

Configuring TACACS+ Authentication (NSM Procedure)

To use TACACS+ authentication, you must configure at least one TACACS+ server. Configuring TACACS+ authentication involves identifying the TACACS+ server, specifying the secret (password) of the TACACS+ server, and setting the source address of the device's TACACS+ requests to the loopback address of the device.

To configure TACACS+ authentication:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to configure TACACS+ authentication.
3. Click the **Configuration** tab. In the configuration tree, select **System > TACACS+ Server**.
4. Add or modify TACACS+ settings as specified in Table 1.
5. Click one:
 - **New**—Adds a new TACACS+ server.
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: TACACS+ Authentication Configuration Details

Option	Function	Your Action
Name	Specifies the IP address of the TACACS+ server.	Enter the IP address of the TACACS+ server.
Secret	Specifies the shared secret (password) of the TACACS+ server. The secret is stored as an encrypted value in the configuration database.	Enter the shared secret of the TACACS+ server.
Source Address	Specifies the source address to be included in the TACACS+ server requests by the device. In most cases, you can use the loopback address of the device.	Enter the loopback address of the device.

- Related Topics**
- Configuring RADIUS Authentication (NSM Procedure)
 - Configuring Authentication Order (NSM Procedure)
 - Configuring User Access (NSM Procedure)

