ACOS 6.0.8
Management Access and Security Guide

December, 2025

Information in this document is subject to change without notice.

PATENT PROTECTION

A10 Networks, Inc. products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc. products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at: a10-virtual-patent-marking.

TRADEMARKS

A10 Networks, Inc. trademarks are listed at: a10-trademarks

CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc. or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc. has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc. assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc. for current information regarding its products or services. A10 Networks, Inc. products and services are subject to A10 Networks, Inc. standard terms and conditions.

ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location, which can be found by visiting www.a10networks.com.

Table of Contents

Administrator Accounts

This chapter describes how to configure and modify administrator accounts for management access to ACOS.

NOTE: The user can now manage the passwords for local authentication in the ACOS device. This password policy management feature helps the user with more secured log-in options. For more information on this topic, see Configuring Password Policy for Local Authentication.

The following topics are covered:

Overview

The following topics are covered:

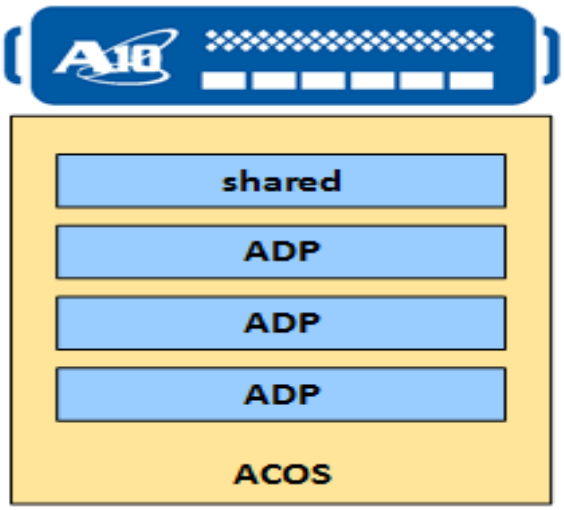
Default Administrator Account, “Admin”

By default, ACOS is provisioned with one administrator account named “admin” and one partition named “shared.” The default admin account has root access to ACOS. Root access means that “admin” has read-write privileges to all ACOS objects across all partitions.

Default Partition, “Shared”

By default, all configurations run in the shared partition. To run configurations in isolation from each other, as if they were running on multiple separate ACOS devices, the user can create multiple partitions, called Application Delivery Partitions (ADPs), as illustrated in Figure 1.

Figure 1 : Application Delivery Partitions



Partitioning and Partition Administrators

The Ethernet interfaces and other physical ACOS objects are configured and run only in the shared partition. All other ACOS objects can be configured and run in any partition.

If an ACOS object is configured in the shared partition, it is available to processes and users of all the ADPs. However, if an ACOS object is created in an ADP, it is available only to processes and users in that ADP. In other words, partitioning allows the ACOS device to be logically segmented to support separate systems for separate customers. This provides isolation of configuration objects and also isolates administration of these components.

Each ADP has its own set of Layer 3 - 7 (L3V) or Layer 4 - 7 (Service) independently running processes. Communication between partitions is through routed interfaces.

NOTE: ADPs are also called private partitions in the ACOS User Guides and reference books.

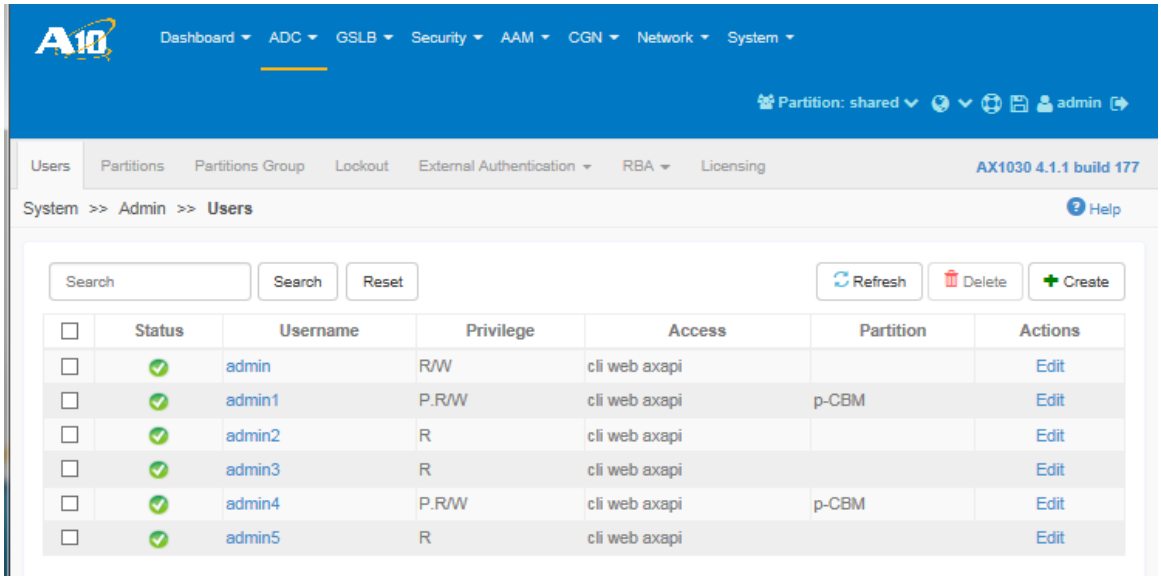
The section Configuration Instructions and Examples shows how to create administrator accounts.

NOTE: Also see "**Configuring Admin Access to Partitions**" and "**Configuring Partition Admin Accounts**" in the *Configuring Application Delivery Partitions* Guide.

Showing the Administrator Accounts in the GUI Mode

The **Users** window in the ACOS GUI displays the administrator accounts. Navigate to **System** >> **Admin** >> **Users**. The following screen capture shows an example of this window for five admin accounts, one of which the root admin account is admin:

Figure 2 : Administrator Account in GUI Mode



Showing the Administrator Accounts in the CLI Mode

Use the `show admin` command to show the administrator accounts. The following example shows the default `admin` account plus one other admin account with the

username, `adminuser1`:

```
ACOS(config-admin:adminuser1)# show admin
Total number of configured users:  2
  Privilege   R: read-only, W: write, P: partition, HM: external health
monitor, En: Enable
  Access Type   C: cli, W: web, A: axapi

UserName                        Status    Privilege Access UserType
Partition
-------------------------------------------------------------------------
admin                           Enabled   R/W/HM    C/W/A  Local
adminuser1                      Enabled   P.R/W     C/W/A  Local
companyA
```

Configuration Instructions and Examples

The following topics are covered:

Overview

The “**admin**” account has global read/write privileges and can configure additional administrator accounts with the following settings:

- A username and password

NOTE: Administrator username is case insensitive. For more information on the supported special characters in password, refer Special Character Support in Passwords.

- An IP host or subnet address from which the administrator can log in
- A user interface that the administrator can use (CLI, GUI, or aXAPI)
- Authorization to access and manage External Health Monitor files.
- A private partition, if applicable
- An account state (enabled or disabled)

NOTE: If you are configuring an administrator account for a private partition, see "Configuring Partition Admin Accounts" in the *Configuring Application Delivery Partitions* guide.

Special Character Support in Passwords

Table 1 list the special characters supported for each type of password you can enter in the CLI.

Table 1 : Special Characters in Passwords and Strings

Password Type	Special Character Support
Admin and Enable password	Admin and enable passwords can contain any of the following ASCII characters: `a-z A-Z 0-9 <space> ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~`
ACOS device hostname	Strings for these items can contain any of the following ASCII characters: `a-z A-Z 0-9 - . ( )`
SNMPv3 user authentication passwords	Strings for these items can contain any of the following ASCII characters: `a-z A-Z 0-9 - . ( )`
RADIUS shared secrets	The device hostname can contain any of the following

Table 1 : Special Characters in Passwords and Strings

Password Type	Special Character Support
	ASCII characters: a-z A-Z 0-9 - . ( )
MD5 passwords for OSPF or BGP	MD5 passwords can be up to 16 characters long. A password string can contain any of the following ASCII characters: a-z A-Z 0-9 <space> ! # $ % ( ) * + , - . : ; = @ [ ] ^ _ ` { | } ~ The password string cannot begin with a blank space, and can not contain any of the following special characters: ' " < > & \ / ?
Passwords used for file import or export	The following characters are supported: a-z A-Z 0-9 ! $ % ( ) * + , - . : [ ] ^ _ ` { } | ~ =
Passwords used for server access in health monitors	The following characters are supported: a-z A-Z 0-9 <space> ! # $ % ( ) * + , - . : ; = @ [ ] ^ _ ` { | } ~ The following characters are not supported: " < > & \ / ?
SSL certificate passwords	The following characters are supported: a-z A-Z 0-9 <space> ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
SMTP passwords	The following characters are not supported: ' " < > & \ / ?

How To Enter Special Characters in the Password String

You can use an opening single-or double-quotation mark without an ending one.

In this case, '" becomes ", and "' becomes '.

Escape sequences are required for a few of the special characters:

- " – To use a double-quotation mark in a string, enter the following:\"
- ? – To use a question mark in a string, enter the following sequence:\077
- \ – To use a back slash in a string, enter another back slash in front of it:\\

For example, to use the string a"b?c\d, enter the following: "a\"b\077c\\d"

The \ character will be interpreted as the start of an escape sequence only if it is enclosed in double quotation marks. (The ending double quotation mark can be omitted.) If the following characters do not qualify as an escape sequence, they are taken verbatim; for example, \ is taken as \, "\x41" is taken as A (hexadecimal escape), "\101" is taken as A (octal escape), and "\10" is taken as \10.

NOTE: To use a double-quotation mark as the entire string, "\"". If you enter \", the result is \. Using a single character as a password is not recommended. It is recommended not to use i18n characters. The character encoding used on the terminal during password change might differ from the character encoding on the terminal used during login.

Configuring a Global Admin Account using GUI

The user can configure a Global Admin Account through the GUI mode. The following are the various steps and modes to configure an administrator account for **exampleadmin** who has the global read and write privileges, and perform the following steps:

1. Navigate to **System** >> **Admin** >> **Users**.
2. Click **Create**. The **Create User** window appears.
3. Enter **exampleadmin1** in the **Username** field.
4. Enter a password for the new administrator account.
5. Verify that **Enable** is selected in the Enable field (selected by default).

6. In the **Access** section, verify that all three user interfaces are selected (they should be selected by default).
7. In the **Privilege Type** field, to create a global admin account that has access to all partitions, select **Global**.
8. In the **Privilege** field, select **Read/Write** from the drop-down list.
9. Click **Create**.
10. Return to the **Admin** table and verify that the new administrator, **exampleadmin1**, appears in the list.

Configuring a Partition Admin Account using GUI

The user can configure a Partition Admin Account through the GUI mode. The following are the various steps and modes to configure an administrator account that has read and write privileges only in the **p-CBM** partition, perform the following steps:

1. Navigate to **System** >> **Admin** >> **Users**.
2. Click **Create**. The **Create User** window appears.
3. Enter **exampleadmin2** in the **Username** field.
4. Enter a password for the new administrator account.
5. Verify that **Enable** is selected in the Enable field (selected by default).
6. In the **Access** section, verify that all three user interfaces are selected (they should be selected by default).
7. In the **Privilege Type** field, to create a global admin account that has access to all partitions, select **Partition**.
8. In the **Privilege** field, select **Read/Write** from the drop-down list.
9. In the **Partition Privileges** field, select the **p-CBM** partition from the drop-down list.
10. In the **Action** box, save the selected partition by clicking the red floppy disk icon.
11. Click the **Create** button.
12. Return to the **Admin** table and verify the new administrator, **exampleadmin2**, appears in the list.

Configuring Admin Accounts in the CLI Mode

Users can configure Admin Accounts through CLI mode.

The following topics are covered:

Creating a New Admin Account

The user can create a new Admin Account through the CLI. The following are the steps and modes:

1. Specify the admin username and password using the `admin` command

```
ACOS(config)# admin adminuser1 password
Password:
Retype password:
Modify Admin User successful!
```

   The password is entered as an obfuscated text.

2. Check the status and privileges of the newly created `adminuser1`. By default, global read-only privilege is granted to the CLI, the GUI (Web), and the AXAPI:

```
ACOS(config-admin:adminuser1)# show admin
UserName                        Status    Privilege   Access UserType
Partition
-------------------------------------------------------------------
admin                           Enabled   R/W/HM      C/W/A  Local
adminuser1                      Enabled   R           C/W/A  Local
```

Changing the Admin Interface (CLI, GUI, and AXAPI)

Administrators can manage ACOS through its command line interface (CLI), its graphical user interface (GUI), or its application program interface (AXAPI).

1. To change admin interfaces that `adminuser1` has access to, enter the `access` command specifying the allowed interfaces:

```
ACOS(config-admin:adminuser1)# access cli axapi
```

2. Modify Admin User successful!

   Verify the modified `adminuser1`:

```
ACOS(config-admin:adminuser1)# show admin
UserName                        Status    Privilege   Access UserType
Partition
-------------------------------------------------------------------
admin                           Enabled   R/W/HM      C/W/A  Local
adminuser1                      Enabled   R           C/A    Local
```

Changing the Read and Write Privileges

The user can change the Read and Write Privileges. The following are the steps and modes:

1. To modify the global read/write user privileges, enter the `privilege` command. The option `write` includes read:

```
ACOS(config-admin:adminuser1)# privilege write
```

2. Modify Admin User successful!

```
Verify the modified adminuser1:
ACOS(config-admin:adminuser1)# show admin
UserName                        Status    Privilege   Access UserType
Partition
-------------------------------------------------------------------
admin                           Enabled   R/W/HM      C/W/A  Local
adminuser1                      Enabled   R/W         C/A    Local
```

Changing HM (Health Monitor) Privilege

HM privilege enables an administrator to access and manage External Health Monitor files. An account with write privilege that does not include HM privilege cannot import, edit, create, or delete External Health Monitor files.

By default, only the ACOS root admin is authorized for HM privilege. It should only be enabled only for other admins sufficiently trusted to perform these operations without malicious purpose or malicious content which could otherwise compromise security in the ACOS system and its deployed environment.

For deployments using the external health monitor feature, the most secure configuration would be to not enable this privilege for configured admins and have all health monitor file operations performed by the ACOS root admin.

Deployments not using the external health monitor feature of ACOS should avoid enabling this privilege for any admins.

NOTE: For more information, see the following:

- Authorization
- A10 Schema File for OpenLDAP
- *Application Delivery and Server Load Balancing Guide* (*Using External Health Methods* section)

The following steps are for authorizing and verifying the privileges:

1. To authorize external health monitor privileges, in addition to all read/write access, enter the `privilege hm` command.

```
ACOS(config-admin:adminuser1)# privilege hm
```

2. Modify Admin User successful!

```
Verify the modified adminuser1:
ACOS(config-admin:adminuser1)# show admin
UserName                        Status    Privilege   Access UserType
Partition
-------------------------------------------------------------------------
admin                           Enabled   R/W/HM      C/W/A  Local
adminuser1                      Enabled   R/W/HM      C/A    Local
```

Changing the Partition Privileges

The user can change the Partition Privileges. The following are the steps and modes:

1. To set per-partition enable-disable user privileges, remove the global privileges and enter the `privilege` command with the name of the partition:

```
ACOS(config-admin:adminuser1)# no privilege write
Modify Admin User successful!
ACOS(config-admin:adminuser1)# privilege partition-enable-disable
Partition1
Modify Admin User successful!
```

2. Verify the modified `adminuser1`:

```
ACOS(config-admin:adminuser1)# show admin
UserName                        Status    Privilege   Access UserType
Partition
-------------------------------------------------------------------------
admin                           Enabled   R/W/HM      C/W/A  Local
adminuser1                      Enabled   P.En        C/A    Local
Partition1
```

Configuring a Trusted Host IP Address

The user can configure a Trusted Host IP Address. The following are the steps and modes:

1. To set up a trusted host IP, enter the `trusted-host` command:

```
ACOS(config-admin:adminuser1)# trusted-host 255.255.255.255 /24
```

2. To disable the `adminuser1`, enter the `disable` command:

```
ACOS(config-admin:adminuser1)# disable adminuser1
Modify Admin User successful!
```

Configuring Partition Admin Account for L3V Partition in CLI Mode

The partition admin account for L3V partition can be configured using the `admin` or `partition-admin` command. Although these commands are similar, when the

`partition-admin` command is used, the created user is valid even if the creator admin user is removed. This command is supported only in the L3V partitions, Service Partitions are not supported. Also, the current L3V partition is assigned automatically to the user account.

For more information on `partition-admin` command, refer to the *Command Line Interface Reference Guide*.

Creating a Partition Admin Account for L3V partition

Follow the steps given below to create a partition admin account in L3V partition:

1. Specify the partition admin username and password using the `partition-admin` command.

```
ACOS[Partition_1234](config)# partition-admin user1 password <password>
```

2. Check the status and privileges of the newly created account using the `show admin` command. By default, `partition-read` privilege is set for a new account.

```
ACOS[Partition_1234](config-admin:user1)# show admin
Total number of configured users: 2
Privilege R: read-only, W: write, P: partition, HM: external health
monitor, En: Enable
Access Type   C: cli, W: web, A: axapi

UserName Status Privilege Access UserType Partition
------------------------------------------------------------------------
admin Enabled R/W/HM      C/W/A Local
user1 Enabled P.R         C/W/A Local    Partition_1234
```

Changing Privileges of Partition Admin Account

Follow the steps given below to changes privilege of the partition admin account:

1. Change the privilege of the partition admin account using the `privilege` command:

```
ACOS[Partition_1234](config-admin:user1)# privilege partition-write
Modify Admin User successful!
```

2. Verify the change in the privilege using the `show admin` command:

```
ACOS[Partition_1234](config-admin:user1)# show admin
Total number of configured users: 2
Privilege R: read-only, W: write, P: partition, HM: external health
monitor, En: Enable
Access Type   C: cli, W: web, A: axapi

UserName Status Privilege Access UserType Partition
-----------------------------------------------------------------------
admin Enabled R/W/HM C/W/A Local
user1 Enabled P.R/W C/W/A Local   Partition_1234
```

Deleting an Administrator Account

The following topics are covered:

Overview

An administrator with root privileges can delete other administrator accounts.

Before you delete an administrator account, complete the following tasks:

- Determine whether the administrator has active sessions.
- Clear any sessions the administrator has open.

To delete an admin account, you first must terminate any active sessions the administrator account has open. The account is not deleted if open sessions exist.

Deleting an Administrator Account in the GUI Mode

The user can delete an Administrator Account through the GUI mode. The following are the steps and modes to delete an administrator account:

1. Navigate to **System** >> **Admin** >> **Users**.
2. Select the checkbox next to the administrator name that you want to delete.

3. Click **Delete**.

Deleting an Administrator Account in the CLI Mode

The user can delete an Administrator Account through the CLI mode. The following are the steps and modes to delete an administrator account:

To delete an admin account enter the **no admin** command with the username of the administrator.

```
ACOS(config)# no admin adminuser1
```

Configuring Password Policy for Local Authentication

The user can now manage the passwords for local authentication in the ACOS device. The password management feature helps the user with more secured log-in options.

The following topics are covered:

Overview

The password policy management is designed with a key focus on the following parameters:

- Complexity (Password Complexity)
- Aging (Password Aging)
- History (Password History)
- Checks (Password Checks)

Complexity (Password Complexity)

The system password-policy complexity is used for the configuration of the password policy management.

Password Complexity Matrix

A password policy management is implied for the better security and safety of the accounts/user information. A pre-defined set of complex password uses different types of characters in unique ways to increase the security.

The following Table 2 lists out the applicable matrix for password policy management in the ACOS systems in numbers.

Table 2 : Password Complexity Matrix

Complexity	**Minimum Length**	**Minimum Lowercase**	**Minimum Uppercase**	**Minimum Numbers**	**Minimum Special Characters**	**Change Minimum Char-acters**
DEFAULT	9	1	1	1	1	1
STRICT	8	2	2	2	1	8
MEDIUM	6	2	2	1	1	6
SIMPLE	4	1	1	1	0	4

If a password does not meet the respective complexity requirements, a message 'Invalid password. Does not match password requirements' is displayed.

If a new password entered is same as the previous password, a message 'The password could not be same with previous one' is displayed.

Password Complexity in the CLI

The **`system password-policy complexity`** *`policy_level`* command is used for the configuration of the password policy management for the following supported options:

- Strict
- Medium

- Default
- Simple

Based on the policy configured, the password strength is allowed, and it is applicable for all the incoming new users with the admin credentials.

The regulatory requirements for the password policy management in the CLI can be configured using the following syntax:

```
system password-policy complexity [Strict | Medium | Default | Simple]
{aging [Strict | Medium | Simple]  | history [Strict | Medium | Simple]  |
min-pswd-len <8-63> | username-check [enable|disable] | repeat-character-
check [enable|disable] | forbid-consecutive-character <3-5>}
```

For more information on **system password-policy complexity** command, see *Command Line Interface Reference Guide*.

Table 3 lists out the applicable matrix for the password policy management in the ACOS systems using the CLI modes.

Table 3 : Password Complexity Matrix in the Command Line

SEVERITY	Command Line	Minimum Value
DEFAULT	#define DEFAULT_POLICY_LEN	9
	#define DEFAULT_UCASE_LEN	1
	#define DEFAULT_LCASE_LEN	1
	#define DEFAULT_NUMBER_LEN	1
	#define DEFAULT_SPL_CHR_LEN	1
STRICT	#define STRICT_POLICY_LEN	8
	#define STRICT_UCASE_LEN	2
	#define STRICT_LCASE_LEN	2
	#define STRICT_NUMBER_LEN	2
	#define STRICT_SPL_CHR_LEN	1
MEDIUM	#define MEDIUM_POLICY_LEN	6
	#define MEDIUM_UCASE_LEN	2
	#define MEDIUM_LCASE_LEN	2

SEVERITY	Command Line	Minimum Value
	#define MEDIUM_NUMBER_LEN	1
	#define MEDIUM_SPL_CHR_LEN	1
SIMPLE	#define SIMPLE_POLICY_LEN	4
	#define SIMPLE_UCASE_LEN	1
	#define SIMPLE_LCASE_LEN	1
	#define SIMPLE_NUMBER_LEN	1
	#define SIMPLE_SPL_CHR_LEN	0

Default

Password Complexity Combination

The number of characters, in which, at least, **one** instance of the position must be changed within the existing password.

Password Complexity Option

The following details list the applicable matrix for **Default** option in numbers for the password policy management in the ACOS systems.

- Severity: **Medium**
- Minimum Length: **9**
- Minimum Lowercase: **1**
- Minimum Uppercase: **1**
- Minimum Numbers: **1**
- Minimum Special Characters: **1**

Strict

Password Complexity Combination

The number of characters, in which, at least, **eight** instances of the position must be changed within the existing password.

Password Complexity Option

The following details list the applicable matrix for the **Strict** option in numbers for the password policy management in the ACOS systems.

- Severity: **Strict**
- Minimum Length: **8**
- Minimum Lowercase: **2**
- Minimum Uppercase: **2**
- Minimum Numbers: **2**
- Minimum Special Characters: **1**

Medium

Password Complexity Combination

The number of characters, in which, at least, **six** instances of the position must be changed within the existing password.

Password Complexity Option

The following details list the applicable matrix for the **Medium** option in numbers for the password policy management in the ACOS systems.

- Severity: **Medium**
- Minimum Length: **6**
- Minimum Lowercase: **2**
- Minimum Uppercase: **2**
- Minimum Numbers: **1**
- Minimum Special Characters: **1**

Simple

Password Complexity Combination

The number of characters, in which, at least, **four** instances of the position must be changed within the existing password.

Password Complexity Option

The following details list the applicable matrix for **Simple** option in numbers for the password policy management in the ACOS systems.

- Severity: **Simple**
- Minimum Length: **4**
- Minimum Lowercase: **1**
- Minimum Uppercase: **1**
- Minimum Numbers: **1**
- Minimum Special Characters: **0**

Configuration Commands, Details, and Examples

Users can verify the password configuration for a new admin user, under the password-policy. The verification of the new admin password validation is based on password-policy complexity such as Default, Strict, Medium, and Simple, whichever the level of complexity chosen.

Password-Policy Complexity Default

For the **Default** option, the characters must be changed at least ***one*** instance of the position within the changed password.

```
ACOS(config)(NOLICENSE)#admin a10
ACOS(config-admin:a10)(NOLICENSE)#pas
ACOS(config-admin:a10)(NOLICENSE)#password  <<If you enter 'WorlD@182', it
is a valid password>>
ACOS(config-admin:a10)(NOLICENSE)#password  <<If you enter 'a10network',
it is an invalid password>>
Invalid password. Does not match password requirements
```

Password-Policy Complexity Strict

For the **Strict** option, the characters must be changed at least ***eight*** instances of the position within the changed password.

```
ACOS(config)(NOLICENSE)#admin a10
ACOS(config-admin:a10)(NOLICENSE)#pas
ACOS(config-admin:a10)(NOLICENSE)#password  <<If you enter 'A10Network',
it is an invalid password>>
```

```
Invalid password. Does not match password requirements
ACOS(config-admin:a10)(NOLICENSE)#password  <<If you enter 'WorlD@12', it
is a valid password>>
ACOS(config-admin:a10)(NOLICENSE)#password  <<If you re-enter 'WorlD@12',
it is an invalid password>>
The password could not be same with previous one.
```

Password-Policy Complexity Medium

For the **Medium** option, the characters must be changed at least ***six*** instances of the position within the changed password.

```
ACOS(config)(NOLICENSE)#admin a10
ACOS(config-admin:a10)(NOLICENSE)#pas
ACOS(config-admin:a10)(NOLICENSE)#password <<If you enter '@10NeT', it is
an invalid password>>
Invalid password. Does not match password requirements
ACOS(config-admin:a10)(NOLICENSE)#password  <<If you enter 'A10Net!123',
it is a valid password>>
```

Password-Policy Complexity Simple

For the **Simple** option, the characters must be changed at least ***four*** instances of the position within the changed password.

```
ACOS(config)(NOLICENSE)#admin a10
ACOS(config-admin:a10)(NOLICENSE)#password <<If you enter 'A10n', it is a
valid password>>
ACOS(config-admin:a10)(NOLICENSE)#password <<If you enter 'a10n', it is an
invalid password>>
Admin password error
```

Configuration Commands for Complexity (Password Complexity)

The default password policy complexity is enforced under the following conditions:

- When a user logs in for the first time on a new ACOS device.
- When the **`system-reset`** command is executed.
- When the **`erase`** command is run without the "preserve-accounts" flag.

However, the system does not enforce you to change the admin password as per the default password-policy complexity after you execute the reboot, reload, and upgrade commands.

To enable password-policy complexity options, use the following command:

```
password-policy complexity <policy_level>
Complexity Default:
!
system password-policy complexity Default
!
Complexity Strict:
!
system password-policy complexity Strict
!
Complexity Medium:
!
system password-policy complexity Medium
!
Complexity Simple:
!
system password-policy complexity Simple
!
```

Aging (Password Aging)

This parameter defines the number of defined days for the global password complexity matrix for all the users with admin privilege of the device.

The aging factor is determined by a shadow entry for the admin user. A new shadow file is provided for the new admin user. This file contains the lastly modified change history, password change time, warning for the aging factor, expiry day, for the user.

NOTE: The components of the password policy aging are not applicable for the default admin user. Only the password policy complexity is applicable for the default admin user.

Strict

The maximum validity of the number of days, the user can use the stored passwords: **60 Days**

Medium

The maximum validity of the number of days, the user can use the stored passwords: **90 Days**

Simple

The maximum validity of the number of days, the user can use the stored passwords: **120 Days**

Configuration Commands for Aging (Password Aging)

To enable this feature enhancement, a new set of commands is added. This new command is disabled by default. The commands are as follows:

```
Strict:
!
system password-policy complexity Strict aging Strict
!

Medium:
!
system password-policy complexity Strict aging Medium
!

Simple:
!
system password-policy complexity Strict aging Simple
!
```

Old Passwords

The ACOS is designed to store the old passwords of the user.

NOTE: A cron job scheduler, which is a time-based, automated scheduler, running in the background, and performing repetitive tasks, is added. It helps in determining the aging of the password and evaluating the old password matrix, by running a script.

History (Password History)

The ACOS is designed to store the previous instances of the passwords of a user, based on the options the user selects.

NOTE: The components of the password policy history are not applicable for the default admin user. Only the password policy complexity is applicable for the default admin user.

Strict

The number of previous passwords stored: **5**

Medium

The number of previous passwords stored: **4**

Simple

The number of previous passwords stored: **3**

Configuration Commands for History (Password History)

To enable this feature enhancement, a new set of commands is added. This new command is disabled by default. The commands are as follows:

```
Strict:
!
system password-policy complexity Strict history Strict
!

Medium:
!
system password-policy complexity Strict history Medium
!
```

```
Simple:
!
system password-policy complexity Strict history Simple
!
```

Checks (Password Checks)

The following checks are introduced under all password-policy complexity options to improve the password strength and they are enabled in CLI mode.

Username check

The username-check allows or prevents a user to create a password containing the username for which the password is configured. This check is case-sensitive and is enabled by default.

When this check is enabled, the password cannot contain the corresponding username with the same capitalization of letters.

To enable or disable this check, use the following command:

```
ACOS(config)#system password-policy complexity [Strict | Medium | Default
| Simple] username-check [enable | disable]
```

When this check is enabled, the password cannot contain the corresponding username with the same capitalization of letters. For example, 'pass!@admin1QW' password is invalid for 'admin' user whereas 'pass!@Admin1QW' is valid.

Repeat Character check

The repeat-character-check allows or prevents a user to create a password containing consecutive repeated characters of the same letter or number. This check is case-sensitive and is enabled by default.

To enable or disable this check, use the following command:

```
ACOS(config)#system password-policy complexity [Strict | Medium | Default
| Simple] repeat-character-check [enable | disable]
```

When this check is enabled, the password containing consecutive repeated characters of the same letter or number with the same capitalization of letters is

prohibited. For example, a password containing 'aa', 'AA', '11' is invalid whereas a password containing 'aA', 'Aa' is valid.

Forbid Consecutive Character check

The forbid-consecutive-character check allows or prevents a user to create a password containing sequential row keyboard input of letters or numbers. This check allows sequential row keyboard input of special characters and the letters or numbers not in the same keyboard row. The unallowed repeated length can be configured within the range <3-5> characters. If the length value is set to either 3, 4, or 5, the check is enabled and if it is set to 0, the check is disabled. This check is case-sensitive and is enabled by default.

To enable this check, use the following command:

```
ACOS(config)#system password-policy complexity [Strict | Medium | Default | Simple] forbid-consecutive-character 4
```

When this check is enabled, the password containing sequential row keyboard input of letters or numbers is prohibited. For example, a password containing 'asdf' or 'fdsa' is invalid whereas a password containing 'asd', '123', 'fsa', 'ASdf', '!@#$', 'klzx', 'opas', '90qw' is valid.

To disable this check, use the following command:

```
ACOS(config)#system password-policy complexity [Strict | Medium | Default | Simple] forbid-consecutive-character 0
```

Known Issues/Limitations

The following are the known issues and limitation of the password management for local authentications, which the user must be aware of:

- The length of the password characters supported by the system.
- The number of admin users, which is supported by the system.
- Password Policy is not supported on AWS and OCI platforms.

Configuring the Password Policy Management in the CLI Mode

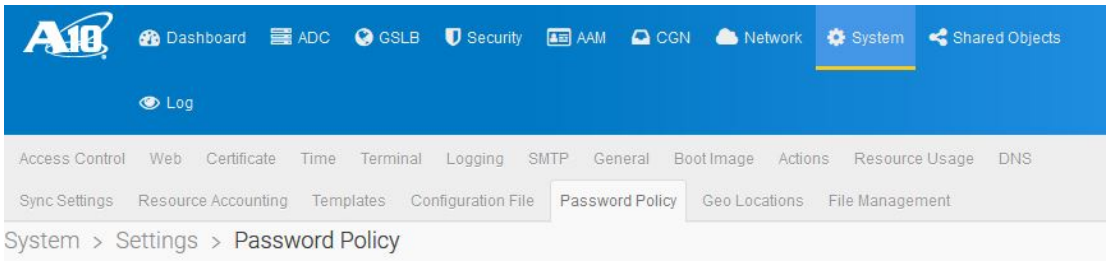
The user can apply the password policy management through the CLI mode using the **`system password-policy complexity`** command:

```
ACOS(config)#system password-policy complexity ?
Strict   Strict: Min length:8, Min Lower Case:2, Min Upper Case:2, Min
Numbers:2, Min Special Character:1, CHANGE Min 8 Characters
Medium   Medium: Min length:6, Min Lower Case:2, Min Upper Case:2, Min
Numbers:1, Min Special Character:1, CHANGE Min 6 Characters
Default  Default: Min length:9, Min Lower Case:1, Min Upper Case:1, Min
Numbers:1, Min Special Character:1, CHANGE Min 1 Character
Simple   Simple: Min length:4, Min Lower Case:1, Min Upper Case:1, Min
Numbers:1, Min Special Character:0, CHANGE Min 4 Characters
```

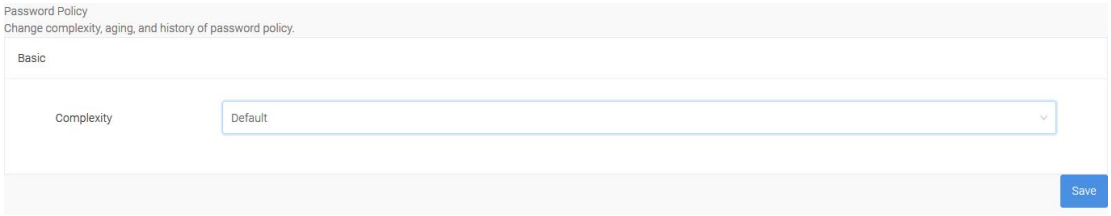
Configuring the Password Policy Management in the GUI Mode

By default, the **Default** password policy is applied. If the user wants to change the password policy management through the GUI mode, perform the following steps:

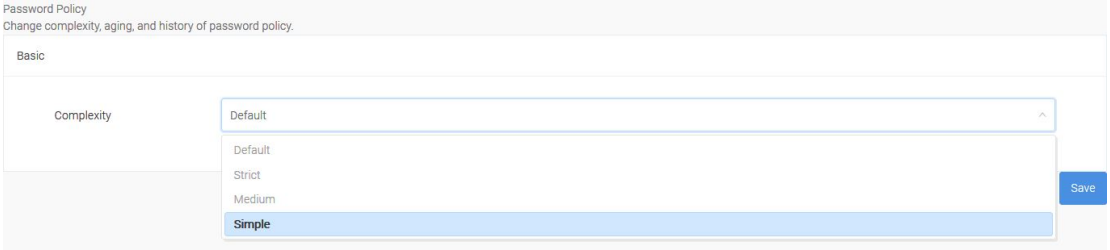
1. Navigate to **System** >> **Settings** >> **Password Policy**.



2. Select **Password Policy**. The **User Interface** window appears.



3. The default screen is **Complexity** with **Default** as the default value.



Navigate to the drop-down menu option under this parameter to see the following options:

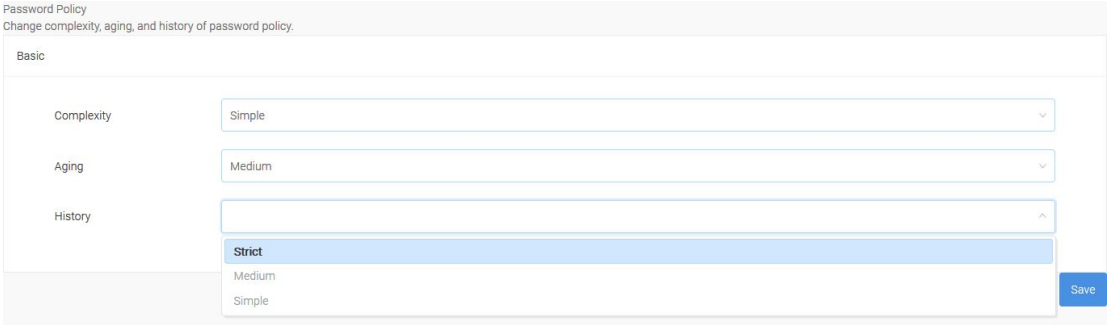
- Strict
- Medium
- Simple

4. Select any option as per your requirement. It leads to the next parameter **Aging**.
5. The default value for Aging is blank or no value.

