

## Configuring a Secure Access Local Authentication Server Instance (NSM Procedure)

The Secure Access device enables you to create one or more local databases of users who are authenticated by the device. You might want to create local user records for users who are normally verified by an external authentication server that you plan to disable or if you want to create a group of temporary users. Note that all administrator accounts are stored as local records, but you can choose to authenticate administrators using an external server by creating authentication policies.

To configure a local authentication server instance:

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 a local authentication 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. Specify a name to identify the server instance.
6. Select **Local Authentication** 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: Secure Access Local Authentication Server Instance Configuration Details**

Option	Function	Your Action
<b>Local Auth Settings</b>		
Minimum password length (characters)	Specifies the minimum character length for passwords.	Set the minimum character length for passwords.
Maximum password length	Specifies the maximum character length for passwords. <b>NOTE:</b> This is optional.	Set the maximum character length for passwords. <b>NOTE:</b> The maximum length cannot be less than the minimum length. There is no maximum limit to the length.

**Table 1: Secure Access Local Authentication Server Instance Configuration Details (continued)**

Option	Function	Your Action
Minimum number of digits required in the password (digits)	Specifies the minimum number of digits that is required in the password.	Set the minimum number of digits that is required in the password.
Minimum number of letters required in the password (letters)	Specifies the minimum number of letters that is required in the password.	Set the minimum number of letters that is required in the password.
Require password to have a mix of UPPER and LOWER CASE letters	Specifies if the password must contain both uppercase and lowercase letters.	Select <b>Local Auth Settings &gt; Require passwords to have a mix of UPPER and LOWER CASE letters</b> to enable this option.
Require password to be different from username	Specifies if you want users to set the password to be different from the username.	Select <b>Local Auth Settings &gt; Require password to be different from username</b> to enable this option.
Require new passwords to be different from previous password	Specifies if you want users to set the new password to be different from the previous password.	Select <b>Local Auth Settings &gt; Require new passwords to be different from previous password</b> to enable this option.
Allow users to change their passwords	Specifies that users can change their passwords.	Select <b>Local Auth Settings &gt; Allow users to change their passwords</b> to enable this option.
Force user to change password (days)	Specifies the user the number of days after which the password expires.	Set the number of days after which the password expires.
Prompt user to change password (days)	Specifies the number of days before password expiration to prompt the user.	Set the number of days before password expiration to prompt the user.
<b>Users</b>		
Username	Specifies the username.	Enter the username.
Full name	Specifies the user's full name.	Enter the user's full name.
Password	Specifies the password.	Enter the password.
One-time user	Specifies if you want to limit the user to one login.	Select <b>Users &gt; One-time user</b> to enable this option.
Enabled	This option is used by the administrator.	Select <b>Users &gt; Enabled</b> to enable this option.
Require users to change password at next sign in	Specifies if you want to force users to change their password at the next login.	Select <b>Users &gt; Require users to change password at next sign in</b> to enable this option.
<b>Server Catalog &gt; Expressions tab</b>		

**Table 1: Secure Access Local Authentication Server Instance Configuration Details** *(continued)*

Option	Function	Your Action
name	Specifies the name of the local authentication server instance.	Enter a name.
value	Specifies the value of the local authentication server instance.	Enter a value.

- Related Topics**
- Configuring a Secure Access LDAP Server Instance (NSM Procedure)
  - Configuring a Secure Access RADIUS Server Instance (NSM Procedure)
  - Configuring a Secure Access ACE Server Instance (NSM Procedure)

---

Published: 2009-08-20