

Configuring an Infranet Controller Local Authentication Server Instance (NSM Procedure)

The Infranet Controller enables you to create one or more local databases of users who are authenticated by the Infranet Controller. You might want either to create local user records for users who are normally verified by an external authentication server that you plan to disable or to create a group of temporary users.

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 Infranet Controller for which you want to configure a local authentication server instance.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify local authentication server instance settings as specified in Table 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Local Authentication Server Instance Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies the local auth server instance name.	Enter a name for the local authentication server instance.
Auth Server Type	Specifies the auth server type.	Select Local Authentication .
Local Auth Settings		
Minimum password length (characters)	Specifies the minimum number of characters that a password must have.	Enter the minimum password length.
Maximum password length	Specifies the maximum number of characters that a password can consist of.	Enter the maximum length of the password.
Minimum number of digits required in the password (digits)	Specifies the minimum number of digits that must be present in the password.	Enter the minimum number of digits that must be present in the password.
Minimum number of letters required in the password (letters)	Specifies the minimum number of letters that must be present in the password.	Enter the minimum number of digits that must be present in the password.

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

Option	Function	Your Action
Require passwords to have a mix of UPPER and LOWER CASE letters	Specifies that the password contain both upper- and lowercase letters.	Select Local Auth Settings > Require passwords to have a mix of UPPER and LOWER CASE letters to enable this option.
Require password to be different from username	Specifies that the password must be different from the username.	Select Local Auth Settings > Require password to be different from username to enable this option.
Require new passwords to be different from previous password	Specifies that the new password must be different from the previous password.	Select Local Auth Settings > Require new passwords to be different from previous password to enable this option.
Allow users to change their passwords	Specifies that users can change their passwords.	Select Local Auth Settings > Allow users to change their passwords to enable this option.
Force user to change password (days)	Specifies the days after which the user would be forced to change the password.	Enter the number of days after which the password expires.
Prompt user to change password (days)	Specifies the number of days after which users are prompted to change their password.	Enter the number of days after which users are prompted to change their password.
Password stored as clear text	Enables CHAP and EAP-MD5-Challenge to work with local auth servers.	Select the check box. NOTE: Be aware of the security implications of storing passwords as clear text.
Users		
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 that the user is limited to one login.	Select Users > One-time user to enable this option.
Enabled	Allows the administrator to selectively enable or disable any user (one time or permanent).	Select Users > Enabled to enable this option.
Require user to change password at next sign in	Specifies that users must change their password at the next login.	Select Users > Require users to change password at next sign in to enable this option.
Admin Users		

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

Option	Function	Your Action
	<p>You can create user administrators to give individuals with user-level permissions some administrative capabilities on the Infranet Controller. A user administrator can add new users, change passwords, delete existing users, specify an expiration time, and specify one-time privileges for guest accounts.</p> <p>NOTE: User administrators can only administer local authentication servers.</p>	
Username	Specifies the username of the user who you want to manage accounts for the selected authentication server. This user does not need to be added as a local user on the server.	Enter the username.
Realm name	Specifies the authentication realm that the user administrator maps to when signing in to the Infranet Controller.	Select the authentication realm.
Server Catalog > Expressions tab		
name	Specifies the name of the expression.	Enter a name for the expression.
value	Specifies the value(s) of the expression.	Enter a value for the expression.

- Related Topics**
- Configuring an Infranet Controller LDAP Server Instance (NSM Procedure)
 - Configuring an Infranet Controller RADIUS Server Instance (NSM Procedure)
 - Configuring an Infranet Controller RSA ACE/Server Instance (NSM Procedure)

Published: 2009-08-20