Navigate to the drop-down menu option under this parameter to see the following options:

- Strict
- Medium
- Simple

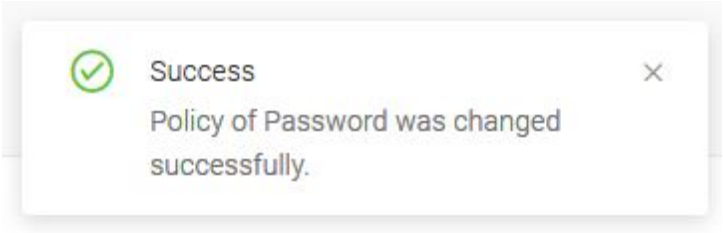
6. Select any option as per your requirement. It leads to the next parameter **History**.
7. The default value for History is blank or no value.



Navigate to the drop-down menu option under this parameter to see the following options:

- Strict
- Medium
- Simple

8. Select any option as per your requirement. Click **Save** button to store this password policy management option for the user.



A confirmation note with **Success** appears, once the creation of this password policy management profile is accepted.

Enforcing the Password Policy for Enable Password

The **`enable-password`** command is used to configure the password of the Privileged EXEC level of the CLI. Administrators can enforce the password policy complexity configured at the system level to the privileged EXEC level password. To do so:

1. Configure the password-policy complexity using the following command:

```
ACOS(config)#system password-policy complexity <Strict>
```

2. Enforce the password policy complexity to the privileged level users using the following command:

```
ACOS(config)#system enable-password follow-password-policy
```

3. Verify the password-policy complexity configuration is enforced using the following command:

```
ACOS (config)#enable-password
Password:          <<If  you enter 'a10network', it is an invalid
password as it does not comply with the Strict password policy.>>
Retype password:
Invalid password. Does not match password requirements. Password
Invalid.

ACOS(config)#enable-password
Password:  <<input 'a10$PasSword'>>
Retype password:
ACOS(config)# <<Indicates that the password change is successful.>>
```

If the system password policy complexity is not configured, the system does not check for the **enable-password** input even when the **system enable-password follow-password-policy** command is configured. When the system is reset, this configuration is reset, and the system does not check or validate the **enable-password** input.

Recovering an Administrator Password

This section describes how to recover in the event your admin password is lost.

This procedure can only be performed through the security console, and only within the first five minutes of rebooting the ACOS device.

1. Use the **show version** or **show hardware** commands and record the serial number for your device.
2. Reboot the ACOS device.
3. Connect to the serial console.
4. When prompted for the user name and password, enter the following:
   a. User Name: **reset**
   b. Password: serial number for your device

c. Use the serial number recorded in , or locate the serial number on the rear of your ACOS device.

5. After logging in, the CLI presents the following questions:

   a. Do you want to reset admin password to default?[y/n]:

      Answering **y** to this question resets the admin user name and password to the factory default **admin** and **a10**.

   b. Do you want to reset enable password to default?[y/n]:

      Answering **y** to this question resets the enable password to the factory default, which is no password.

   c. Do you want to erase startup config?[y/n]:

      Answering **y** to this question clears the startup config, thus returning the device to its factory default settings.

   CAUTION: Answering **y** to this questions means you must reconfigure the device.

6. Answer **y** to the first question so that the user can log on to the device; answer the other two questions as desired for your needs.
7. After you log on to the device, change the admin password for security purposes.

Configuring the Administrator Lockout Feature

The following topics are covered:

Overview

Administrator lockout occurs after a number of failed login attempts.

This section shows how to enable this feature and specify the parameters that determine how it operates.

By default, administrator lockout is not enabled and there is no limit to the number of times the user can enter an incorrect password with an administrator account to log in.

Configuring the Administrator Lockout Feature in the GUI Mode

The user can configure the Administrator Lockout feature through the GUI mode. The following are the steps and modes to configure an administrator lockout feature:

1. Navigate to **System** >> **Admin** >> **Users**.
2. Click the **Lockout** tab. The Lockout Policy window appears.
3. Enter values in the **Duration**, **Threshold** and **Reset Time** fields. These fields determine the parameters of the administrator lockout feature.
4. After you have entered values, select the **Enable** checkbox and click **OK**.

Configuring the Administrator Lockout Feature in the CLI Mode

The user can configure the Administrator Lockout feature through the CLI mode.

The following topics are covered:

Enabling Administrator Lockout

To enable this feature, enter the following command. The default settings for this feature are enabled.

```
ACOS(config)# admin-lockout enable
```

Changing the Number of Failed Login Attempts Allowed

By default, the user is locked out after 5 failed login attempts. To change this number use the `admin-lockout threshold` command as in the following example:

To lock an administrator account after 15 failed attempts, enter the following command:

```
ACOS(config)# admin-lockout threshold 15
```

Changing the Lockout Duration

By default, the user is locked out 10 minutes. To change this number use the `admin-lockout duration` command as in the following examples:

To lock an administrator account for 15 minutes, enter the following command:

```
ACOS(config)# admin-lockout duration 15
```

To lock an administrator account permanently or until the root administrator unlocks the account, enter the following command:

```
ACOS(config)# admin-lockout duration 0
```

Changing the Lockout Reset Time

By default, if the login attempts are forgotten after 10 minutes. Any failed login attempt that has aged the 10 minute reset time is not counted toward the threshold. To change this number use the `admin-lockout reset-time` command as in the following example:

```
ACOS(config)# admin-lockout reset-time 10
```

Showing the Lockout Status

To view the lockout status:

To view the lockout status of the account for `adminuser1`, enter the following command:

```
ACOS(config)# show admin adminuser1 detail
```

Unlocking a Locked Admin Account

To unlock an admin account, access the configuration level for the admin, then enter the **unlock** command:

```
ACOS(config)# admin adminuser1
ACOS(config-admin:adminuser1)# unlock
```

Additional CLI Reference Information

Additional information is found in the Command Line Interface Reference.

The following topics are covered:

Admin Configuration Mode Commands

The following commands are accessed in the admin configuration level (also called admin configuration mode) To access this level, enter the `configure` command followed by the `admin` command. The CLI prompt "`ACOS`(config-admin:adminuser1)#" seen in the following example shows that you have entered this level for the administrator name `adminuser1`:

```
ACOS# configure
ACOS(config)# admin adminuser1
ACOS(config-admin:adminuser1)#
```

The following CLI commands are available in the `admin` configuration mode:

```
  access         Config access type
  password       Config admin user password
  privilege      Config admin user privilege
  ssh-pubkey     Config openssh authorized public keys management
  trusted-host   Set trusted network administrator can login in
  unlock         Unlock admin user
  enable         Enable user
  disable        Disable user
```

Global Configuration Commands

The `admin-lockout` command is accessed in the global configuration level (also called global configuration mode) To access this level, enter the `configure` command. The CLI prompt "`ACOS(config)#`" seen in the following example shows that you have entered this level:

```
ACOS# configure
ACOS(config)# admin adminuser1
```

The following global configuration commands are relevant to the features configured in this chapter:

- **admin**
- **admin-lockout**

Configuring Role-Based Access (RBA) and Fine Tuning Privileges

Role-Based Access (RBA) provides the ability to fine-tune the permissions and privileges of admin accounts.

An *RBA role* is a named bundle of individual administrative privileges that can be bound collectively, like a template, to admin accounts. Using roles provides a consistent and efficient method of setting the privileges of administrators that have similar roles or the same role.

An *RBA group* is a named collection of individual admin accounts that can be bound either to individual privileges or to RBA roles or both.

Because the user can bind individual privileges to admin accounts upon which a role is also bound, the user can insert individual differences in privilege as needed.

The following topics are covered:

Overview

This section describes how the RBA Fine Tunes Admin Accounts.

The following topics are covered:

Prerequisites

Before the user can fine tune your admin accounts using RBA consider the following:

- The admin user accounts must be created before they can be fine tuned using RBA.

NOTE: See Configuration Instructions and Examples for instructions.

- If you plan to use an RBA role, it must be configured before it can be bound to admin accounts.

To set your RBA Admin Accounts, perform the following steps:

1. Enable RBA.
2. Create RBA user(s) with the same name(s) as existing admin accounts. Optionally, create an RBA group that includes multiple admin accounts.
3. Specify the partition for the RBA user or group.
   The user can specify the shared partition in this step.

NOTE: RBA privileges for users or groups must be set per partition, including the shared partition. The shared partition is described in the *Configuring Application Delivery Partitions* guide.

4. Inside the partition, bind individual privileges or RBA role to the RBA user or group.

   The user can configure privileges explicitly using the *lineage of the object class* with the permitted operation (for example, **`slb`**`.virtual-server read`) or you specify a role (for example, `role1`).
   See RBA User GUI Privileges for instructions on using object class lineage for RBA privileges.
   A *role* is a collection of explicitly specified privileges.
   See Configuring an RBA Role for instructions on configuring RBA roles.

5. The user can give the RBA users and groups to have privileges in multiple partitions. Optionally, repeat steps 3 and 4 for additional partitions.

RBA Privilege Levels

Table 4 RBA Privilege Levels defines the privilege levels that can be configured using RBA:

Table 4 : RBA Privilege Levels

Privilege	Description
No-Access (Hidden)	The ACOS object at this privilege level does not appear in the `show running-config` command output. The command or operation that configures or operates on the object is hidden from the user or group.
Read	The ACOS object at this privilege level will appear in the **`show running-config`** command object. All instances of the object will appear. The command or operation that configures or operates on the object is hidden from the user or group.
Write	The ACOS object at this privilege level, users and groups have complete access to the ACOS object and its instances. The user can change, add to, and delete the object instance configurations using GUI operations or CLI commands. The output of the `show running-config` command will display the object and its instances.

RBA User GUI Privileges

lists the user GUI privileges when RBA is disabled:

User Type	RBA Enabled	RBA Disabled
A remote user with only one pre-defined role A Remote and local	RBA check is performed based on the pre-defined role definition	To be consistent with GUI since 4.1.4.x does RBA check based on the pre-defined role definition

User Type	RBA Enabled	RBA Disabled
RBA user without the same name		
A remote user with only one pre-defined role Remote and local RBA user with the same name A Local RBA user bound with custom RBA rules.	RBA check is performed based on the pre-defined role definition on the remote and local RBA user configuration	Following are the predefined user roles and privilege on the GUI: NetworkAdmin - Write for all objects NetworkOperator - Write for all objects PartitionNetworkOperator - Partition-write for all objects PartitionReadOnly - Partition-read for all objects PartitionReadWrite - Partition-write for all objects PartitionSlbServiceAdmin - Partition-write for all objects PartitionSlbServiceOperator - Partition-write for all ob-jects ReadOnlyAdmin - Read for all objects ReadWriteAdmin - Write for all objects SlbServiceAdmin - Write for all objects

User Type	RBA Enabled	RBA Disabled
		SlbServiceOperator- Write for all objects SystemAdmin - Write for all objects **Note**: The local RBA user configuration does not get affected when RBA is disabled.
Local user (admin user and RBA user having same name)	RBA check is performed based on the combined result of admin user privilege and RBA rules/role/group	Following are the Admin and RBA user GUI privilege: Read Write Hm Partition-read Partition-write Partition-enable-disable is changed to Partition-write (for Admin User) **Note**: The local RBA user configuration does not get affected when RBA is disabled.

Object Class Lineage

When you configure the RBA privileges of a user or a role, the first part of the *`object class lineage`* is a dot-separated string that specifies a set of permitted operations. For example, `slb.template.virtual-server`, means that the permitted operations applies to the ACOS SLB Virtual-Server Template configuration and operation. The permitted operations are read, write, or enable/disable. If the permitted operation is

read, the admin would not be able to configure virtual server templates, instead, it can just view their status and configuration.

Every GUI element such as a menu, button, field, form, and so on have its own lineage but different GUI elements of the same component can have the same lineage across ACOS. For example, the lineage for the **ADC** >> **Health Monitors** >> **Health Monitors** page is `health.monitor` and the lineage for the **Health Monitor** field in **ADC** >> **SLB** >> **Servers** >> form is also `health.monitor`.

Each lineage has only one permitted operation which means, there is a one-to-one mapping between each lineage and only one permitted operation. For example, lineage `health.monitor` can have only read privilege, or only write privilege, or only no-access privilege.

NOTE: There is no one-to-one mapping between a GUI element and a lineage because several GUI elements can have the same lineage. Therefore, it is challenging for an RBA user or role to control the showing or hiding of a GUI element.

If the object class lineage is configured as `health.monitor no-access`, both **ADC** >> **Health Monitors** >> **Health Monitors** page and the **Health Monitor** field in **ADC** >> **SLB** >> **Servers** form are hidden.

If the object class lineage is configured as `slb read`, the permitted operation `read` is applied to all the objects whose lineage begins with `slb` in ACOS.

The next section describes what happens if you configured multiple lineages and multiple permitted operations for the same user (or role).

Longest Match Takes Precedence Rule

When specifying ACOS objects, each level in the object hierarchy is separated from the next level by a dot (.) For example, **`slb.template.virtual-server`** is a third-level object, while **`slb.template`** is a second-level object. Objects at the third level are more specific than objects at the second level. The third level object, **`slb.template.virtual-server`** is said to be “longer” because it has two dots separating three names as opposed to **`slb.template`** which has only one dot separating two names. Privileges for a longer (and more specific) object take precedence over a shorter and less specific ACOS object.

RBA Configuration Examples

The following topics are covered:

Configuring an RBA User

This section provides instructions for configuring RBA users. The RBA user name must be an exact match of an existing admin user who can be authenticated either locally or remotely using LDAP, RADIUS, or TACACS+. See Configuration Instructions and Examples for step-by-step configuration of admin users.

The following topics are covered:

Configuring an RBA User in the GUI Mode

The user can configure an RBA User through the GUI mode. The following are the steps and modes to configure an RBA user.

In this example, an admin user called **admin1** is created. In partition **companyA**. This user will have write access to SLB operations, but will be limited to read-only access to SLB virtual-servers and no access to SLB servers:

1. Navigate to **System** >> **Admin** >> **Users**.
2. Select **Users** from the drop-down list of the **RBA** tab.
3. Click **Create**. The **Create RBA User** window appears.
4. In the **Name** field, enter **admin1**.

5. In the **Rule List** field, click the **+Add** box.
   a. Select **companyA** from the **Partition** drop-down list.
   b. Select **slb** from the **Object** drop-down list.
   c. Select **write** from the **Operation** drop-down list.
   d. In the **Action** box, click the floppy disk icon to save the configure Rule.
6. In the **Rule List** field, click the **+Add** box.

NOTE: To configure an RBA role, follow the same steps as configuring an RBA user, but in the second step select Role from the drop-down list of the RBA tab.

7. In the **Rule List** field, click the **+Add** box again.
   a. Select companyA from the Partition drop-down list.
   b. Select slb.server from the Object drop-down list.
   c. Select no-access from the Operation drop-down list.
   d. In the Action box, save the configure Rule by clicking the disk icon.
8. Click the **Create** button to save the new administrator account.

NOTE:

- Because of the “Longest Match Takes Precedence Rule” below, **admin1** does not have write access to SLB virtual-servers and does not any access SLB real servers. However, for all other SLB objects in ACOS, the **admin1** account has read/write access.
- If there is a configured RBA role that specifies all the permissions that you want to grant the user, the user can apply the role at the partition level rather than configuring each privilege separately by using the **Role List** field instead of the **Rule List** field on this screen (see Configuring an RBA Role).

Configuring an RBA User in the CLI Mode

The user can configure an RBA User through the CLI mode. The following are the steps and modes to configure an RBA User:

Select an existing admin user account to which to add RBA attributes. See Configuring Admin Accounts in the CLI Mode for a step-by-step configuration of admin user accounts:

```
ACOS(config)# admin adminuser1 password
Password:
Retype password:
Total number of configured users:  3
   Privilege     R: read-only, W: write, P: partition, En: Enable
   Access Type   C: cli, W: web, A: axapi

UserName                        Status    Privilege Access Partition
-------------------------------------------------------------------
admin                           Enabled   R/W       C/W/A
adminuser1                      Enabled   P.R/W     C/W/A   Partition1
adminuser2                      Enabled   P.R/W     C/W/A   Partition2
```

Enable RBA.

```
ACOS(config)# rba enable
```

Create the RBA user with the same name as the existing admin user.

```
ACOS(config)# rba user adminuser1
```

Specify the admin partition of the RBA user. If the admin partition does not already exist for the administrator, this step assigns the RBA user to it.

```
ACOS(config-user:adminuser1)# partition Partition1
```

Configure the RBA privileges for the user in the partition the *object class lineage* syntax. Alternatively to this step, the user can assign privileges using RBA roles. See step 6.

Specify the privileges by starting with the highest CLI level and then using a dot (.) to indicate the next level.

In the following, the first configuration line gives the adminuser1 read-write privileges to all SLB commands, the second line gives the user read-only privilege to the SLB virtual-server commands, and the third line give the user no-access to SLB real server commands:

```
ACOS(config-user:adminuser1-partition:Partition1)# slb write
ACOS(config-user:adminuser1-partition:Partition1)# slb.virtual-server read
ACOS(config-user:adminuser1-partition:Partition1)# slb.server no-access
```

Use the `show rba` command to verify this configuration:

```
ACOS(config-user:adminuser1-partition:Par...)# show config rba
!Section configuration: 104 bytes
!
rba user adminuser1
  partition Partition1
    slb write
    slb.virtual-server read
    slb.server no-access
```

Alternatively to step 5, assign an RBA role or roles (Configuring an RBA Role) that specifies all the privileges that you want to grant the user, the user can apply the role at the partition level rather than configuring each privilege separately. For example:

```
ACOS(config)# rba user adminuser1
ACOS(config-user:adminuser1)# partition Partition1
ACOS(config-user:adminuser1-partition:Partition1)# role role1
```

Use the `show rba` command to verify this configuration:

```
ACOS(config-user:adminuser1-partition:Par...)# show config rba
!Section configuration: 147 bytes
!
!
rba role role1
  slb write
  slb.virtual-server read
```

```
  slb.server no-access
!
rba user adminuser1
  partition Partition1
    role role1
```

Understanding Object Class Lineage in this Configuration Example

The following `slb` **`read`** command specifies the adminuser1 has read-write privilege to SLB commands.

```
ACOS(config-user:adminuser1-partition:Partition2)# slb write
```

To restrict the user to a subset of options available at the command level, enter a dot (.) followed by a keyword option. For example, the following commands restricts adminuser1 to read-only access to the `slb virtual-server` commands and no access to `slb server` commands, but it does restrict the use of other `slb` commands.

```
ACOS(config-user:adminuser1-partition:Partition2)# slb.virtual-server read
ACOS(config-user:adminuser1-partition:Partition2)# slb.server no-access
```

NOTE: *Longest match takes precedence.* The longer and more specific **`slb.virtual-server`** and **`slb.server`** command lineages take precedence over the less specific and shorter **`slb`** set of command lineage.

The following example configures RBA for user `adminuser3`. In partition `Partition1`, this user has read privileges for SLB virtual server objects (that is commands), write privileges for SLB server objects, but no access to all other SLB objects. In partition `Partition2`, this user has all privileges defined by RBA role `role1`:

```
ACOS# show config rba user adminuser3
!
rba user adminuser3
  partition Partition1
    slb no-access
    slb.server write
    slb.virtual-server read
  partition Partition2
    role role1
!
```

NOTE: The keyword `root` in a privilege command specifies the root level of the CLI command set. Root includes the entire set of ACOS commands. The default `admin` user has root read-write privileges.

Configuring an RBA Group

An RBA group combines admin users who can be configured with similar privileges. When you modify the permissions in a partition for an RBA group, the permissions are applied to all of the users in that group.

After creating a group, select the users to add to the group or select a partition for which you want to modify the permissions. The user can add users at any time, so you do not need to create users before creating the group; if you specify a user that does not already exist, the user will be created along with the group. The group's permissions are configurable for multiple partitions, although each partition must be configured separately.

The following topics are covered:

Configuring an RBA Group in the GUI Mode

The user can configure an RBA Group through the GUI mode. The following are the steps and modes to configure an RBA Group.

This example shows how to configure a group containing two pre-existing users on the system. In partition **companyA**, all users in the group have write access at the SLB operations, read-only privilege for SLB virtual-server operations, but no-access to SLB server operations.

1. Navigate to **System** >> **Admin** >> **Users**.
2. Select the **RBA** tab, then select **Groups** from the drop-down list.
3. Click **Create**. The **Create Group** window appears.
4. In the **Name** field, enter **group1**.
5. In the In the **User** field, select the check box for the existing user, **admin1**.

6. In the **Rule List** field, click the **+Add** box.
   a. Select **companyA** from the **Partition** drop-down list.
   b. Select **slb** from the **Object** drop-down list.
   c. Select **write** from the **Operation** drop-down list.
   d. In the **Action** box, click the floppy disk icon to save the configure Rule.

NOTE: To configure an RBA role, follow the same steps as configuring an RBA user, but in the second step select Role from the drop-down list of the RBA tab.

7. In the Rule List field, click the +Add box again.
   a. Select companyA from the Partition drop-down list.
   b. Select slb.server from the Object drop-down list.
   c. Select no-access from the Operation drop-down list.
   d. In the Action box, save the configure Rule by clicking the disk icon.
8. Click the Create button to save the new administrator account.

NOTE:

- Because of the “Longest Match Takes Precedence Rule” below, admin1 does not have write access to SLB virtual-servers and does not any access SLB real servers. However, for all other SLB objects in ACOS, the admin1 account has read/write access.
- If there is a configured RBA role that specifies all the permissions that you want to grant the user, the user can apply the role at the partition level rather than configuring each privilege separately by using the Role List field instead of the Rule List field on this screen (see Configuring an RBA Role)

Configuring an RBA Group in the CLI Mode

The user can configure an RBA Group through the CLI mode. The following are the steps and modes to configure an RBA Group.

To create an RBA group, enter the **rba group** command at the global configuration level to specify privileges and then assign admin users and their define partitions to the group.

Enable RBA:

```
ACOS(config)# rba enable
```

1. Select existing admin user accounts to which to add RBA attributes. See the configuration Configuring Admin Accounts in the CLI Mode for a step-by-step configuration of admin user accounts. In this example, create an RBA group that includes both `adminuser2` and `adminuser3`:

```
ACOS(config)# rba group group1
ACOS(config-group:group1)# user adminuser2
ACOS(config-group:group1)# user adminuser3
```

2. Specify a partition for the RBA group.

```
ACOS(config-group:group1)# partition Partition2
```

3. Configure the RBA privileges for the group.

```
ACOS(config-group:group1-partition:Partition2)# role role1
```

4. Verify the RBA group configuration:

   ACOS(config-group:group1-partition:Partit...)# **show config rba**

```
!Section configuration: 226 bytes
!
!
rba role role1
  slb write
  slb.virtual-server read
  slb.server no-access
!
rba group group1
  user adminuser2
  user adminuser3
  partition Partition2
    role role1
!
```

NOTE: *User privileges take precedence over group privileges.* An individual user's privileges whether assigned by role or individually take precedence over the group privileges whether assigned by role or individually.

Configuring an RBA Role

An *RBA role* is a named set of operations or commands that an admin user or group of users has permission or does not have permission to access. Creating an RBA role profile can help simplify the management of permissions. The privileges defined in the role can be applied to any user or any group; when applied to a group, the permissions in the role apply to all members of the group. The user can assign multiple roles to an admin user or group.

Configure the Custom RBA role with remote user scenario including the sample radius and thunder configuration.

The following topics are covered:

Configuring an RBA Role in the GUI Mode

The user can configure an RBA Role through the GUI mode. The following are the steps and modes to configure an RBA Role.

1. Navigate to **System** >> **Admin** >> **Users**.
2. Select the **RBA** tab, then select **Roles** from the drop-down list.
3. Click **Create** and the **Create RBA Role** window appears.
4. In the **Name** field, enter **slb1**.
5. In **Partition Only** field, select the check box to set privilege only for the partition.
6. In the **Default Privilege** field, select privilege from the drop down list.
7. In the **Rule List** field, click the **+Add** box.
    a. Select **companyA** from the **Partition** drop-down list.
    b. Select **slb** from the **Object** drop-down list.

c. Select **write** from the **Operation** drop-down list.

d. In the **Action** box, click the floppy disk icon to save the configure Rule.

8. Repeat **step 6** to add read-only privileges for SLB virtual-server operations, but no access to SLB server operations.
9. Click **Create** to create and save the role, **slb1** in partition **CompanyA**.

Because longest match takes precedence, admin users that are assigned the role, **slb1**

NOTE:

- Have permission to create, edit, or delete all ACOS SLB objects (such as slb configuration commands) except SLB virtual servers and SLB (real) servers.
- Have permission to view the configuration and status of SLB virtual servers.
- Have permission to neither configure nor view SLB (real) servers.

Configuring an RBA Role in the CLI Mode

The user can configure an RBA Role through the CLI mode. The following are the steps and modes to configure an RBA Role.

The following example illustrates the commands used in creating the CLI role named, `role1`:

Specify the privileges by starting with the highest level and enter a dot (.) to indicate the next level. For example, to configure write access at the SLB command level, read-only privileges for SLB virtual-servers, but no access to SLB servers, enter the following commands:

```
ACOS(config)# rba role role1
ACOS(config-role:role1)# slb write
ACOS(config-role:role1)# slb.virtual-server read
ACOS(config-role:role1)# slb.server no-access
```

NOTE: Because longest match takes precedence, admin users that are assigned the role, `role1`:

- Have permission to create, edit, or delete all ACOS SLB objects (such as slb configuration commands) except SLB virtual servers and SLB (real) servers.
- Have permission to view the configuration and status of SLB virtual servers.
- Have permission to neither configure nor view SLB (real) servers.

NOTE: *Individual privileges take precedence over role privileges.* If the user or group has individual permissions defined in addition to the role, a combination of the individual and role permissions are applied. If there are conflicting privileges between a group's uniquely configured privileges and an RBA role's privileges, the group's unique privileges are used.

Additive and Subtractive Methods

There are two ways in which the user can configure object privileges using RBA:

- Additive RBA, which is more useful for granting admins privileges to access certain objects. For more information, see Understanding Additive RBA.
- Subtractive RBA, which is more useful to denying admins privileges to access certain objects. For more information, see Understanding Subtractive RBA.

Understanding Additive RBA

An existing admin user with write privileges is able to create, edit, or delete any object. The additive method of RBA involves the following:

1. Use the **`root no-access`** command to overwrite the default write privileges of the admin, thus removing all of the admin's create, edit, and delete privileges.
2. Use RBA commands to selectively add the desired privileges.

Consider the following example with admin `admin_so` who has write privileges by default. The admin is able to create a health monitor with the default privileges:

```
ACOS(config)# health monitor hm1
ACOS(config-health:monitor)# exit
ACOS(config)#
```

The RBA configuration will remove all of the default write privileges (**`root no-access`**), and allow only creation of SLB objects (**`slb write`**):

```
ACOS(config)# rba user admin_so
ACOS(config-user:admin_so)# partition shared
ACOS(config-user:admin_so-partition:shared)# root no-access
ACOS(config-user:admin_so-partition:shared)# slb write
When admin_so tries to configure a health monitor again, they will not be
able to:
ACOS(config)# health monitor hm1
Access Denied
ACOS(config)#
```

But `admin_so` is able to configure SLB objects, as defined by the RBA configuration:

```
ACOS(config)# slb server rs1 192.168.9.9
ACOS(config-real server)#
```

The user `admin_so` had their default write privileges removed, and SLB privileges added back to their profile.

Understanding Subtractive RBA

An existing admin user with write privileges is able to create, edit, or delete any object. The subtractive method of RBA selectively removes a subset of these privileges. Consider the following example with `admin_nt` with default write privileges. This user is able to view SLB templates in the **`show running-config`** output:

```
ACOS(config)# show run | inc slb tem
slb template ftp FTP_TEMP1
slb template ftp FTP_TEMP2
slb template HTTP HTTP_TEMP1
```

Now, we add the RBA configuration to give **no-access** privileges to user admin_nt for SLB templates:

```
ACOS(config)# rba user admin_nt
ACOS(config-user:admin_nt)# partition shared
ACOS(config-user:admin_nt-partition:shared)# slb.template no-access
```

When admin_nt tries to run the show command again, no SLB template are visible:

```
ACOS(config)# show run | inc slb tem
ACOS(config)#
```

The admin admin_nt will still have all normal privileges to create, edit, or delete all other objects on the device, just not SLB templates as this has been subtracted from the user's privileges.

Additional CLI Reference Information

The following commands are described in the *Command Line Interface Reference*.

NOTE: The clear, do, end, exit, no, show. user-tag, and write commands are not shown in the following because they are common to all CLI modes and not specific to any configuration mode.

The following topics are covered:

RBA Global Commands

To enter the admin configuration mode, create a new administration account or modify an existing account. For example:

```
ACOS(config)# rba ?
  group    RBA configuration for a group
  role     Role configuration for RBA support
  user     RBA configuration for a user
  enable   Enable RBA
  disable  Disable RBA
```

RBA-Group Commands

```
ACOS(config)# rba group group1
ACOS(config-group:group1)# ?
  partition           RBA configuration for the access privilege of a
group within one partition
  user                Users in the group
```

RBA-Group Partition Commands

```
ACOS(config)# rba group group1
ACOS(config-group:group1)# partition Partition1
ACOS(config-group:group1-partition:Partit...)# ?
  role                Role in a given partition
  NAME<length:1-128>  Lineage of object class for permitted operation
```

RBA-User Commands

```
ACOS(config)# rba group useradmin1
ACOS(config-user:useradmin1)# ?
  partition  RBA configuration for the access privilege of a group within
one partition
  user       Users in the group
```

RBA-User Partition Commands

```
ACOS(config)# rba user adminuser1
ACOS(config-user:adminuser1)# partition Partition1
ACOS(config-user:adminuser1-partition:Partit...)# ?
  role                Role in a given partition
  NAME<length:1-128>  Lineage of object class for permitted operation
```

RBA SSLi Commands

This section describes the Thunder SSLi RBA configuration for the following types of administrators:

The following topics are covered:

Network Administrator Commands

Network administrators are allowed to change only the network-related configurations. The following operations cannot be performed:

- Modify or export certificates and keys
- Modify SSLi Interception Policy

Certificate Administrator Commands

Certificate administrators are allowed to change only the PKI-related configurations such as creating, importing and updating certificates/keys.

The following operations cannot be performed:

- Modify SSLi Interception Policy
- Modify network settings

Policy Administrator Commands

Policy administrators are allow to change only SSLi-interception policies. The following operations cannot be performed:

- Modify network settings
- Modify or export certificates and keys

Auditor Commands

Internal auditors analyze the administrative activities, control SSLi interception policies or cipher suites are compliant to approved policies and procedures. The auditor cannot export certificates.

Access Based on the Management Interface

By default, certain types of management access through the ACOS device's Ethernet interfaces are blocked. This chapter describes how to configure management access based on the interface.

The following topics are covered:

Default Management Access Settings

Table 5 provides the default settings for each management service.

Table 5 : Default Management Access Settings

Management Service	Ethernet Management Interface	Ethernet and VE Data Interface
SSH	Enabled	Disabled
Telnet	Disabled	Disabled
HTTP	Enabled	Disabled
HTTPS	Enabled	Disabled
NTP	Enabled	Enabled
SNMP	Enabled	Disabled
Ping	Enabled	Enabled

The user can enable or disable management access for each access type and interface. You also can use an Access Control List (ACL) to permit or deny management access through the interface by using specific hosts or subnets.

NOTE: By default, the NTP service is enabled on all the interfaces.

Configuring Access by using Access Control Lists

This section contains the important information about ACL support:

The following topics are covered:

Configuring ACL Support on the Management Interface

The management interface supports only one ACL, which can be bound to the interface as an enable-management ACL or directly to the interface as a filter. To replace the current ACL with a different one, you must first remove the ACL that is currently bound to the interface.

For example, enter only one of the following sets of commands:

- ACOS(config)# **enable-management service** acl-v4 1
- ACOS(config)# **interface management**

```
ACOS(config-if:management)# access-list 1 in
```

Additionally, if you apply an enable-management ACL to the management interface, an ACL for an individual service is not supported. For example, the user **cannot** enter the following rule on the management interface:

```
ACOS(config)# enable-management service ping
ACOS(config-enable-management ping)# acl-v4 1
```

Configuring ACL Support on Data Interfaces

Data interfaces can support multiple ACLs, including multiple enable-management ACLs. If a data interface has multiple enable-management ACLs, the ACLs are applied in the following order:

1. **enable-management service** {**ping** | **ssh** | **telnet** | **http** | **https**} **acl** {*id* | *name*} {**ethernet** *port-num* [**to** *port-num*] | **lif** *lif_name* | **ve** *ve-num* [**to** *ve-num*]}
2. **enable-management service acl** {*id* | *name*} {**ethernet** *port-num* [**to** *port-num*] | **lif** *lif_name* | **management** | **priority** | **ve** *ve-num* [**to** *ve-num*]}

NOTE: The **priority** option is supported only on FTA platforms and applies only to **acl-v4** and **acl-v6** services. If configured, it is applicable to configured VE, Ethernet, DOT1Q LIF, and all data interfaces.

Implicit Deny Rule

Each ACL has an implicit **deny any any** rule at the end. If the management traffic's source address does not match a permit rule in the ACL, the implicit **deny any any** rule is used to deny access.

Configuring Management Access through Ethernet Interfaces

The user can configure management access through Ethernet interfaces in one of the following ways.

The following topics are covered:

Configuring Management Access in the GUI Mode

The user can configure the Management Access through the GUI mode. The following are the steps and modes to configure management access settings for the interfaces:

1. Navigate to **System** >> **Settings** >> **Access Control**.
2. For each interface, select or deselect the appropriate access type checkboxes.
3. To use an ACL to control access, select an ACL from the **ACLv4** or **ACLv6** drop-down lists.
4. Click **OK**.

Configuring Management Access in the CLI Mode

The user can configure the Management Access through the CLI mode.

NOTE: The user can enable or disable management access by using the CLI.

The following topics are covered:

Disabling Management Access in the CLI Mode

The user can disable the Management Access through the CLI mode. The following are the steps and modes to disable management access settings for interfaces.

To disable management access, enter the **`disable-management service`** command at the global configuration level of the CLI.

The following example command disables HTTP access to the out-of-band management interface:

```
ACOS(config)# disable-management service http
You may lose connection by disabling the http service.
Continue? [yes/no]:yes
ACOS(config-disable-management http)# management
```

The following example command stops ACOS from responding to the incoming NTP client requests on the specified port:

```
ACOS(config)# disable-management service ntp
You may lose connection by disabling the ntp service.
Continue? [yes/no]:yes
ACOS(config-disable-management ntp)# ethernet 3
```

ACOS stops responding to the incoming NTP client requests on the ethernet 3 port and the status of NTP for ethernet 3 is displayed as "off" in the output of the `show management` command. For more information, see the Command Line Interface Reference Guide.

Enabling Management Access in the CLI Mode

The user can enable the Management Access through the CLI mode. The following are the steps and modes to change management access settings for interfaces.

To enable management access, enter the **`enable-management service`** command at the global configuration level of the CLI:

The following example command enables Telnet access to data interface 6:

```
ACOS(config)# enable-management service telnet
ACOS(config-enable-management telnet)# ethernet 6
```

The following example commands configure an ACL for incoming NTP requests on ethernet 1:

```
ACOS(config)# enable-management service ntp
ACOS(config-enable-management ntp)# acl-v4 1
ACOS(config-enable-management ntp-acl-v4)# ethernet 1
```

The following example commands configure an ACL on all interfaces:

```
ACOS(config)# enable-management service acl-v4 1
ACOS(config-enable-management acl-v4 1)# ethernet 3
```

An ACL is configured on ethernet 3 and the ACL ID is displayed for all the services of the ethernet 3 in the output of the `show management` command. For more information, see the Command Line Interface Reference guide.

