Configuring Windows NT Servers for AAA

This chapter describes how to configure Windows NT servers used in AAA and includes the following sections:

Information About Windows NT Servers

The ASA supports Microsoft Windows server operating systems that support NTLM Version 1, collectively referred to as NT servers.

Note Windows NT servers have a maximum length of 14 characters for user passwords. Longer passwords are truncated, which is a limitation of NTLM Version 1.

Licensing Requirements for Windows NT Servers

Model	License Requirement
All models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

IPv6 Guidelines

Supports IPv6.

Additional Guidelines

- You can have up to 100 server groups in single mode or 4 server groups per context in multiple mode.
- Each group can have up to 16 servers in single mode or 4 servers in multiple mode.
- If you need to configure fallback support using the local database, see the "Fallback Support" section on page 33-2 and the "How Fallback Works with Multiple Servers in a Group" section on page 33-2.

Configuring Windows NT Servers

This section includes the following topics:

Task Flow for Configuring Windows NT Servers

Step 1 Add a AAA server group. See the "Configuring Windows NT Server Groups" section on page 37-3.

Step 2 For a server group, add a server to the group. See the "Adding a Windows NT Server to a Group" section on page 37-4.

Configuring Windows NT Server Groups

If you want to use a Windows NT server for authentication, authorization, or accounting, you must first create at least one Windows NT server group and add one or more servers to each group. You identify Windows NT server groups by name.

To add a Windows NT server group, perform the following steps:

Detailed Steps

	Command	Purpose

Step 1	**aaa-server** *server_tag* **protocol nt**
	
	Example:
	`ciscoasa(config)# aaa-server servergroup1 protocol nt`
	`ciscoasa(config-aaa-server-group)#`
		Identifies the server group name and the protocol.
		
		When you enter the **aaa-server protocol** command, you enter aaa-server group configuration mode.

Step 2	**max-failed-attempts** *number* **Example:** `ciscoasa(config-aaa-server-group)# max-failed-attempts 2`	Specifies the maximum number of requests sent to a Windows NT server in the group before trying the next server. The *number* argument can range from 1 and 5. The default is 3. If you configured a fallback method using the local database (for management access only), and all the servers in the group fail to respond, then the group is considered to be unresponsive, and the fallback method is tried. The server group remains marked as unresponsive for a period of 10 minutes (by default), so that additional AAA requests within that period do not attempt to contact the server group, and the fallback method is used immediately. To change the unresponsive period from the default, see the **reactivation-mode** command in the next step. If you do not have a fallback method, the ASA continues to retry the servers in the group.
Step 3	**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**} **Example:** `ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20`	Specifies the method (reactivation policy) by which failed servers in a group are reactivated. The **depletion** keyword reactivates failed servers only after all of the servers in the group are inactive. The **deadtime** *minutes* keyword-argument pair specifies the amount of time in minutes, between 0 and 1440, that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers. The default is 10 minutes. The **timed** keyword reactivates failed servers after 30 seconds of down time.

Examples

The following example shows how to add a Windows NT domain server group:

```
ciscoasa(config)# aaa-server NTAuth protocol nt
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server NTAuth (inside) host 10.1.1.4
ciscoasa(config-aaa-server-host)# nt-auth-domain-controller primary1
ciscoasa(config-aaa-server-host)# exit
```

Adding a Windows NT Server to a Group

To add a Windows NT server to a group, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**aaa-server** *server_group* [*interface_name*] **host** *server_ip* **Example:** `ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1`	Identifies the Windows NT server and the server group to which it belongs. When you enter the **aaa-server host** command, you enter aaa-server host configuration mode.
Step 2	**timeout** *hh:mm:ss* **Example:** `ciscoasa(config-aaa-server-host)# timeout 15`	Specifies the length of time, in hours, minutes, and seconds, that the ASA waits for a response from the primary server before sending the request to the backup server.
Step 3	**server-port** *port_number* **Example:** `ciscoasa(config-aaa-server-host)# server-port 139`	Specifies the server port as port number 139, or the TCP port number used by the ASA to communicate with the Windows NT server.
Step 4	**nt-auth-domain-controller** *string* **Example:** `ciscoasa(config-aaa-server)# nt-auth-domain controller primary1`	Specifies the name for the Windows NT authentication domain controller. The *string* argument represents the hostname (no more than 15 characters) of the NT Primary Domain Controller for this server (for example, PDC01). You must enter a name, and it must be the correct hostname for the server whose IP address you added in the Authentication Server Address field. If the name is incorrect, authentication fails.

Examples

The following example shows how to add a Windows NT domain server to the NTAuth server group:

```
ciscoasa(config)# aaa-server NTAuth (inside) host 10.1.1.4
ciscoasa(config-aaa-server-host)# timeout 15
```

```
ciscoasa(config-aaa-server-host)# server-port 139
ciscoasa(config-aaa-server-host)# nt-auth-domain-controller primary1
ciscoasa(config-aaa-server-host)# exit
```

Monitoring Windows NT Servers

To monitor Windows NT servers,enter one of the following commands:

Command	Purpose
show aaa-server	Shows the configured Windows NT server statistics. To clear the Windows NT server statistics, enter the **clear aaa-server statistics** command.
show running-config aaa-server	Shows the Windows NT server running configuration. To clear Windows NT server configuration, enter the **clear configure aaa-server** command.

Feature History for Windows NT Servers

Table 37-1 lists each feature change and the platform release in which it was implemented.

Table 37-1 Feature History for Windows NT Servers

Feature Name	Platform Releases	Feature Information
Windows NT Servers for AAA	7.0(1)	Describes support for Windows NT Servers and how to configure them for AAA. We introduced the following commands: **aaa-server protocol**, **max-failed-attempts**, **clear configure aaa-server**, **clear aaa-server statistics**, **reactivation-mode, aaa-server host, server-port**, **timeout**, **nt-auth-domain-controller**, **show aaa-server**, **show running-config aaa-server**.