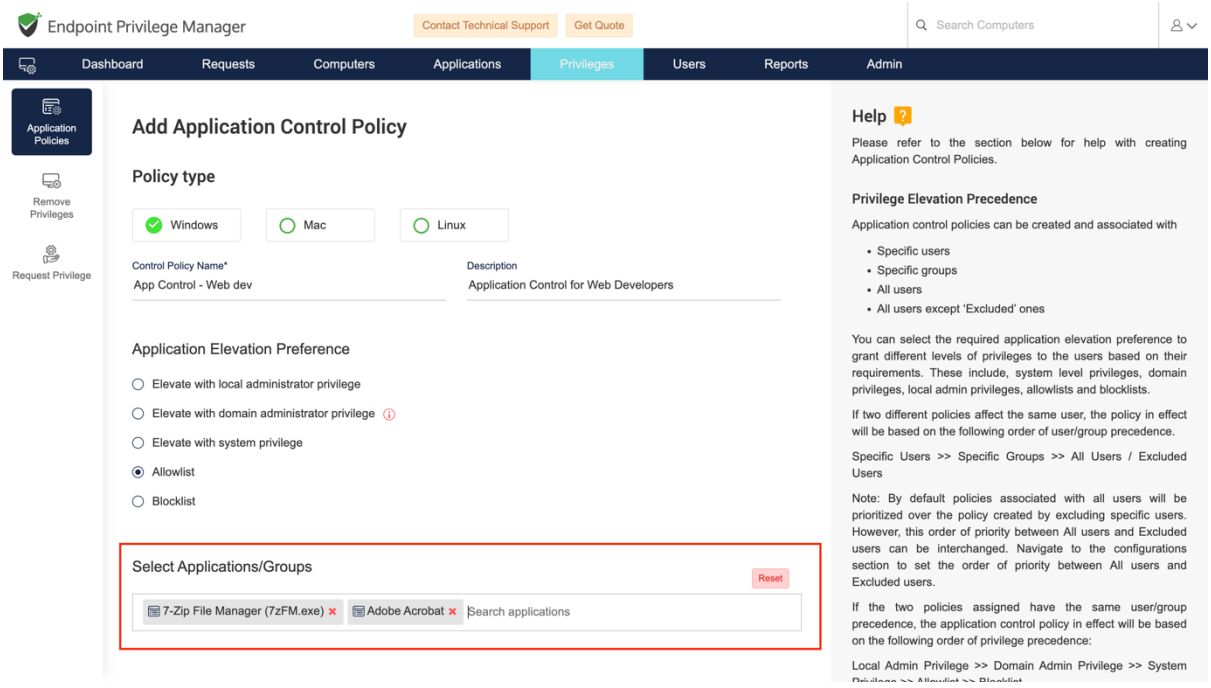
Step 1: Creating an Allowlist/Blocklist

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.



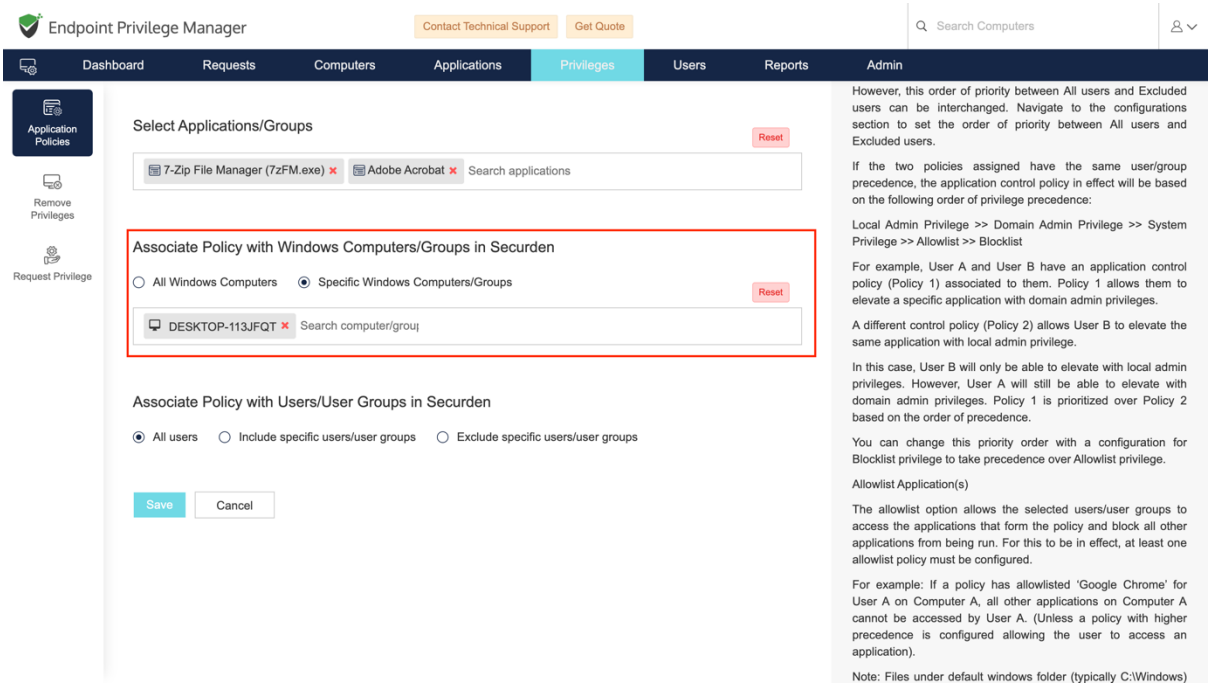
Note: Refer to the sections **How does an Allowlist work?** And **How does a Blocklist work?**

