

Configuring Secure Access Authentication Policies (NSM Procedure)

An authentication policy is a set of rules that controls one aspect of access management—whether or not to present a realm’s sign-in page to a user. An authentication policy is part of an authentication realm’s configuration, specifying rules for the Secure Access device to consider before presenting a sign-in page to a user.

To configure an authentication realm policy:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure an authentication realm policy.
2. Click the **Configuration** tab, and then select **Administrators > Admin Realms** or **User** or **Users Realms**. The corresponding workspace appears.
3. Click the **New** button. The New dialog box appears.
4. Configure the server using the settings described in Table 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Authentication Realm Policies Configuration Details

Option	Function	Your Action
Authentication Policies > Source IP tab		
Allow	Controls from which IP addresses users can access a Secure Access device sign-in page, be mapped to a role, or access a resource.	Select any one of the following options from the drop-down list: <ul style="list-style-type: none"> ■ Users from any IP address— Enables users to sign into the Secure Access device from any IP address to satisfy the access management requirement. ■ User from IP addresses which pass the specified matching policies—Enables users to sign into the Secure Access device from IP addresses that have passed the specified matching policies.
Source IP Address	Specifies the IP address of the sender.	Enter the IP address. NOTE: The new button is enabled only when you select User from IP addresses which pass the specified matching policies option from the Allow drop-down list.

Table 1: Authentication Realm Policies Configuration Details (continued)

Option	Function	Your Action
Source IP Netmask	Specifies the IP Netmask.	Enter the IP netmask. NOTE: The new button is enabled only when you select Allow or deny users from the following IP addresses option from the Allow drop-down list.
Access	Allows or denies users to sign in from the specified IP address.	Select one of the following options from the drop-down list: Allow —Allows users to sign in from the specified IP address. Deny —Prevents users from signing in from the specified IP address.
Authentication Policies > Browser tab		
Allow	Controls from which Web browsers users/admins can access the sign-in page of the Secure Access device, be mapped to a role, or access a resource. You are prompted with a sign-in attempt failed error message when you try to sign in to the device using an unsupported browser.	Select one of the following options from the drop-down list: Browsers with any user-agent —Allows you to sign into the device from any browser and the device submits the user credentials to the authentication server. Browsers whose user-agents pass the matching policies defined below —Allows you to sign in from a browser whose user-agent string meets the specified pattern requirements for the selected authentication realm.
User agent pattern	Specifies the user agent pattern.	Enter a string in the format * <browser_string> * NOTE: This option is enabled only when you select Browsers whose user-agents pass the matching policies defined below from the Allow drop-down list and then by clicking New .

Table 1: Authentication Realm Policies Configuration Details (continued)

Option	Function	Your Action
Action	Allows or denies users to use a browser that has a user-agent header containing the < browser-string > substring.	<p>Select one of the following options from the drop-down list:</p> <p>Allow—Allows users to use a browser that has a user-agent header containing the < browser_string > substring.</p> <p>Deny—Prevents users from using a browser that has a user-agent header containing the < browser_string > substring.</p> <p>NOTE: This option is enabled only when you select Browsers whose user-agents pass the matching policies defined below from the Allow drop-down list and then by clicking New.</p>
Authentication Policies > Certificate tab		
Allow	Restricts the Secure Access device and resource access by requiring client-side certificates.	<p>Select one of the following options from the drop-down list:</p> <p>All users—Does not require a user’s client to have a client-side certificate.</p> <p>All users, remember certificate while user is signed in—Does not require a user’s client to have a client-side certificate, but if the client does have a certificate, the Secure Access device remembers the certificate information during the entire user session.</p> <p>Users with a trusted client certificate—Requires a user’s client to have a client-side certificate to satisfy the access management requirement. To restrict access even further, you can define unique certificate attribute-value pairs. Note that the user’s certificate must have all the attributes you define.</p>
Certificate Field	Specifies any additional criteria that the admin realm should use when verifying the policies.	<p>Enter a value. For example, enter uid.</p> <p>NOTE: This field is enabled only when you select Users with trusted client certificate from the Allow drop-down list and by clicking New.</p>
Expected Value	Specifies values in the client certificate.	<p>Enter a variable, for example, enter < userAttr.uid > .</p> <p>NOTE: This field is enabled only when you select Users with trusted client certificate from the Allow drop-down list and by clicking New.</p>
Authentication Policies > Password tab		

