WiNG 5.X Feature Guide

How To TACACS+

Part No. TME-03-2016-01 Rev. B

`

`

Table of Contents

1. Overview

TACACS+ (Terminal Access Controller Access-Control System Plus) is a Cisco Systems proprietary protocol which provides access control for routers, switches, network access servers and other network infrastructure devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

WiNG 5 supports management user access to the device using local database or using an external radius server. WiNG 5.2 introduces authentication, authorization and accounting via TACACS+ servers providing another method for management user authentication and access into WiNG 5 devices.

TACACS+ is an AAA protocol designed to provide controlled user access to network devices. It supports authentication, authorization and accounting services separately unlike RADIUS protocol, which clubs authentication and authorization into a single service. TACACS+ protocol follows a client-server model where the client uses the services provided by the server to authenticate, authorize and account user details.

1.1 TACACS+ Authentication

TACACS+ supports various kinds of authentication services including login, enable, PPP etc. WiNG 5.2 only supports the login authentication service. Within the login authentication service TACACS+ supports different authentication types including ASCII, PAP, CHAP, and MSCHAP. WiNG 5.2 only supports the ASCII authentication type.

When a user attempts to access a management interface on a Wireless Controller or Access Point, the user is prompted for a username and password. The Wireless Controller or Access Point talks to the TACACS+ server to authenticate the user using the entered credentials. If the authentication is successful, the user is provided access to the device with the roles and privileges configured for the user on the TACACS+ server.

During TACACS+ authentication the management user's access permissions into the WiNG 5.2 device is also evaluated. Each management user can be permitted access to one or more management interfaces which is defined on the TACACS+ server as attributes and forwarded to the WiNG 5 device. If a management user attempts to access a management interface they are not permitted to access, the authentication is denied. Access permissions attributes and value can be assigned to groups of users based on group membership or to individual users.

Attribute	Supported Values	Examples
moto-user-access	▪ all ▪ console ▪ ssh ▪ telnet ▪ web	moto-user-access*all moto-user-access*ssh moto-user-access*web moto-user-access*"console ssh web"

Table 1.1 – Access Permission Attributes

1.2 TACACS+ Authorization

TACACS+ allows authorizing various services that a user is allowed to run on the device. For WiNG 5 we support the ability to authorize each CLI command entered by a management user. WiNG 5 allows a specific set of CLI commands to be executed by a management user based on the user's assigned role. Role attributes and value can be assigned to groups of users based on group membership or to individual users. Each user can only be assigned to one role.

Attribute	Supported Values	Examples
moto-user-role	▪ device-provisioning-admin ▪ helpdesk ▪ monitor ▪ network-admin ▪ security-admin ▪ superuser ▪ system-admin ▪ web-user-admin	moto-user-role*monitor moto-user-role*superuser
zebra-user-allow-loc	▪ String value that would match ***"allowed-locations"*** object in WiNG management policy configuration. Applicable only to Zebra NSight to provide multi-tenant access.	zebra-user-allow-loc*us-branches zebra-user-allow-loc*office-1

Table 1.2 – User Role Attributes

In addition the network administrator can configure specific CLI commands from the allowed list to be permitted or denied on a per user basis on the TACACS+ server. Each CLI command that a user executes can be authorized by the TACACS+ server using the user's credentials.

1.3 TACACS+ Accounting

TACACS+ allows accounting of various user activities. For WiNG 5.2 we support accounting of each CLI command a user executes. CLI command accounting only functions for management sessions using the serial console, SSH or telnet management interfaces. CLI command accounting is not supported for management sessions using the Web-UI.

In addition the session's start/stop details for the management user can also be logged. Session details are forwarded to the TACACS+ server when the management user is initially authenticated and when the user logs out or the session times out.

