

Configuring a Secure Access Active Directory or NT Domain Instance (NSM Procedure)

To configure an Active Directory or Windows NT domain 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 an Active Directory or NT domain 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 to identify the server instance.
6. Select **AD/NT 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: Active Directory or NT Domain Instance Configuration Details

Option	Function	Your Action
AD/NT Settings > General tab		
Primary Domain Controller or Active Directory	Specifies the name or IP address for the primary domain controller or Active Directory server.	Enter the name or IP address.
Secondary Domain Controller or Active Directory	Specifies the name or IP address for the backup domain controller or Active Directory server.	Enter the name or IP address.
Domain	Specifies the domain name of the Active Directory or Windows NT server.	Enter the domain name of the Active Directory or Windows NT domain. NOTE: For example, if the Active Directory domain name is us.amr.asgqa.net and you want to authenticate users who belong to the US domain, enter US as the domain.

Table 1: Active Directory or NT Domain Instance Configuration Details (continued)

Option	Function	Your Action
Allow domain to be specified as part of username	Allows users to sign in by entering a domain name in the Username box in the format: domain\username	Select AD/NT Settings > General > Allow domain to be specified as part of username to enable this feature.
Allow trusted domains	Allows users to get group information from all trusted domains within a forest.	Select AD/NT Settings > General > Allow trusted domains to enable this feature.
Domain Controller is a Windows 2008 server	Specifies if the backend domain controller is a Windows 2008 server. TIP: The Windows 2008 server has several enhancements to the Active Directory server, which is now called Active Directory Domain Services.	Select Domain Controller is a Windows 2008 server to enable this feature.
Admin Username	Specifies an administrator username for the AD or NT server.	Enter an administrator username for the AD or NT server.
Admin Password	Specifies an administrator password for the AD or NT server.	Enter an administrator password for the AD or NT server.
Kerberos (most secure)	Allows the Secure Access device to send user credentials to Kerberos.	Select AD/NT Settings > General > Kerberos (most secure) to enable this feature.
NTLMV2 (moderately secure)	Allows the Secure Access device to send user credentials to NTLMv2.	Select AD/NT Settings > General > NTLMV2 (moderately secure) to enable this feature.
NTLMV1 (least secure)	Allows the Secure Access device to send user credentials to NTLMv1.	Select AD/NT Settings > General > NTLMV1 (least secure) to enable this feature.
Use LDAP to get Kerberos realm name	Allows the Secure Access device to retrieve the Kerberos realm name from the Active Directory server using the specified administrator credentials.	Select AD/NT Settings > General > Specify Kerberos realm name to enable this feature.
Specify Kerberos realm name	Specifies Kerberos realm name.	Enter the name.
AD/NT Settings > Advanced tab		
User may belong to Domain Local Groups across trust boundaries	Specifies that the selected user belongs to the Domain Local Groups who honor trust relationships in the Active Directory.	Select AD/NT Settings > Advanced > User may belong to Domain Local Groups across trust boundaries to enable this feature.
Container Name	Specifies the name that the Secure Access device uses to join the specified Active Directory domain as a computer.	Enter the computer name.

Table 1: Active Directory or NT Domain Instance Configuration Details (continued)

Option	Function	Your Action
Server Catalog > Expressions tab		
Name	Specifies a name for the user expression in the Active Directory or NT domain server user directory.	Enter a name.
Value	Specifies a value for the user expression in the Active Directory or NT Domain server user directory.	Enter a value.
Server Catalog > Groups tab		
Name	Specifies the name of the group	Enter a name.
Groups	Specifies the admin's domain local groups information.	Enter a name.
AD Group	Specifies the group that contains the administrators to enable centralized administration in an Active Directory domain.	Enter a name.

- Related Topics**
- Configuring a Secure Access NIS Server Instance (NSM Procedure)
 - Configuring Secure Access Authentication Realms (NSM Procedure)
 - Configuring a Secure Access SAML Server Instance (NSM Procedure)

Published: 2009-08-20