

Configuring a Network Connect Connection Profile Resource Policy (NSM Procedure)

Use the Network Connect (NC) Connection Profiles tab to create an NC resource profile. When a Secure Access device receives a client request to start an NC session, the device assigns an IP address to the client-side NC agent. The device assigns this IP address based on the DHCP server or IP address pool policies that apply to a user's role. In addition, this feature allows users to specify the transport protocol, encryption method, and whether or not to employ data compression for the NC session.

To configure an NC connection profile:

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 NC connection profile.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Network Connect > NC Connection Profile**.
3. Click **New** and then enter the name and the description for the NC connection profile.
4. Add or modify more settings as specified in Table 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.
6. On the **NC Connection Profiles** page, users can prioritize the profiles to show how the device needs to be evaluated.

Table 1: Configuring Network Connect Connection Profile Details

Options	Your Action
General tab	
Name	Enter a name for the NC connection profile.
Description	Enter a description for the NC connection profile.
Transport	Select one of the following options: <ul style="list-style-type: none">■ ESP (maximize performance) —This option uses a UDP encapsulated ESP transfer method to securely transfer data between the client and the device. NOTE: ESP is not supported on FIPS 4500/6500 appliances. You must use oNCP/NCP. Even if you select ESP on a FIPS 4500/6500 appliance it will use oNCP/NCP.■ oNCP/NCP (maximize compatibility) —This option uses the standard oNCP/NCP transport method for this connection profile.
UDP Port	Enter a value for the UDP port to customize the date transfer parameters. This option provides the device port through which you intend to direct UDP connection traffic. The default port number is 4500.

Table 1: Configuring Network Connect Connection Profile Details (continued)

Options	Your Action
ESP-to-NCP fallback time-out (seconds)	Enter a value for the ESP-to-NCP fallback time-out. This option provides a period of time (in seconds) to fall back to the NCP connection already established following UDP connection failure. The default time period is 15 seconds.
Key lifetime (time based) (minutes)	Enter a value for the key lifetime. This option provides the period of time (in minutes) the device continues to employ the same ESP encryption key for this connection profile. Both the local and remote sides of the encrypted transmission tunnel use the same encryption key only for a limited period of time to help prevent unauthorized access. The default time period is 20 minutes.
Key lifetime (bytes transferred) (minutes)	Enter a value for the key lifetime for the bytes that are transferred. The default value is 0.
Replay Protection	Select the check box to enable this option. When enabled, this option helps protect against hostile “repeat attacks” from the network.
Encryption	<p>Specify the encryption method by choosing one of the following:</p> <ul style="list-style-type: none"> ■ AES128/MD5 (maximize performance) —This option instructs the device to employ Advanced Encryption Standard (AES) 128-bit encryption on the data channel and the MD5 authentication method for Network Connect sessions. ■ AES128/SHA1 —This option instructs the device to employ AES 128-bit encryption on the data channel and the SHA1 authentication method during Network Connect sessions. ■ AES256/MD5 —This option instructs the device to employ AES 256-bit encryption on the data channel and the MD5 authentication method for Network Connect sessions. ■ AES256/SHA1 (maximize security) —This option instructs the device to employ AES 256-bit encryption on the data channel and the SHA1 authentication method during Network Connect sessions.
Compression	Select No Compression from the drop-down list if you do not want to employ compression for the secure connection.
Applies to roles	Select Selected from the drop-down list if you want to select roles for the connection profile. Upon selection, the Role Selections tab is enabled.
IP Allocation tab	

Table 1: Configuring Network Connect Connection Profile Details (continued)

Options	Your Action
IP Address Assignment	<p>Specify the method of client-side IP address assignment. Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ DHCP server —This option allows you to specify the hostname or IP address of a network Dynamic Host Configuration Protocol (DHCP) server responsible for handling client-side IP address assignment. By default, the client’s hostname is sent by the device to the DHCP server in the DHCP hostname option (option12.) Passing the user ID in the DHCP hostname option is no longer supported. As an alternative, you can configure the following entry in the DHCP options table: <i>option number = 12, option value = <username> <authmethod>, option type = String.</i> Or you can pass a value by adding an entry in the DHCP options table for hostname with whatever value you want. For example: <i>option number = 12, option value = foo, option type = String.</i> <p>NOTE: The Secure Access device does not send a DHCP release to the DHCP server after the Network Connect session terminates.</p> <ul style="list-style-type: none"> ■ IP Pool —This option allows you to specify IP addresses or a range of IP addresses for the device to assign to clients that run the Network Connect service. Use the canonical format: <i>ip_range</i>. IP address pool also supports attribute substitution. For example, you can enter a RADIUS role-mapping attribute in this field, such as <i><userAttr.Framed-IP-Address></i>.
DNS tab	
Custom DNS settings	Select this option to enable the DNS setting options. Upon selecting this option, the DNS settings box gets enabled.
DNS Settings	<p>Select of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Custom DNS Settings —This option sends the custom device DNS settings. ■ DHCP DNS Settings—This option sends the values the DHCP server sends to the device.
Primary DNS	Enter the IP address for the primary DNS.
Secondary DNS	Enter the IP address for the secondary DNS.
DNS Domain(s)	Enter the DNS domain(s), such as “yourcompany.com”, “yourcompany.net”.
WINS	Enter the WINS resolution name or IP address.
Auto-allow IP's in DNS/WINS settings (only for split-tunnel enabled mode)	Select this check box if you want to create an allow rule for the DNS server.
DNS search order	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Search client DNS first, then the device. ■ Search the device’s DNS servers first, then the client.
Proxy tab	

Table 1: Configuring Network Connect Connection Profile Details *(continued)*

Options	Your Action
Network Connect proxy server configuration	Select one of the following options from the drop-down list: <ul style="list-style-type: none">■ No proxy server—Specifies that the new profile requires no proxy server.■ Automatic (URL for PAC file on another server)—Specifies the URL of the server on which the PAC file resides, and the frequency (in minutes) with which Network Connect polls the server for an updated version of the PAC file.■ Manual configuration—Specifies the IP address or the hostname of the server and provides the port assignment.
PAC Server Address	Enter the PAC server address. This option is enabled only when you select Automatic (URL for PAC file on another server) from the Network Connect proxy server configuration option.
PAC Update Frequency (minutes)	Enter the PAC update frequency. The default value is 10.
Static Proxy Server	Enter the static proxy server address. This option is enabled only when you select Manual configuration from the Network Connect proxy server configuration option.
Static Proxy Port	Enter the static proxy port value. The default value is 0.
Roles Selection tab	
Roles Selections	Select the members from the Members list. You can add or remove the non-members to members by using the Add/Remove options.

- Related Topics**
- Configuring Web Rewriting Resource Policies (NSM Procedure)
 - Defining Network Connect Split Tunneling Policies (NSM Procedure)

Published: 2009-08-20