2. Configuration

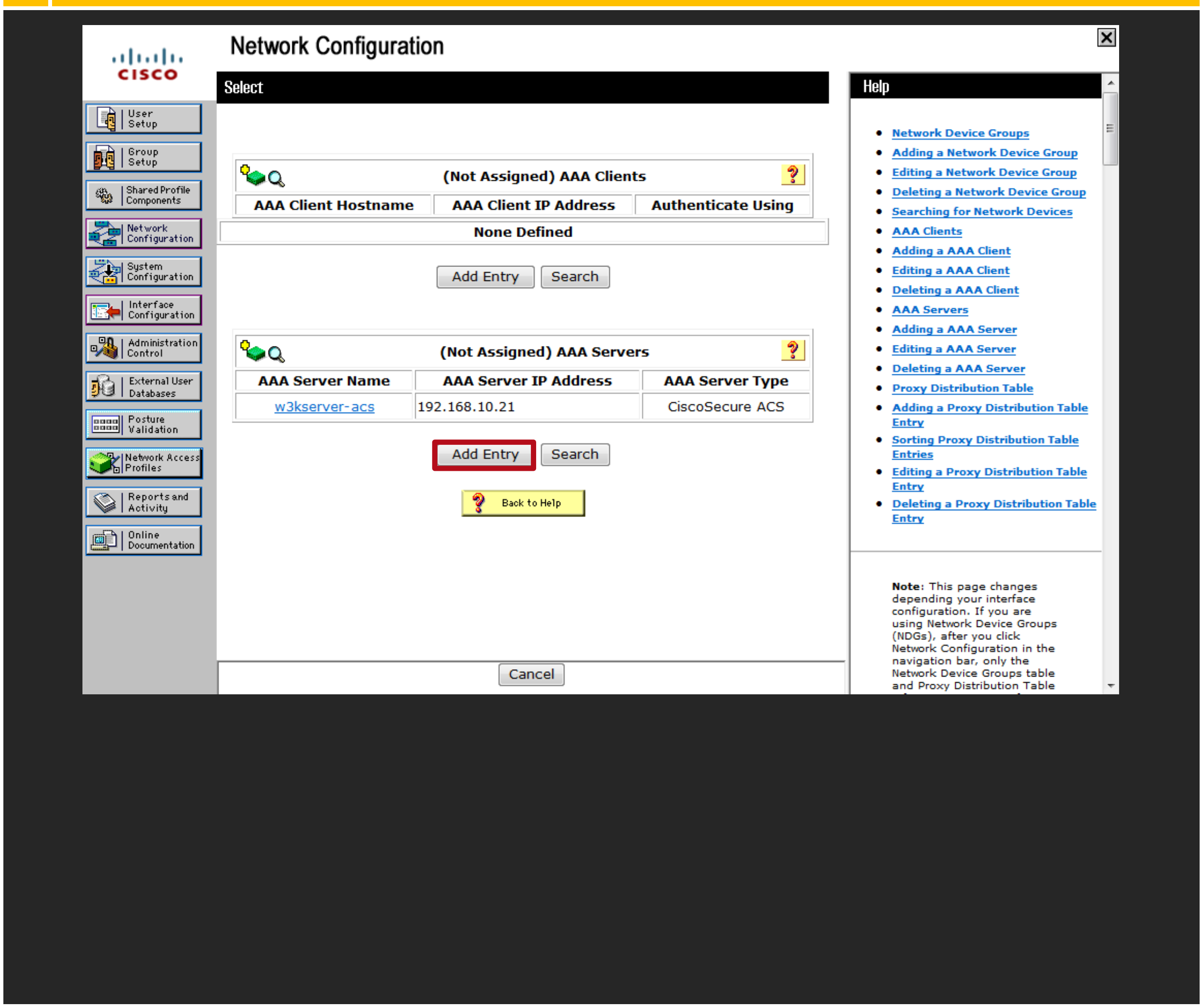
2.1 Cisco Secure ACS 4.X

The following provides example for configuring a Cisco Secure ACS 4.X server to support TACACS+ authentication, authorization and accounting on Zebra Wireless Controllers and Access Points. In this configuration example Zebra vendor specific attributes and values will be assigned to groups on the Cisco Secure ACS server to determine each user's role and access permissions. The attributes and values are assigned to the group using user defined services and protocols enabled on each group.

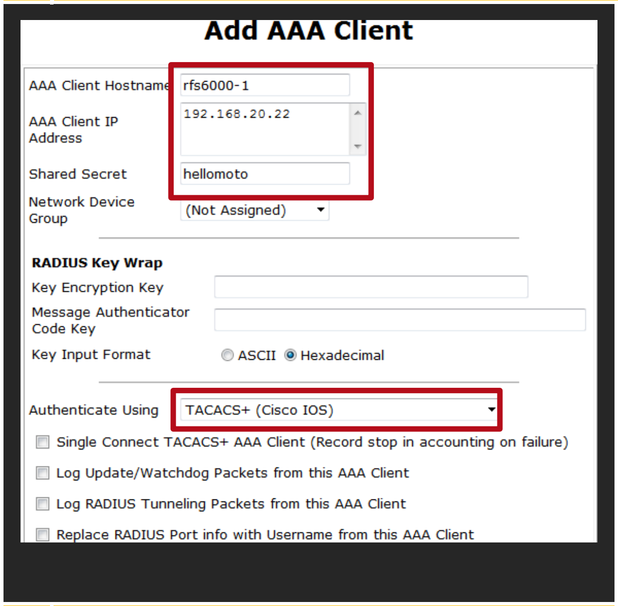
2.1.1 Network Configuration

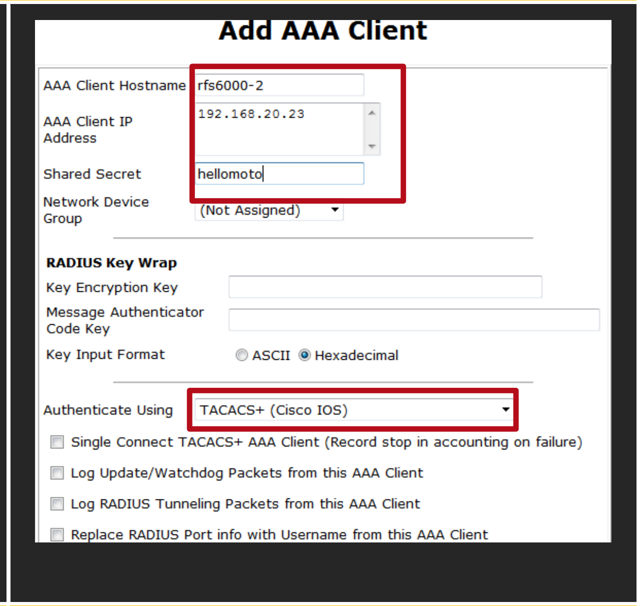
The following provides an example of how to add a WiNG 5 device as an AAA Client to the Cisco Secure ACS 4.x server. For the WiNG 5 device to be supported as a TACACS+ client, the *Authenticate Using* option must be set to *TACACS+ (Cisco IOS)*.

1	**Within Cisco Secure ACS select *Network Configuration* → *Network Device Group* → *Add Entry*:**

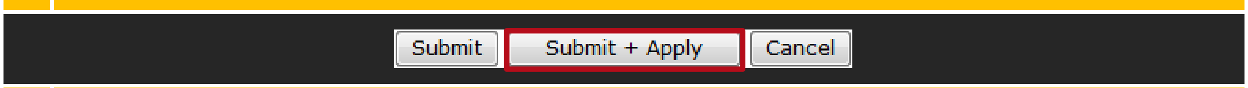


2	For each WiNG 5 device enter a *AAA Client Hostname*, *AAA Client IP Address* and *Shared Secret*. Select the *Authenticate Using* option *TACACS+ (Cisco IOS)*:

