

Configuring Network Connect on a Secure Access Device User Role (NSM Procedure)

The Network Connect option provides secure, SSL-based network-level remote access to all enterprise application resources using the Secure Access device over port 443.

To configure network connect on a user role:

1. In the 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 a user-role access option.
2. Click the **Configuration** tab. Select **Users > User Roles**.
3. Click the **New** button. The New dialog box appears.
4. Add or modify settings as specified in Table 1 on page 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: User Role Network Connect Configuration Details

Option	Function	Your Action
Network Connect tab		

Table 1: User Role Network Connect Configuration Details *(continued)*

Option	Function	Your Action
Split Tunneling Modes	Allows you to enable split tunneling.	

Table 1: User Role Network Connect Configuration Details (continued)

Option	Function	Your Action
		<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Disable Split Tunneling—When Network Connect successfully establishes a connection to the Secure Access device, the device removes any predefined local (client) subnet and host-to-host routes that might cause split-tunneling behavior. If any changes are made to the client’s route table during an active Network Connect session, the Secure Access device terminates the session. ■ Allow access to local subnet—The Secure Access device preserves the route on the client, retaining access to local resources such as printers. If needed, you can add entries to the client’s route table during the Network Connect session. The Secure Access device does not terminate the session. This is the default option. ■ Enable Split Tunneling—This option activates split-tunneling and requires you to specify the network IP address/netmask combinations. For the specified network IP address/netmask combinations, the Secure Access device handles traffic passed between the remote client and the corporate intranet. ■ Enable Split Tunneling with route change monitor— This option retains access to local resources such as printers. ■ Enable Split Tunneling with allowed access to

Table 1: User Role Network Connect Configuration Details (continued)

Option	Function	Your Action
		<p>local subnet—This option activates split-tunneling and preserves the route on the client, retaining access to local resources such as printers.</p>
Auto-launch Network Connect	Specifies whether or not Network Connect automatically launches when an authenticated user maps to one or more roles that enable Network Connect sessions.	Select the Auto-Launch Network Connect check box to enable this feature.
Auto-Uninstall Network Connect	Specifies whether or not Network Connect uninstalls itself from the remote client when a user signs-out of the Network Connect session.	Select the Auto-Uninstall Network Connect check box to enable this feature.
Enable TOS Bits Copy	Specifies that Network Connect to copy IP TOS bits from the inner IP packet header to the outer IP packet header.	Select the Enable TOS Bits Copy check box to enable this feature.
Multicast	Specifies whether or not you want Network Connect to operate in multicast mode.	Select the Multicast check box to enable this feature.
Install GINA with Network Connect	Additionally installs GINA on a client system when you install Network Connect.	Select the Install GINA with Network Connect check box to enable this feature.
GINA Options	Specifies whether or not to enable GINA installation for a role and specifies the GINA sign-in behavior.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Require NC to start when logging into Windows (Note that this may require a reboot when NC is installed)—Automatically launches the Network Connect sign-in function at every Windows user sign-in. ■ Allow user to decide whether to start NC when logging into Windows—Allows the user to determine, at each Windows startup, whether or not to launch Network Connect after GINA installation.

Table 1: User Role Network Connect Configuration Details (continued)

Option	Function	Your Action
Windows: Session start script location	Specifies the location of Network Connect start scripts for Windows.	Enter the start script location.
Windows: Session end script location	Specifies the location of Network Connect end scripts for Windows.	Enter the end script location.
Skip if GINA Enabled	Bypasses the specified Windows session start script. The sign-in script may be identical to the specified Network Connect start script. This feature avoids executing the same script twice.	Select the Skip if GINA enabled check box to enable this feature.
Linux: Session start script location	Specifies the location of Network Connect start scripts for Linux.	Enter the start script location.
Linux: Session end script location	Specifies the location of Network Connect end scripts for Linux.	Enter the end script location.
Mac: Session start script location	Specifies the location of Network Connect start scripts for Macintosh.	Enter the start script location.
Mac: Session end script location	Specifies the location of Network Connect end scripts for Macintosh.	Enter the end script location.

- Related Topics**
- Configuring Secure Application Manager on a Secure Access Device User Role (NSM Procedure)
 - Configuring Secure Meeting on a Secure Access Device User Role (NSM Procedure)

