

Configuring Sensors (NSM Procedure)

The IDP sensor is a powerful tool to counter users who initiate attacks. Integration with the Secure Access device allows you to configure automatic responses as well as manually monitor and manage users.

To configure IDP sensors:

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 sensors.
2. Click the **Configuration** tab, and select **System > Configuration > Sensors**. 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 IDP Sensor Details

Option	Function	Your Action
Sensors tab		
Name	Specifies the name that the Secure Access device uses to identify the new connection entry.	Enter the name.
Hostname	Specifies the hostname or IP address of the IDP sensor to which the Secure Access device connects to receive application and resource attack alert messages.	Enter the hostname or IP address.
TCP Port	Specifies the TCP port on the IDP sensor to which the Secure Access device listens when receiving application and resource attack alert messages.	Enter the port.
One Time Password	Specifies the encrypted password the Secure Access device uses when conducting the initial Transport Layer Security (TLS) handshake with the IDP sensor.	Enter the encrypted Secure Access device OTP password as displayed on the IDP ACM configuration summary screen.
Addresses to monitor > New Addresses to monitor	Allows you to specify individual IP addresses and address ranges the IDP sensor monitors for potential attacks, one entry per line. IDP reports attack information only for the IP addresses that you specify.	Enter the IP addresses.

Table 1: Configuring IDP Sensor Details (continued)

Option	Function	Your Action
Severity Filter	Specifies the severity level from 1 to 5, where 1 is informational and 5 is critical.	Select one of the options available from the drop-down list.
Enable/Disable Sensor	Enables the specified IDP sensor entries, respectively.	Select the Enable/Disable Sensor check box to enable this feature.
Sensor Event Policies tab		
Name	Specifies the rule name of the action(s) the Secure Access device takes when it receives attack alert messages from an IDP sensor.	Enter the rule name.
Event	Allows you to specify an event.	Select an event from the drop-down list.
Event Count	Determines the number of times an event must occur before action is taken.	Enter a number between 1 and 256 to determine the number of times an event must occur before action is taken.
Action to be taken	Allows you to specify the action(s) the Secure Access device takes when it receives attack alert messages from an IDP sensor.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Ignore (just log the event)— Secure Access device logs the event, and takes no further action against the user profile to which this rule applies. ■ Terminate user session— Secure Access device immediately terminates the user session and requires the user to sign in to the Secure Access device again. ■ Disable user account—Secure Access device disables the user profile associated with this attack alert message, thus rendering the client unable to sign in to the Secure Access device until the administrator reenables the user account. (This option is only applicable for users who have a local Secure Access device user account.) ■ Replace user role—Specifies that the role applied to this user’s profile should change to the role you select from the associated drop-down list. This new role remains assigned to the user profile until the session terminates.

Table 1: Configuring IDP Sensor Details (continued)

Option	Function	Your Action
Replace user role with this role	Allows you to change the user role applied to this user's profile with this role. NOTE: This option is enabled only when you select Replace user role from the Action to be taken drop-down list.	Select a role from the drop-down list.
Replace user role..	Allows you to make this role assignment. NOTE: This option is enabled only when you select Replace user role from the Action to be taken drop-down list.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> ■ Permanent—User remains in the quarantined state across subsequent logins until the administrator releases the user from the quarantined state. ■ For this session only—Default. User can log in to another session.
Applies to Roles	Allows you to apply this policy to all roles or only to the users mapped or only to the users who are not mapped to roles.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> ■ All—Applies this policy to all users. ■ Selected—Applies this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list. ■ Except those selected—Applies this policy to all users except for those who are mapped to the roles in the members list. Make sure to add roles to this list from the Available roles list.
Role Selection	Allows you to select and map roles to user.	Select a role and click Add .
Sensor Events tab		
Name	Specify a name for the event.	Enter the name.
Expressions	Specifies the expressions.	Enter the expressions or select one or more clauses from the expressions dictionary and click insert expression . For example, to check for all critical/highest severity level attacks, enter the following expression: idp.severity > = 4

- Related Topics**
- Configuring General Network Settings (NSM Procedure)
 - Configuring Global Security (NSM Procedure)