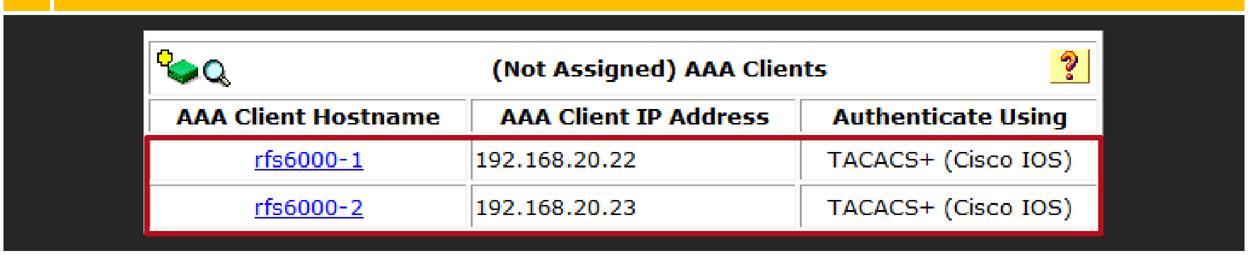




3	Click *Submit + Apply*:



4	The Controllers have now been added as AAA Clients to the Cisco Secure ACS Server:



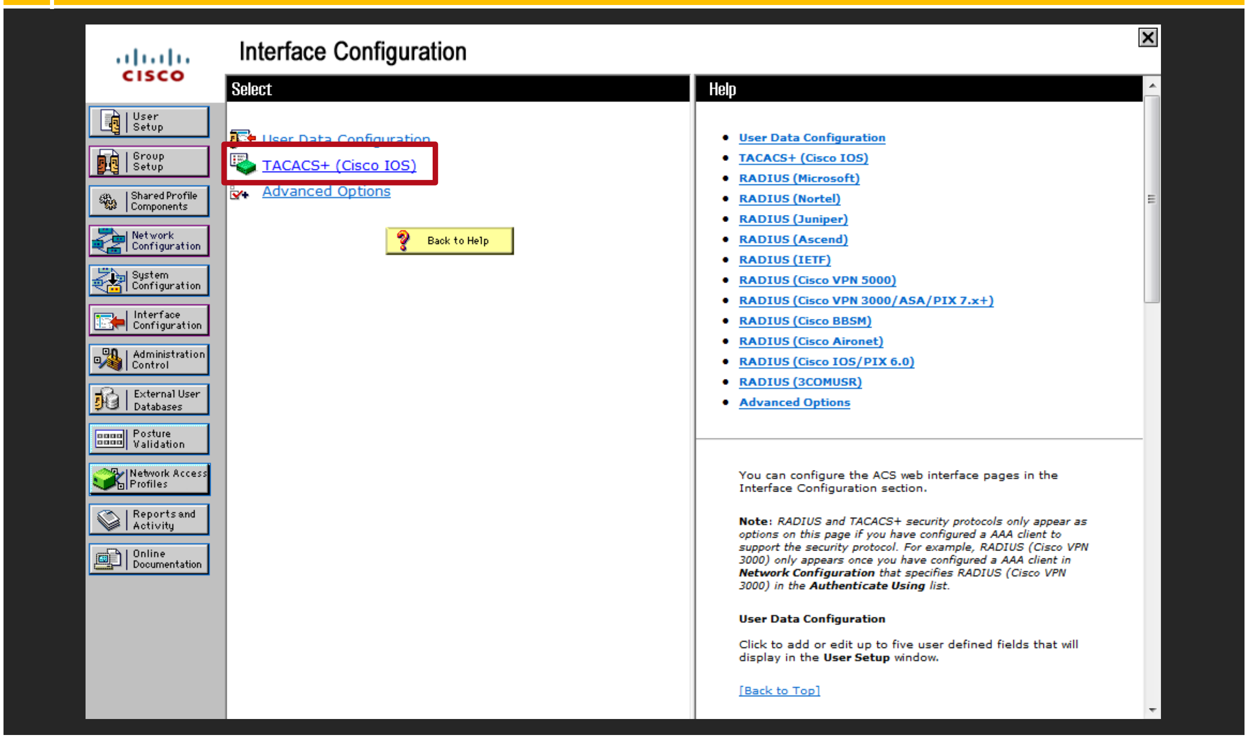
(Not Assigned) AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
rfs6000-1	192.168.20.22	TACACS+ (Cisco IOS)
rfs6000-2	192.168.20.23	TACACS+ (Cisco IOS)