Configure Management Access Through LIF Interfaces

Management services including IPv4/IPv6 ACLs, HTTP, HTTPS, Ping, SNMP, SSH, and Telnet can be bound to LIF interfaces, allowing better access control and improved network management.

This is useful in specific scenarios. For example, this configuration allows a Loopback IP to be reachable via a DOT1Q-tagged LIF interface i.e., management traffic can be routed through a VLAN-based LIF while still using the Loopback IP as the preferred management endpoint. This ensures that management access remains consistent, even if the physical interface or the VLAN configuration changes, thereby improving stability and reliability.

Configuration Overview

- To bind a management service to a LIF interface, use the following command:

```
ACOS(config)# enable-management service <service_name>
ACOS(config-enable-management <service_name>)# lif <lif_name>
```

  All services under **enable-management service** command i.e., **acl-v4**, **acl-v6**, **http**, **ping**, **snmp**, **ssh**, and **telnet** also support the **lif** option.

- To view the management services bound to LIF interfaces, use the **show management** command. See Viewing the Current Management Access Settings.

Configuration Example

The following example configuration binds the HTTPS management service to the specified LIF interface (*lif_test*):

```
ACOS(config)# interface lif lif_mgmt
ACOS(config-if:lif:lif_mgmt)# encapsulation dot1q 2006
ACOS(config-if:lif:lif_mgmt-dot1q)# trunk 1
ACOS(config-if:lif:lif_mgmt-dot1q)# exit
ACOS(config-if:lif:lif_mgmt)# ip address 1.1.6.38 255.255.255.0
ACOS(config-if:lif:lif_mgmt)# ipv6 address 2006::85/64
ACOS(config-if:lif:lif_mgmt)# exit

ACOS(config)# enable-management service https
```

```
ACOS(config-enable-management https)# lif lif_mgmt
```

Additional Information

- It applies only to incoming management traffic directed to ACOS; outgoing traffic from ACOS remains unchanged and follows existing routing logic.
- If priority is configured for the service, it is applied only for LIFs that use VLAN tagging (DOT1Q).
- A maximum of 16 LIF interfaces can be configured for management access.
- A LIF cannot be deleted while a management service is bound to it; it must be unbound first.

Viewing the Current Management Access Settings

To view the management access settings that are currently in effect, enter the **show management** command at any level of the CLI.

The following example shows an ACOS device with 12 Ethernet data ports. In this example, all the access settings are set to their default values:

```
ACOS# show management
PING    SSH     Telnet          HTTP            HTTPS           SNMP
     ACL
-------------------------------------------------------------------------------
----------------
mgmt    on      on              off             on              on
     on       -
eth1    on      off             off             off             off
     off      -
eth2    on      off             off             off             off
     off      -
eth3    on      off             off             off             off
     off      -
eth4    on      off             off             off             off
     off      -
eth5    on      off             off             off             off
     off      -
```

```
eth6     on       off              off              off              off
     off       -
eth7     on       off              off              off              off
     off       -
eth8     on       off              off              off              off
     off       -
eth9     on       off              off              off              off
     off       -
eth10    on       off              off              off              off
     off       -
eth11    on       off              off              off              off
     off       -
eth12    on       off              off              off              off
     off       -
ve3      on       off              off              off              off
     off       -
ve5      on       off              off              off              off
     off       -
lif 1   ACL 1    ACL 1            ACL 1            ACL 1            ACL 1
    ACL 1      1
lif 2   ACL 1    ACL 1            ACL 1            ACL 1            ACL 1
    ACL 1      1
lif 3   ACL 1    ACL 1            ACL 1            ACL 1            ACL 1
    ACL 1      1
```

Regaining Access if You Accidentally Block All Access

If you disable the type of access that you are using at the time you enter the **`disable-management`** command, your management session will end. If you accidentally enter the **`all`** option for all interfaces, which locks you out of the device completely, the user can still access the CLI by connecting a computer to the ACOS device's serial port.

Additional CLI Reference Information

The Command Line Interface Reference provides additional information on the CLI commands used in this document.

Configuring Web Access

The following topics are covered:

Default Web Access Settings

Table 6provides information about the default settings for web access.

Table 6 : Default Web Access Setting

Parameter	Description	Default
`Auto-redirect`	Automatically redirects requests for the unsecured port (HTTP) to the secure port (HTTPS).	Enabled
`HTTP server`	HTTP server on the ACOS device.	Enabled
`HTTP port`	Protocol port number for the unsecured (HTTP) port.	80
`HTTPS server`	HTTPS server on the ACOS device.	Enabled
`HTTPS port`	Protocol port number for the secure (HTTPS) port.	443
`Timeout`	Number of minutes a Web management session can remain idle before it times out and is terminated by the ACOS device.	Range: 0-60 minutes To disable the timeout, specify 0. Default: 10 minutes
`aXAPI Timeout`	Number of minutes an aXAPI session can remain idle before	0-60 minutes. If you specify 0, sessions

Parameter	Description	Default
	being terminated. Once the aXAPI session is terminated, the session ID generated by the ACOS device for the session is no longer valid. For more information about aXAPI, see the aXAPI Reference documentation.	never time out. Default: 10 minutes
`aXAPI Token Sharing`	Enables sharing of aXAPI tokens within multiple hosts without the need to authenticate the hosts.	Disabled

NOTE: If you disable HTTP or HTTPS access, sessions on the management GUI are immediately terminated.

Configuring Web Access

By default, access to the ACOS management HTTP Graphical User Interface (GUI) is enabled and is secure. A valid administrator username and password are required to log in. The user can configure the web access through the CLI mode.

The following topics are covered:

- Default Web Access Settings
- Configuring Web (HTTP) Access in the GUI Mode
- Configuring Web (HTTP) Access in the CLI Mode

Configuring Web (HTTP) Access in the GUI Mode

This feature is not applicable.

Configuring Web (HTTP) Access in the CLI Mode

To configure web access, enter the **web-service** command at the global configuration level of the CLI.

- By default, the web server is enabled on the system. The following command disables the web server:

```
ACOS(config)# web-service server disable
```

- The following command sets the HTTP port to 80:

```
ACOS(config)# web-service port 80
```

Public Key Authentication for SSH

The following topics are covered:

Overview

ACOS provides an option to simplify management access through the CLI, with support for public key authentication.

Public key authentication allows an ACOS administrator to log in through SSH without entering a password. When the administrator enters a username and presses **Enter**, the SSH client on the administrator's computer sends a signature file for the administrator.

The ACOS device compares the signature file to the administrator's public key that is stored on the ACOS device. If they match, the administrator is granted access.

Generating a Key Pair From the Remote Client

On the remote client (for example, a computer) from where the administrator accesses the ACOS device's CLI, use the computer's SSH client to generate an RSA key pair for the administrator. The key pair consists of a public key and a private key.

NOTE: In the current release, only the OpenSSH client is supported.

The following example show you how to generate a key pair from a remote client with the administrator account *admin2*:

```
OpenSSHclient$ mkdir ~/.ssh
```

```
OpenSSHclient$ chmod 700 ~/.ssh
OpenSSHclient$ ssh-keygen -q -f ~/.ssh/ACOS_admin2 -t rsa
Enter passphrase (empty for no passphrase): …
Enter same passphrase again: …
```

NOTE: At the passphrase prompts, press **Enter** and do not enter any characters.

Importing the Public Key to the ACOS Device

After the key pair is generated, to import the public key to the ACOS device:

1. Log in to the ACOS device with root or global read-write privileges.
2. Access the configuration level for the administrator account.
3. Import only the public key, and **not** the private key, to the ACOS device.

The user can import public keys in separate files or grouped in one file.

NOTE: The *admin* account has root privileges and can manage the public certificates for all administrators. Other administrators accounts can manage only the public key that belongs to that administrators account.

The following example shows you how to import a public key for the administrator user *admin2*:

```
ACOS(config)# admin admin2
ACOS(config-admin:admin2)# ssh-pubkey import scp:
Address or name of remote host []? 10.10.10.69
User name []? ACOSadmin2
Password []? *********
File name [/]? /home/admin2/.ssh/ACOS_admin2.pub
ACOS(config-admin:admin2)# ssh-pubkey list
```

For more information, see the **admin** command in the *Command Line Interface Reference*, in the section were the **ssh-pubkey import** command is described.

The user can enter the **ssh-pubkey list** command to view the public keys on your system.

Deleting a Public Key

To delete an SSH public key from the ACOS device, enter the following command:

```
ACOS(config-admin:admin2)# ssh-pubkey delete num
```

The *num* option specifies the key number on the ACOS device. The user can display the key numbers and the keys by entering the **ssh-pubkey list** command.

Additional Reference Information

The following commands that appear in the examples of this document are described in the Command Line Interface Reference.

```
ACOS(config-admin:adminuser1)# ssh-pubkey ?
  delete  Delete an authorized public key
  import  Import an authorized public key
  list    List all authorized public keys
```

Lightweight Directory Access Protocol

This chapter describes how an ACOS device can use Lightweight Directory Access Protocol (LDAP), an AAA protocol, to authenticate administrators and authorize management access based on the account information on external LDAP servers.

The following topics are covered:

Overview

The user can use one of the following types of LDAP servers:

- OpenLDAP
- Microsoft Active Directory (AD)

Configuring LDAP for ACOS Administrators

To configure LDAP authentication and authorization for ACOS administrators:

1. To enable LDAP authentication, enter the following command:

```
ACOS(config)# authentication type ldap local
```

2. To add the LDAP server(s) to the ACOS configuration, enter the **ldap-server host** command. For example:

```
ACOS(config)# ldap-server host 192.168.4.0 cn cn dn example-dn-string
port 638 ssl timeout 5
```

3. The following list provides additional information on the options:
   - If you do not use SSL, the default port is 389. If you use SSL, the default port is 636.
   - The default timeout value is 3.
4. Prepare the LDAP server.

   For more information, see the one of the following sections:
   - Configuring an OpenLDAP Server
   - Configuring Microsoft Active Directory
5. Test the configuration by using an ACOS administrator account to log in to the LDAP server.

Configuring an LDAP Server

The user can configure an LDAP server by using the GUI or the CLI.

The following topics are covered:

Configuring using GUI

The user can configure the LDAP server through the GUI mode. The following are the various steps and modes to configure an LDAP server on the ACOS device:

1. Navigate to **System >> Admin**.
2. Select **LDAP** from the **External Authentication** tab.
3. Verify that **System** >> **Admin** >> **External Authentication** >> **LDAP** is displayed.
4. Click **Create**. The **Create LDAP Server** window appears.
5. Select one of the following for the LDAP **Type**:

- **Name**
- **IPv4**
- **IPv6**

6. Complete one of following tasks:

   If you selected **Name,** complete the following steps:

   a. Select either **Domain Name** or **Common Name**.
   b. If you selected **Domain Name**, enter the **Domain Name** in its text box.
   c. If you selected **Common Name**, enter both the **Common Name** and the **Distinguished Name** in their text boxes.

      Do not use quotation marks for the distinguished names. For example:

      - The string syntax `cn=xxx3,dc=mACOScrc,dc=com` DN string syntax is valid.
      - The string `"cn=xxx3,dc=mACOScrc,dc=com"` is **not** valid.

        To use nested OUs, specify the nested OU first, then the root.

   d. Enter a port number in the **Port** text box or accept the default.
   e. Enter a timeout value in the **Timeout (Seconds)** text box or accept the default.

      The Timeout field displays the maximum number of seconds that the ACOS device waits for a reply from the LDAP server for a given request. The user can specify 1-60 seconds. If the LDAP server does not reply before the timeout, authentication of the admin fails.

   f. Determine whether you want to enable or disable SSL.
   g. Click **Create**.
   h. Verify that you have returned to the **System** >> **Admin** >> **External Authentication** >> **LDAP** window and that an LDAP server has been created.

      If you selected **IPv4**, complete the following steps:

      i. Enter the host IP address of the LDAP server in the **Server** text box.
      ii. Select either **Common Name** or **Domain Name**.

If you selected **Common Name**, enter both the **Common Name** and the **Distinguished Name** in their text boxes.

If you selected **Domain Name**, enter the **Domain Name** in its text boxes.

iii. Enter a port number in the **Port** text box or accept the default.

iv. Enter a timeout value in the **Timeout (Seconds)** text box or accept the default.

The Timeout field displays the maximum number of seconds that the ACOS device waits for a reply from the LDAP server for a given request. The user can specify 1-60 seconds. If the LDAP server does not reply before the timeout, authentication of the admin fails.

v. Determine whether you want to enable or disable SSL.

vi. Click **Create**. Verify that you have returned to the

vii. Verify that you have returned to the **System** >> **Admin** >> **External Authentication** >> **LDAP** window and that an LDAP server has been created.

If you selected **IPv6**, complete the following steps:

i. Enter the host IPv6 address of the LDAP server in the **Server** text box.

ii. Select either **Common Name** or **Domain Name**.

If you selected **Common Name**, enter both the **Common Name** and the **Distinguished Name** in their text boxes.

If you selected **Domain Name**, enter the **Domain Name** in its text boxes.

iii. Enter a port number in the **Port** text box or accept the default.

iv. Enter a timeout value in the **Timeout (Seconds)** text box or accept the default.

The Timeout field displays the maximum number of seconds that the ACOS device waits for a reply from the LDAP server for a given

request. The user can specify 1-60 seconds. If the LDAP server does not reply before the timeout, authentication of the admin fails.

v. Determine whether you want to enable or disable SSL.

vi. Click **Create**. Verify that you have returned to the

vii. Verify that you have returned to the **System** >> **Admin** >> **External Authentication** >> **LDAP** window and that an LDAP server has been created.

Configuring using CLI

The user can configure the LDAP server through the CLI mode. The following are the various steps and modes to enable LDAP authentication and enter the following command at the global configuration level of the CLI:

```
ACOS(config)# authentication type ldap
```

- To use backup methods, specify the methods in the order in which you want to use them. For more information, see Multiple Authentication Methods and Tiered Authentication.

  For example:

  ```
  ACOS(config)# authentication type ldap local radius tacplus
  ```

- To configure an LDAP server on the ACOS device, use the **ldap-server host** command at the global configuration level of the CLI:

  ```
  ACOS(config)# ldap-server host 192.168.101.24 cn UserName dn
  cn=UserName,dc=UserAccount,dc=example,dc=com
  ```

  Do not use quotation marks for the **dn** option. For example, the following DN string syntax is valid:

  ```
  cn=xxx3,dc=mACOScrc,dc=com
  ```

  The following string is **not** valid:

  ```
  "cn=xxx3,dc=mACOScrc,dc=com"
  ```

  Spaces are not allowed in the **dn** specification.

- Multi-domain admin authentication and authorization can be achieved by configuring ACOS's LDAP server to point to the AD Global Catalog. To configure the ACOS's LDAP server to support this mode, specify the following:
  - Authentication type
  - Authentication mode
  - ldap-server host

  NOTE:
  - Multi-domain admin authentication and authorization will work as expected for AD (Active Directory) only; it will not work for multi-disjointed domains.
  - The input format for the admin name should be domain\usernmae or username@domain. Other formats are not supported.
  - All current authorization attributes are supported: OU, A10AdminRole, A10AdminPartition, A10AccessType.

- To configure the ACOS device and provide LDAP AAA for *UserAccUser1*, enter a command like the following:

```
ACOS(config)# ldap-server host ldapserver.ad.example.edu cn ExampleUser dn
ou=StaffElevatedAccounts,ou=ServiceAccounts,dc=ad,dc=example,dc=edu
```

  To use nested OUs, specify the nested OU first, then the root. For example, a user account could be nested in the following way:

```
Root OU= Service Accounts -> OU=StaffElevatedAccounts -> UserAccUser1
```

For more information about these commands, see the *Command Line Interface Reference.*

Configuring an OpenLDAP Server

The following topics are covered:

Overview

When logging in to the ACOS device via LDAP, the ACOS devices needs to send LDAP packets to LDAP server (for example, OpenLDAP or Windows AD). OpenLDAP can be installed on Windows or Linux.

To configure an OpenLDAP server and provide authentication and authorization for ACOS administrators:

1. Add the A10 schema file by copying the file and pasting it in the following location:

   `openldap_install_directory\schema`

   For example, on your server, the location might be `C:\Program Files\OpenLDAP\schema`.

   For more information, see A10 Schema File for OpenLDAP.

2. Add the administrator accounts.

   For more information, see A10 Administrator Account Files for LDAP.

3. Restart the LDAP service.

A10 Schema File for OpenLDAP

The following text is an example of the schema file that is required on the OpenLDAP server to provide authentication and authorization to ACOS administrators:

```
# all a10 LDAP OID be placed in 1.3.6.1.4.1.22610.300.
# all attributetype start from 1.3.6.1.4.1.22610.300.1.
# all objectclass start from 1.3.6.1.4.1.22610.300.2.

attributetype ( 1.3.6.1.4.1.22610.300.1.1
   NAME 'A10AdminRole'
   DESC 'admin Role'
   syntax 1.3.6.1.4.1.1466.115.121.1.15
```

```
   SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.22610.300.1.2
   NAME 'A10AdminPartition'
   DESC 'admin Partition'
   EQUALITY caseIgnoreMatch
   SUBSTR caseIgnoreSubstringsMatch
   syntax 1.3.6.1.4.1.1466.115.121.1.15  )

attributetype ( 1.3.6.1.4.1.22610.300.1.3
   NAME 'A10AccessType'
   DESC 'admin Access Type'
   syntax 1.3.6.1.4.1.1466.115.121.1.15
   SINGLE-VALUE )

objectclass ( 1.3.6.1.4.1.22610.300.2.1
   NAME 'A10Admin' SUP top AUXILIARY
   DESC 'A10 Admin object class '
   MAY ( A10AdminRole $ A10AdminPartition $ A10AccessType ) )
```

The LDAP schema file for ACOS administrator authentication and authorization contains the following items:

- **A10Admin**

  This is the object class for A10 Networks, and can contain one or more of the following attribute types.

  The user can specify the values to assign to these attributes in the definition file for the administrator. (See A10 Administrator Account Files for LDAP.)

- **A10AdminRole**

  This attribute type specifies the administrator's role, which defines the scope of read-write operations the administrator is allowed to perform on the ACOS device.

  The ACOS device has the following predefined roles:

  - **ReadOnlyAdmin**
  - **ReadWriteAdmin**
  - **PartitionSlbServiceOperator**

- **PartitionReadOnly**
- **PartitionReadWrite**

NOTE: When RBA is disabled, in CLI, login users with the role "**PartitionSlbServiceOperator**" can configure other objects, except for the role "**PartitionSlbServiceOperator**".
On GUI, login users with role "**PartitionSlbServiceOperator**" can access objects or pages that are under the role "**PartitionSlbServiceOperator**".

- To specify one of these roles in the definition file for the administrator account, use the role name as the attribute value. For example:

  ```
  A10AdminRole: ReadWriteAdmin
  ```

  If you do not use this attribute in the definition file for the administrator account, the ReadOnlyAdmin role is assigned to the administrator.

- A10AdminPartition – This attribute type specifies the ACOS partition the administrator is authorized to log onto.
  - For the shared partition, enter “shared”. For example:

    ```
    A10AdminPartition: shared
    ```

  - For a private partition, enter the partition name. For example:

    ```
    A10AdminPartition: privpart1
    ```

    If you do not use this attribute in the definition file for the administrator account, the administrator is allowed to log into the shared partition.

- A10AccessType – This attribute type specifies the user interface(s) for which the administrator is authorized and whether the administrator is authorized to create, import, or modify External Health Monitor files. The user can specify one or more of the following:
  - `cli` – CLI
  - `web` – GUI
  - `axapi` – aXAPI
  - `hm` – External Health Monitors

An administrator is not allowed to log into the device if the corresponding admin account does not enable at least one of the `cli`, `web`, or `axapi` parameters.

The hm parameter attribute can only be specified for administrator accounts with system-wide, read+write (R/W) privilege to allow them to be able to create, import, or modify External Health Monitor files.

CAUTION: The `hm` attribute should be enabled only for other admins sufficiently trusted to perform these operations without malicious or malicious content which could otherwise compromise security in the ACOS system and its deployed environment.

NOTE: For more information, see the *Application Delivery and Server Load Balancing Guide* (*Using External Health Methods* section) and Configuring LDAP for ACOS Administrators.

A10 Administrator Account Files for LDAP

Administrator accounts managed by an LDAP server are stored in files on the server.

The following is an example for creating an LDAP user:

```
dn: cn=user1,dc=my-domain,dc=com
cn: user1
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: A10Admin
userPassword: 123456
sn: sn
ou: guest
A10AdminRole: ReadWriteAdmin
```

This file configures admin “user1”. The objectClass value `A10Admin` and the `A10AdminRole` attribute are specific to A10 Networks and are defined in the schema file, which also must be added to the LDAP server.

In this example, the `A10AdminPartition` and `A10AccessType` attributes are omitted. The default values are used. (See A10 Schema File for OpenLDAP.)

Configuring Microsoft Active Directory

The user can configure Microsoft Active Directory for LDAP authentication and authorization of ACOS administrators. When the user logs into the ACOS device, the device sends the user name and password to Active Directory to validate the credentials.

NOTE: The information in this section is based on Windows Server 2008.

The following topics are covered:

Summary

The following is a summary of this configuration for Microsoft Active Directory.

1. Install Active Directory on your Windows server.
   a. For more information, see http://technet.microsoft.com/en-us/library/jj574166.aspx.
2. Configure the administrator accounts.

   For more information, see Configuring ACOS Administrator Accounts.

3. Add a user name and password to Active Directory.

   For more information, see http://technet.microsoft.com/en-us/library/dd894463(v=WS.10).aspx.

4. (Optional) Add the A10 LDAP attribute types to the server. See Adding A10 LDAP Attribute Types.

NOTE: If you plan to use the default settings for all the A10 attributes, the user can skip this step.

Configuring ACOS Administrator Accounts

This section describes how to configure an administrator account.

The following topics are covered:

Creating a Read-Only Administrator

To create an administrator with the ReadOnlyAdmin role:

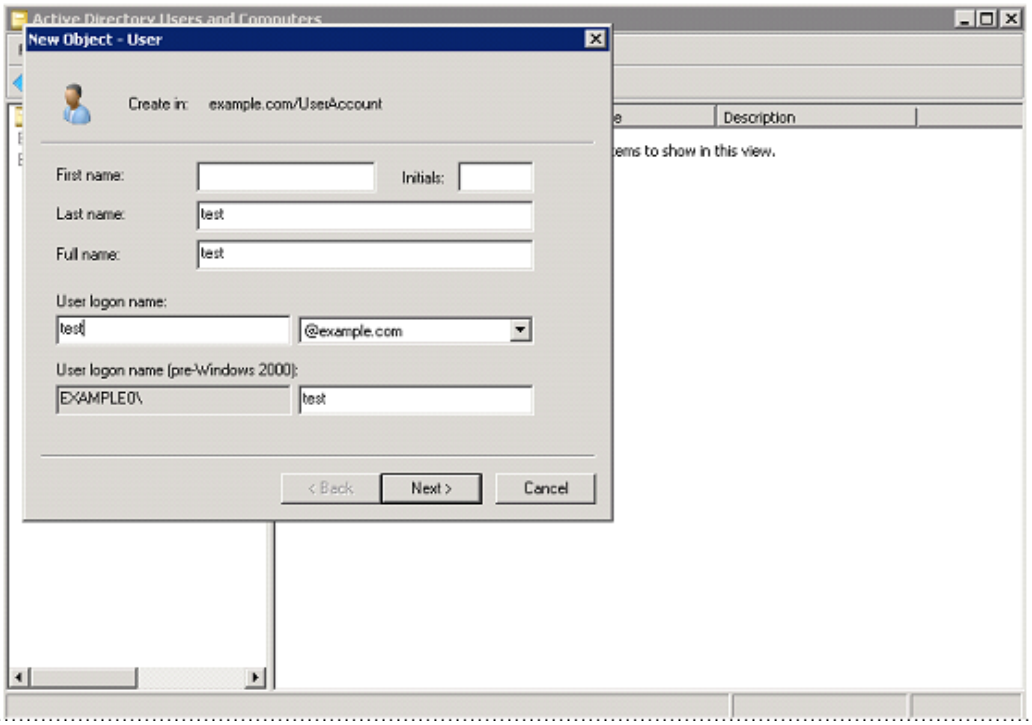
1. Go to the **Active Directory Users and Computers**.
2. Click **File** > **New**.
3. Complete the following steps in the **New Object - User** window:
   a. Enter a first name.
   b. Enter a last name.
   c. Enter a full name.
   d. Enter a user logon name.
   e. Select the domain.

f. If applicable, enter the pre-Windows 2000 logon name.

g. Click **Next**.

4. Select **User Account** in the left pane to see the user that you just created displayed in the right pane.

Figure 3 : Creating a Read-Only Administrator



Testing the Read-Only Administrator Account

The following is the LDAP server configuration on the ACOS device:

```
ldap-server host 192.168.101.24 cn cn dn ou=UserAccount,dc=example,dc=com
!
authentication type ldap
!
```

The following is an example of the session login by the read-only admin. Access to the configuration level by this admin is not allowed.

```
[root@Linux-PC-148 ~]# ssh -l test 192.168.100.46
Password:
Last login: Thu Jun 21 13:05:51 2012 from 192.168.100.148
```

```
ACOS system is ready now.
[type ? for help]
ACOS>
ACOS> enable
Password: <blank>
ACOS# show admin session
 Id    User Name   Start Time                    Source IP        Type
Partition Authen  Role            Cfg
-------------------------------------------------------------------------------
----------------
*99    test        13:08:10 CST Thu Jun 21 2012  192.168.100.148  CLI
      Ldap    ReadOnlyAdmin   No
ACOS# config
          ^
% Unrecognized command.Invalid input detected at '^' marker.
ACOS#
```

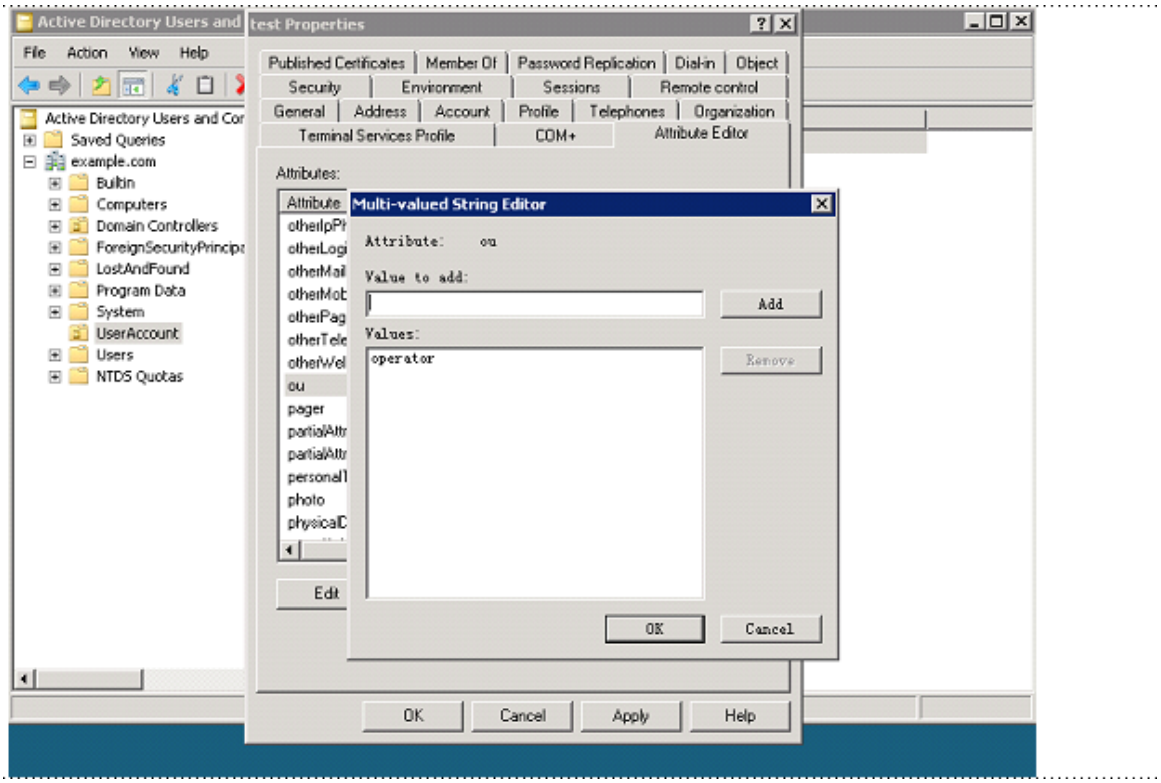
Configuring a Read-Write Administrator

In this example, the *ou* attribute is set to **operator**.

To configure a read-write administrator with a *ReadWriteAdmin* role:

1. Go to **Active Directory Users and Computers**.
2. Right-click **User Account**, and in the right-pane, select a user name.
3. Right-click on the user name and select **Properties**.
4. On the **Attribute Editor** tab, click **ou**, and click **Edit**.
5. In the **Multi-value String Editor**, in **Value to add**, enter **Operator**.
6. Click **OK**.

Table 7 : Multi-valued String Editor



Testing the Read-Write Administrator Account

The following is the LDAP server configuration on the ACOS device:

```
ldap-server host 192.168.101.24 cn cn dn ou=UserAccount,dc=example,dc=com
!
authentication type ldap
!
```

The following is an example of the session login by the read-write administrator:

NOTE: This administrator is allowed to access the configuration level.

```
[root@Linux-PC-148 ~]# ssh -l test 192.168.100.46
Password:
Last login: Thu Jun 21 13:08:10 2012 from 192.168.100.148
ACOS system is ready now.
[type ? for help]
ACOS> enable
```

```
Password: <blank>
ACOS# show admin session
 Id    User Name    Start Time                    Source IP        Type
Partition Authen  Role            Cfg
-------------------------------------------------------------------------
----------------
*101    test         13:22:16 CST Thu Jun 21 2012  192.168.100.148  CLI
      Ldap    ReadWriteAdmin  No
ACOS# config
ACOS(config)#
```

A10 LDAP Object Class and Attribute Types

The user can add A10 LDAP attribute types to the server.

NOTE: If you plan to use the default settings for all the A10 attributes, the user can skip the rest of this section.

CAUTION: Please add the attributes carefully. Once they are added, they can not be changed or deleted.

The following topics are covered:

Admin Role

The LDAP object class for A10 Networks is A10Admin, and can contain one or more of the following attribute types. The user can specify the values to assign to these attributes in the definition file for the admin.

- A10AdminRole

This attribute type specifies the administrator's role, which defines the scope of read-write operations that the administrator is allowed to perform on the ACOS device.

The following predefined roles are included on the ACOS device:

- **ReadOnlyAdmin**
- **ReadWriteAdmin**
- **PartitionReadWrite**
- **PartitionSlbServiceOperator**
- **PartitionReadOnly**

NOTE: When RBA is disabled, in CLI, login users with the role "**PartitionSlbServiceOperator**" can configure other objects, except for the role "**PartitionSlbServiceOperator**".
On GUI, login users with role "**PartitionSlbServiceOperator**" can access objects or pages that are under the role "**PartitionSlbServiceOperator**".

Adding A10 LDAP Attribute Types

To specify one of these roles in the definition file for the administrator account, enter the role name as the attribute value.

For example,

```
a10AdminRole: ReadWriteAdmin
```

If you do not use this attribute in the definition file for the administrator account, the ReadOnlyAdmin role is assigned to the administrator.

- A10AdminPartition specifies the ACOS partition that the administrator is authorized to access.
  - For the shared partition, enter "shared".

    For example,

    ```
    a10AdminPartition: shared
    ```
  - For a private partition, enter the partition name.

For example,

```
a10AdminPartition: privpart1
```

If you do not use this attribute in the definition file for the administrator account, the administrator can log in to the shared partition.

- A10AccessType specifies the user interface(s) that the administrator authorized to use.

  The user can specify one or more of the following interfaces:

  - `cli`
  - `web`
  - `axapi`
  - `hm` – External Health Monitors

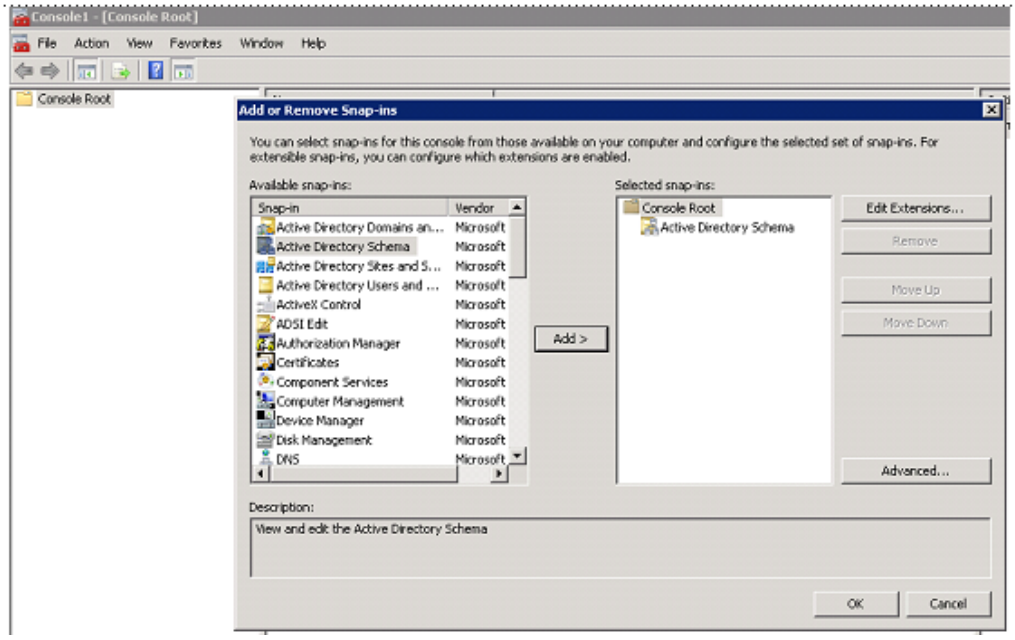
    When you do not enable these attributes in the definition file for the administrator account, the admin is not allowed to log in though any of these interfaces. Furthermore, the admin cannot create, import, or modify External Health Monitor files. The `hm` parameter can only be specified for administrator accounts with system-wide, read and write (R/W) privilege.

Adding the Attribute Type in the GUI Mode

The user can add the Attribute Type through the GUI mode. The following are the various steps and modes to configure in Windows, to add the attribute type:

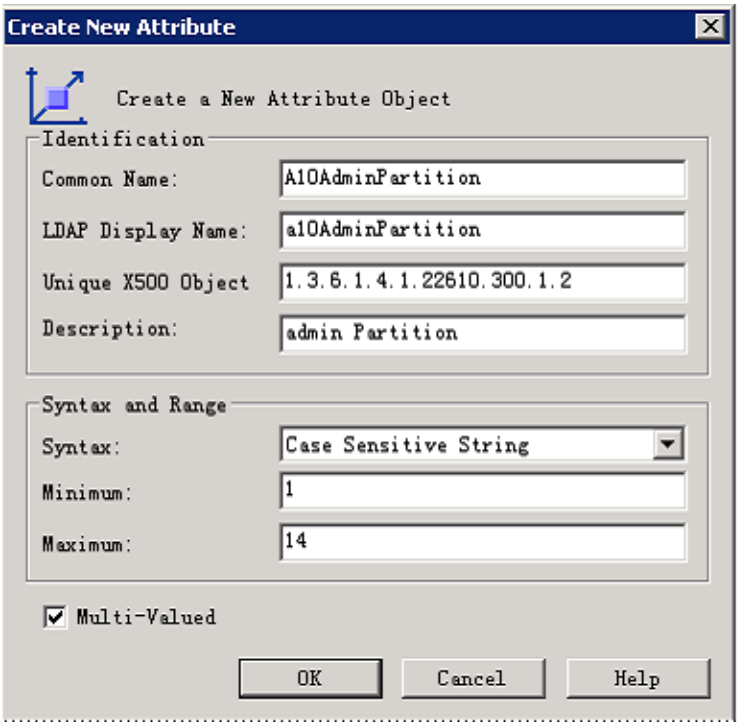
1. Click **Start** > **All Programs** > **Accessories** > **Run**.
2. To start Microsoft Management Console, enter **mmc**.
3. In the console, click **File** > **Add/Remove Snap-In**.
4. In Add or Remove Snap-ins, select **Active Directory Schema** in the left pane and click **Add**.
5. Click **OK**.
6. In the Console, right-click the **Attributes** folder, and click **New** > **Attribute**.