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



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.

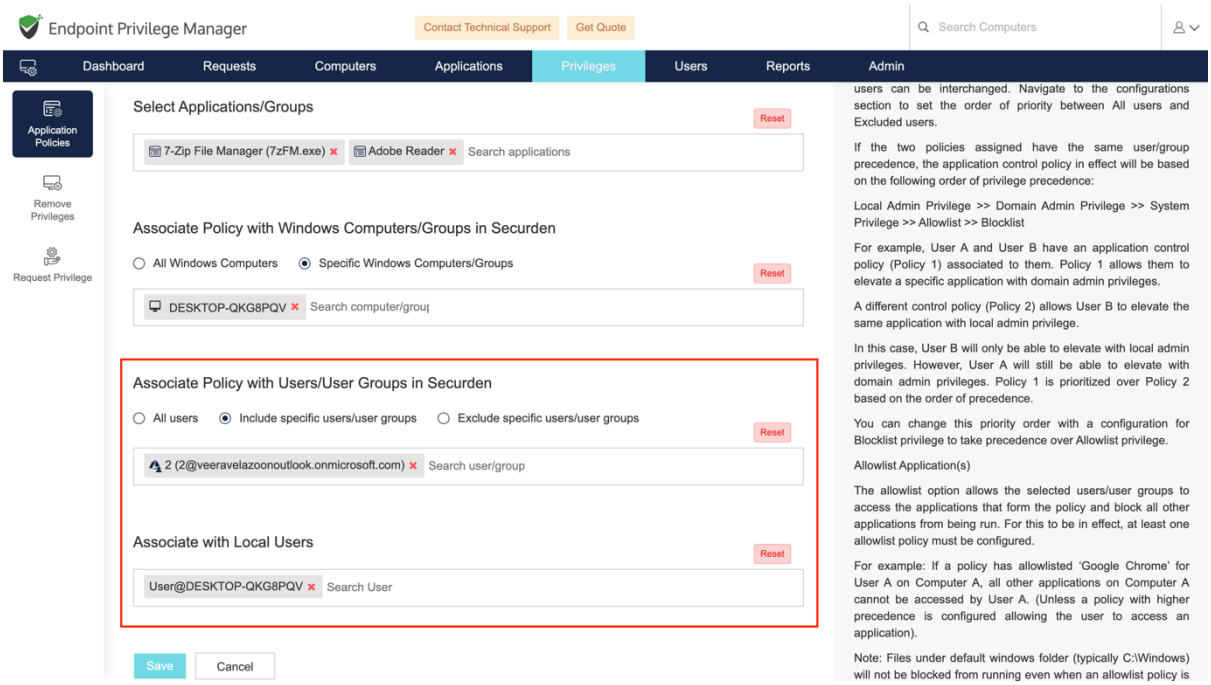
Note: To test the policy, ensure that you are associating the device on which you would like to test the application control feature.



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.



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.