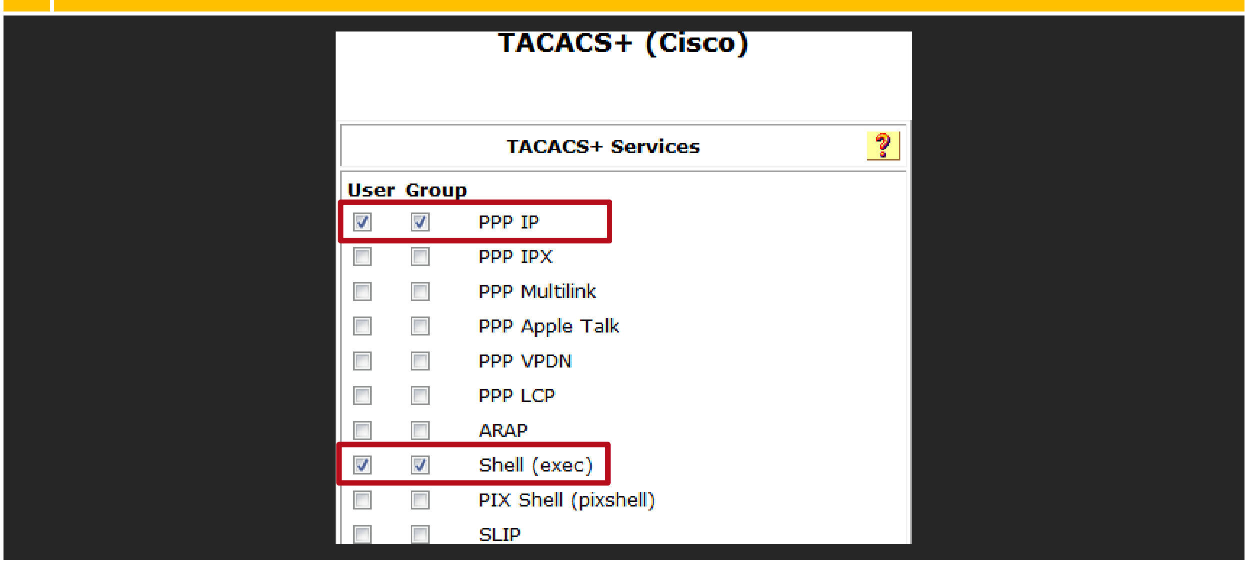
2.1.2 Interface Configuration

The following provides an example of how to configure TACACS+ services and protocols on a Cisco Secure ACS 4.x server. In this example two services and protocols are defined which will be used to provide read-only or read-write access into WiNG 5 devices. If existing TACACS+ existing services and protocols have already been defined, these can be supported by the WiNG 5 devices. The service and protocol names defined on the Cisco Secure ACS server must match the service and protocol names defined in the TACACS AAA policy defined on the Wireless Controller or Access Point.

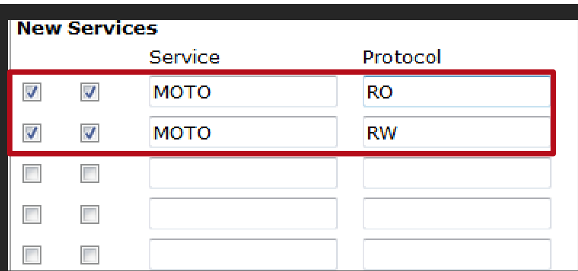
1 Within Cisco Secure ACS select *Interface Configuration → TACACS+ (Cisco IOS)*:



2 Under *TACACS+ Services* enable *PPP IP* and *Shell (exec)*:



3	**Under *New Services* define the required TACACS+ *services* and *protocols* to add. You can use existing *services* and *protocols* or create your own. The following example defines services and protocols named *Wing RO* and *Wing RW* which will be used to provide read-only or read-write access into WiNG 5 devices:**



4	**Click *Submit*:**

Note – The TACACS+ security protocol only appears as an option if you have first configured an AAA client to support the security protocol.

Note – For existing TACACS+ deployments you can use existing TACACS+ protocols and services. These can be assigned to the WiNG 5 device using the AAA TACACS Policy.

Note – The protocol and service names defined on the Cisco Secure ACS server must match the protocol and names defined in the TACACS AAA policy on the Wireless Controller or Access Points.

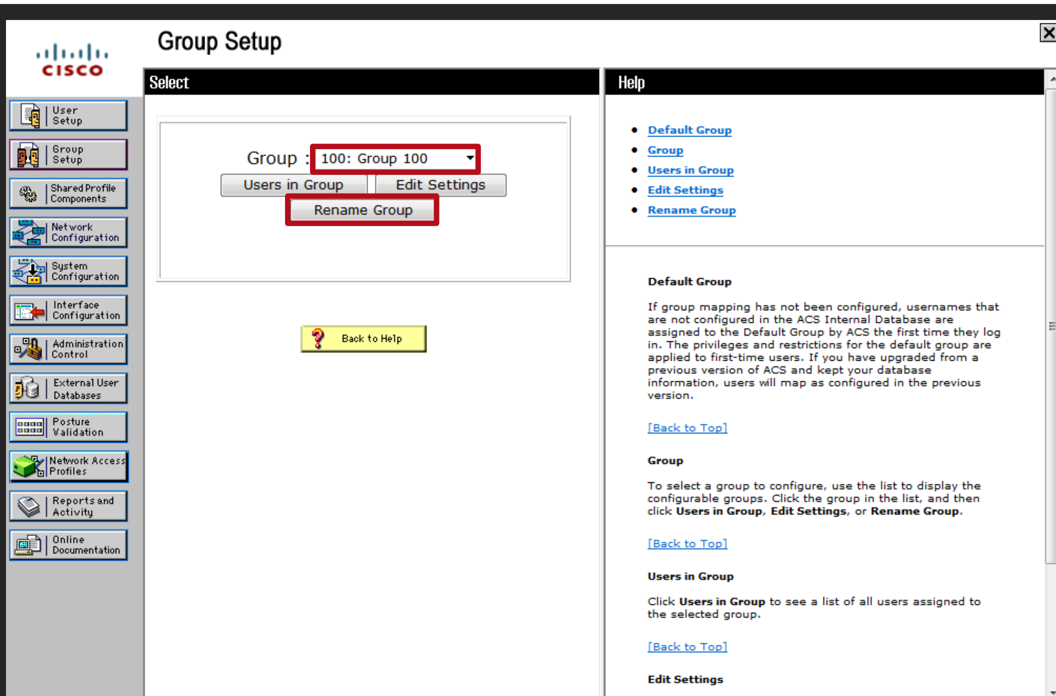
2.1.3 Group Setup

When an administrative user attempts to access the management interfaces on a WiNG 5 device, the user's role and access permissions is determined based on group membership. Each TACACS+ management group is assigned the necessary Zebra Solutions attributes and values that determines the role the users are assigned and management interfaces the users are permitted to access.

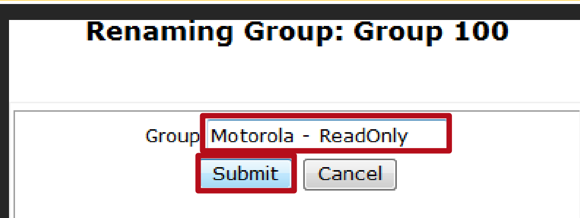
The following provides an example of how to assign Zebra Solutions attributes and values to the TACACS+ services and protocols for groups named ***Zebra - ReadOnly*** and ***Zebra - ReadWrite***.

Users that are assigned to the ***Zebra – ReadOnly*** group will be assigned to the ***Monitor*** role with access to the Web management interface. Users that are assigned to the ***Zebra – ReadWrite*** group will be assigned to the ***Superuser*** role with access to ***All*** management interfaces.