Figure 4 : Attribute Add Schema



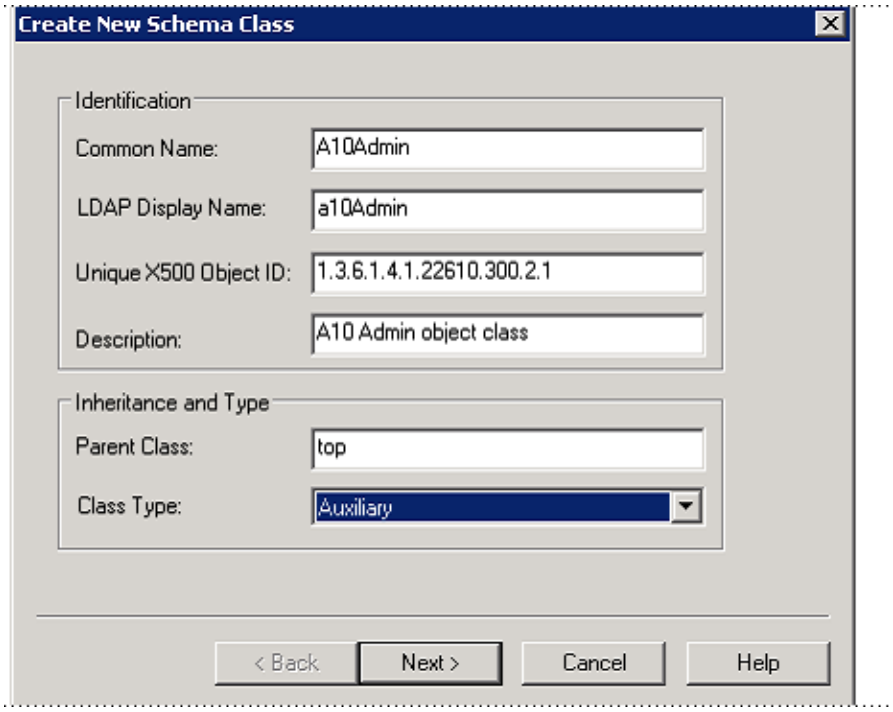
7. In **Create New Attribute**, complete the fields, and click **OK**.

Figure 5 : Creating a New Attribute



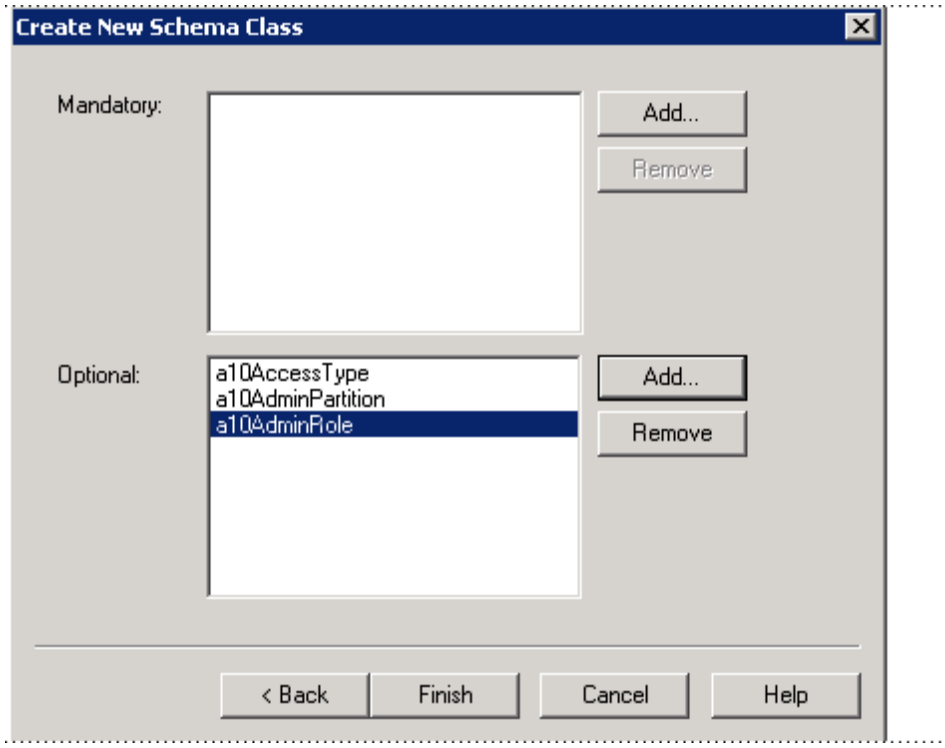
8. In **Console**, right-click **Classes**, and click **New** > **Class**.
9. Enter the appropriate information in the **Identification** and **Inheritance and Type** sections and click **Next**.

Figure 6 : Creating a New Class



10. Enter the appropriate information in the **Mandatory** and **Optional** sections and click **Finish**.

Figure 7 : Mandatory and Optional fields



Adding “a10Admin” to the object Class

Figure 8and Figure 9change the *object Class* and add *a10Admin* to the *objectClass*. After this, all the attributes can be added to administrator *test*.

Figure 8 : Adding Admin *Test* to the objectClass

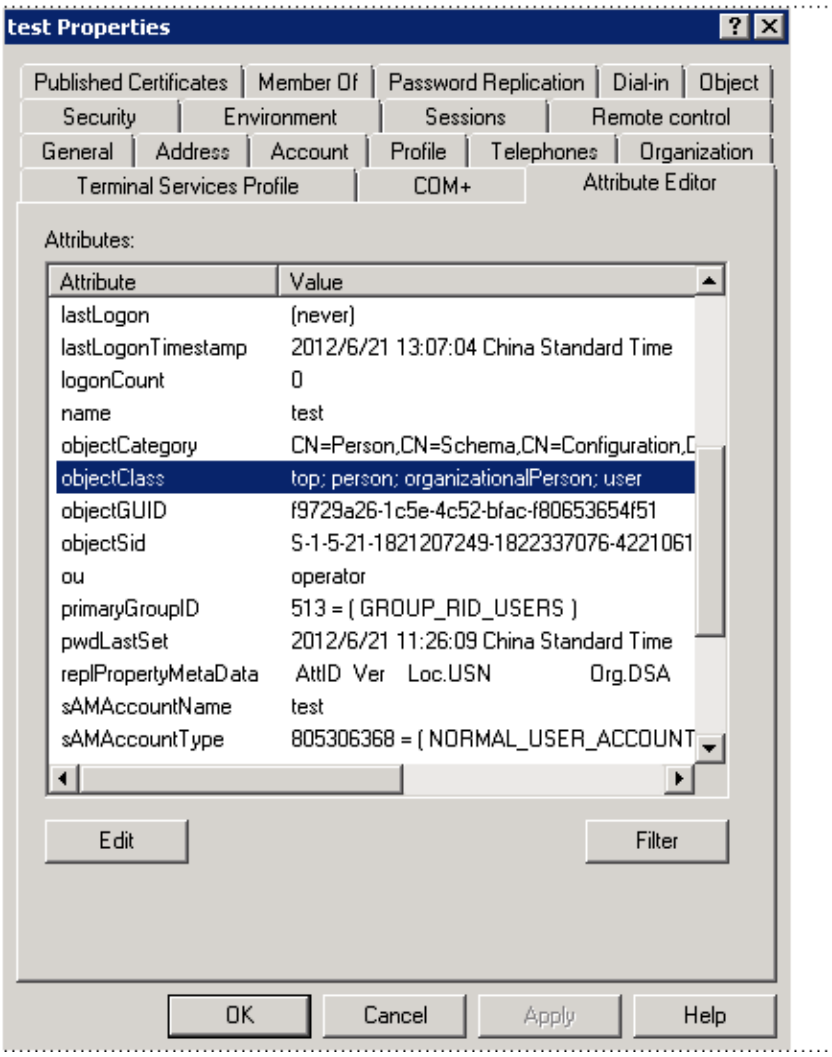
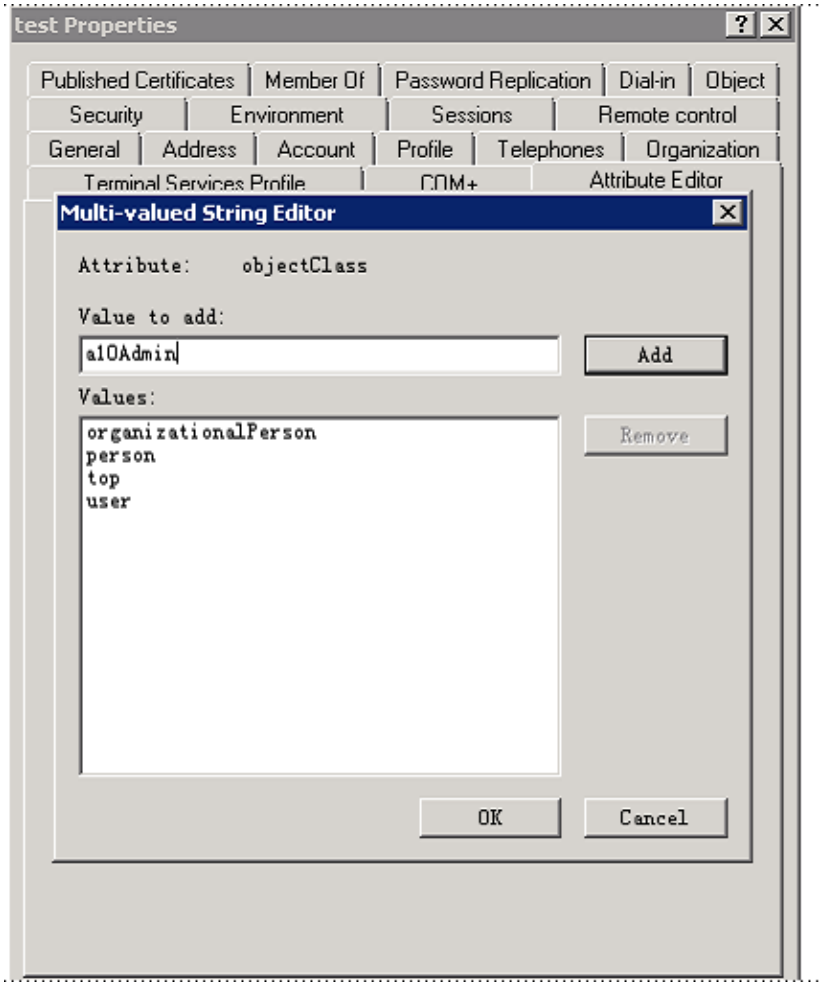


Figure 9 : Editing the Values



Restarting the LDAP Process

To place the LDAP changes into effect, restart the LDAP process on the server. To access the process controls, under Administrative Tools, select Services.

Figure 10 : Restarting the LDAP Process - Step 1

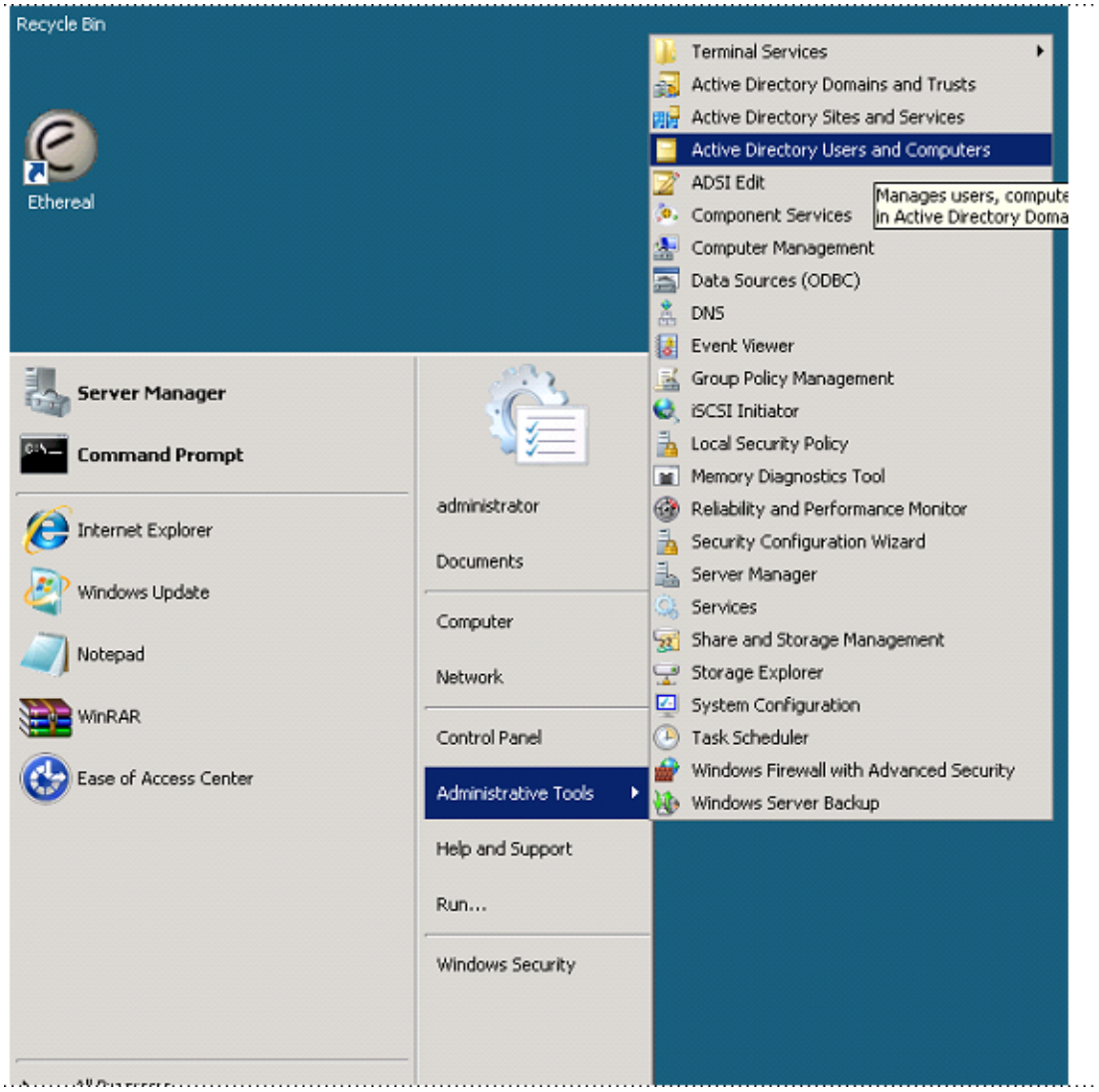
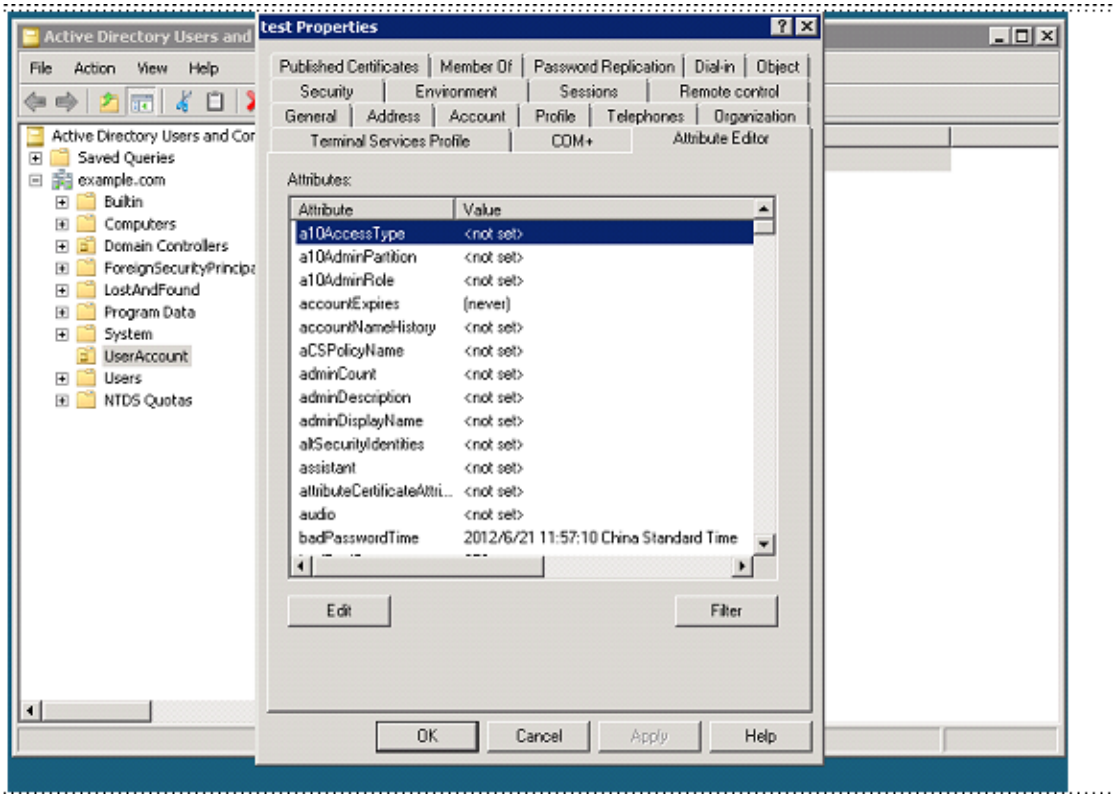


Figure 11 : Restarting the LDAP Process - Step 2



Changing the Administrator Role (A10AdminRole)

Changing the Administrator Role and Clearing the ou Attribute set the administrator role for administrator *test* to *ReadWriteAdmin*.

Figure 12 : Changing the Administrator Role

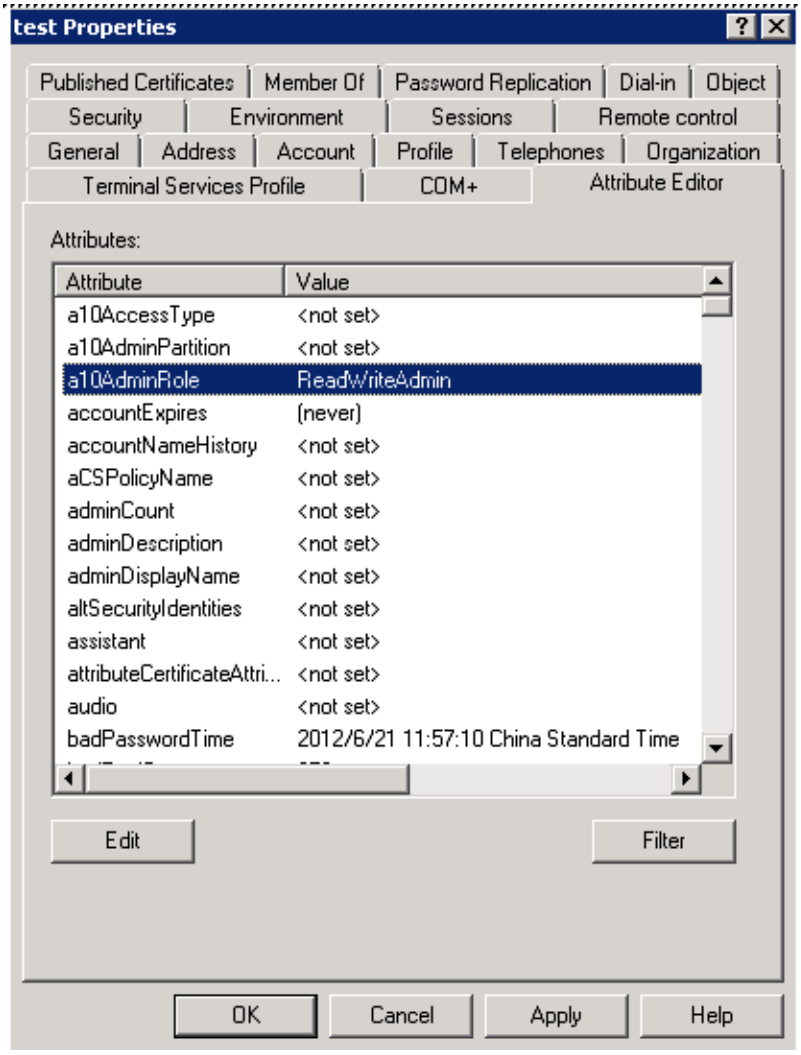
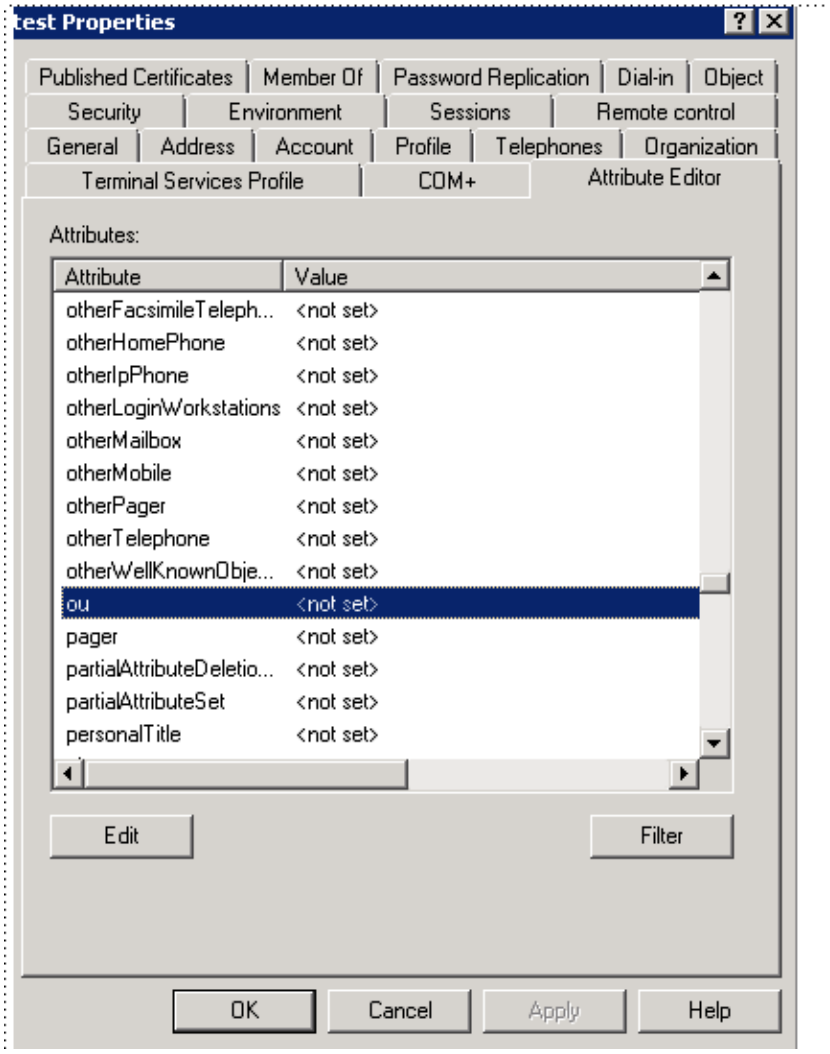


Figure 13 : Clearing the *ou* Attribute



Login Example

The following is a login example for an administrator:

```
[root@Linux-PC-148 ~]# ssh -l test 192.168.100.46
Password:
Last login: Thu Jun 21 13:22:16 2014 from 192.168.100.148
ACOS system is ready now.
[type ? for help]
ACOS> enable
Password: <blank>
ACOS#
```

```
ACOS# show admin session
 Id    User Name   Start Time                    Source IP        Type
Partition Authen  Role            Cfg
-------------------------------------------------------------------------------
----------------
*106   test        14:15:13 CST Thu Jun 21 2014 192.168.100.148  CLI
     Ldap    ReadWriteAdmin  No
ACOS#
ACOS# config
ACOS(config)#
```

Adding Private Partition Information (A10AdminPartition)

The following screen configures admin `test` as an private partition administrator and assigns the administrator to partition `test1`.

NOTE: The shared partition does to need to be added to the LDAP server. If the `a10AdminPartition` attribute is not set, the admin is permitted to access the shared partition.

ACOS Configuration

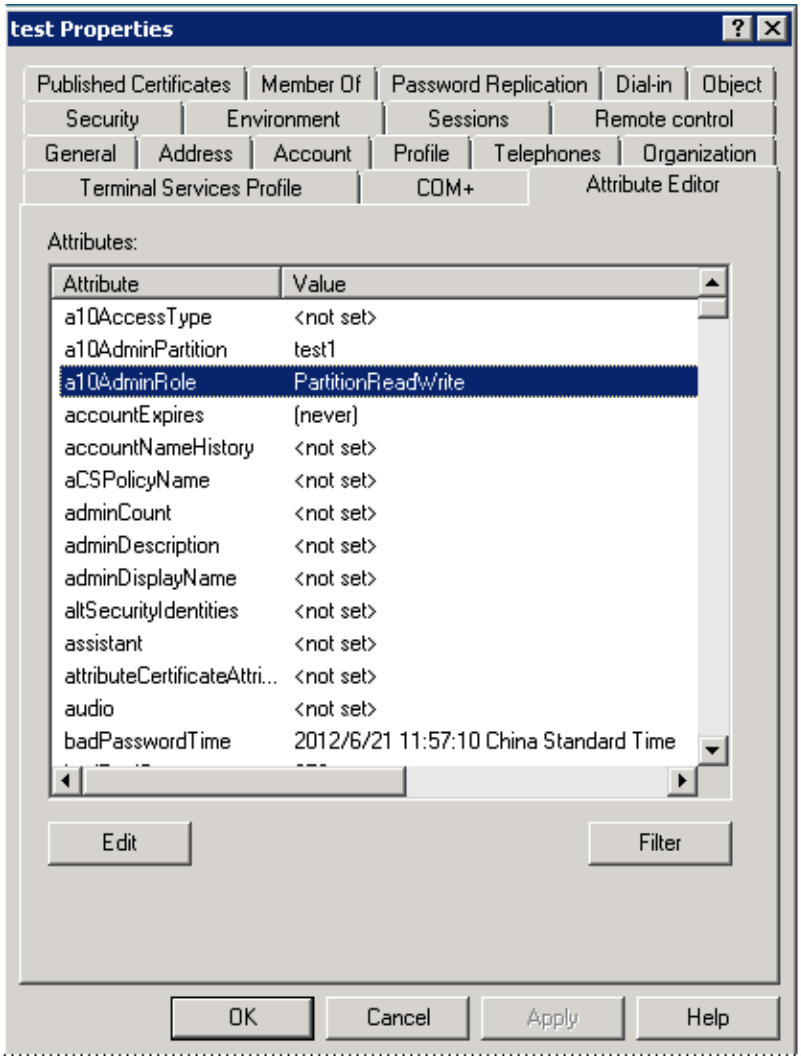
The following is the partition configuration on the ACOS device:

```
ACOS# configure
ACOS(config)# partition test1 id 1
```

LDAP Server Configuration

Figure 14 sets the `a10AdminPartition` attribute to `test1`. This indicates that the admin can access the private partition called `test1`. The `a10AdminRole` attribute is set to `PartitionReadWrite`. This restricts the administrator to read-write operations in the private partition.

Figure 14 : LDAP Server Configuration



Login Example

When administrator `test` logs in, the session opens in partition `test1`.

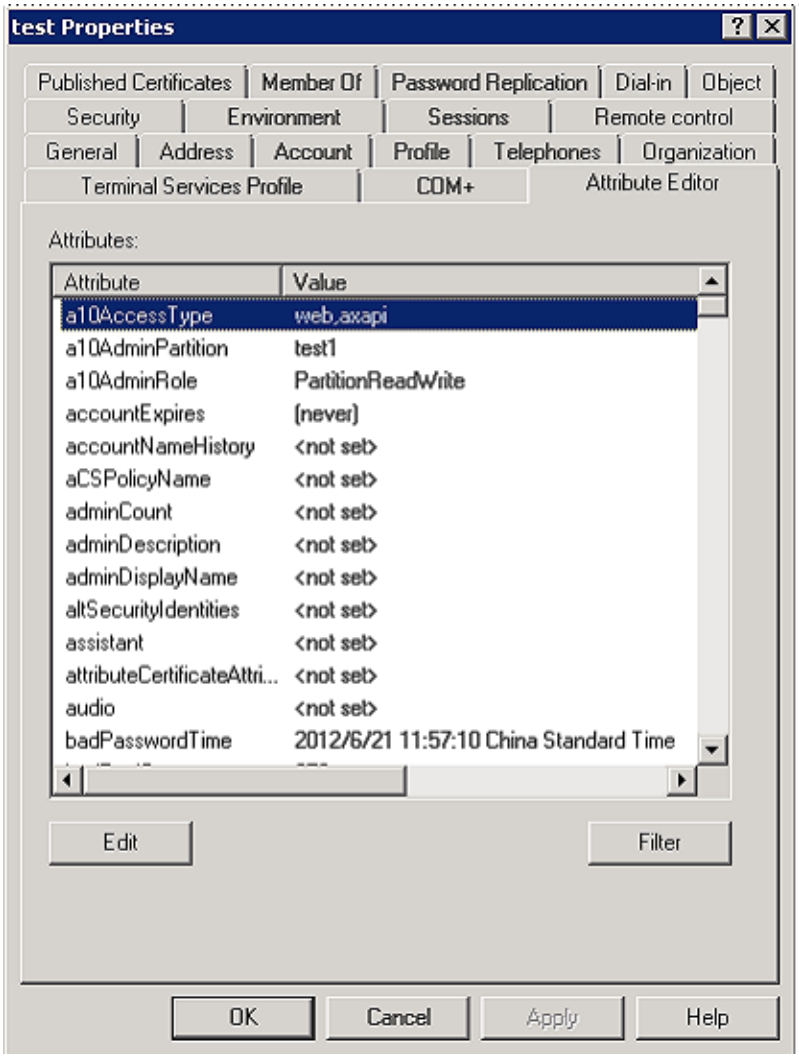
```
[root@Linux-PC-148 ~]# ssh -l test 192.168.100.46
Password:
Last login: Thu Jun 21 14:19:41 2012 from 192.168.3.196
ACOS system is ready now.
[type ? for help]
ACOS2500-1[test1]>
ACOS2500-1[test1]> enable
Password: <quick>
```

```
ACOS2500-1[test1]#
ACOS2500-1[test1]# config
ACOS2500-1[test1](config)# show admin session
 Id    User Name   Start Time                    Source IP        Type
Partition Authen  Role            Cfg
-------------------------------------------------------------------------
----------------
*108   test        14:22:51 CST Thu Jun 21 2012  192.168.100.148  CLI
test1     Ldap    PatitionReadWriteYes
```

Changing the Access Type (A10AccessType)

Figure 15sets the access type for the `PartitionReadWrite` administrator to web (GUI) and aXAPI. This configuration prohibits the administrator from logging in through the CLI.

Figure 15 : Changing the Access Type



Login Example

The following example shows what happens if the admin tries to log in through the CLI:

```
[root@Linux-PC-148 ~]# ssh -l test1 192.168.100.46
Password:***
Password:***
Couldn't login via CLI, check the log message with admin/a10
ACOS2500-1# show log
Log Buffer: 30000
```

```
Jun 21 2012 14:30:42 Error   [SYSTEM]:The user, test1, from the remote
host, 192.168.100.148, failed in the CLI authentication.
Jun 21 2012 14:30:42 Warning [SYSTEM]:Ldap authentication failed(user:
test1): The user access interface is not authenticated.
```

Additional Reference Information

The authentication command has the following options.

To understand these options and how they affect the authentication process, see Command Line Interface Reference.

```
ACOS(config)# authentication ?
  console                Configure console authentication type
  enable                 The enable-password authentication type
  login                  The login mode
  mode                   Configure authentication mode
  multiple-auth-reject   Multiple same user login reject
  type                   The login authentication type
ACOS(config)# ldap-server host ?
  NAME<length:1-63>  Hostname of LDAP server
  A:B:C:D:E:F:G:H    IPV6 address of ldap server
  A.B.C.D            IPV4 address of ldap server
```

NOTE: To get additional information on the commands that appear in the examples of this document, see Command Line Interface Reference.

TACACS+ and RADIUS

The user can configure the ACOS device to use remote servers for Authentication, Authorization, and Accounting (AAA) for administrative sessions. The ACOS device supports RADIUS, TACACS+, and LDAP servers. This sections provides information on the following RADIUS and TACACS+ features.

NOTE: For information about LDAP support, see Lightweight Directory Access Protocol.

The following topics are covered:

Authentication and Modes

The following topics are covered:

Overview

Authentication grants or denies access to the device based on the credentials provided by the user (admin user name and password).

By default, when someone attempts to log in to the ACOS device, the device determines whether the username and password exist in the local administrative database. Without additional configuration, the authentication process stops at this point. If the administrator username and password exist in the local database, the user is granted access; otherwise, access to the device is denied.

The user can configure the ACOS device to also use external RADIUS, TACACS+ or LDAP servers for authentication.

Multiple Authentication Methods

The user can specify multiple methods for authenticating ACOS administrators. For example, the user can configure the ACOS device to try the these servers in the following order:

- LDAP
- TACACS+
- RADIUS
- Local database

In this example, the ACOS device tries to use the LDAP servers first. If no LDAP servers respond, the ACOS device tries to use the TACACS+ servers. If no TACACS+ servers respond, the ACOS device tries the RADIUS servers. If no RADIUS servers respond, the ACOS device uses the local database.

Tiered Authentication

In addition to selecting multiple methods of authentication, if the primary authentication method is unavailable, the user can configure the ACOS device to use tiers of authentication and configure backup authentication methods. By default, the

backup authentication method is used only if the primary method does not respond. If the primary method responds and denies access, the secondary method is not used. The administrator is not granted access.

The user can enable the ACOS device to check the next method if the primary method does respond and authentication fails. This option is called “tiered authentication”. For example, the primary method is RADIUS and the next method is TACACS+. If RADIUS rejects the administrator, tiered authentication attempts to authenticate the administrator by using TACACS+.

Figure 16provides information about the ACOS authentication behavior based on tiered authentication.

Figure 16 : Tiered Authentication

Tiered Authentication Setting	ACOS Behavior
Single (default)	1. Try method1. If a method1 server replies, permit or deny access based on the server reply. 2. **Only** if no method1 servers reply, try method2. If a method2 server replies, permit or deny access based on the server reply. 3. **Only** if no method2 servers reply, try method3. If a method3 server replies, permit or deny access based on the server reply. 4. **Only** if no method3 servers reply, try method4. If authentication succeeds, the admin is permitted. Otherwise, the admin is denied.
Multiple	1. Try method1. If a method1 server replies, permit access based on the server reply. 2. If no method1 servers reply **or** a method1 server denies access, try method2. If a *method2* server replies, permit access based on the server reply. 3. If no method2 servers reply **or** a method2 server denies access, try method3. If a *method3* server replies, permit access based on the server reply.

Tiered Authentication Setting	ACOS Behavior
	4. If no method3 servers reply **or** a method3 server denies access, try method4. If authentication succeeds, the admin is permitted. Otherwise, the admin is denied.

By default, tiered authentication is disabled and is set to single. The user can enable it on a global basis.

Authentication Process

The following topics are covered:

Overview

First, the user must specify whether to check one of the following:

- Local Database (Scenario: Authentication Process When Remote Authentication Is First (Two Remote Servers Configured) – RADIUS)

or

- Remote Server (Scenario: Authentication Process When Remote Authentication Is First (one remote server configured) – TACACS+)

They show the authentication processes that are used if the ACOS device is configured to check remote AAA servers first.

If the RADIUS, TACACS+, or LDAP server responds, the local database is not checked, and one of the following situations occurs:

- If the administrator's credentials are found on the RADIUS, TACACS+, or LDAP server, the administrator is granted access.

- If the administrator credentials are not found on the RADIUS, TACACS+, or LDAP server, the administrator is denied access.

If there is no response from RADIUS, TACACS+, or LDAP server, the ACOS device checks its local database for the administrator name and password.

