

Configuring Cache Cleaner Restrictions (NSM Procedure)

You can restrict Secure Access device and resource access by requiring Cache Cleaner in the following options:

- **Realm authentication policy**—When users try to sign in to the Secure Access device, the Secure Access device evaluates the specified realm’s authentication policy to determine if the preauthentication requirements include Cache Cleaner. You can configure a realm authentication policy to download Cache Cleaner, download and start running Cache Cleaner, or not require Cache Cleaner. The user must sign in using a computer that adheres to the Cache Cleaner requirements specified for the realm. If the user’s computer does not meet the requirements, then the user is denied access to the Secure Access device.
- **Role**—When the Secure Access device determines the list of eligible roles to which it can map an administrator or user, it evaluates each role’s restrictions to determine if the role requires Cache Cleaner to run on the user’s workstation. If it does and the user’s machine is not already running Cache Cleaner, then the Secure Access device does not map the user to that role.
- **Resource policy**—When a user requests a resource, the Secure Access device evaluates the resource policy’s detailed rules to determine whether or not Cache Cleaner needs to be installed or running on the user’s workstation. The Secure Access device denies access to the resource if the user’s machine does not meet the Cache Cleaner requirement.
-

To configure Cache Cleaner restrictions at the realm level:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure global Cache Cleaner restrictions in realm level.
3. Click the **Configuration** tab and select **Users > User Realms > Select Realm > Authentication Policies > Cache Cleaner** . The corresponding workspace appears.
4. Configure the cache cleaner restrictions at the role level using the settings described in Table 1 on page 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Configuring Cache Cleaner Restrictions Details at Realm Level

Option	Function	Your Action
	Files and Folders	

Table 1: Configuring Cache Cleaner Restrictions Details at Realm Level (continued)

Option	Function	Your Action
Cache Cleaner option	Specifies whether or not Cache Cleaner is running for the user to meet the access requirement.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Disable Cache Cleaner—Does not require Cache Cleaner to be installed or running for the user to meet the access requirement. ■ Just load Cache Cleaner (Loads after IVE maps the user to a realm)—Does not require Cache Cleaner to be running for the user to meet the access requirement but ensures that it is available for future use. If you choose this option for a realm’s authentication policy, then the Secure Access device downloads Cache Cleaner to the client machine after the user is authenticated and before the user is mapped to any roles on the system. ■ Load and enforce Cache Cleaner (Loads before IVE maps the user to a realm)—Requires the Secure Access device to download and run Cache Cleaner for the user to meet the access requirement. If you choose this option for a realm’s authentication policy, then the Secure Access device downloads Cache Cleaner to the client machine before the user may access the Secure Access device sign-in page.

To configure cache cleaner restrictions at the role level:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure global Cache Cleaner restrictions at the role level.
3. Click the **Configuration** tab and select **Users > User Roles > Select Role > General > Restrictions > Cache Cleaner Restrictions**. The corresponding workspace appears.
4. Configure the Cache Cleaner restrictions at the role level using the settings described in Table 2 on page 2.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 2: Configuring Cache Cleaner Restriction Details at role level

Option	Function	Your Action
Require Cache Cleaner (must be loaded by the Realm)	Specifies Cache Cleaner to be running in order for the user to meet the access requirement.	Select the Require Cache Cleaner (must be loader by the Realm) check box to enable this option.

To configure Cache Cleaner restrictions at the resource policy level:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure global Cache Cleaner restrictions at the resource policy level.
3. Click the **Configuration** tab and select **Users > Resource Policies > Select Resource > Select Policy > Detailed Rules**.
4. Select or create the rule and configure the Cache Cleaner restrictions at the resource policy level using the settings described in Table 3 on page 3.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 3: Configuring Global Cache Cleaner Restriction Detail at Resource Policy Level

Option	Function	Your Action
General tab		
Name	Specifies the resource policy's detailed rule name.	Enter the name.
Action	Specifies the action to allow the Secure Access device to access the resource if the user's machine does not meet the Cache Cleaner requirement.	Select Allow or Deny from the drop-down list.
Resources	Specifies the resource or a partial list of the resources.	Enter specific URL, directory path, file, or file type.
Conditions	Specifies a custom expression in a detailed rule for the Secure Access device to determine whether or not Cache Cleaner needs to be installed or running on the user's workstation.	Enter the custom expression.

- Related Topics**
- Configuring the Network Communications Protocol (NSM Procedure)
 - Configuring Global Cache Cleaner Options (NSM Procedure)