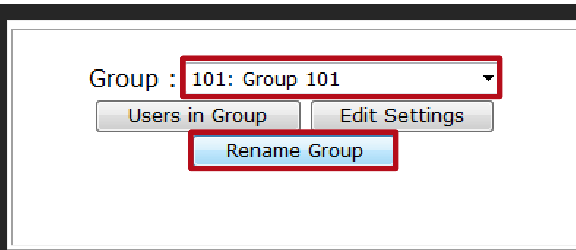
1 **Within Cisco Secure ACS select *Group Setup*. Select a group for *Read Only* access users then click *Rename Group*:**



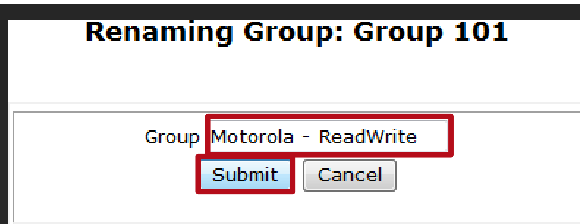
2 **Rename the group then click *Submit*:**



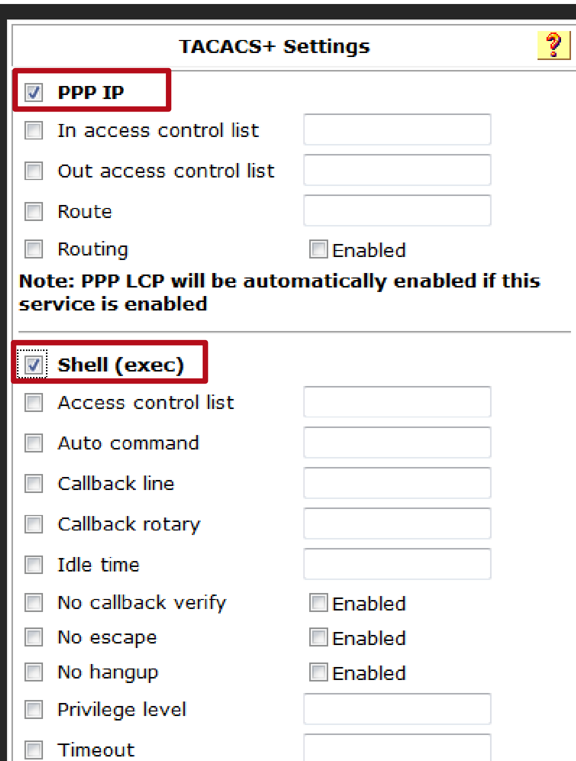
3	Select a group for *Read Write* access users then click *Rename Group*:



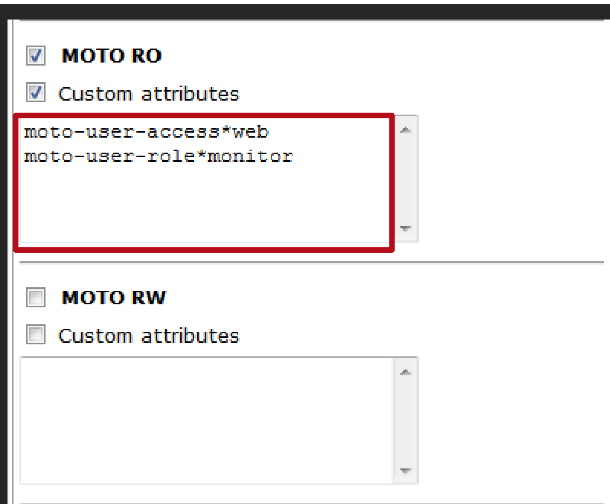
4	Rename the group then click *Submit*:



5	Select the *Read Only* group then click *Edit Settings*. Under *TACACS+ Settings* enable the options *PPP IP* and *Shell (exec)*:

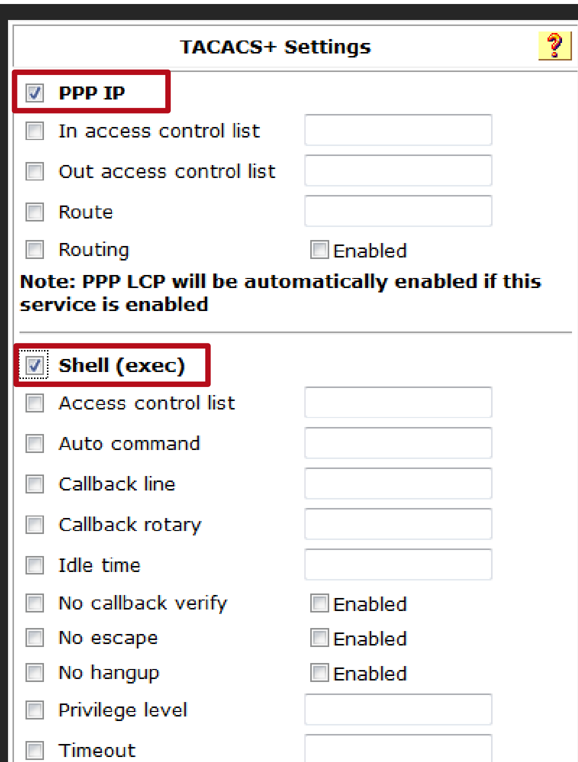


6 **Enable the protocol and service named *Wing RO* and define the desired attributes to determine the users role and access permissions. In this example read-only users will be assigned to the *Monitor* role and access permissions to the *Web* management interfaces:**