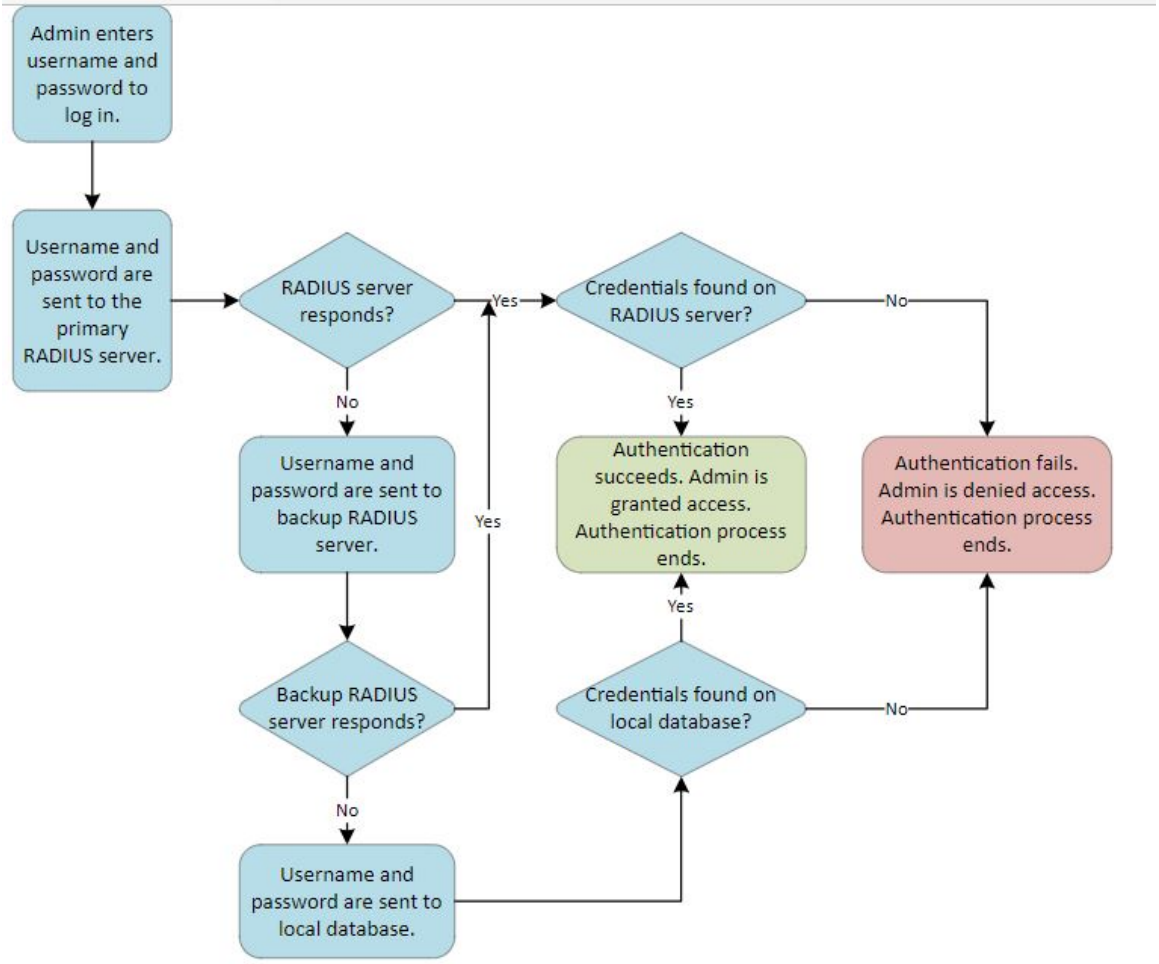
- An exception is made for the `admin` account; by default, the ACOS device always uses local authentication for `admin`.
- Local authentication can be disabled for `admin`, in which case the authentication process is the same as for other administrator accounts.

NOTE: For more information, see Disabling Local Authentication for the Administrator Account in the CLI Mode.

Scenario: Authentication Process When Remote Authentication Is First (Two Remote Servers Configured) – RADIUS

Authentication Process When Remote Authentication Is First (Two Remote Servers Configured) – RADIUS

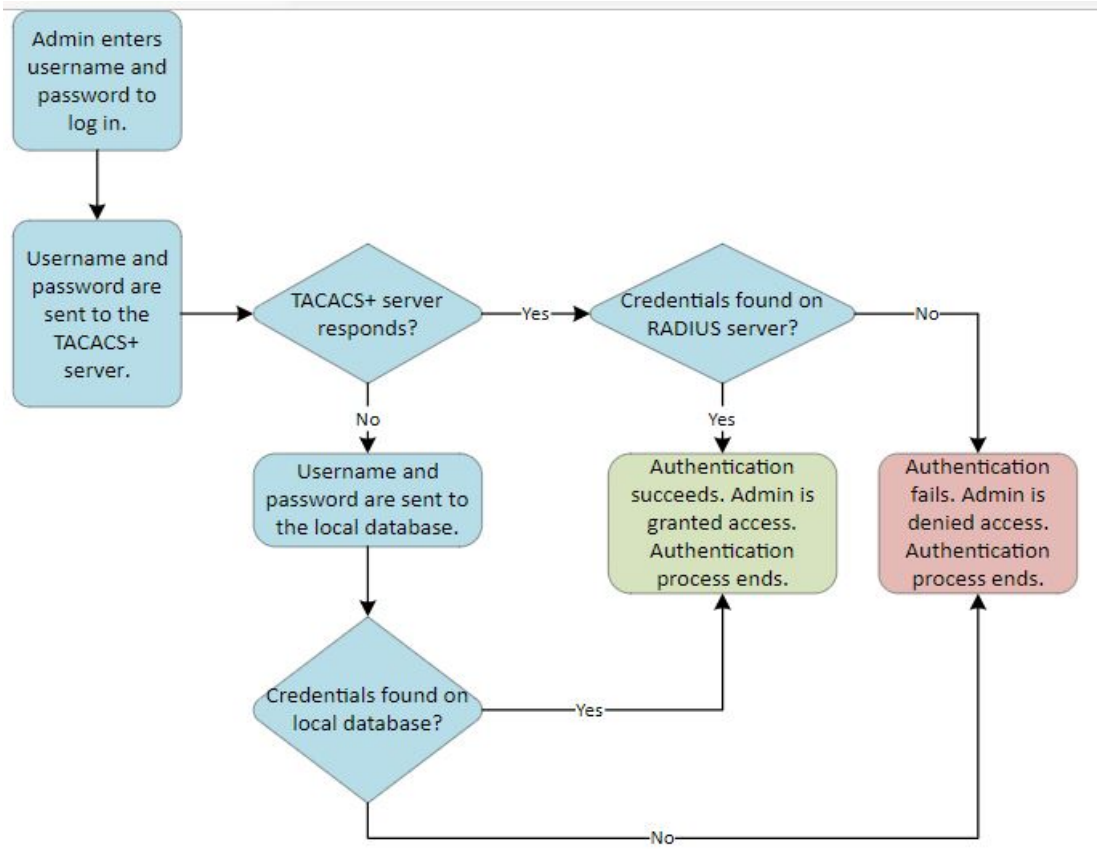
Figure 17 : Two Remote Server Configured



Scenario: Authentication Process When Remote Authentication Is First (one remote server configured) – TACACS+

Authentication Process When Remote Authentication Is First (one remote server configured) – TACACS+

Figure 18 : One Remote Server Configured.



Disabling Local Authentication for the Administrator Account in the CLI Mode

The user can disable the local authentication for the administrator account through the CLI mode. The following are the steps and modes to disable these settings for the interfaces:

By default, the ACOS device always locally authenticates `admin` even if RADIUS, TACACS+, or LDAP is used as the primary authentication method.

To disable automatic local authentication for the administrator account, access the admin configuration level for the admin you want to disable, then use the **`disable`** command. For example:

```
ACOS(config)# admin exampleuser password <password>
```

```
ACOS(config-admin:exampleuser)# disable
Modify Admin User successful!
ACOS(config-admin:exampleuser)#
```

NOTE: If the RADIUS, TACACS+, or LDAP server can not be reached, the ACOS device then uses local authentication for `admin`. This behavior is also used for other administrator accounts when the remote AAA server can not be reached.

Token-based Authentication Support for RADIUS

This chapter provides information about configuring an ACOS device to authenticate users by using RSA SecureID token on a RADIUS server.

The following topics are covered:

Overview

The ACOS Series supports RSA token-based RADIUS authentication, which provides additional login security by requiring the administrator to enter a string and a token in addition to the username and password. This enhancement supports the Access-Challenge function in RFC 2865.

Configuring Token-based Authentication for RADIUS

The user can configure token-based authentication for RADIUS by using the GUI or the CLI.

The following topics are covered:

Using the GUI to Configure Token-based Authentication for RADIUS

"Token-based Authentication"is not supported on GUI.

Using the CLI to Configure Token-based Authentication for RADIUS

After the administrator enters a username and a password, the ACOS device sends the credentials to the RADIUS server. If the username and password are valid, and the server is configured to use token-based authentication, the server replies with an Access-Challenge message. The ACOS device displays a prompt for the required token.

The ACOS device attempts to verify the token, and one of the following situations occurs:

- If the token is valid, the administrator is granted access.
- If the token is invalid, even though the username and password are valid, access is denied.

By default, support for token-based RADIUS authentication is enabled and cannot be disabled. No additional configuration is required on the ACOS device.

In the following CLI example, an administrator initiates the log in process by entering a username and a password. The ACOS device presents a challenge value and prompts for the response.

```
login as: admin2
Using keyboard-interactive authentication.
Password: ********
Using keyboard-interactive authentication.
Challenge: 133420
 Response: ******
Last login: Fri Jul  1 21:51:35 2011 from 192.168.32.153
[type ? for help]
ACOS>
```

Authorization

The following topics are covered:

Authorizing User Interface and External Health Monitor Access

The following topics are covered:

Overview

The user can control administrator access to the ACOS device by using one or more of the following user interfaces:

- CLI
- GUI
- aXAPI

By default, administrators are allowed to use all three user interfaces.

The user can also permit or deny administrator access to edit, create, import, or delete External Health Monitor files. By default, administrators are not allowed to manage External Health Monitor files.

RADIUS Configuration for User Interface and External Health Monitor Access

To configure RADIUS authorization based on user interface and External Health Monitor access, use:

```
A10-Admin-Access-Type
```

The following `A10-Admin-Access-Type` values provide access to the corresponding user interface:

- **cli**
- **web**
- **axapi**

To authorize access to more than one user interface, enter a comma between each value. For example, to authorize access to the CLI and web interfaces, enter `cli,web`.

The following `A10-Admin-Access-Type` value provides access to configure External Health Monitors:

- **hm**

An `A10-Admin-Access-Type` command that includes the **hm** value must also include at least one user interface value.

For example, to authorize access to the CLI and web interfaces, enter `cli,web`.

CAUTION: The `hm` value should be enabled only for other admins sufficiently trusted to perform these operations without malicious purpose or malicious content which could otherwise compromise security in the ACOS system and its deployed environment.

NOTE: For more information, see the *Application Delivery and Server Load Balancing Guide* (**Using External Health Methods** section) and Configuring LDAP for ACOS Administrators.

TACACS+ Configuration for User Interface and External Health Monitor Access

To configure authorization based on the user interface and External Health Monitor access, enter the following Attribute Value Pair (AVP):

```
a10-access-type=user-interface
```

- Replace *user-interface* with one or more of the following options:
- **cli**
- **web**
- **axapi**
- **hm**

An AVP pair statement that includes the `hm` option must also specify a second option. To authorize access to more than one user interface, enter a comma between each value, for example,

```
a10-access-type=cli,hm
```

CAUTION: The `hm` value should be enabled only for other admins sufficiently trusted to perform these operations without malicious purpose or malicious content which could otherwise compromise security in the ACOS system and its deployed environment.

NOTE: For more information, see the *Application Delivery and Server Load Balancing Guide* (**Using External Health Methods** section) and Configuring LDAP for ACOS Administrators.

NOTE: An AVP is the combination of an attribute, which is a parameter that is associated with an ACOS administrator account, and the value of the parameter.

Authorizing Admin Privileges

The following topics are covered:

Overview

The privileges for each admin are the same across all three user interfaces. For example, if you create an admin with global read and write privileges, then the same privileges apply to both the CLI and GUI.

Compatibility with Privilege Levels Assigned by RADIUS or TACACS+

It is required to assign a proper privilege level (defined on the ACOS device) to the external user on the RADIUS or TACACS+ server, so that the user may be authenticated and be granted access to the ACOS device. After the ACOS device authenticates the privilege level, it will use the GUI access role assigned to the user to manage the device.

It is not required to assign a privilege level to an ACOS admin on the RADIUS or TACACS+ server used to authenticate the admin. The ACOS device uses the GUI access role assigned to the admin in the admin's account on the ACOS device.

However, if a privilege level is assigned to the admin on the RADIUS or TACACS+ server, that privilege level must match the privilege assigned to the admin in the ACOS configuration. Otherwise, the admin will be denied access.

Table 8 : lists the RADIUS and TACACS+ privilege levels that match the GUI privileges.

GUI Access Role	Privilege Level		Partition Role
	RADIUS	TACACS+	
ReadWriteAdmin1	2	15	N
SystemAdmin	3	14	N
NetworkAdmin	4	13	N
NetworkOperator	5	12	N
SlbServiceAdmin	6	11	N
SlbServiceOperator	7	10	N
ReadOnlyAdmin	1	0	N
PartitionReadWrite	8	9	Y
PartitionNetworkOperator	9	8	Y
PartitionSlbServiceAdmin	10	7	Y
PartitionSlbServiceOperator	11	6	Y
PartitionReadOnly	12	5	Y

1 The ReadWriteAdmin role includes enabled support for External Health Monitor file access as described above.

The Partition Role column indicates whether the privilege is for a partition admin and requires specification of a private partition name. If the privilege level for a partition

role is specified on the RADIUS or TACACS+ server, the partition name also must be specified on the server. If the privilege level is for a non-partition role, it is invalid to specify a partition name on the server.

NOTE: The LDAP configuration on private partitions are private and overwrite any LDAP configuration on the shared private partition. However, AAA configuration (RADIUS-server, TACAS-server, authentication, authorization, and accounting) for administrators is global and not partition specific. When you enter the `show running config` command from a private partition, the local partition LDAP configuration is displayed while the shared partition AAA is displayed.

NOTE: When RBA is disabled, in CLI, login users with the role "**`PartitionSlbServiceOperator`**" can configure other objects, except for the role "**`PartitionSlbServiceOperator`**".

On GUI, login users with role "**`PartitionSlbServiceOperator`**" can access objects or pages that are under the role "**`PartitionSlbServiceOperator`**".

CAUTION: Given that the **`ReadWriteAdmin`** roll enables External Health Monitor File access, it should only be assigned for admins sufficiently trusted to perform these operations as performingwithout malicious purpose or malicious content which could otherwise compromise security in the ACOS system and its deployed environment.

NOTE: For more information, see the *Application Delivery and Server Load Balancing Guide* (**Using External Health Methods** section) and Configuring LDAP for ACOS Administrators.

RADIUS Configuration for GUI Privileges

To configure admin privileges for RADIUS, use the `A10-Admin-Role` option. For example, to authorize PartitionReadWrite privileges, use the following statement in the admin definition:

```
A10-Admin-Role = "PartitionReadWrite"
```

TACACS+ Configuration for GUI Access Roles

To configure admin privileges for TACACS+, use the following attribute-value pair (AVP):

```
a10-admin-role=role-name
```

Performing Authorization for CLI Access

The following topics are covered:

Overview

The user can configure the ACOS device to use external RADIUS, TACACS+, or LDAP servers to authorize CLI commands. After a successful authentication, the authenticated party is granted access to specific system resources by authorization. For an ACOS administrator, authorization specifies the CLI levels that they can access.

Disabled Commands for Read-Only Administrators

Administrators who are authenticated by using RADIUS, TACACS+, or LDAP, and are authorized for read-only access directly to the Privileged EXEC level of the CLI, cannot run the following operational commands:

- **backup**
- **config**
- **import**
- **locale**
- **reboot**

- **reload**
- **shutdown**

This includes administrators with the ReadOnlyAdmin or PartitionReadOnly privileges.

RADIUS CLI Authorization

To configure RADIUS CLI Authorization, enter the following settings on the RADIUS server:

```
VALUE A10-Admin-Privilege Read-only-Admin 1
VALUE A10-Admin-Privilege Read-write-Admin 2
```

The first line grants access to the User EXEC level and Privileged EXEC level. The administrator's CLI session begins at the User EXEC level. The administrator can access the Privileged EXEC level without entering an enable password, but the administrator cannot access the configuration level:

```
login as: admin
Using keyboard-interactive authentication.
Password: ********
Last login: Fri Mar 26 20:03:39 2010 from 192.168.1.140
[type ? for help]
ACOS> enable
ACOS#
```

The second line grants access to all levels, and the administrator's CLI session begins at the Privileged EXEC level:

```
login as: admin2
Using keyboard-interactive authentication.
Password: ********
Last login: Fri Mar 26 20:03:39 2010 from 192.168.1.140
[type ? for help]
```

NOTE: For more information, see Performing RADIUS Authorization Based on Service-Type.

TACACS+ CLI Authorization

To configure TACACS+ CLI authorization, complete the following tasks:

- Configure the TACACS+ server to authorize or deny the execution of specific commands or command groups.
- Configure the ACOS device to send commands to the TACACS+ server for authorization before executing those commands.

This authorization process does not apply to administrators who log in by using the GUI.

NOTE: For more information, see Authorizing Admin Privileges.

CLI Access Levels

The user can use TACACS+ to authorize an administrator to execute commands at one of the following CLI access levels:

- 15 (admin) – This is the most extensive level of authorization. The commands at all CLI levels, including those used to configure administrative accounts, are sent to TACACS+ for authorization.
- 14 (config) – Commands at all CLI levels, except the commands that are used to configure administrative accounts, are sent to TACACS+ for authorization. The commands that are used to configure administrator accounts are automatically allowed.
- 1 (admin) – This is the most extensive level of authorization and is the same as access level 15. The commands at the Privileged EXEC and User EXEC levels are sent to TACACS+ for authorization, and the commands at other levels are automatically allowed.
- 0 (user EXEC) – This is the equivalent of Read-only privileges. The commands at the User EXEC level are sent to TACACS+ for authorization, and the commands at other levels are automatically allowed.

Access levels 1-15 grant access to the Privileged EXEC level or higher, without challenging the administrator for the enable password. Access level 0 grants access only to the User EXEC level.

NOTE: Privilege level 1 supports Read-write or admin privileges. The highest privilege level is 1 and 15 (Read-write), and the lowest privilege level is 0 (Read-only).

TACACS+ Authorization Debug Options

The user can enable the following TACACS+ debug levels for troubleshooting:

- 0x1 – Common system events such as “trying to connect with TACACS+ servers” and “getting response from TACACS+ servers”. These events are recorded in the syslog.
- 0x2 – Packet fields sent out and received by the Thunder device, not including the length fields. These events are written to the terminal.
- 0x4 – Length fields of the TACACS+ packets will also be displayed on the terminal.
- 0x8 – Information about TACACS+ MD5 encryption will be sent to the syslog.

Performing Authorization Based on Private Partitions

The following topics are covered:

Overview

If the ACOS device is configured with private partitions, the user can specify which partitions a remotely authenticated administrator can access. The user can authorize an administrator to access up to 8 partitions. The partition name that is specified on the RADIUS or TACACS+ server must match the partition name that is specified in the administrator’s account configuration on the ACOS device.

NOTE: For administrators with global access, which means access to the shared partition, do not specify a partition name.

RADIUS Configuration for Partition Access

To authorize an administrator to access only the resources in a specific private partition, use the A10-Admin-Partition option. For example, to authorize an administrator to access only the resources in **partition1**, enter the following statement in the administrator definition:

```
A10-Admin-Partition = "partition1"
```

To authorize an administrator for access to multiple partitions, use the following syntax:

```
A10-Admin-Partition = "partition-name1”
A10-Admin-Partition += " partition-name2”
A10-Admin-Partition += " partition-name3”
A10-Admin-Partition += " partition-name4”
A10-Admin-Partition += " partition-name5”
A10-Admin-Partition += " partition-name6”
A10-Admin-Partition += " partition-name7”
A10-Admin-Partition += " partition-name8”
```

TACACS+ Configuration for Partition Access

To configure TACACS+ to access partitions:

- To authorize an administrator to access only the resources in a specific private partition, use the following AVP:

```
a10-partition=partition-name
```

- To authorize an administrator to access multiple partitions, use the following syntax:

```
a10-partition = partition-name1,partition-name2,
partition-name3,partition-name4,partition-name5,
partition-name6,partition-name7,partition-name8
```

NOTE: To view the TACACS+ server statistics you must run the command on the shared partition. If you execute this command on the L3V partition, the TACACS+ statistics will not be displayed.

Configuring LDAP for Partition Access

Authorization for LDAP is based on a schema file.

NOTE: For more information, see A10 Schema File for OpenLDAP.

Performing RADIUS Authorization Based on Service-Type

The ACOS device supports the RADIUS Service-Type attribute values listed in Table 9:

Table 9 : Supported Radius Service Attribute Value

Attribute Value	Description
`Service-Type=Login`	Allows access to the EXEC level of the CLI and read-only access to the GUI. The EXEC level of the CLI is denoted by the following prompt (as an example): `ACOS>`
`Service-Type=NAS Prompt`	Allows access to the Privileged EXEC level of the CLI and read-only access to the GUI. The Privileged EXEC level of the CLI is denoted by the following prompt (as an example): `ACOS#`
`Service-Type=Administrative`	Allows access to the configuration level of the CLI and read-only access to the GUI. The configuration level of the CLI is denoted by the following prompt (as an example): ACOS `(config)#`

By default, if the Service-Type attribute or the A10 vendor attribute is not used, successfully authenticated administrators are authorized for read-only access. The user can change the default privilege that is authorized by RADIUS from read-only to read-write. To change the default access level authorized by RADIUS, enter the following command at the global configuration level of the CLI:

```
ACOS(config)# radius-server default-privilege-read-write
```

Configuring Accounting

The following topics are covered:

Overview

Accounting keeps track of user activities while the user is logged on. The user can configure the ACOS device to use external RADIUS or TACACS+ for accounting for the following activities:

- Log in/log off activity

  When the user logs in, the accounting process starts, and when the user logs off, the accounting process stops.

- Commands

Command Accounting (TACACS+ only)

Table 10 shows the CLI levels in which the user can use TACACS+ servers to track attempts to execute commands:

Table 10 : Accounting Command

Access Level	Description
15 (admin)	This is the most extensive accounting level. Commands at all CLI levels, including those used to configure administrator accounts, are tracked.
14 (config)	Commands at all CLI levels, **except** the commands that are used to configure administrator accounts, are tracked. The commands that are used to configure administrator accounts are not tracked.
1 (privileged EXEC)	Commands at the Privileged EXEC and User EXEC levels are tracked. Commands at other levels are not tracked.
0 (user EXEC)	Commands at the User EXEC level are tracked. Commands at other levels are not tracked.

NOTE: Command levels 2-13 are equivalent to command level 1 (privileged EXEC).

TACACS+ Accounting Debug Options

The same debug levels that are available for TACACS+ Authorization are also available for TACACS+ Accounting.

NOTE: For more information, see TACACS+ Authorization Debug Options.

Configuring Authentication, Authorization, and Accounting (AAA) for Administrator Access

To configure authentication, authorization, and accounting (AAA):

1. Prepare the AAA servers:
   a. Add administrator accounts (user names and passwords).
   b. Add the ACOS device as a client.

      For the client IP address, specify the ACOS IP address.

   c. For authorization, configure the following settings for the administrator accounts:

      - Specify the user interfaces that the administrator is allowed to access (CLI, GUI, or aXAPI).
      - If you are using TACACS+, specify the CLI commands or command groups that are to be allowed or denied execution.
      - If you are using RADIUS, specify the admin privileges for the CLI and GUI.
      - If you are using LDAP, for more information, see Lightweight Directory Access Protocol.
      - For private partition administrators, specify the partition name.
2. To use RADIUS, TACACS+, or LDAP for authentication:
   a. Add the RADIUS, TACACS+, or LDAP server(s) to the ACOS device.
   b. Add a RADIUS, TACACS+, or LDAP server as an authentication method to use

with the local database.

c. To use more than one AAA protocol, see Authentication and Modes.

3. Configure the authorization:
   a. Add the TACACS+, RADIUS, or LDAP servers for authentication, if necessary.
   b. Specify the access level:
      - If you are using TACACS+, specify the CLI command levels to be authorized.
      - If you are using RADIUS, specify the admin privilege levels for CLI and GUI.
      - If you are using LDAP, see Lightweight Directory Access Protocol.
4. Configure accounting:
   a. Add the TACACS+, RADIUS, or LDAP servers for authorization, if necessary.
   b. Specify whether to track log-on/log-off activity.

      The user can track log ons and log offs, log offs only, or neither.

   c. If you are using TACACS+, specify the command levels to track.

Configuring Remote Authentication

Configure remote authentication by using the GUI or the CLI.

The following topics are covered:

Configuring using CLI

Configure the remote authentication through the CLI.

NOTE: For more information on these configuration and details, see CLI Examples.

Configuring using GUI

Configure the remote authentication through the GUI.

The following topics are covered:

Configuring Global Authentication Settings on the ACOS Device

To configure global authentication settings,

1. Navigate to **System >> Admin >> External Authentication**.

   There are no mandatory fields that need to be completed on the Authentication Settings page; the user can configure your desired global authentication settings as needed.

   NOTE: Refer to the **GUI Online Help** for more information about the fields on this page.

2. Click **Authentication Settings** when you are finished specifying your desired configuration.

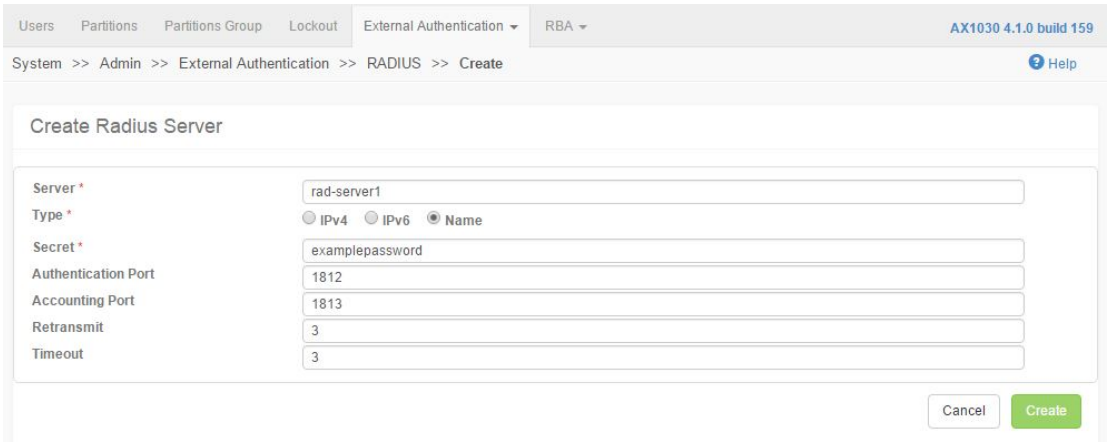
Configuring a RADIUS Server

The user can configure a RADIUS server through the GUI mode.

The following are the steps and modes to configure a RADIUS server:

1. Navigate to **System** >> **Admin** >> **External Authentication** >> **RADIUS**.
2. Click **Create** to designate a RADIUS server and enter settings.
3. Enter the hostname or IP address of the server in the Server field.
4. In the Type field, indicate whether the specified server is an IPv4 or IPv6 address, or a name.

5. In the Secret field, enter the shared secret (password) expected by the server when it receives requests.
6. Complete the other fields on this page as desired; refer to the online help for additional information.
7. RADIUS Server Configuration



8. Click **Create**.

The first RADIUS server configured will act as the primary server and the ACOS device will attempt to use this server first for authentication. The user can configure additional RADIUS servers as needed, if you want to have any backup servers.

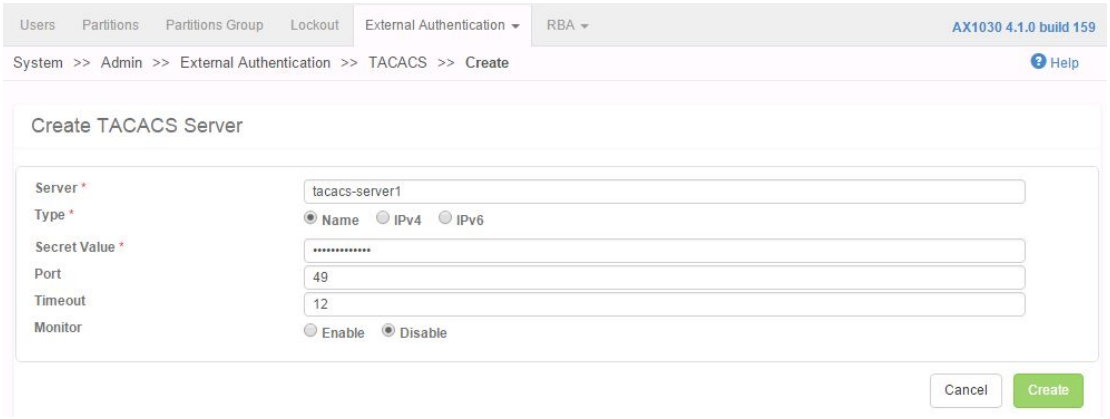
Configuring a TACACS+ Server

The user can configure a TACACS+ server through the GUI mode.

The following are the steps and modes to configure a TACACS+ server:

1. Navigate to **System** >> **Admin** >> **External Authentication** >> **TACACS Host**.
2. Click **Create** to designate a TACACS+ server and enter settings.
3. Enter the hostname or IP address of the server in the Server field.
4. In the Type field, indicate whether the specified server is an IPv4 or IPv6 address, or a name.
5. In the Secret Value field, enter the password expected by the server when it receives requests.

6. Complete the other fields on this page as desired; refer to the online help for additional information.
7. TACACS+ Server Configuration



8. Click **Create**.

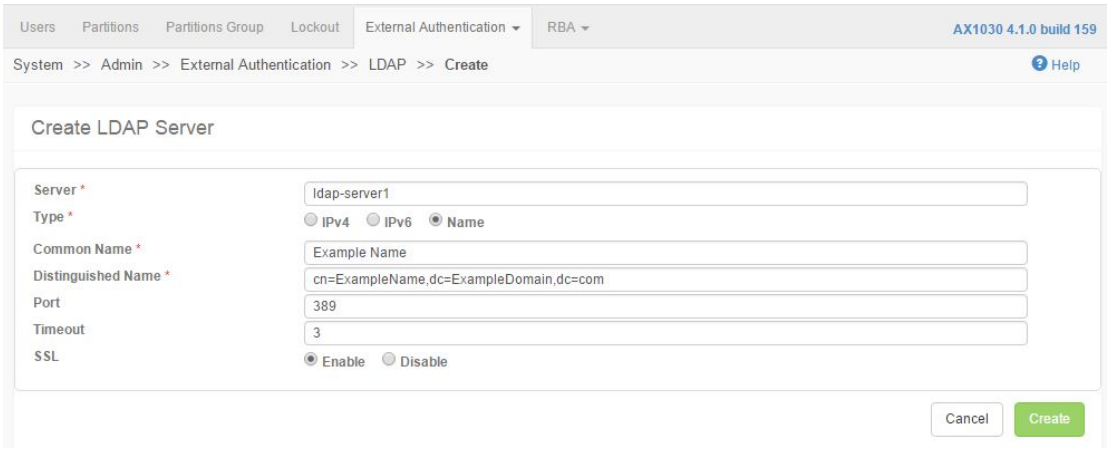
The first TACACS server configured will act as the primary server and the ACOS device will attempt to use this server first for authentication. The user can configure additional TACACS servers as needed, if you want to have any backup servers.

Configuring an LDAP Server

The user can configure an LDAP server through the GUI mode.

The following are the steps and modes to configure an LDAP server:

1. Navigate to **System** >> **Admin** >> **External Authentication** >> **LDAP**.
2. Click **Create** to designate a TACACS+ server and enter settings.
3. Enter the hostname or IP address of the server in the Server field.
4. In the Type field, indicate whether the specified server is an IPv4 or IPv6 address, or a name.
5. Specify the LDAP common name and distinguished name.
6. Complete the other fields on this page as desired; refer to the online help for additional information.
7. Primary and Secondary Information for an LDAP Server



8. Click **Create**.

The first LDAP server configured will act as the primary server and the ACOS device will attempt to use this server first for authentication. The user can configure additional LDAP servers as needed, if you want to have any backup servers.

NOTE: For more information on LDAP servers, refer to Lightweight Directory Access Protocol.

Additional TACACS+ Authentication Options

This section describes about the additional TACACS+ AAA options.

The following topics are covered:

Password Self-Service

ACOS supports TACACS+ TAC_PLUS_AUTHEN_CHPASS (password change) messages. When this option is enabled on the TACACS+ server, the server sends a TACACS+ TAC_PLUS_AUTHEN_CHPASS message in response to an authentication request from the ACOS device. The ACOS device prompts the administrator for the current and new passwords and sends the password change to the TACACS+ server. The ACOS device then grants access to the administrator.

Password self-service is enabled by default and cannot be disabled and is activated only when the TACACS+ server sends a password change message.

NOTE: The current release supports **TAC_PLUS_AUTHEN_CHPASS** messages only for login to the CLI.

Configuring Access to the Privileged EXEC Level

The following topics are covered:

Configuring using GUI

To enable direct access to the Privileged EXEC level of the GUI for TACACS+-authenticated admin:

1. Click **System** > **Admin** > **External Authentication** > Settings.
2. Select the **Login Privilege-Mode** check box.
3. Click **Authentication Settings**.

Configuring using CLI

- The user can enable TACACS+-authenticated administrators to log in at the Privileged EXEC level of the CLI instead of at the User EXEC level.

  NOTE: This option is disabled by default, and the user can enable it on a global basis.

- To enable access to the Privileged EXEC level of the CLI for TACACS+-authenticated administrators, enter the following command at the global configuration level:

```
ACOS(config)# authentication login privilege-mode
```

Configuring using CLI

To enable access to the Privileged EXEC level of the CLI for TACACS+-authenticated administrators, enter the following command at the global configuration level:

```
ACOS(config)# authentication login privilege-mode
```

Configuring TACACS Server with Data Interface Preference

To ensure uninterrupted and reliable TACACS communication, configure the **prefer-data-interface** option while configuring the TACACS server. When this option is configured, TPS performs a route lookup against the TACACS server IP to determine the optimal path, prioritizing the Data plane. Based on the lookup results, TACACS requests are handled as follows:

- If the TACACS server is reachable through the Data plane, the requests are sent through the Data interface. If an error occurs, ACOS falls back to the Management interface for sending requests.
- If the TACACS server is reachable through the Management plane, the requests are sent through the Management interface. However, if an error occurs, ACOS does not fall back to the Data interface.

This helps strengthen the reliability and redundancy of device authentication and access control.

CLI Configuration

To send TACACS requests through an optimal path, with preference to the data plane, configure the following command:

```
ACOS(config)# tacacs-server host <tacacs-server_host_name> secret encrypted <encrypted-secret-string> source loopback 0 prefer-data-interface
```

NOTE:

- The **prefer-data-interface** option is only supported when the source is a loopback IP address.
- Configuring **ip control-apps-use-mgmt** on the management interface does not affect TACACS request.

Configuration Example

The following example demonstrates command usage:

```
ACOS(config)# tacacs-server host 10.65.16.105 secret encrypted 4L/R7ql3fq7iXNlFWhZxhxbJujg7/8VBQxOjJ2ABUgBaKVou6QizCT0Hcu9rjsjo source loopback 0 prefer-data-interface
```

Configuring TACACS+ over TLS Authentication

The following topics are covered:

Overview

ACOS supports TACACS+ over Transport Layer Security (TLS) authentication providing encrypted, certificate-based authentication for secure administrative access. TACACS+ over TLS (1.3) authentication can be configured with or without Certificate Authority (CA) verification, depending on security requirements. This feature is designed to work only with Cisco Identity Services Engine (ISE) version 3.4 Patch 2 or later. Additionally, both IPv4 and IPv6 TACACS+ hosts are supported.

