

Configuring Access Options using Remote Access Mechanisms Overview

This chapter contains the following information about configuring access in NSM to various applications, servers, and other resources using remote access mechanisms.. When you enable an access feature, make sure to create corresponding resource policies. To enable access features See “Configuring Secure Access Device User Roles (NSM Procedure).”

For instance, if you want to secure access to Microsoft Outlook, you can use the Secure Application Manager (SAM). The Secure Application Manager intermediates traffic to client/server applications including Microsoft Outlook, Lotus Notes, and Citrix. Or, if you want to secure access to your company Intranet, you can use the Web rewriting feature. This feature uses the Secure Access devices Content Intermediation Engine to intermediate traffic to Web-based applications and Web pages.

However, you can only access features through a user role if you are licensed for the feature. For instance, if you are using an SA-700 appliance and have not purchased a Core Clientless Access upgrade license, you cannot enable Web rewriting for a user role.

This chapter contains the following information about the access options using remote mechanisms in NSM:

- Configuring File Rewriting on a Secure Access Device User Role (NSM Procedure)
- Configuring Network Connect on a Secure Access Device User Role (NSM Procedure)
- 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)
- Configuring Web Rewriting on a Secure Access Device User Role (NSM Procedure)
- Configuring Telnet/SSH on a Secure Access Device User Role (NSM Procedure)

Related Topics

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

Published: 2009-08-20