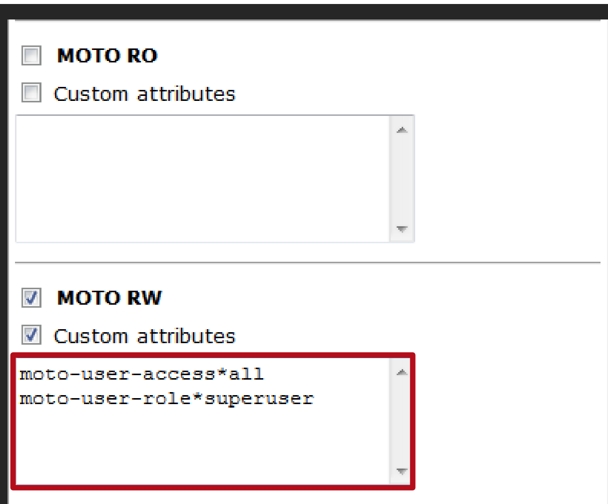


7 **Click *Submit + Restart*:**

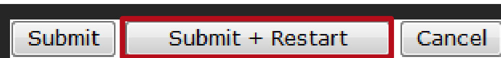
8 **Select the *Read Write* group then click *Edit Settings*. Under *TACACS+ Settings* enable the options *PPP IP* and *Shell (exec)*:**



9 **Enable the protocol and service named *Wing RW* and define the desired attributes to determine the users role and access permissions. In this example read-write users will be assigned to the *Superuser* role and access permissions to *All* management interfaces:**



10 **Click *Submit + Restart*:**



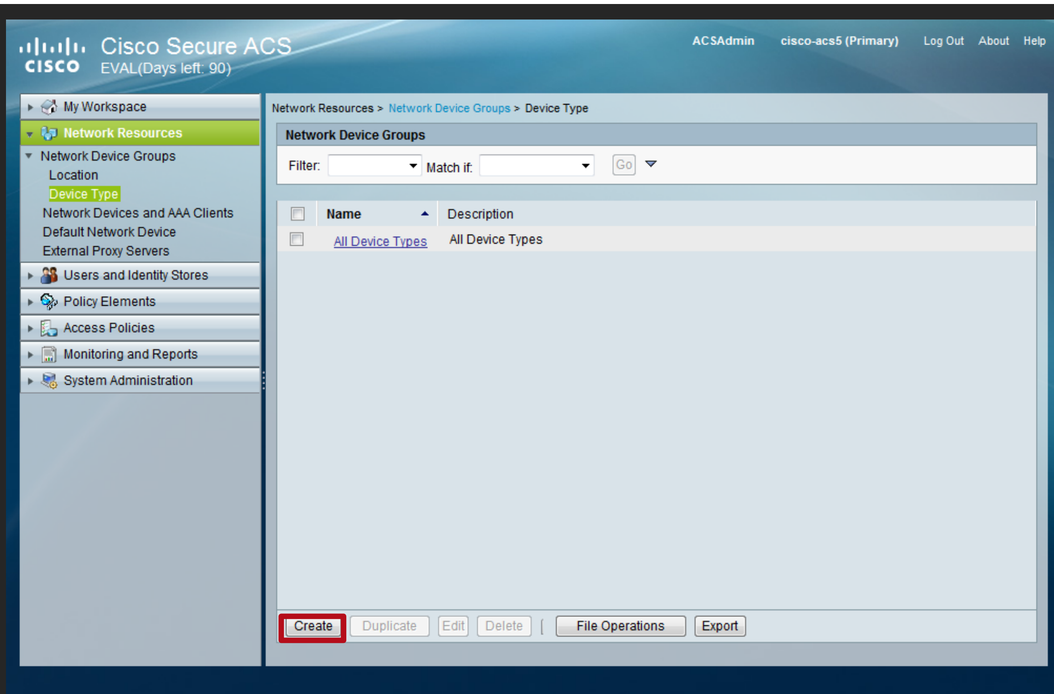
2.2 Cisco Secure ACS 5.X

The following provides example for configuring a Cisco Secure ACS 5.X server to support TACACS+ authentication, authorization and accounting on Zebra Wireless Controllers and Access Points. In this configuration example Zebra vendor specific attributes and values will be assigned to groups on the Cisco Secure ACS server to determine each user’s role and access permissions. The attributes and values are assigned to the group using user defined services and protocols enabled on each group.

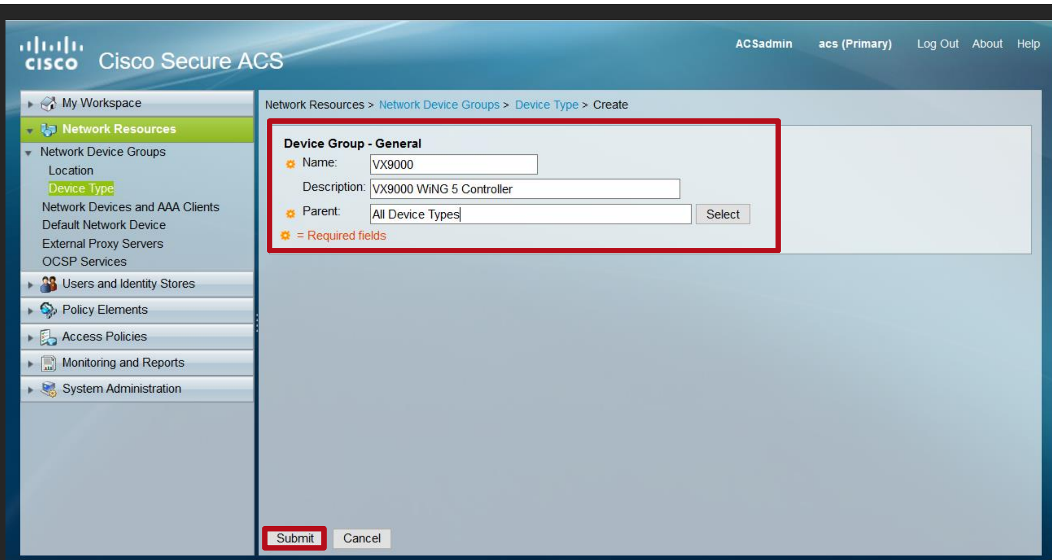
2.2.1 Device Types

The following provides an example of how to define WiNG 5 devices as device types on a Cisco Secure ACS 5.x server. Device types allow devices to be grouped in Cisco Secure ACS 5.x which will be used when defining device authorization policies.