Use TACACS+ over TLS authentication in environments where:

- Device authentication security is paramount.
- Cisco ISE (version 3.4 Patch 2 or later) is deployed as the TACACS+ server.
- Certificate-based trust between client and server is required for AAA communication.

Limitation:

- A server instance can support either “TACACS+” or “TACACS+ over TLS” authentication, but not both. These modes are mutually exclusive.
- TACACS+ over TLS is currently an Internet-Draft, and not yet an official RFC.

TACACS+ over TLS Authentication Process

The following steps describe how ACOS processes TACACS+ over TLS authentication requests:

1. The Thunder device receives a login request.
2. The device attempts each configured “**authentication type**” in sequence.
3. When the method is “**tacplus**”, the device selects a server instance in the order specified by the “`tacacs-server host`” configuration and initiates an authentication request to that server.

4. The request is performed using either **TACACS+** or **TACACS+ over TLS**, depending on the server instance configuration.
   - If the **`over-tls`** option is enabled for the server, TACACS+ over TLS is used.
   - Otherwise, standard TACACS+ is used.
5. If the authentication is successful, the process is completed, and access is granted.
6. If the authentication attempt fails, the device attempts the next configured TACACS+ server, if available.
7. If all TACACS+ servers fail, ACOS switches to the next configured authentication method until no methods remain.

Prerequisites

Before setting up TACACS+ over TLS authentication, make sure that the following requirements are met:

- **Software Requirements**
  - Cisco ISE 3.4 Patch 2 or later (supports TACACS+ over TLS).
- **Certificates and Keys**
  - **`cert`**
    - Specifies the client certificate file used for TACACS+ over TLS authentication.
    - Use the **`import cert <client-certificate-name>`** command to import the client certificate.
  - **`private-key`**
    - Specifies the private key associated with the client certificate.
    - Use the **`import key <client-private-key-name>`** command to import the private key associated with the client certificate.
  - **`custom-ca`**
    - Specifies the CA certificate used to validate the ISE server certificate during authentication.
    - Use the **`import ca-cert <ca-certificate-name>`** command to import the CA certificate.

- **Network Requirements**
  - Ensure network connectivity between the ACOS device and ISE server on TCP port 6049 (default TACACS+ over TLS port).
  - If the Cisco ISE server is located outside the management subnet, configure a route before starting TACACS+ over TLS configuration.

  For more information on setting up CISCO ISE, refer to CISCO documentation.

Configuring TACACS+ over TLS Authentication with CA Verification

This section explains how to configure the TACACS+ over TLS authentication with CA verification. In this configuration, the ACOS device uses the client certificate and private key to authenticate the Cisco ISE server and validates the server certificate using a trusted CA certificate. This setup ensures secure, mutual authentication between ACOS and the Cisco ISE server.

To configure the TACACS+ over TLS authentication with CA verification, perform the following command sequence.

1. Enable TACACS+ over TLS with the certificate, private key, and CA.

```
ACOS(config)# tacacs-server host <ISE-IP> secret <shared-secret> port
6049 over-tls cert <client-cert-name> private-key <client-key-name>
custom-ca <ca-name>
```

   The following example provides TACACS+ over TLS configuration with CA.

```
ACOS(config)#tacacs-server host 10.19.4.210 secret 1 port 6049 over-tls
cert TH_test private-key TH_test custom-ca  X_CA
```

2. Execute the **`show running-config tacacs-server`** command to verify the configuration.

```
ACOS(config)#show running-config tacacs-server
!Section configuration: 183 bytes
!
!
tacacs-server host 10.19.4.210 secret encrypted
RM5z53JTnTWIyXDK19Y4kNuCCLe3h1/iDgyH9Anpt6f/o1gAjjW2T7favOioibXi port
6049 over-tls cert TH_test private-key TH_test custom-ca CA
!
```

Configuring TACACS+ over TLS Authentication without CA Verification

This section explains how to configure TACACS+ over TLS authentication without CA verification.. In this configuration, ACOS uses the client certificate and private key for authentication but does not validate the server certificate because the skip-cert-verification option is enabled.

To configure the TACACS+ over TLS skipping the certificate validation, perform the following command sequence.

1. Enable TACACS+ over TLS with the certificate, private key, and without CA certificate.

```
ACOS(config)# tacacs-server host <ISE-IP> secret <shared-secret> port 6049 over-tls <client-cert-name> private-key <client-key-name> skip-cert-verification
```

The following example provides TACACS+ over TLS configuration without CA .

```
ACOS(config)# tacacs-server host 10.19.4.210 secret 1 port 6049 over-tls cert TH_test private-key TH_test skip-cert-verification
```

2. Execute the **`show running-config tacacs-server`** command to verify the configuration.

```
ACOS(config)#show running-config tacacs-server
!Section configuration: 193 bytes
!
!
tacacs-server host 10.19.4.210 secret encrypted
ygg5iG/P6IJCWOWuYYhzDUZ7qnPi7/U94V6Qr1M8gCl0GYuMstbKmQHPKfCjSSTQ port 6049 over-tls cert TH_test private-key TH_test skip-cert-verification
!
```

TACACS Server Number Increment and the Limitation

The following topics are covered:

Overview

There is a need to increase the limit of the number of the TACACS server from two to three, due to the following necessities.

- The Exchange server has three TACACS servers for their thousands of devices which are functionally deployed and active with high volume or traffic.
- These deployed devices are running into the limit of two servers configured as the maximum number of servers on ACOS.
- The user experience and traffic are enhanced once the limit is increased from the current limit of two TACACS servers to three servers or as an optional number that user can configure.

Known Issues or Limitations

Although the increment in the limit of the number of the TACACS server from two to three is necessary, it has the following known issues or limitations.

- The TACACS monitor needs to be configured to use the most recently used server as the primary server.
- The hard limit on the number of the TACACS server is increased to three servers and it starts behaving in the following modes:
  - **Active:** The first configured server as the Active Server.
  - **Standby:** The other remaining two servers as the Standby Servers.
- In the eventuality of the request going to the first server, and fails, then the request is sent to the other two servers, as well to check, whether if it passes the other servers or not.

Requirements

To configure the three TACACS servers in running the configuration, the user must ensure the following:

- The first assigned or dedicated server must be **Active** and the other two servers must be on the **Standby** Mode.
- The authorization request of any given session must go to the server, which authenticates the session.

Scenario

The scenario of this feature is as the following:

- The first server is considered as the **Active** Server by *Default*.
- The second and the third servers are considered as the **Standby** Servers.
- If the TACACS Server monitor is configured, then;
  - The user uses the logic of requests which is sent to the most recently used server.
  - If not, then the active server gets the requests by *Default*.

GUI

For this, there are no GUI changes required.

CLI

For this, there are no new CLI changes required or introduced.

aXAPI

For this, there are no changes in aXAPI regarding TACACS.

Important

In this scenario, the following are the important points to consider:

- The new CLI or aXAPI changes or corrections must not work in L3V partitions.
- The changes are only applicable in the Shared Partition.

- All the new CLI or aXAPI changes must be device independent.

CLI Examples

The following topics are covered:

RADIUS Authentication

The following commands configure a pair of RADIUS servers for remote authentication and configure the ACOS device to use these servers before using the local database. Since the RADIUS server *10.10.10.12* is added first, this server is used as the primary server. Server *10.10.10.13* is used only if the primary server is unavailable.

The following text is an example of configuring RADIUS authentication:

```
ACOS(config)# radius-server host 10.10.10.12 secret radp1
ACOS(config)# radius-server host 10.10.10.13 secret radp2
ACOS(config)# authentication type radius local
```

TACACS+ Authorization

The following commands configure the ACOS device to use TACACS+ server *10.10.10.13* to authorize commands at all CLI levels. In this example, the **none** option is not used. As a result, if TACACS+ authorization cannot be performed, for example, due to server unavailability, the command is denied.

The following text is an example of configuring TACACS+ authorization:

```
ACOS(config)# tacacs-server host 10.10.10.13 secret SharedSecret
ACOS(config)# authorization commands 15 method tacplus
```

TACACS+ Accounting

The following commands configure the ACOS device to use the same TACACS+ server for the accounting of log on, log off, and all command activity:

```
ACOS(config)# accounting exec start-stop tacplus
ACOS(config)# accounting commands 15 stop-only tacplus
```

RADIUS Server Setup

This example shows the ACOS commands that the user can enter to complete the following tasks:

- Configure an ACOS device to use a RADIUS server
- Display the changes that the user can make on the RADIUS server

The RADIUS server in this example is FreeRADIUS, the IP address is *192.168.1.157*, and the shared secret is *a10rad*.

To implement this solution:

1. On the ACOS device, to add the RADIUS server and enable RADIUS authentication, enter run the following commands:

```
ACOS(config)# radius-server host 192.168.1.157 secret a10rad
ACOS(config)# authentication type local radius
```

2. Complete the following steps on the FreeRADIUS server:
   a. In the `/usr/local/etc/raddb/clients.conf` file, to add the ACOS device as a client, enter the following commands:

```
client 192.168.1.0/24 {
   secret = a10rad
   shortname = private-network-1
}
```

NOTE: In this example, the ACOS device's subnet is added as the client.

   b. To add the `/usr/local/share/freeradius/dictionary.a10networks` RADIUS

dictionary file for vendor *a10networks* (**22610** is the vendor code) and add the file to the RADIUS dictionary, enter the following commands:

NOTE: After authenticating an administrator, the RADIUS server must return the A10-Admin-Privilege attribute, with one of the values shown in the following example.

```
# A10-Networks dictionary
# Created by Software Tools of A10 Networks.
#
VENDOR A10-Networks 22610
BEGIN-VENDOR A10-Networks
ATTRIBUTE A10-App-Name    1    string
ATTRIBUTE A10-Admin-Privilege    2    integer
ATTRIBUTE A10-Admin-Partition    3    string
ATTRIBUTE A10-Admin-Access-Type    4    string
ATTRIBUTE A10-Admin-Role        5    string
VALUE     A10-Admin-Privilege    Read-only-Admin    1
VALUE     A10-Admin-Privilege    Read-write-Admin    2
VALUE     A10-Admin-Privilege    Partition-SlbService-Operator 11
VALUE     A10-Admin-Privilege    Partition-Read_write    8
VALUE     A10-Admin-Privilege    Partition-Read-Only    12
END-VENDOR A10-Networks
```

3. In the `/usr/local/share/freeradius/dictionary` directory, to add the file to the RADIUS dictionary, enter the following command:

```
$INCLUDE dictionary.a10networks  # new added for a10networks
```

4. In the `/usr/local/etc/raddb/users` file, to add each ACOS admin as a user, enter the following commands:

NOTE: The following text contains examples of ACOS administrator definitions in a RADIUS users file on the RADIUS server.

```
# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
# this is a read-write user
rw Cleartext-Password := "111111"
     A10-Admin-Privilege = Read-write-Admin,
# this is a read-only user
```

```
ro Cleartext-Password := "111111"
     A10-Admin-Privilege = Read-only-Admin,
# this is a partition read-only
pro Cleartext-Password := "111111"
     A10-Admin-Privilege = Partition-Read-Only,
     A10-Admin-Partition = "aa"
# this is a partition enable-disable
ped Cleartext-Password := "111111"
     A10-Admin-Privilege = Partition-SlbService-Operator,
     A10-Admin-Partition = "aa"
# this is partition read-write, has role PartitionReadWrite, only login
from web.
prw_r_w Cleartext-Password := "111111"
     A10-Admin-Privilege = Partition-Read-Write,
     A10-Admin-Partition = "aa",
     A10-Admin-Role = "PartitionReadWrite",
     A10-admin-Access-type = "web"
```

Windows IAS Setup for RADIUS

This section describes how to configure Windows Server 2003 Internet Authentication Service (IAS) with ACOS RADIUS authentication. These steps assume that IAS and Active Directory (AD) are already installed on the Windows 2003 server.

The following topics are covered:

Configuring Windows IAS for ACOS RADIUS Authentication

To configure Windows IAS for ACOS RADIUS authentication:

1. On the IAS server, create the following access groups (see Configuring Access Groups):
   - ACOS-Admin-Read-Only
   - ACOS-Admin-Read-Write
2. On the IAS server, configure a RADIUS client for the ACOS device (Configuring RADIUS Client for the ACOS Device).
3. On the IAS server, configure the following remote access policies (Configuring Remote Access Policies):
   - ACOS-Admin-Read-Only-Policy
   - ACOS-Admin-Read-Write-Policy).
4. On the IAS server, add AD users to appropriate ACOS device access groups (Adding Active Directory Users to ACOS Access Groups).
5. Register the IAS server in AD (Registering the IAS Server in Active Directory).
6. Configure RADIUS on the ACOS device (Configuring RADIUS on the ACOS Device).
7. Test the configuration by attempting to log onto the ACOS device with AD users added in (Verifying the Configuration).

The following sections provide detailed steps for each of these tasks.

Configuring Access Groups

The following topics are covered:

Overview

To configure access groups, select Select Start > All programs > Administrator tools > Active directory user and computers.

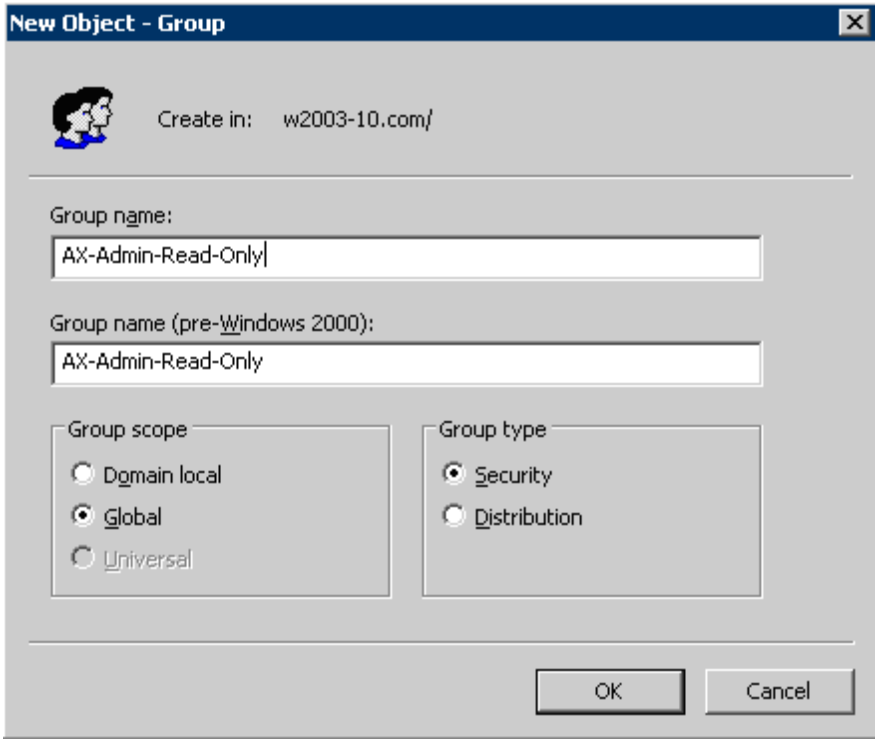
If Active Directory Is Not Installed

If AD is not installed on the IAS server, the user can use the following steps to add the users and groups. However, the rest of this section assumes that AD will be used.

Open the Computer Management tool by selecting **Start > Programs > Administrative Tools > Computer Management**.

1. Open the System Tools and Local Users and Groups items, if they are not already open.
2. Right click on Group and select New Group.
3. Enter the following information for the first group:
   - Group Name – AX-Admin-Read-Only
   - Group Description – Read-Only Access to ACOS devices
   - Members – Add the members using the Add button.

   Figure 19 : Add Member



4. Click Create.

- Enter the following information for the second group:
- Group Name – AX-Admin-Read-Write
- Group Description – Read-Write to ACOS devices
- Members – Add members as desired using the Add button

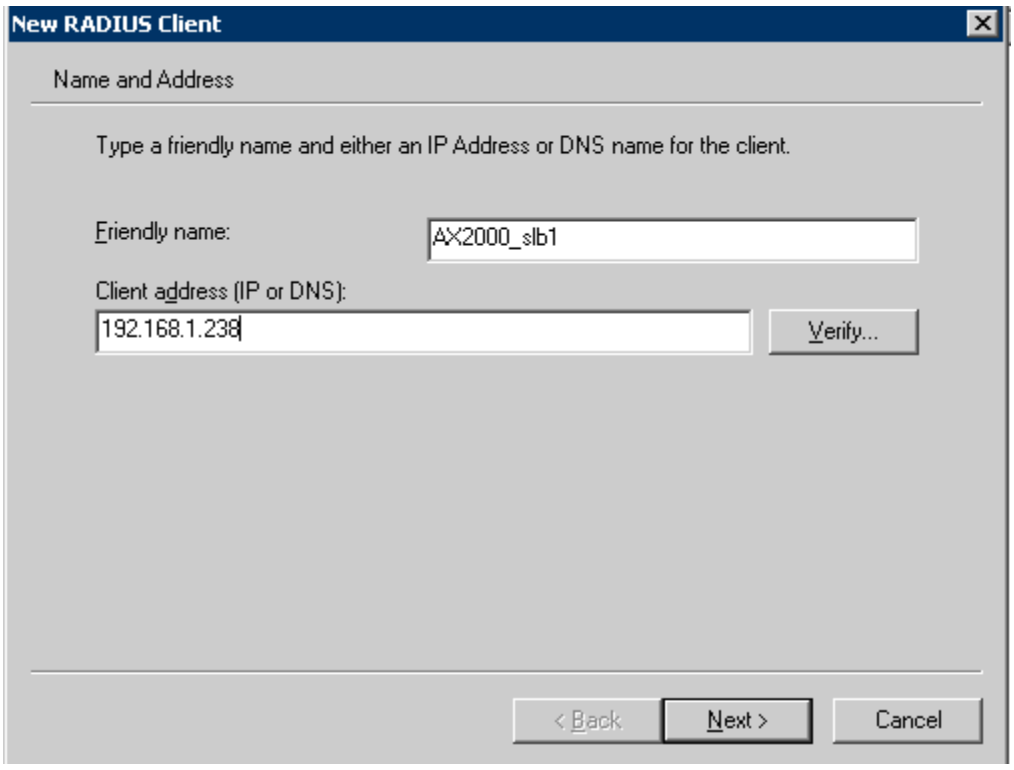
5. Click Create.
6. Click Close.

Configuring RADIUS Client for the ACOS Device

The user can configure the RADIUS client for the ACOS device through the GUI mode. The following are the steps and modes to change the configuration settings for this interface:

1. Open Internet Authentication Service, by selecting **Start > Programs > Administrative Tools > Internet Authentication Service**.
2. Right-click on Client and select New Client.
3. Enter the following information in the Add Client dialog box:
   - Friendly name – Useful name for the ACOS device; for example, ACOS2000_slb1
   - Protocol – RADIUS

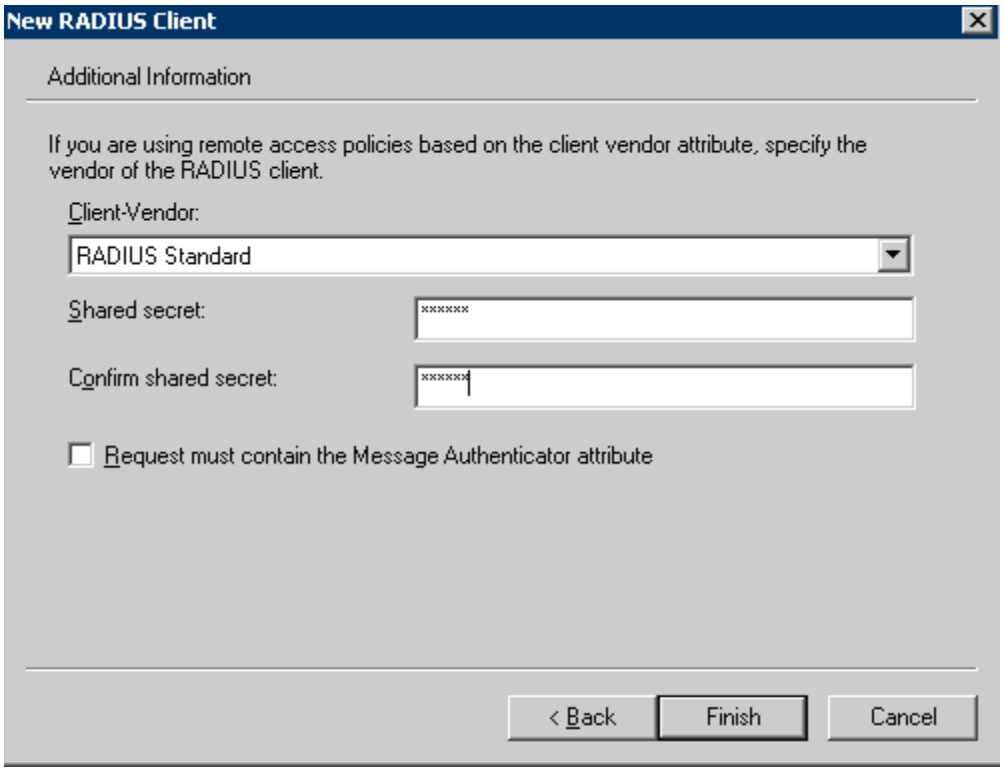
Figure 20 : Radius



NOTE: 192.168.1.238 is the IP address of the ACOS device that will use the IAS server for external RADIUS authentication.

4. Click Next.
5. Enter the following information in the Add RADIUS Client dialog box:
   - Client address – IP address or domain name for the client (ACOS device)
   - Client-Vendor – RADIUS Standard
   - Shared secret – Secret to be shared between IAS and ACOS. You also will need to enter this in the RADIUS configuration on the ACOS device.
   - Confirm shared secret – Same as above

NOTE: Do not select “Request must contain the Message Authenticator attribute”. ACOS RADIUS authentication does not support this option.



6. Click Next.

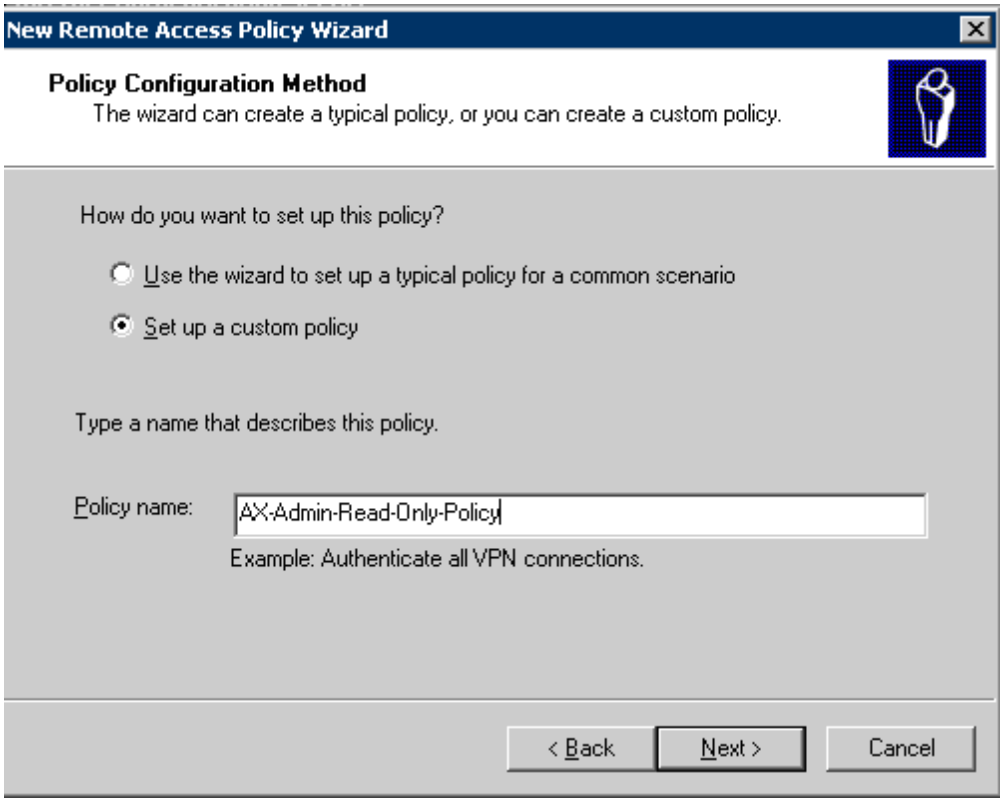
Configuring Remote Access Policies

The user can configure the remote access policies through the GUI mode. The following are the steps and modes to configure the remote access policies:

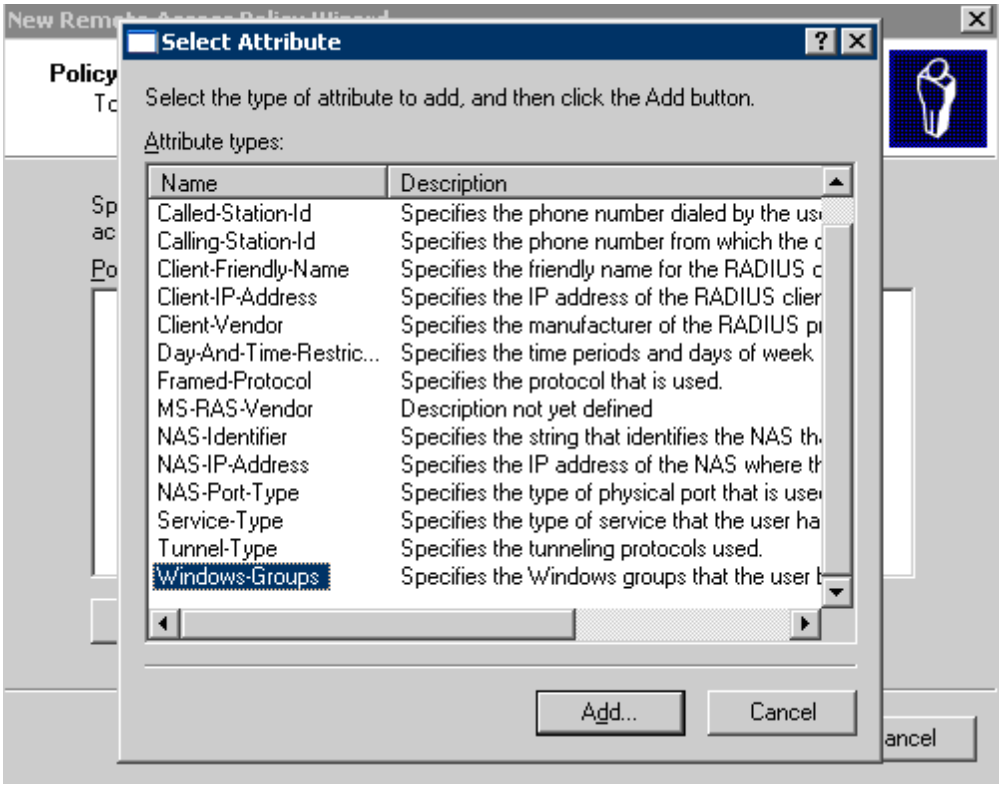
1. Open the Internet Authentication Service, if not already open.
2. To create the first remote access policy, right-click on Remote Access Policies, select New Remote Access Policy, and enter the following information:

   Policy Friendly name – AX-Admin-Read-Only-Policy

Figure 21 : Admin Read Only Policy

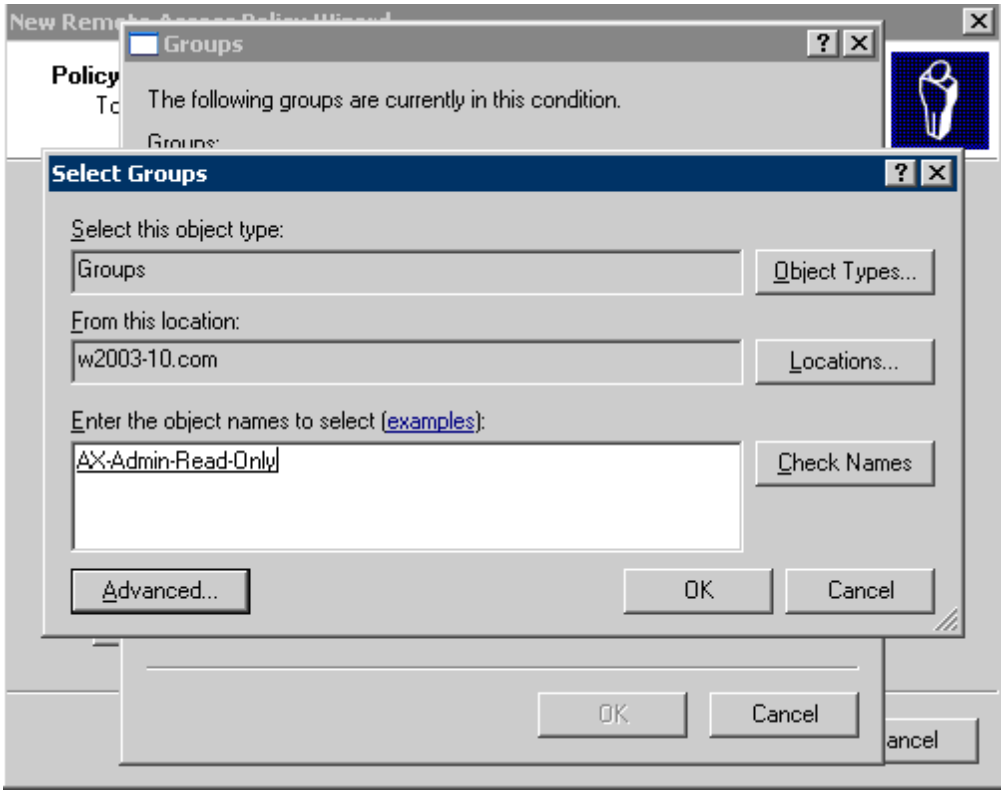


3. Click **Next**.
4. In the Add Remote Access Policy dialog box, click **Add**.
5. In the Select Attribute dialog box, double-click **Client Friendly Name**.
6. In the Client-Friendly-Name dialog box, enter the friendly name used to define the ACOS device (for example, AX-Admin-Read-Only-Policy) and click **OK**.
7. In the same Add Remote Access Policy dialog box as before, click **Add** again.
8. In the Select Attribute dialog box, double-click **Windows-Groups**.



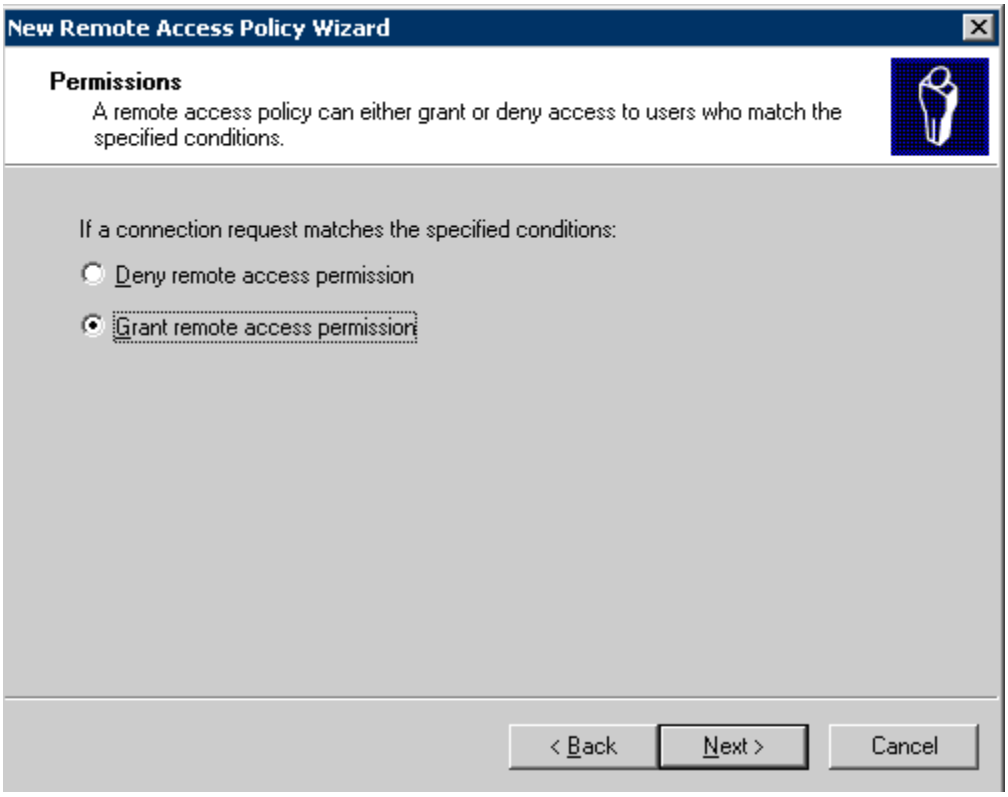
9. In the Groups dialog box, click Add, then double-click **AX-Admin-Read-Only** group, Click **OK** to add the group, then click **OK** once more to confirm the groups.

Figure 22 : Group Dialog Box



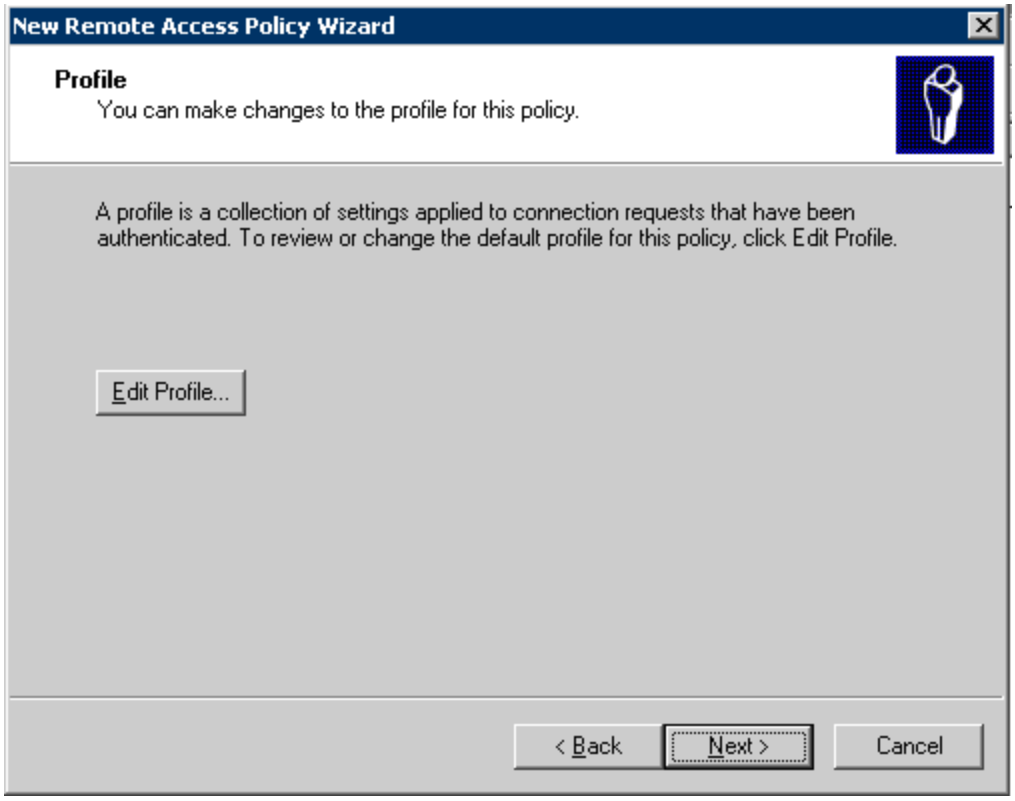
10. In the same Add Remote Access Policy dialog box as before, click **Next**.
11. Select Grant remote access permission, and click **Next**.

