

Configuring a Secure Access RADIUS Server Instance (NSM Procedure)

A Remote Authentication Dial-In User Service (RADIUS) server is a type of server that allows you to centralize authentication and accounting for remote users. When using a RADIUS server to authenticate Secure Access device users, you need to configure it to recognize the Secure Access device as a client and specify a shared secret for the RADIUS server to use to authenticate the client request.

To configure a connection to the RADIUS server on the Secure Access device:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure RADIUS server instance.
3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box, and perform the Steps 5 through 8.

4. Click the **New** button. The New dialog box appears.
5. In the Auth Server Name list, specify a name for the RADIUS Server.
6. Select **Radius Server** from the Auth Server Type list.
7. Configure the server using the settings described in Table 1.
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: RADIUS Server Configuration Details

Option	Function	Your Action
Primary Server tab		
Radius Server	Specifies a unique name or IP address for the RADIUS server.	Enter the name or IP address.
NAS-Identifier	Identifies the Secure Access device network access server client that communicates with the RADIUS server.	Enter the name.
Authentication Port	Specifies the authentication port value for the RADIUS server.	Enter the port value. NOTE: Typically this port is 1812, but some legacy servers might use 1645.

Table 1: RADIUS Server Configuration Details (continued)

Option	Function	Your Action
Shared Secret	Specifies a string for the shared secret.	Enter a string for the shared secret.
Accounting Port	Specifies the accounting port value for the RADIUS server.	Enter the port value. NOTE: Typically this port is 1813, but some legacy servers might use 1646.
NAS-IP-Address	Controls the NAS IP address value passed to RADIUS requests.	Enter the NAS IP address.
Timeout (minutes)	Specifies the time interval for the Secure Access device to wait for a response from the RADIUS server before timing out the connection.	Enter the time.
Retries	Allows Secure Access device to try to make a connection after the first attempt fails.	Enter the number of retries.
Users authenticate using tokens or one-time passwords	Allows you not to submit the password entered by the user to other SSO enabled applications.	Select Users authenticate using tokens or one-time passwords check box.
Backup Server tab		
Backup Radius Server	Specifies a secondary RADIUS server for the Secure Access device to use if the primary server—the one defined in this instance—is unreachable.	Enter a secondary RADIUS server name or IP address.
Backup Authentication Port	Specifies the authentication port for the backup RADIUS server.	Enter the port value.
Backup Shared Secret	Specifies a string for the shared secret.	Enter a string for the shared secret.
Backup Accounting Port	Specifies the accounting port for the backup RADIUS server.	Enter the port value.
Radius Accounting tab		

Table 1: RADIUS Server Configuration Details (continued)

Option	Function	Your Action
User-Name	Specifies the user information that the Secure Access device should send to the RADIUS accounting server.	<p>Enter a name.</p> <p>The default variables for this field are:</p> <ul style="list-style-type: none"> ■ < username > —Logs the user’s Secure Access device username to the accounting server. ■ < REALM > —Logs the user’s Secure Access device realm to the accounting server. ■ < ROLE > —Logs the user’s Secure Access device role to the accounting server. If the user is assigned to more than one role, the Secure Access device comma-separates them.
Interim Update Interval (minutes)	Enables you to accomplish more precise billing for long-lived session clients and in case of a network failure.	Enter the time.
Use NC assigned IP Address for FRAMED-IP-ADDRESS attribute	Uses the IP address returned from the Secure Access device for the framed-IP-address attribute.	Select the Use NC assigned IP Address for FRAMED-IP-ADDRESS attribute check box.

- Related Topics**
- Configuring a Secure Access Anonymous Server Instance (NSM Procedure)
 - Configuring a Secure Access eTrust SiteMinder Server Instance (NSM Procedure)
 - Configuring a Secure Access LDAP Server Instance (NSM Procedure)

Published: 2009-08-20