

Configuring Secure Access General Session Options (NSM Procedure)

To specify session time limits, roaming capabilities, session and password persistency, request follow-through options, and idle timeout application activity, follow these steps:

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 user roles.
2. Click the **Configuration** tab, and select **Users > User Roles**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Click **General > Session Options** to add or modify settings as specified in Table 1 on page 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 1: Session Options Configuration details

Option	Function	Your Action
General > Session Options tab		
Idle Timeout	Specifies the number of minutes a nonadministrative user session may remain idle before ending. The minimum is five minutes. The default idle session limit is 10 minutes, which means that if a user's session is inactive for 10 minutes, the Secure Access device ends the user session and logs the event in the system log (unless you enable session timeout warnings described later).	Enter the session length in minutes.

Table 1: Session Options Configuration details (continued)

Option	Function	Your Action
Max. Session Length	Specifies the number of minutes an active nonadministrative user session may remain open before ending. The minimum is six minutes. The default time limit for a user session is 60 minutes, after which the Secure Access device ends the user session and logs the event in the system log. During an end-user session, prior to the expiration of the maximum session length, the Secure Access device prompts the user to reenter authentication credentials, which avoids the problem of terminating the user session without warning.	Enter the heartbeat interval in seconds.
Reminder Time	Specifies when the Secure Access device should prompt nonadministrative users, warning them of an impending session or idle timeout. Specify in number of minutes before the timeout is reached.	Enter the Reminder Time in minutes.
Enable session timeout warning	Enables users to take the appropriate action when they are close to exceeding their session limits or idle timeouts, helping them to save any in-progress form data that would otherwise be lost. Users approaching the idle timeout limit are prompted to reactivate their session. Users approaching the session time limit are prompted to save data.	Select Enable session timeout warning to notify nonadministrative users when they are about to reach a session or idle timeout limit.
Display sign-in page on max session time out	Displays a new browser sign-in page to the end user when their session times out. This option appears only when you select Enable session timeout warning .	Select Display sign-in page on max session time out .

Table 1: Session Options Configuration details (continued)

Option	Function	Your Action
Roaming session	<p>Allows users to enable, limit, or disable the roaming session.</p> <p>A roaming user session works across source IP addresses, which allows mobile users (laptop users) with dynamic IP addresses to sign in to the Secure Access device from one location and continue working from another. Disable this feature to prevent users from accessing a previously established session from a new source IP address. This helps protect against an attack spoofing a user's session, provided the hacker was able to obtain a valid user's session cookie.</p> <p>Users may sign in from one IP address and continue using their sessions with another IP address as long as the new IP address is within the same subnet.</p> <p>Users who sign in from one IP address may not continue an active Secure Access device session from another IP address; user sessions are tied to the initial source IP address.</p>	<p>Select a roaming session option from the drop-down list:</p> <ul style="list-style-type: none"> ■ Enabled—Enables roaming user sessions for users mapped to this role. ■ Limit to subnet—Limits the roaming session to the local subnet specified in the Netmask box. ■ Disabled—Disables roaming user sessions for users mapped to this role.
Roaming netmask	Specifies the roaming netmask.	Enter a roaming netmask address.
Persistent session	Enables users to write the Secure Access device session cookie to the client hard disk so that the user's Secure Access device credentials are saved for the duration of the Secure Access device session.	Select Enabled from the drop-down list.

Table 1: Session Options Configuration details (continued)

Option	Function	Your Action
Persistent password caching	<p>Enables users to allow cached passwords to persist across sessions for a role.</p> <p>The Secure Access device supports the NT LAN Manager (NTLM) authentication protocol and HTTP Basic Authentication and supports servers that are set up to accept both NTLM and anonymous sign-in. The Secure Access device caches NTLM and HTTP Basic Authentication passwords provided by users so that the users are not repeatedly prompted to enter the same credentials used to sign in to the Secure Access device server or another resource in the NT domain. By default, the Secure Access device server flushes cached passwords when a user signs out.</p>	<p>Select Enabled from the drop-down list.</p> <p>You can delete cached passwords through the Advanced Preferences page. After the end user logs in to the Secure Access device, click Preferences and then click Preferences and then click the Advanced tab.</p>
Browser request follow-through	Enables users to allow the Secure Access device to complete a user request made after an expired user session after the user reauthenticates.	Select Enabled form the drop-down list.
Idle timeout application activity	Enables users to ignore activities initiated by Web applications (such as polling for e-mails) when determining whether a session is active.	<p>Select Enabled form the drop-down list.</p> <p>If you disable this option, periodic pinging or other application activity may prevent an idle timeout.</p>
Enable Upload Logs	Enables users to transmit (upload) client logs to the Secure Access device.	Select the Enable Upload Logs .

- Related Topics**
- Creating and Configuring Secure Access Device Administrator Roles (NSM Procedure)
 - Creating Secure Access Role-Based Source IP Alias (NSM Procedure)
 - Verifying Imported Device Configurations
 - Creating and Applying a Secure Access Device Template