Figure 23 : Grant remote access



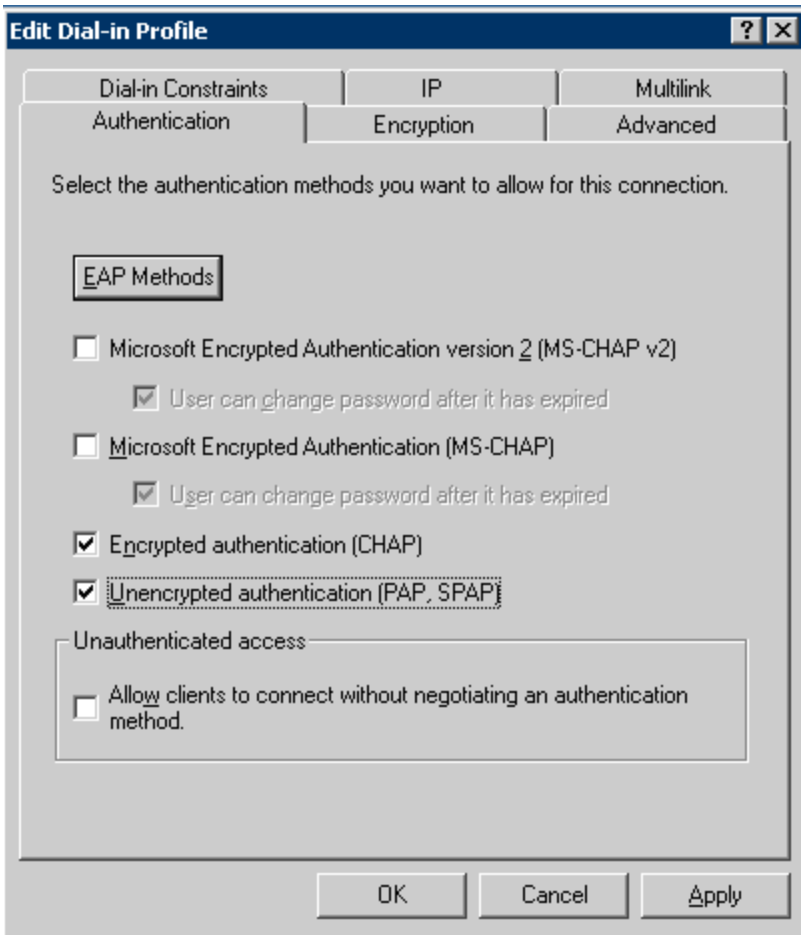
12. Click **Edit Profile**.

Figure 24 : Edit Profile



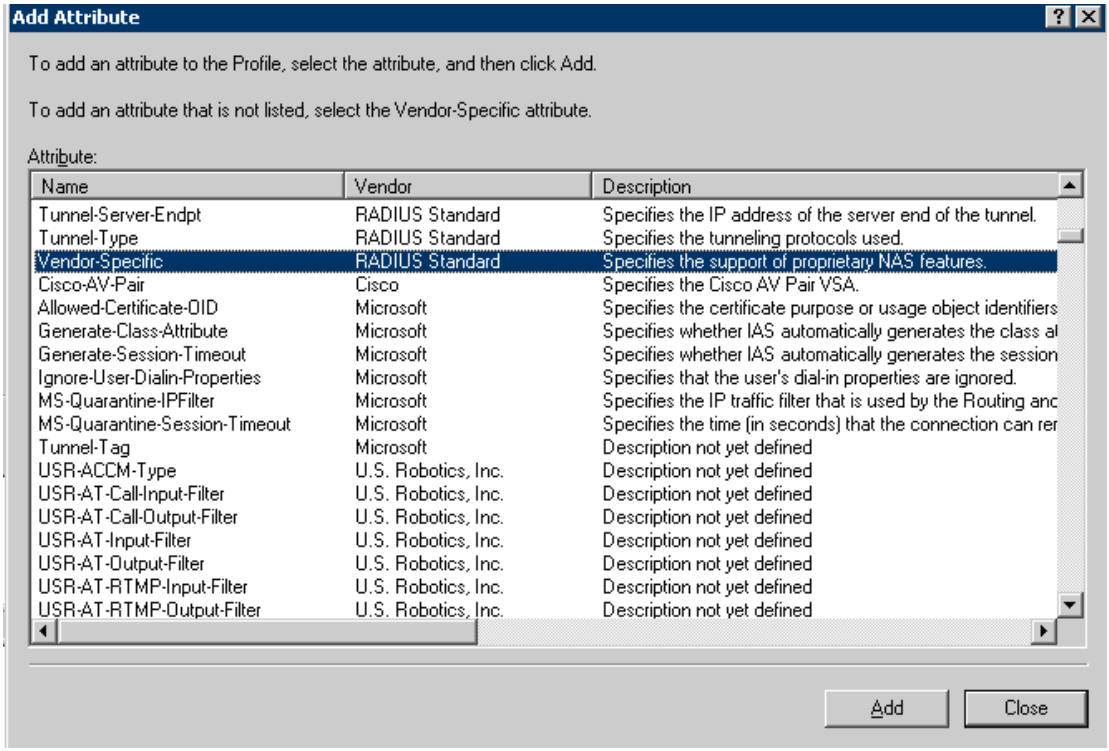
13. In the Edit Dial-in Profile dialog box, select the Authentication tab. Select the type of authentication you are using: CHAP and PAP.

Figure 25 : Edit Dial-in-Profile



14. Select the Advanced tab, and click **Add**.
15. In the RADIUS attributes list, find and double-click the line beginning with **Vendor-Specific**

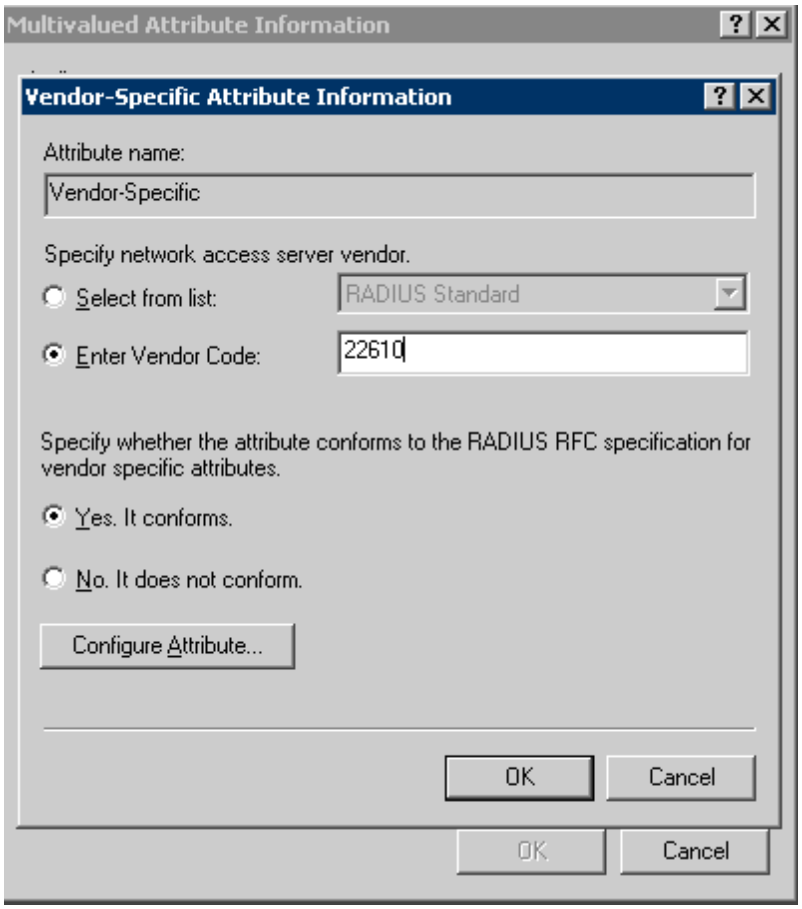
Figure 26 : Radius Attributes



16. In the Multivalued Attribute Information dialog box, click **Add** and enter the following:

    - Enter vendor code – 22610 (for A10 Networks)
    - Conforms to RADIUS RFC – Yes

Figure 27 : Vendor Specific Attribute Information

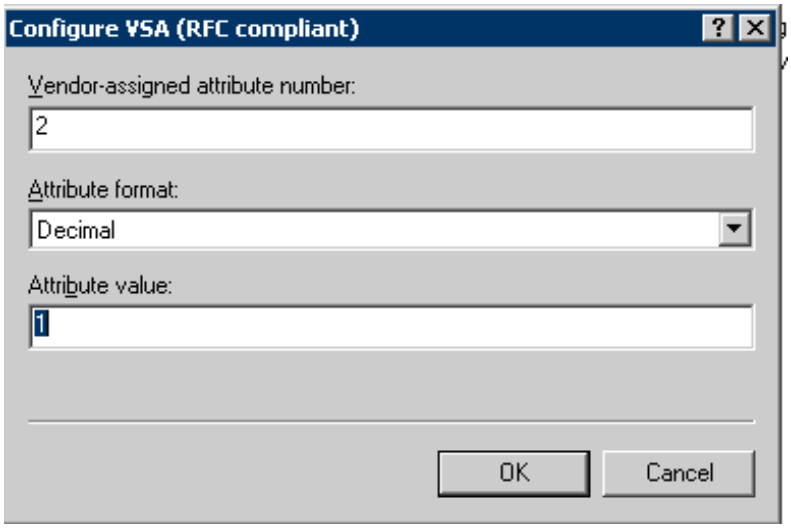


17. Click **Configure Attribute**, and enter the following information:

    - Vendor-assigned attribute number – 2
    - Attribute format – Decimal
    - Attribute value – 1

    NOTE: Attribute value 1 is read-only. Attribute value 2 is read-write.

Figure 28 : Attribute Value



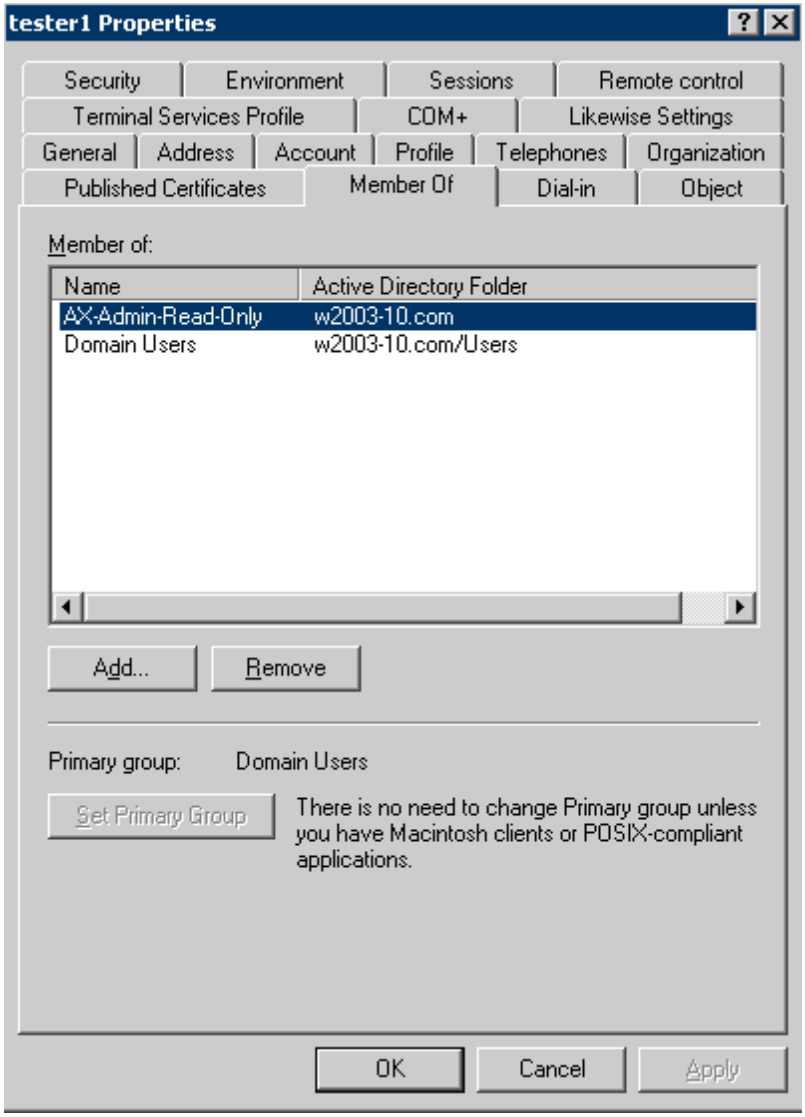
18. Click **OK** for the Configure VSA, Vendor-Specific Attribute Information, and Multivalued Attribute Information dialog boxes.
19. Click **Close** in the Add Attributes dialog box.
20. Click **OK** in the Edit Dial-In Profile dialog box. Optionally, read the suggested help by clicking **OK**.
21. Click **Finish** in the Add Remote Access Policy dialog box.
22. To create the second Remote Access Policy, repeat the above steps with the following changes:

- Policy Friendly name – AX-Admin-Read-Write-Policy
- Group to add – AX-Admin-Read-Write
- Attribute value – 2

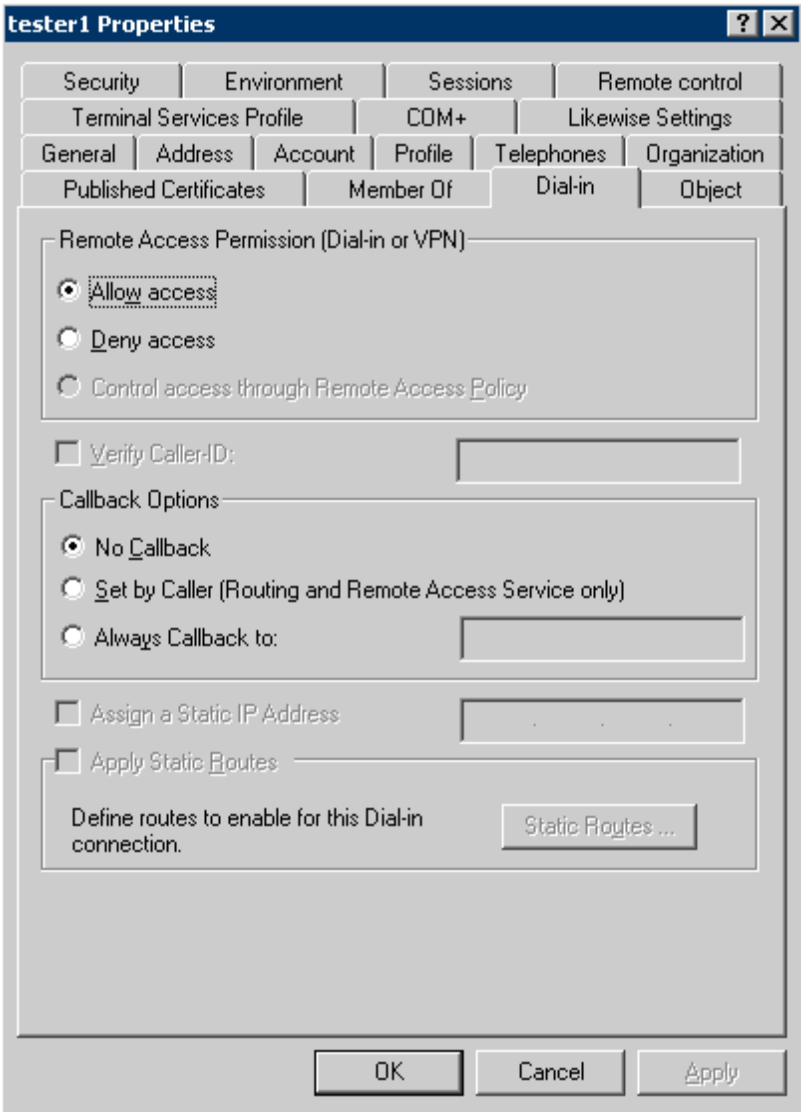
Adding Active Directory Users to ACOS Access Groups

The user can add the Active Directory users to the ACOS Access Groups through the GUI mode. The following are the steps and modes to add Active Directory users to the ACOS access groups:

1. In the Active Directory management console, add the ACOS access group to the user, tester1:



2. Make sure Remote Access Permission is enabled:



Registering the IAS Server in Active Directory

The user can register the IAS server in Active Directory through the GUI mode. The following are the steps and modes to complete this procedure:

The IAS RADIUS server must be registered with AD. Otherwise, RADIUS uses compatibility mode instead of AD to authenticate users.

1. Open the IAS main window.
2. Click **Action** on the menu bar, and click "**register server on active directory**".

Configuring RADIUS on the ACOS Device

To add the RADIUS server (IAS server) to the ACOS device, enter the following commands:

```
ACOS(config)# radius-server host 192.168.230.10 secret shared-secret
ACOS(config)# authentication type local radius
```

NOTE: Ensure that the shared secret is the same as the value that you specified for the RADIUS client that you configured for the ACOS server on the IAS server.

In this example, *192.168.230.10* is the IP address of w2003-10.com, and *shared-secret* is the secret that you entered in the Configuring RADIUS Client for the ACOS Devicein Configuring RADIUS Client for the ACOS Device.

Verifying the Configuration

To verify the configuration:

1. Log in to the ACOS CLI.
2. At the command prompt, enter the username in the following format:
   - **user-name@AD-domain-name**
   - For example, you might enter **tester1@w2003-10.com**.
3. Enter the password.
4. Press **Enter**.

Windows 2022 NPS Setup for RADIUS

This section describes how to configure Windows Server 2022 Network Policy Server (NPS) with ACOS RADIUS authentication. These steps assume that NPS and Active

Directory (AD) are already installed on the Windows 2022 server.

The following topics are covered:

Configuration Workflow

To configure Windows NPS for ACOS RADIUS authentication:

1. On the NPS server, create the following user groups (see Configuring Access Groups):
   - ACOS-Admin-Read-Only
   - ACOS-Admin-Read-Write
2. On the NPS server, configure a RADIUS client for the ACOS device (Configuring RADIUS Client for the ACOS Device).
3. On the NPS server, configure the following Network Policies (Configuring Network Policies):
   - ACOS-Admin-Read-Only-Policy
   - ACOS-Admin-Read-Write-Policy).
4. Configure RADIUS on the ACOS device (Configuring RADIUS on the ACOS Device).
5. Test the configuration by attempting to log onto the ACOS device with AD users added in (Verifying the Configuration).

Configuring Access Groups

To configure access groups, perform the following steps:

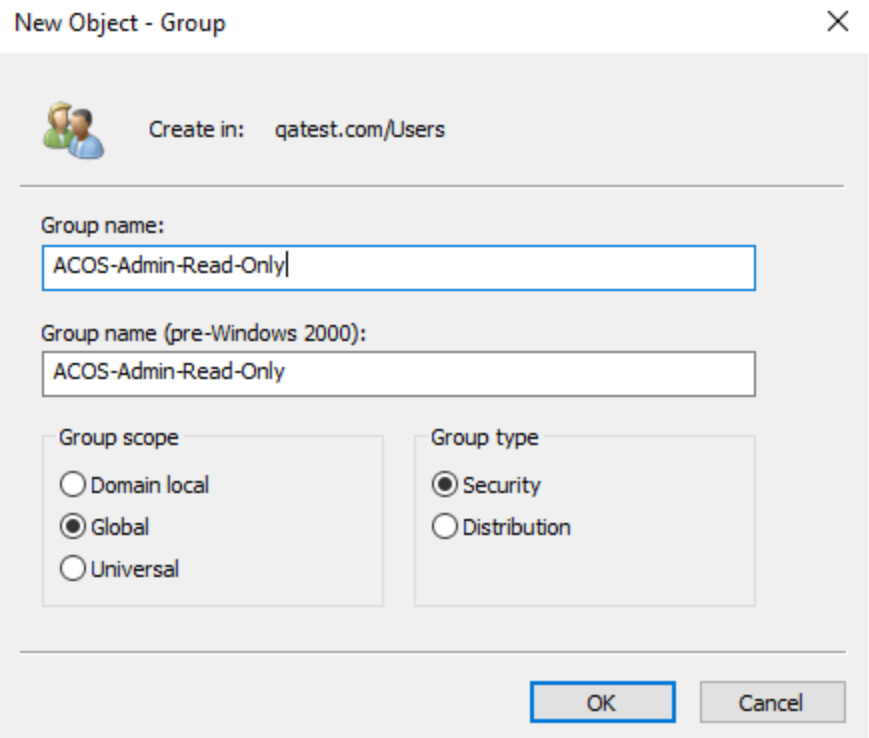
1. Select **Select Start > All programs > Administrator tools > Active directory user and computers**.

   If Active Directory Is Not Installed, you can use the following steps to add the users and groups. However, the rest of this section assumes that AD will be used.

2. Open the Computer Management tool by selecting **Start > Programs > Administrative Tools > Computer Management**.
3. Open the System Tools and Local Users and Groups items, if they are not already open.
4. Right-click **Group** and select **New Group**.
5. Enter the following information for the first group:

   - Group Name – ACOS-Admin-Read-Only.
   - Group Description – Read-Only Access to ACOS devices.
   - Members – Add the members using the Add button.

Figure 29 : Add Group



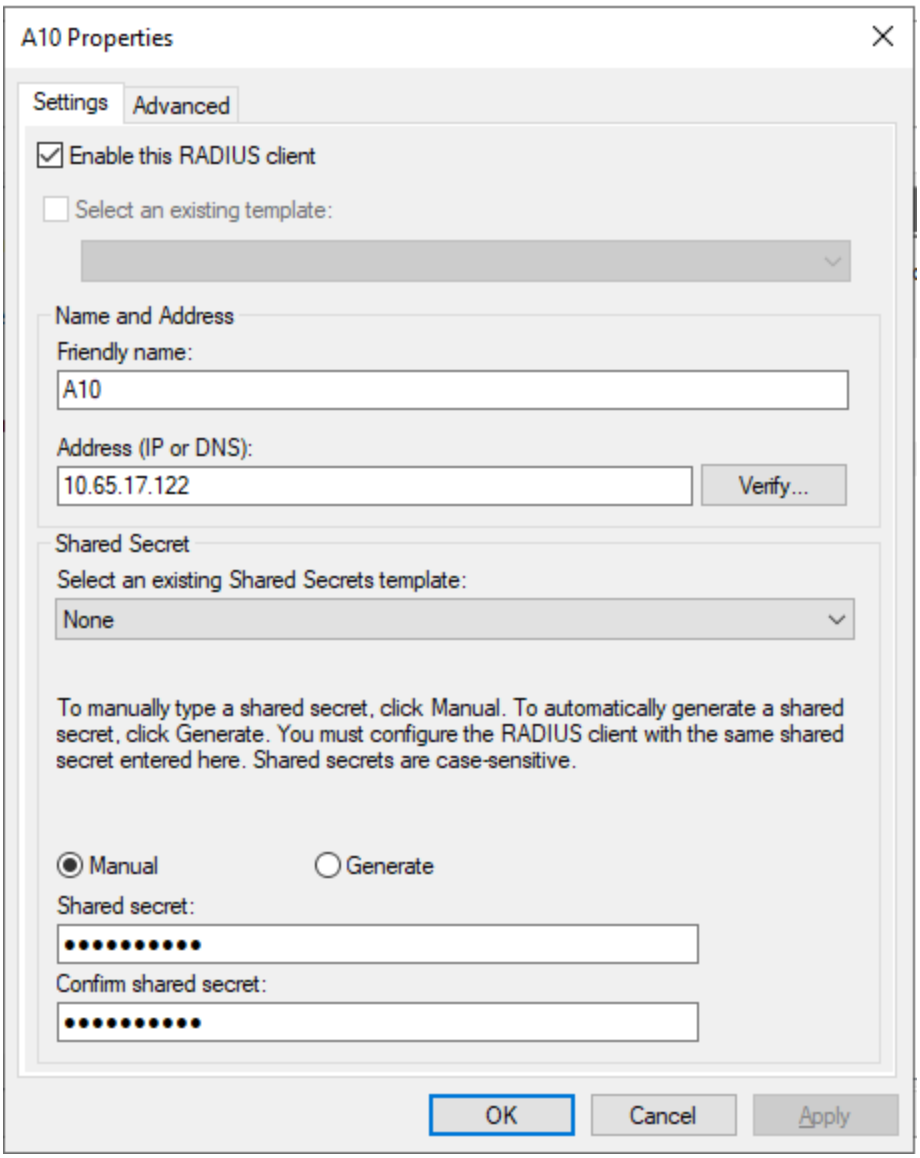
6. Click **Create**.
7. Enter the following information for the second group:
   - Group Name – ACOS-Admin-Read-Write.
   - Group Description – Read-Write to ACOS devices.
   - Members – Add members as desired using the **Add** button.
8. Click **Create**.
9. Click **Close**.

Configuring RADIUS Client for the ACOS Device

The user can configure the RADIUS client for the ACOS device through the GUI mode. The following are the steps and modes to change the configuration settings for this interface:

1. Open Network Policy Server, by selecting **Start > Programs > Administrative Tools > Network Policy Server**.
2. Right-click **Radius Client** and select **New Client**.
3. Enter the following information in the **Add Client** dialog box:
   - Friendly name – Useful name for the ACOS device; for example, A10.
   - Address – IP address or domain name for the client (ACOS device).
   - Shared secret – Secret to be shared between NPS and ACOS. You also need to enter this in the RADIUS configuration on the ACOS device.
   - Confirm shared secret – Same as above.

Figure 30 : A10 Properties



NOTE: 10.65.17.122 is the IP address of the ACOS device that will use the NPS server for external RADIUS authentication.

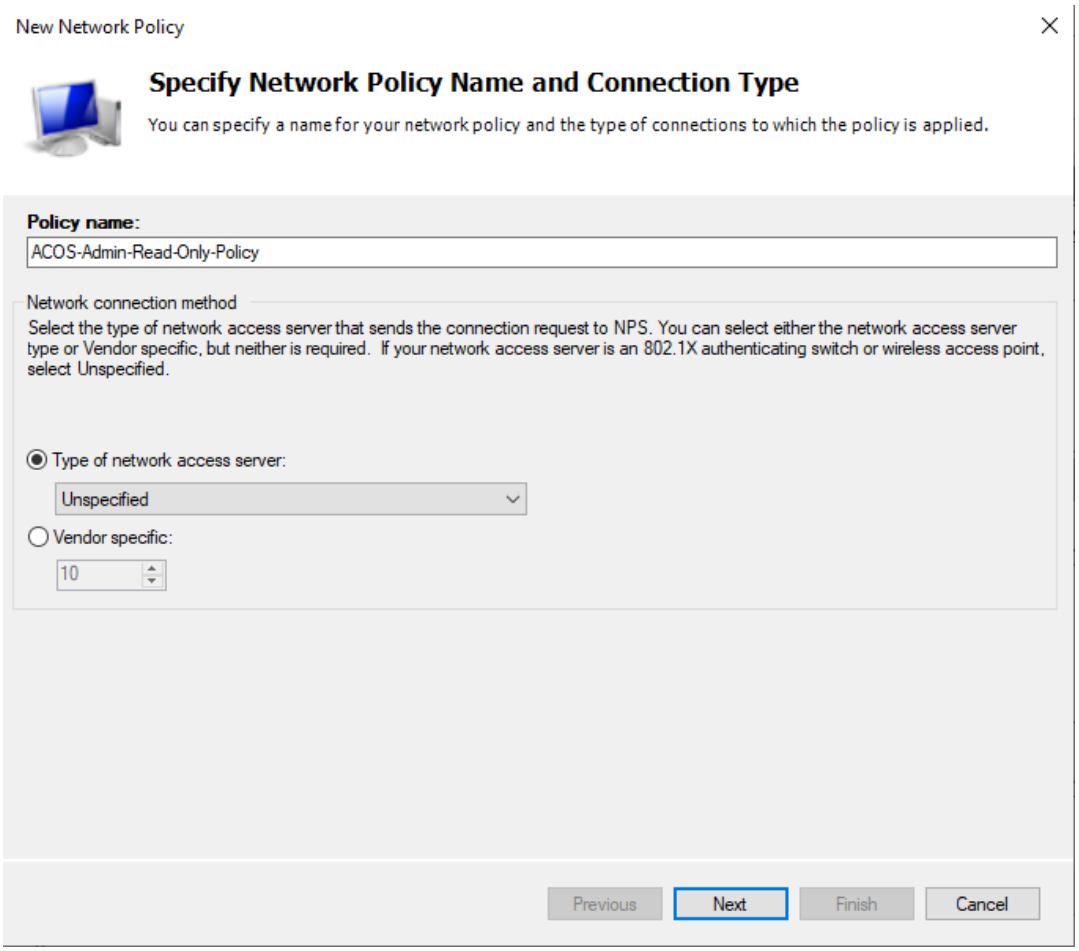
4. Click **OK**.

Configuring Network Policies

The user can configure the network policies through the GUI mode. The following are the steps and modes to configure the remote access policies:

1. Open the Network Policy Server, if not already open.
2. To create the first remote access policy, right-click on network policies, select **New**.
3. Enter the following information:
   - Policy name – ACOS-Admin-Read-Only-Policy.

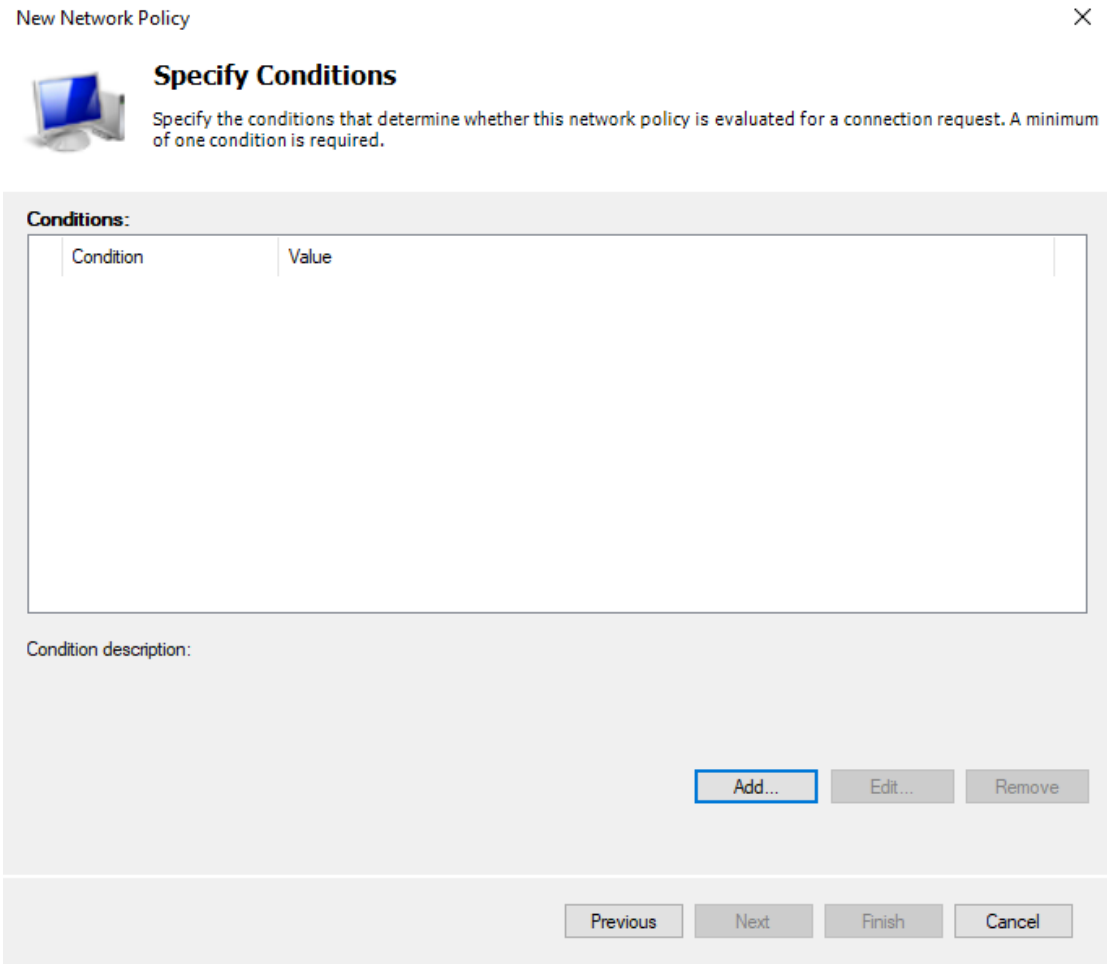
   Figure 31 : Admin Read Only Policy



4. Click **Next**.

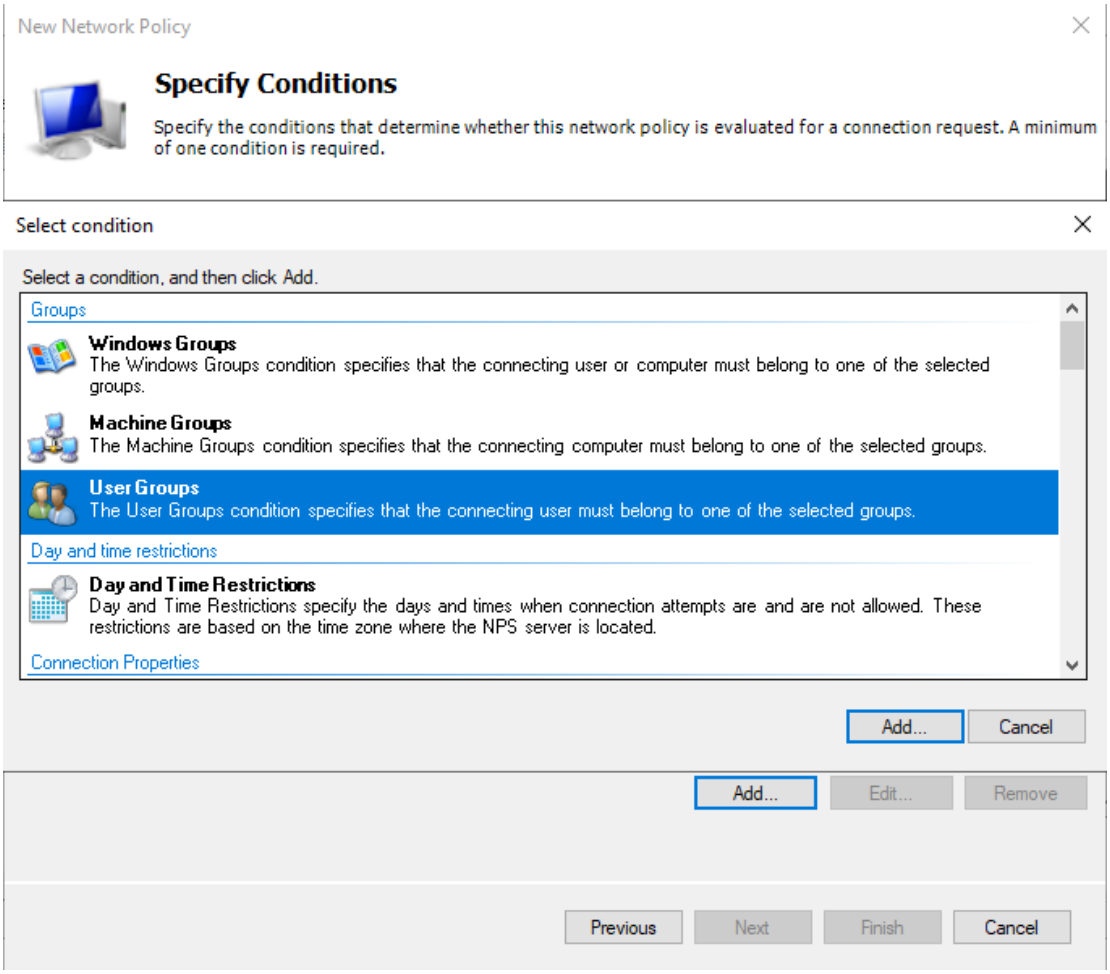
5. In the **Specify Conditions** dialog box, click **Add**.

