

Configuring Global Security (NSM Procedure)

The default global security settings provide maximum security. However, you may need to modify these settings if users cannot use certain browsers or access certain web pages. You can also configure lockout options for protecting the Secure Access device and back-end systems from DoS/DDoS/password guessing attacks from the same IP address.

To configure global security:

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 global security.
2. Click the **Configuration** tab, and select **System > Configuration > Global Security**. The corresponding workspace appears.
3. Add or modify settings as specified in Table 1 on page 1.
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modification.

Table 1: Configuring Global Security Details

Option	Function	Your Action
SSL Settings > General tab		
Allowed SSL and TLS Version	Specifies encryption requirements for Secure Access device users.	<p>Select any one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Accept only TLS V1 (maximize security with reduced compatibility)—For maximize security with reduced compatibility. ■ Accept only SSL V3 and TLS V1 (maximize security)—For maximize security. ■ Accept SSL V2 and V3 and TLS V1 (maximize browser compatibility)—For users who have older browsers that use SSL version 2 to update their browsers or change the Secure Access device setting to allow SSL version 2, SSL version 3, and TLS. <p>NOTE: The Secure Access device requires SSL version 3 and TLS by default.</p>

Table 1: Configuring Global Security Details (continued)

Option	Function	Your Action
strength	Specifies the encryption strength.	<p>Select one of the following options from the drop-down list.</p> <ul style="list-style-type: none"> ■ Accept only 168-bit and greater (maximize security)—Secure Access device gives preference to 256-bit AES over 3DES ■ Accept only 128-bit and greater (security and browser compatibility)—Secure Access device gives preference to RC4 ciphers. ■ Accept 40-bit and greater (maximize browser compatibility)—Secure Access device gives preference to RC4 ciphers. ■ Custom SSL Cipher Selection—Specifies a combination of cipher suites for the incoming connection from the user’s browser.
AES/3DES High (168-bit and greater)	<p>Allows the Secure Access device to provide preference to 256-bit AES over 3DES.</p> <p>NOTE: This option is displayed only when you select Custom SSL Cipher Selection from the strength drop-down list.</p>	Select the AES/3DES High (168-bit and greater) check box to enable this feature.
AES Medium (between 128-bit and 168-bit)	<p>Allows the Secure Access device to use 168-bit or higher ciphers for backend rewriter connections and the device to provide preference to 256-bit AES encryption for backend mail proxy SSL connections.</p> <p>NOTE: This option is displayed only when you select Custom SSL Cipher Selection from the strength drop-down list.</p>	Select the AES Medium (between 128-bit and 168-bit) check box to enable this feature.
RC4 Medium (between 128-bit and 168-bit)	<p>Allows Secure Access device to use 168-bit or higher ciphers for backend rewriter connections and the device provides preference to 256-bit AES encryption for backend mail proxy SSL connections.</p> <p>NOTE: This option is displayed only when you select Custom SSL Cipher Selection from the strength drop-down list.</p>	Select the RC4 Medium (between 128-bit and 168-bit) check box to enable this feature.

Table 1: Configuring Global Security Details (continued)

Option	Function	Your Action
RC2 Medium (between 128-bit and 168-bit)	Allows Secure Access device to use 168-bit or higher ciphers for backend rewriter connections and device gives preference to 256-bit AES encryption for backend mail proxy SSL connections. NOTE: This option is displayed only when you select Custom SSL Cipher Selection from the strength drop-down list.	Select the RC2 Medium (between 128-bit and 168-bit) check box to enable this feature.
DES Low (less than 128-bit)	Allows Secure Access device to use 168-bit or higher ciphers for backend rewriter connections and the device provides preference to 256-bit AES encryption for backend mail proxy SSL connections. NOTE: This option is displayed only when you select Custom SSL Cipher Selection from the strength drop-down list.	Select the DES Low (less than 128-bit) check box to enable this feature.
Do not allow connections from browsers that only accept weaker ciphers	Prevents a browser with a weak cipher from establishing a connection.	Select the Do not allow connections from browsers that only accept weaker ciphers check box to enable this feature.
Settings		
Lockout period (minutes)	Specifies the number of minutes you want the Secure Access device to lock out the IP address.	Enter the time.
Attempts	Specifies the maximum number of failed sign-in attempts to allow before triggering the initial lockout.	Enter the number of attempts.
Rate	Specifies the number of failed sign-in attempts to allow per minute.	Enter the number of sign-in attempts to allow per minute.
Show last login time on user's bookmark page	Displays the day and time the user last logged in to the system in the bookmark page.	Select the Show last login time on user's bookmark page check box to enable this feature.
Show last login IP address on user's bookmark page	Displays the IP address when user last logged in to the system in the bookmark page.	Select the Show last login IP address on user's bookmark page check box to enable this feature.

Table 1: Configuring Global Security Details (continued)

Option	Function	Your Action
Delete all cookies at session termination	Allows Secure Access device to set persistent cookies on the user's machine to support functions such as multiple sign-in, last associated realm, and last sign-in URL. If you desire additional security or privacy, you may choose to not set them.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> ■ Delete all cookies at session termination (maximize security)—Secure Access device deletes all cookies at session termination. ■ Preserve cookies at session termination—Secure Access device preserves cookies at session termination.
Include IVE's session cookie in URL	Allows Secure Access device to include the user session cookie in the URL that launches JSAM or a Java applet. By default, this option is enabled, but if you have concerns about exposing the cookie in the URL, you can disable this feature.	Select any one of the following options from the drop-down list: <ul style="list-style-type: none"> ■ Include session cookie in URL (maximize compatibility)—Secure Access device includes session cookie in URL. ■ Do not include session cookie in URL (maximize security)—Secure Access device does not include the session cookie in URL.
SAML version	Allows you to specify the SAML protocol and schema.	Select SAML 1.0 or SAML 1.1 from the drop-down list.

- Related Topics**
- Configuring Sensors (NSM Procedure)
 - Configuring the Network Communications Protocol (NSM Procedure)