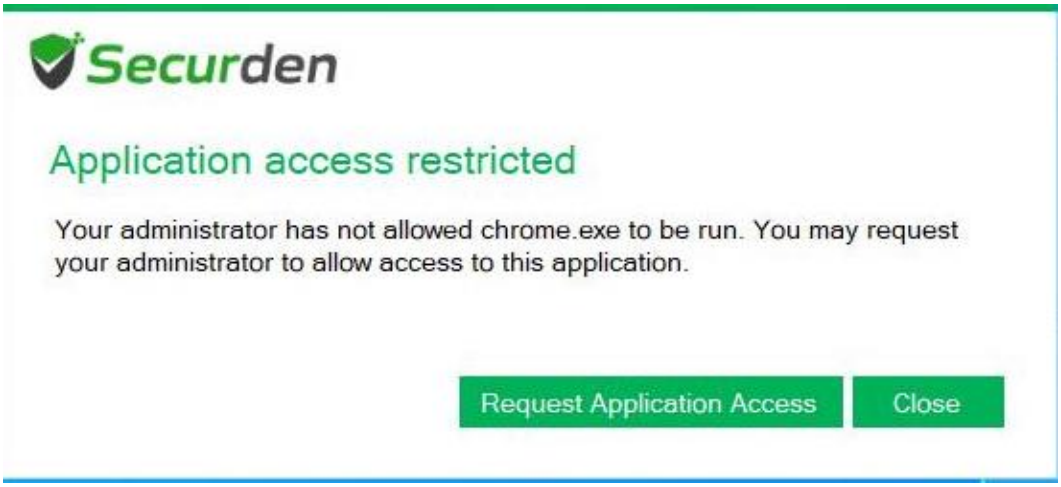
You have successfully tested the application control feature.

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

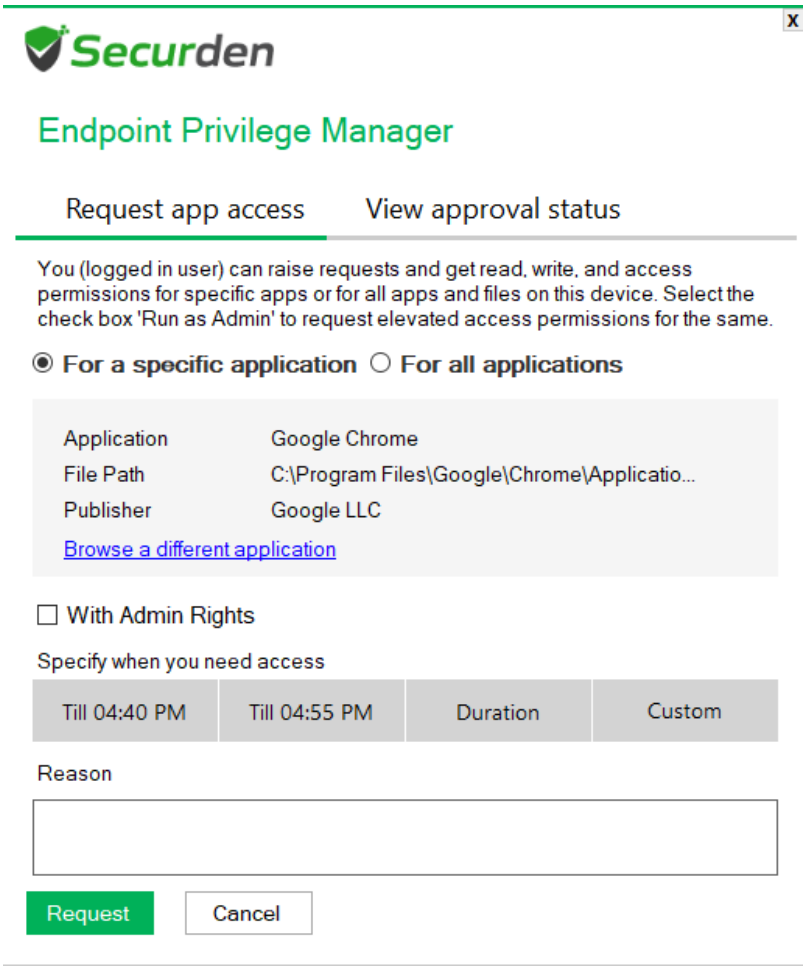
When an allowlist or a blocklist is enforced, the user will not be able to run many applications that are installed on the endpoints. To cater to the needs of the users, Securden provides a request-release workflow for obtaining temporary access to applications. You can test this workflow by following 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.
2. 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.



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

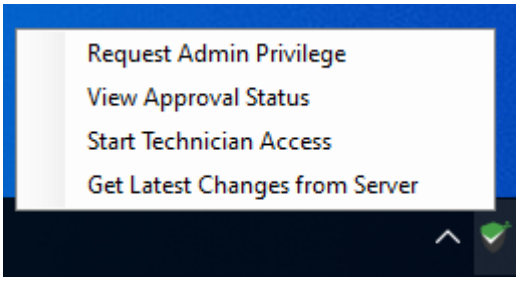
Note: You can also request access to all applications on your device for a limited time. To request access to all applications, select the radio button **For all applications**.

Step 2: Approving the request from the admin console

1. Login to the web-interface as an administrator and go to the **Requests** tab.
2. 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

1. 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.
3. 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.