

Configuring Secure Access Device User Roles (NSM Procedure)

A user role is an entity that defines user session parameters, personalization settings, and enabled access features. You can customize a user role by enabling specific Secure Access device access features, defining Web, application, and session bookmarks, and configuring session settings for the enabled access features. You can create and configure user roles through the User Roles page from the Secure Access device configuration tree.

To configure a user role:

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, select **Users > User Roles**. The corresponding workspace appears.
3. Click the **New** button and the New dialog box appears.
4. Add or modify settings on the General tab page as specified in Table 1.
5. Add or modify global role options on the Global Role Options tab page as specified in Table 2.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: User Role Configuration Details

Option	Function	Your Action
General tab		
Name	Specifies a unique name for the user role.	Enter a name.
General > Overview tab		
Description	Describes the user role.	Enter a brief description for the user role.
VLAN/Source IP	Specifies role-based source IP aliases.	Select General > VLAN/Source IP to apply settings for the role.
Session Options	Specifies the session time limits, roaming capabilities, session and password persistency, request follow-through options, and idle timeout application activity.	Select General > Session Options to apply settings for the role.

Table 1: User Role Configuration Details (continued)

Option	Function	Your Action
UI Options	Specifies customized settings for the Secure Access device welcome page and the browsing toolbar for users mapped to this role.	Select General > UI Options to apply custom settings for the role; otherwise, the Secure Access device uses the default settings.
Web	Enables you to intermediate Web URLs through the Content Intermediation Engine.	Select General > Web to enable this access feature for the role.
Windows Files	Controls access to resources on Windows server shares.	Select General > Windows Files to enable this access feature.
NFS Files	Controls access to resources on UNIX/NFS servers.	Select General > NFS Files to enable this access feature.
Secure Application Manager	Provides secure, application-level remote access to enterprise servers from client applications.	Select General > Secure Application Manager to enable this access feature.
Telnet/SSH	Enables users to connect to internal server hosts in the clear using Telnet protocols or to communicate over an encrypted Secure Shell (SSH) session through a Web-based terminal session emulation.	Select General > Telnet/SSH to enable this access feature.
Terminal Services	Enables terminal emulation sessions on a Windows terminal server, Citrix NFuse server, or Citrix Metaframe server.	Select General > Terminal Services to enable this access feature.
Meeting	Allows users to securely schedule and hold online meetings between both Secure Access devices and non-Secure Access devices.	Select General > Meeting to enable this access feature.
Email	Enables users to use standards-based e-mail clients to access corporate e-mail securely from remote locations without the need for any additional software, such as a VPN client.	Select General > Email to enable this access feature.

Table 1: User Role Configuration Details (continued)

Option	Function	Your Action
Network Connect	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.	Select General > Network Connect to enable this access feature.

Table 2: Global User Role Configuration Details

Option	Function	Your Action
Global Role Options > Global Terminal Services Role Options tab		
Citrix Client CAB File	Allows you to specify a shared binary data object.	Select the plus button to specify the name, color, comment and file name for the object.
Name	Specifies the name of the object. NOTE: The name, color, comment, file name fields are displayed only when you click the plus button in the right side of the Citrix Client CAB File list.	Enter the name.
Color	Specifies the color of the object.	Select a color from Color drop down list.
Comment	Allows you to specify a comment.	Enter the comment.
File Name	Allows you to upload the shared binary data object.	Click Browse and select the file.
Citrix Client CAB File Name	Specifies the custom Citrix client file name.	Enter the file name.
Citrix Client CAB File Version	Specifies the custom Citrix version.	Enter the version.

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

Published: 2009-08-20