Figure 32 : Specify Conditions



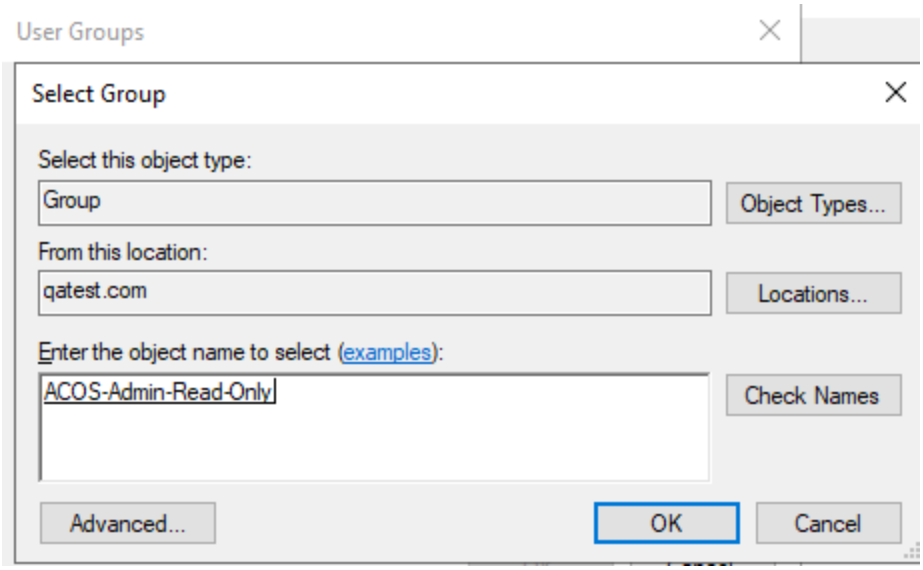
6. In the **Condition** dialog box, select **User Groups**.

Figure 33 : Select Condition



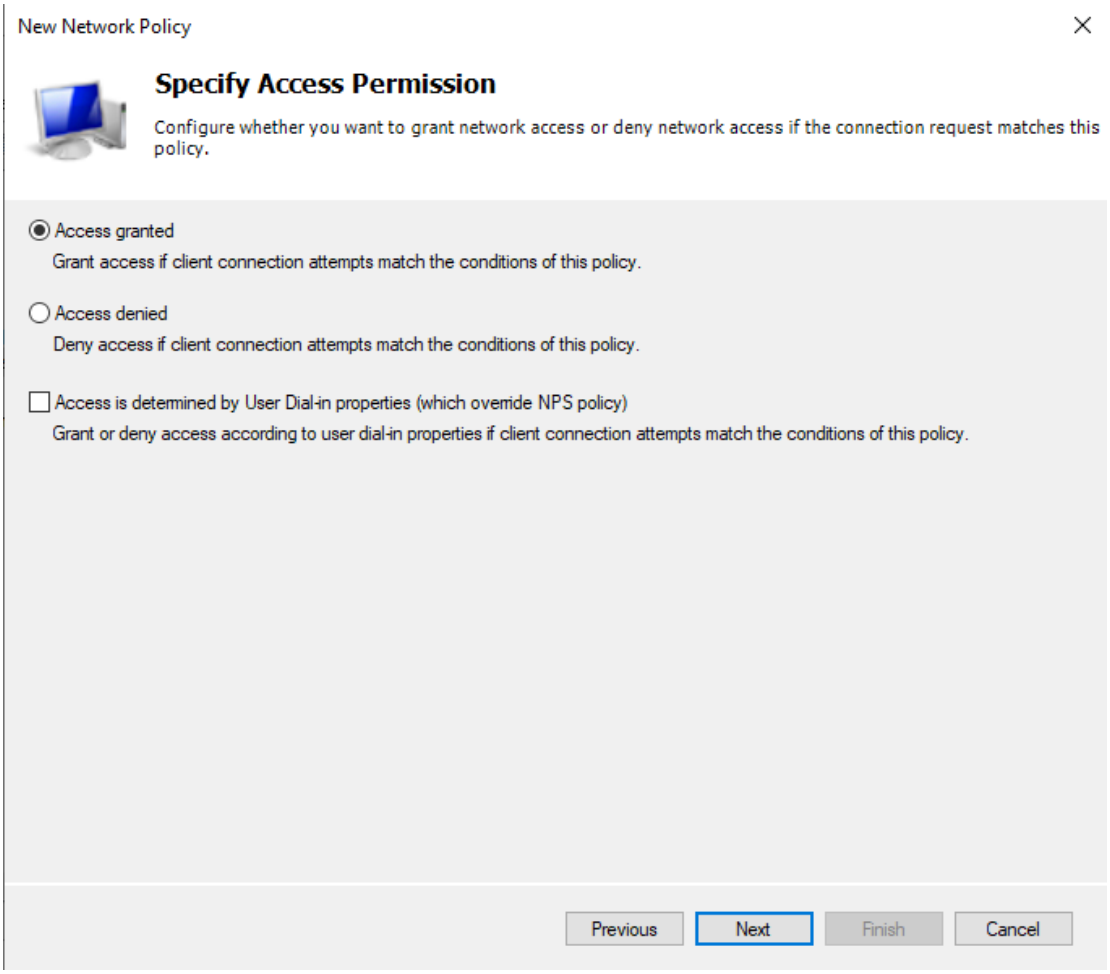
6. Click **Add**.
7. Input name ACOS-Admin-Read-Only, click **Check Names**, click **OK**.

Figure 34 : User Groups



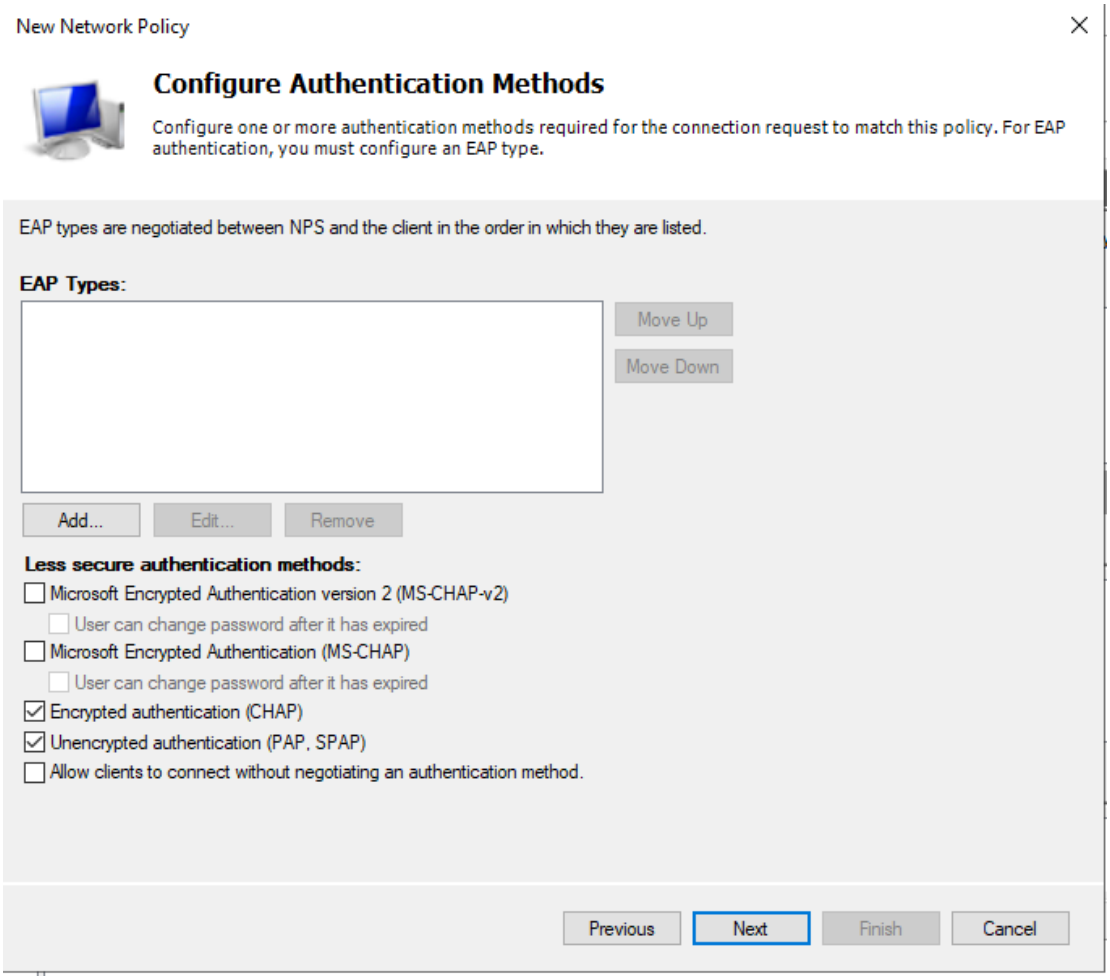
8. Click **Next**, select **Access granted**, click **Next**.

Figure 35 : Specify Access Permission



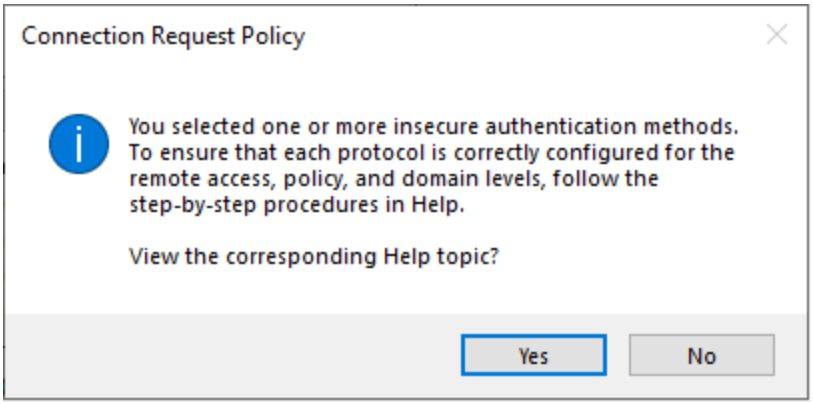
9. Select **Authentication Methods** as **CHAP** and **PAP**, click **Next**.

Figure 36 : Configure Authentication Methods



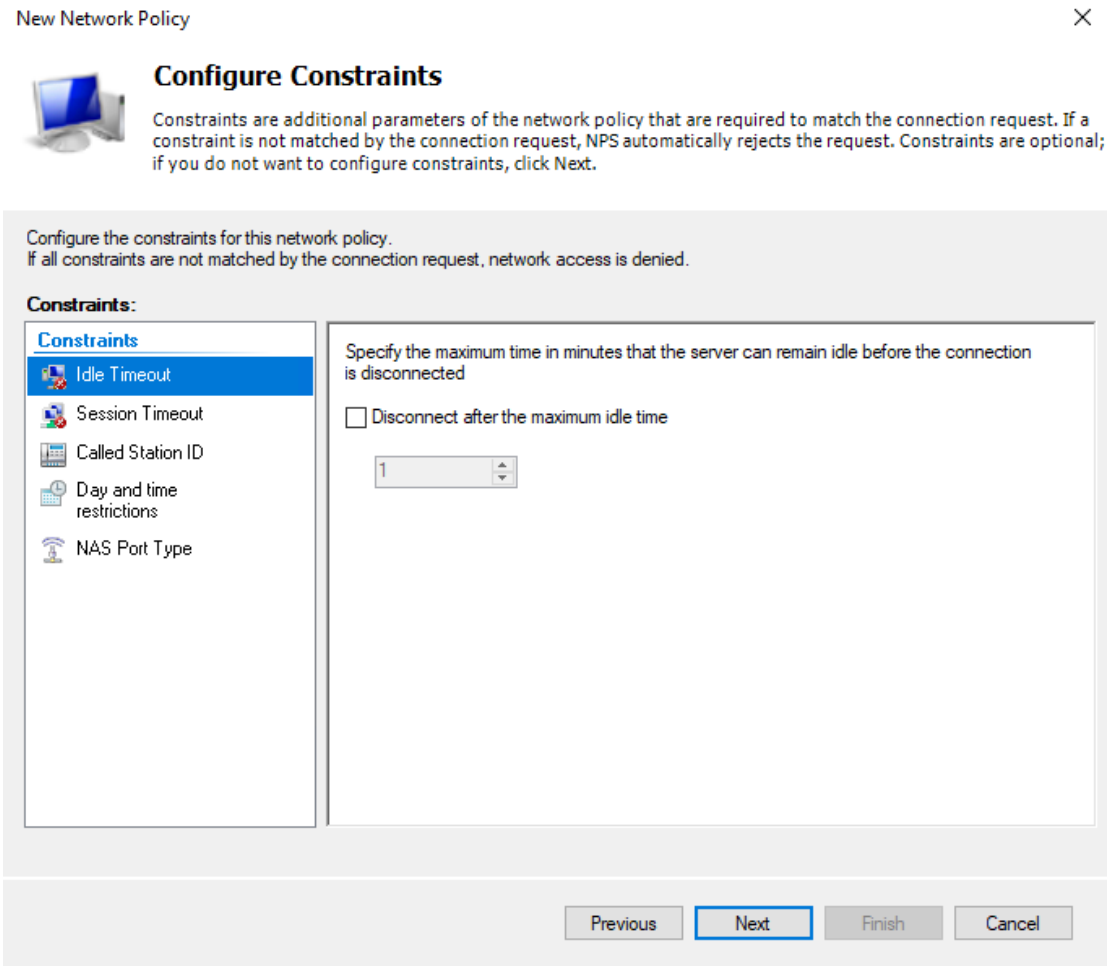
NOTE: When applying PAP authentication method, there is warning about insecure authentication methods, need skip it.

Figure 37 : Connection Request Policy



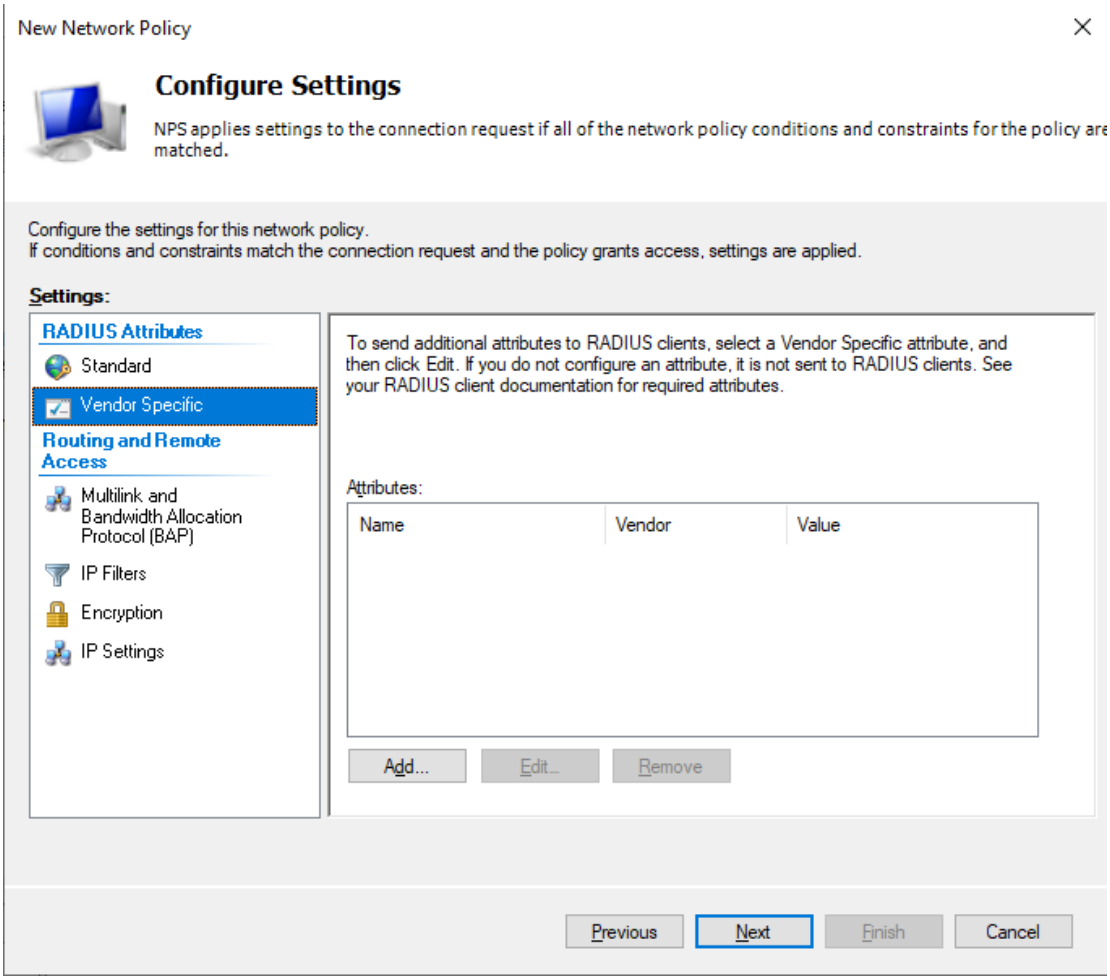
10. In **Configure constraints** dialog box, click **Next**.

Figure 38 : Configure Constraints



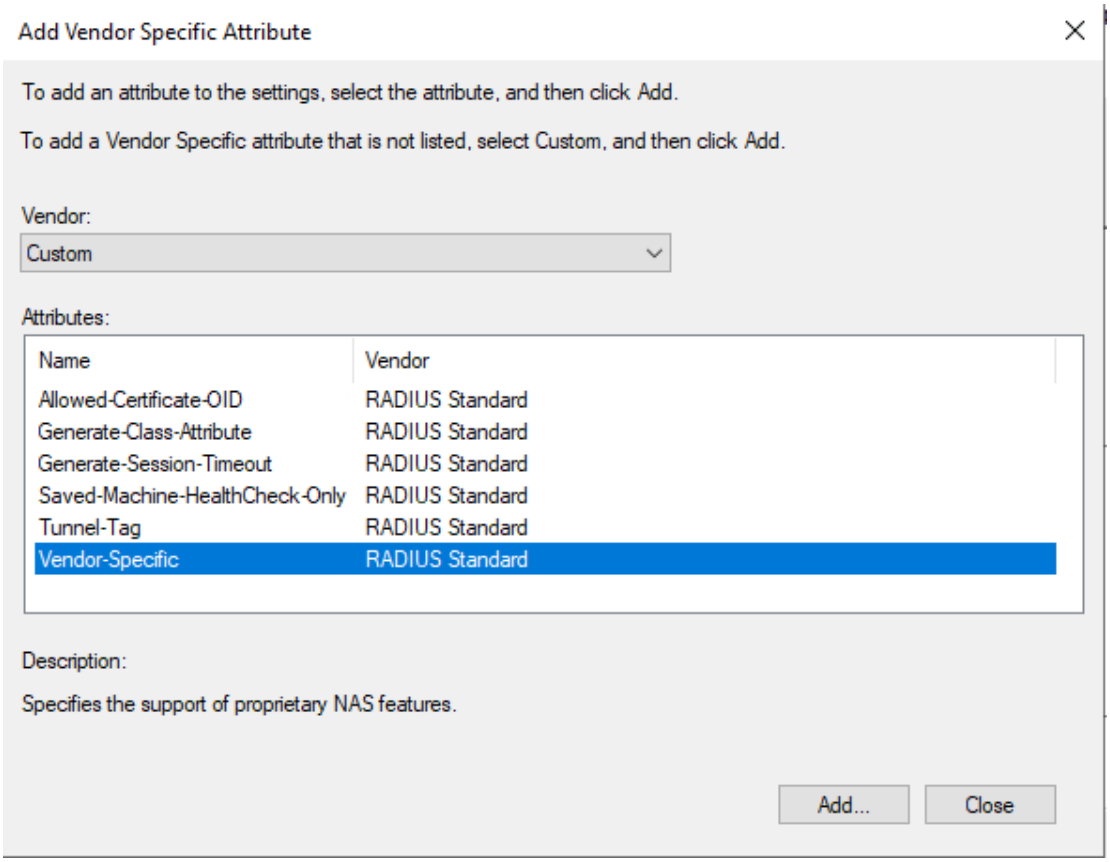
11. In **Setting> Radius Attributes**, select **Vendor Specific** , Click **Add…**.

Figure 39 : Configure Settings



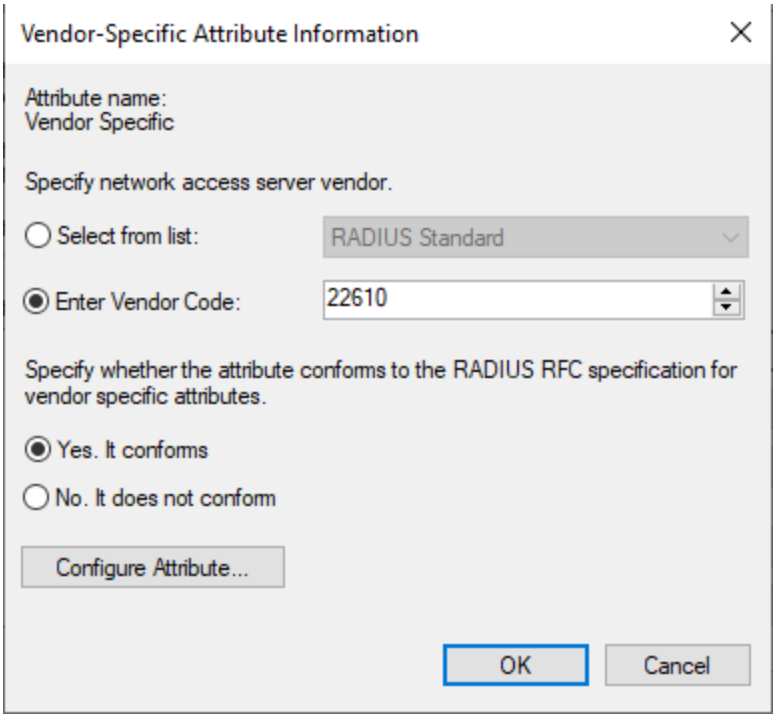
12. In **Add Vendor Specific Attribute** box, select **Vendor as Custom**, select **Vendor Specific**, click **Add**.

Figure 40 : Add Vendor Specific Attribute



13. In the **Vendor- Specific Attribute Information** dialog box, enter the following:
    - Enter vendor code – 22610 (for A10 Networks)
    - Conforms to RADIUS RFC – Yes

Figure 41 : Vendor-Specific Attribute Information

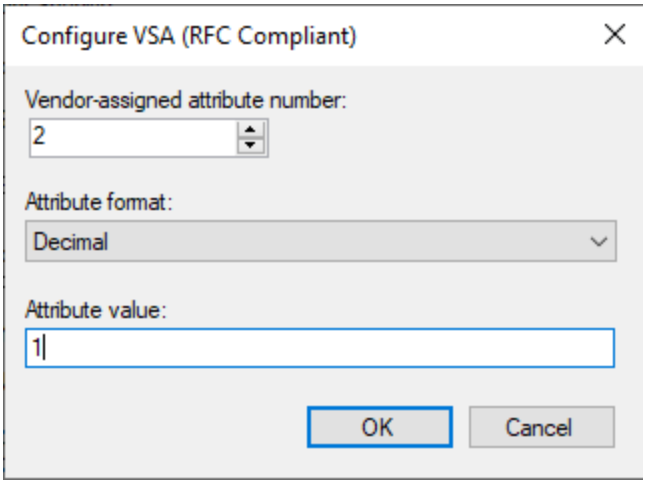


14. Click Configure Attribute, and enter the following information:

    - Vendor-assigned attribute number – 2
    - Attribute format – Decimal
    - Attribute value – 1

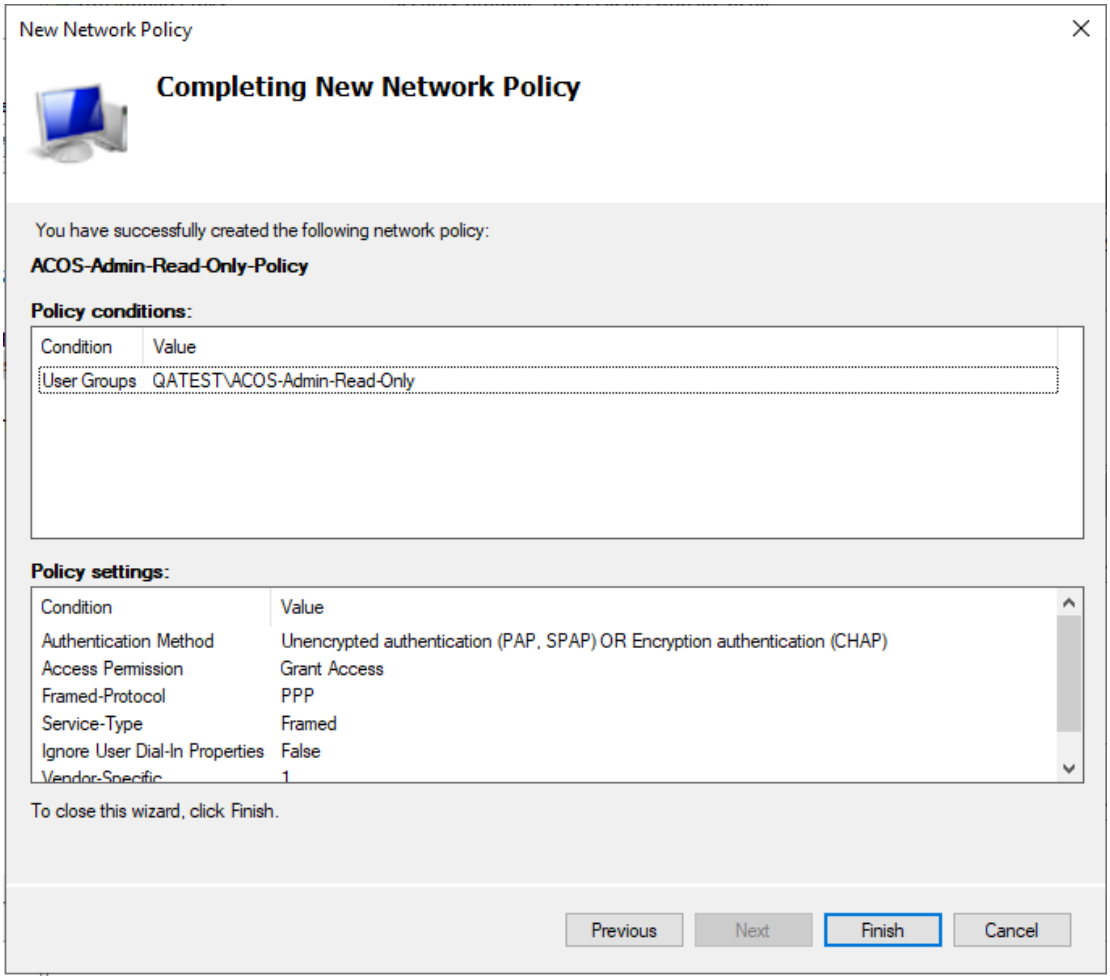
    NOTE: Attribute value 1 is read-only. Attribute value 2 is read-write.

Figure 42 : Attribute Value



15. Click **OK** for the Configure VSA.
16. Click **Ok** to for the Vendor -Specific Attribute Information.
17. Click **OK** for the Attribute Information.
18. Click **Close**.
19. Click **Next**, then click **Finish**.

Figure 43 : Completing New Network Policy



20. To create the second Remote Access Policy, repeat the above steps with the following changes:
    - Policy Friendly name – ACOS-Admin-Read-Write-Policy
    - Group to add – ACOS-Admin-Read-Write
    - Attribute value – 2

Configuring RADIUS on the ACOS Device

To add the RADIUS server (NPS server) to the ACOS device, enter the following commands:

```
ACOS(config)# radius-server host 10.65.17.180 secret shared-secret
```

```
ACOS(config)# authentication type local radius
```

Ensure that the shared secret is the same as the value that you specified for the RADIUS client that you configured for the ACOS server on the NPS server.

In this example, 10.65.17.180 is the IP address of windows, and shared-secret is the secret that you entered in the Configuring RADIUS Client for the ACOS Device.

Verifying the Configuration

To verify the configuration:

1. Log in to the ACOS CLI.
2. On the command prompt, enter the username in the following format:

   ```
   user-name@AD-domain-name
   ```

   For example, you might enter read@qatest.com
3. Enter the password.
4. Press **Enter**.

Authentication and Authorization Based on Group Extraction

The following topics are covered:

Overview

The ACOS device can use the group membership defined in the TACACS+ server to set and control the user access permissions.

If a user logs into the ACOS device using CLI or GUI, its user credentials are sent to the TACACS+ server. The TACACS+ server authenticates the user and extracts the

user's group membership. The extracted information contains user roles, access types, and privilege levels. This information is used to assign the appropriate access permissions to the user. Thus, the user permissions can be managed centrally in the TACACS+ server.

For example, if a user belongs to a read-only group in TACACS, when it logs in to the ACOS device using CLI, it will only be able to execute show commands and not the configuration commands.

Configuring TACACS+ for Group Extraction

To configure TACACS+ for Group Extraction:

1. Configure user attributes to specify the group permission memberships in the TACACS+ server configuration file.
2. Create the required user groups and define their permissions in the TACACS+ server configuration file.
3. Add the A10 Admin Role, Access Type, and Privilege level as required in the TACACS+ server configuration file.

   The following is the sample configuration:

```
<Authorization>
    <UserGroups>
         <UserGroup>Local System Administrators</UserGroup>
    </UserGroups>
         <!--No client group provided so this authorization section
applies to the above user groups from all the clients -->
         <!--this group is allowed to telnet everywhere except from
addresses beginning with 161.-->
    <Shell>
         <!--<deny>telnet 161\.*</deny>
         <Permit>telnet .*</Permit>-->
         <Permit>.*show.*</Permit> <!--This will allow all show
commands -->
         <Deny>.*</Deny>           <!--This will deny all other
commands -->
    </Shell>

    <AutoExec>
         <!--<Set>acl=7</Set>-->
         <!-- When an exec is started, its connection access list will
be 7.  It will also automatically execute this autocmd. If the cmd
element is not provided then the shell entry is used when the shell is
first invoked.-->
         <!--<Set>autocmd=telnet 10.1.1.1</Set>-->
         <Set>a10-admin-role=ReadWriteAdmin</Set>
         <Set>a10-access-type=cli,web</Set>
         <Set>priv-lvl=15</Set>
    </AutoExec>
</Authorization>
```

4. Configure the global authentication and authorization methods to use TACACS+ on the ACOS device.

```
ACOS(config)#authentication type tacplus local
ACOS(config)#authentication enable tacplus local
ACOS(config)#authentication login privilege-mode
ACOS(config)#authorization commands 15 method tacplus
```

5. Configure TACACS+ server setting on the ACOS device.

```
ACOS(config)#tacacs-server host tacacs_server_ip secret encrypted
secret-key
```

6. Configure the management interface to use for automated management traffic.

```
ACOS(config)#interface management
ACOS(config-if:management)#ip address ip_address ip_subnet_mask
ACOS(config-if:management)#ip control-apps-use-mgmt-port
ACOS(config-if:management)#ip default-gateway default_gateway_address
```

7. Log into the Thunder device using the CLI or GUI with the user credentials defined in the TACACS+ server.

8. After the successful login, verify if the access permissions are applied correctly based on the group memberships.

```
ACOS(config)#show admin session
Id  User Name  Start Time                    Source IP     Type
Partition Authen  Role            Cfg
-------------------------------------------------------------------------
-------------------------------
3     admin    20:38:19 GMT Tue Mar 12 2024  172.20.37.243  CLI   Local
           ReadWriteAdmin  No

*24    user1   21:32:41 GMT Tue Mar 12 2024  172.20.16.120  CLI
Tacacs+          ReadWriteAdmin  No
```

For more information on the above commands, see *Command Line Interface Reference*.

Additional Reference Information

The following commands that appear in the examples of this document are described in the Command Line Interface Reference.

```
ACOS(config)# radius-server ?
  default-privilege-read-write  Specify the RADIUS default privilege
  host                          Specify the RADIUS server's hostname or IP
address
ACOS(config)# authentication ?
  console               Configure console authentication type
```

```
  enable                The enable-password authentication type
  login                 The login mode
  mode                  Configure authentication mode
  multiple-auth-reject  Multiple same user login reject
  type                  The login authentication type
ACOS(config)# tacacs-server ?
  host     Specify the hostname of TACACS+ server
  monitor  Configure TACACS+ servers
ACOS(config)# authorization ?
  commands  Commands level for authorization
  debug     Specify the debug level for authorization
ACOS(config)# accounting ?
  commands  Enable level for commands accounting
  debug     Specify the debug level for accounting
  exec      Configuration for EXEC <shell> accounting
```

Command Auditing

This chapter describes how to enable and configure command auditing on your ACOS device.

The following topics are covered:

Overview

The user can enable command auditing to log the commands entered by ACOS administrators.

Command auditing logs the following types of system management events:

- Administrator logins and log outs for CLI, GUI, and aXAPI sessions.
- Unsuccessful administrator login attempts.
- Configuration changes. All attempts to change the configuration are logged, even if they are unsuccessful.
- CLI commands at the Privileged EXEC level (if audit logging is enabled for this level).

NOTE: Previously, the audit log (including all of the aXAPI messages) was being displayed in the console, which affected the scroll back buffers for terminal programs. Starting in release 2.7.2, the audit log is no longer displayed, and the API calls are no longer displayed in the console.

The audit log is maintained in a separate file, apart from the system log. The audit log messages displayed for an admin depend upon the administrator's privilege level.

Administrators with Root, Read Write, or Read Only privileges who view the audit log can view all messages, for all system partitions.

Administrators who have privileges only within a specific partition can view only the audit log messages related to management of that partition.

NOTE: Backups of the system log include the audit log.

Enabling and Configuring Command Auditing

Command auditing is disabled by default. To alter this configuration, the user can perform the following actions.

The following topics are covered:

Configuring using GUI

The user can configure the Command Auditing feature through the GUI mode. The following are the various steps and modes to enable command auditing using the GUI:

1. Navigate to **System >> Settings**.
2. Select the **Logging** tab.
3. In the **Audit log host** field, specify the **IPv4** or **IPv6** address of the audit logging host server, or specify the **Name** of the audit logging host server.
4. Select the logging facility from the **Facility** drop-down list.
5. Click **OK**.

Configuring using CLI

The user can configure the Command Auditing feature through the CLI mode. The following are the various steps and modes to enable command auditing using the CLI:

To enable command auditing from the CLI, use the **audit enable** command at the global configuration level. This command logs configuration command only.

```
ACOS(config)# audit enable
```

To log both configuration and Privileged EXEC commands, use the following command:

```
ACOS(config)# audit enable privilege
```

The following command sets the buffer size to 30,000. When the log is full, the oldest entries are removed to make room for new entries. The default is 20,000 entries.

```
ACOS(config)# audit size 30000
```

Use the following command to disable command auditing:

```
ACOS(config)# no audit enable
```

To show audit log entries, use the **show audit** command:

```
ACOS(config)# show audit
```

Audit Log Examples

The following audit log indicates a change to the image to use for booting, performed using the CLI:

```
Jul 06 2010 23:27:25  admin cli: bootimage hd sec
```

The following audit logs indicate configuration and operational actions related to virtual server “vip1” performed using the GUI:

```
Jun 08 2014 09:06:04 [12] web: [admin] add virtual server [name:vip1,
ip:1.1.1.1, vport1:8001(TCP).] successfully.
Jun 08 2014 09:06:05 [12] web: [admin] edit virtual server [name:vip1,
ip:1.1.1.1, vport1:8001(TCP).] successfully.
Jun 08 2014 09:06:06 [12] web: [admin] disable virtual server [vip1]
successfully.
Jun 08 2014 09:06:06 [12] web: [admin] enable virtual server [vip1]
successfully.
Jun 08 2014 09:06:07 [12] web: [admin] delete virtual server [vip1]
successfully.
```

The following audit logs indicate configuration actions related to virtual server “vip1” performed using the aXAPI:

```
Jun 08 2014 09:06:13  [12] aXAPI: [admin] add virtual server [name:vip1,
ip:1.1.1.1, vport1:8001(TCP).] successfully.
Jun 08 2014 09:06:14  [12] aXAPI: [admin] edit virtual server [name:vip1,
ip:1.1.1.1, vport1:8001(TCP).] successfully.
Jun 08 2014 09:06:15  [12] aXAPI: [admin] delete virtual server [vip1]
successfully.
```

Additional Reference Information

The following commands that appear in the examples of this document are described in the Command Line Interface Reference.

```
ACOS(config)# audit ?
  enable  Enable audit service
  size    Config audit buffer size, default is 20,000
```

Contact Us