Table 1: Authentication Realm Policies Configuration Details (continued)

Option	Function	Your Action
Options for primary authentication server	Restricts the Secure Access device and resource access by password length when administrators or users try to sign in to a Secure Access device. The user must enter a password whose length meets the minimum password-length requirement specified for the realm.	Select one of the following options from drop-down list: Allow all users (passwords of any length) —Does not apply password length restrictions to users signing in to the Secure Access device. Only allow users that have passwords of a minimum length —Requires the user to enter a password with a minimum length of the number specified.
Primary password minimum length (character)	Specifies password length restrictions.	Enter the number.
Options for secondary authentication server	Restricts the Secure Access device and resource access by password-length to the secondary authentication server when administrators or users try to sign in to an Secure Access device. The user must enter a password whose length meets the minimum password-length requirement specified for the realm.	Select one of the following options from the drop-down list: Allow all users (passwords of any length) —Does not apply password length restrictions to users signing in to the Secure Access device. Only allow users that have passwords of a minimum length —Requires the user to enter a password with a minimum length of the number specified.
Secondary password minimum length (character)	Specifies password length restrictions.	Enter the number.
Authentication Policies > Host Checker tab		
Evaluate ALL policies	Evaluates all the policies without enforcing the policy on the client and allows user access.	Select Authentication Policies > Host Checker > Evaluate ALL policies to enable this feature.
Enforce ALL policies	Enforces all the policies on the client for the user to log in to the specified realm.	Select Authentication Policies > Host Checker > Enforce ALL policies to enable this feature.
Evaluate selected policies	Evaluates the selected policies without enforcing the policy on the client and allows user access.	Select the policy, and then click Add .
Enforce selected policies	Enforces the policies on the client for the user to log in to the specified realm.	Select a policy, and then click Add .

Table 1: Authentication Realm Policies Configuration Details (continued)

Option	Function	Your Action
Evaluate logic	Does not require users to meet all of the requirements in all of the selected policies. Instead, the user can access the realm if he meets the requirements of any one of the selected Host Checker policies.	<p>Select one of the following options from the drop-down list:</p> <p>allow access to realm if any ONE of the selected Require & Enforce policies succeed—User can access the realm if he meets the requirements of any one of the selected Host Checker policies.</p> <p>Allow access only if all of the Require & Enforce policies succeed—User can access the realm only if he meets all of the requirements in all of the selected policies.</p>
Authentication Policies > Cache Cleaner tab		
Cache Cleaner option	<p>Specifies the cache cleaner restrictions.</p> <p>NOTE: The Cache Cleaner tab is displayed only when you configure user realm policies.</p>	<p>Select one of the following option:</p> <p>Disable Cache Cleaner— Does not require Cache Cleaner to be installed or running for the user to meet the access requirement.</p> <p>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.</p> <p>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.</p>
Authentication Policies > Limits tab		
Limit number of concurrent users	Limits the number of concurrent users on the realm.	Select Authentication Policies > Limits > Limit number of concurrent users to enable this feature.
Guaranteed minimum	Specifies any number of users between zero (0) and the maximum number of concurrent users defined for the realm, or you can set the number up to the maximum allowed by your license if there is no realm maximum.	Enter a number.

Table 1: Authentication Realm Policies Configuration Details (continued)

Option	Function	Your Action
Maximum	Specifies any number of concurrent users from the minimum number you specified up to the maximum number of licensed users. If you enter a zero (0) into the Maximum box, no users are allowed to login to the realm.	Enter a number.

- Related Topics**
- Configuring Secure Access Role Mapping Rules (NSM Procedure)
 - Configuring Secure Access Sign-In Policies (NSM Procedure)
 - Configuring Secure Access Authentication Realms (NSM Procedure)

Published: 2009-08-20