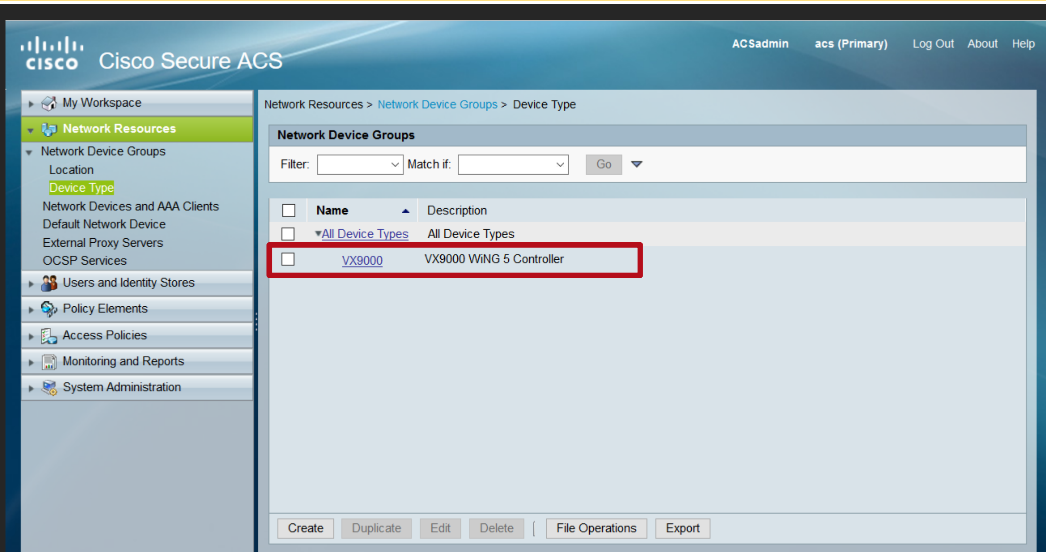
1	**Within Cisco Secure ACS select *Network Resources → Network Device Groups → Device Type → Create*:**



2	Enter a *Name* and *Description* and select a *Parent*. Click *Submit*:



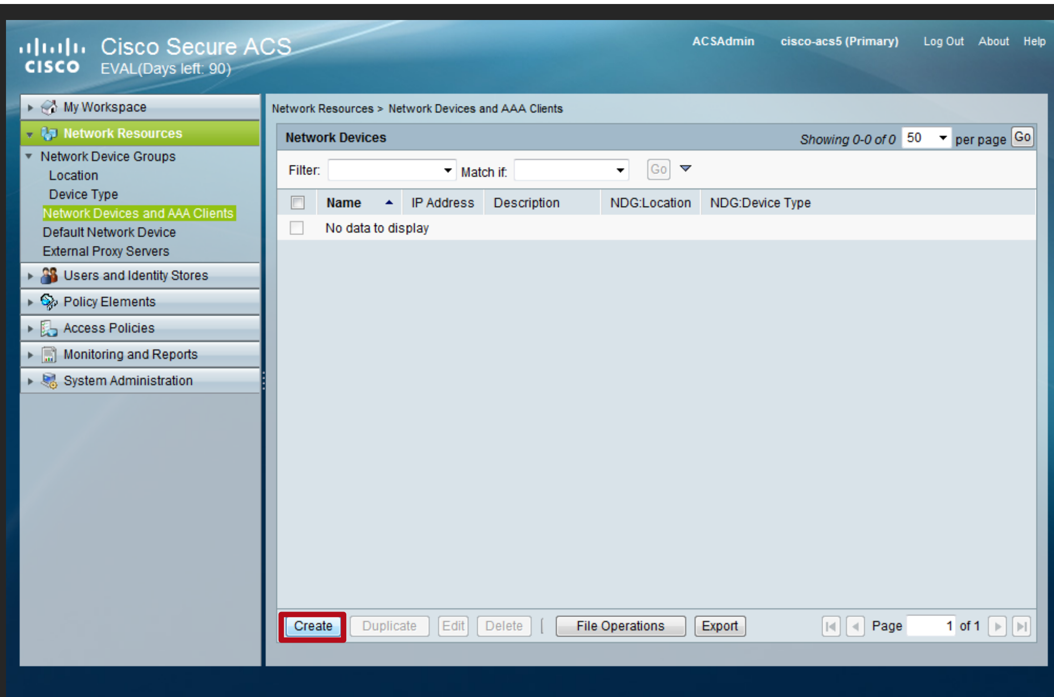
3	A *Network Device Group* for Zebra devices has now been created:



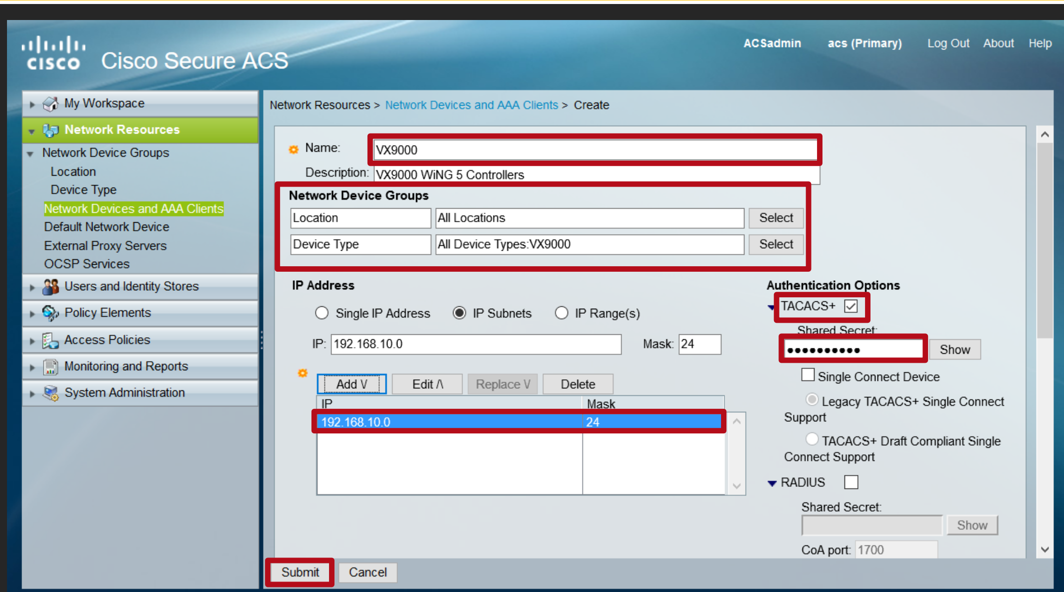
2.2.2 Network Devices and AAA Clients

The following provides an example of how to add a WiNG 5 device as an AAA Client on the Cisco Secure ACS 5.x server.

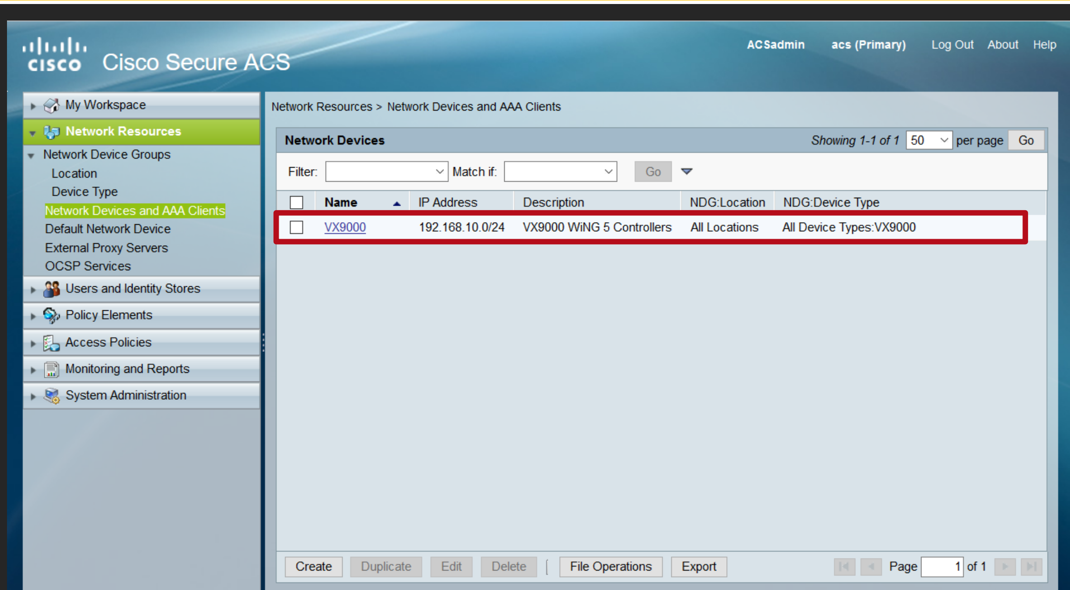
1	**Within Cisco Secure ACS select *Network Resources* → *Network Devices and AAA Clients* → *Create*:**



2 **Enter friendly *Name* for the Wireless Controller(s) then select a *Location*. Assign the *Device Type* created in the previous step then enable the *TACACS+* checkbox. Enter a *Shared Secret* then select an *IP Address* option. In this example *IP Rang(s) By Mask* has been selected and the IPv4 subnet the Wireless Controllers are connected to *192.168.20.0/24* defined. Click *Submit*:**



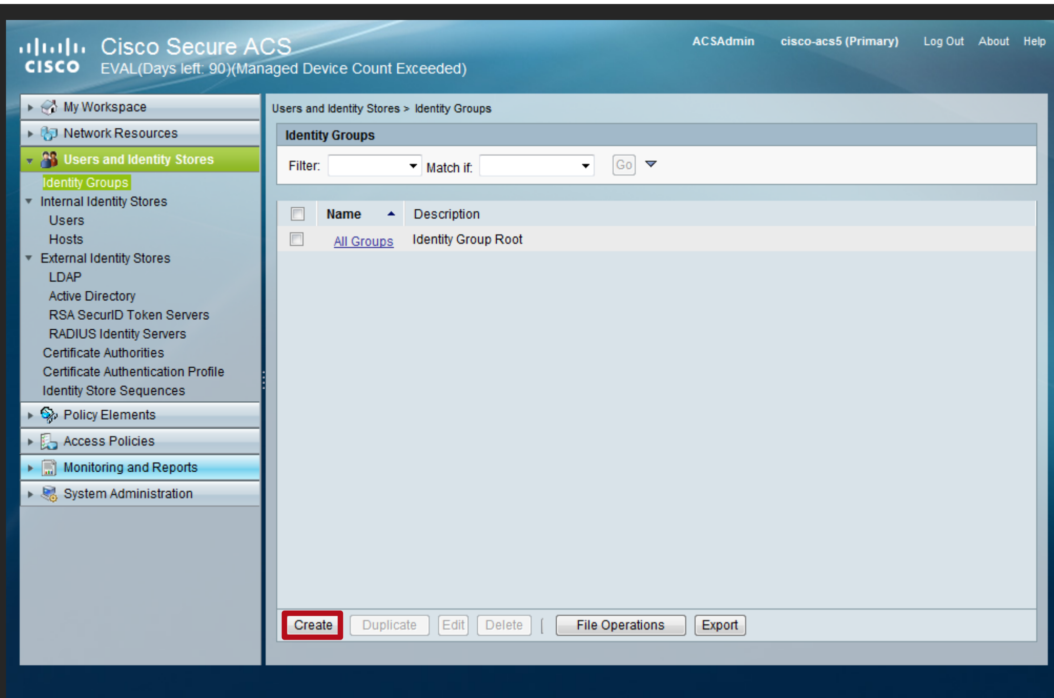
3 **The Wireless Controller(s) have now been defined as *Network Devices and AAA Clients*:**



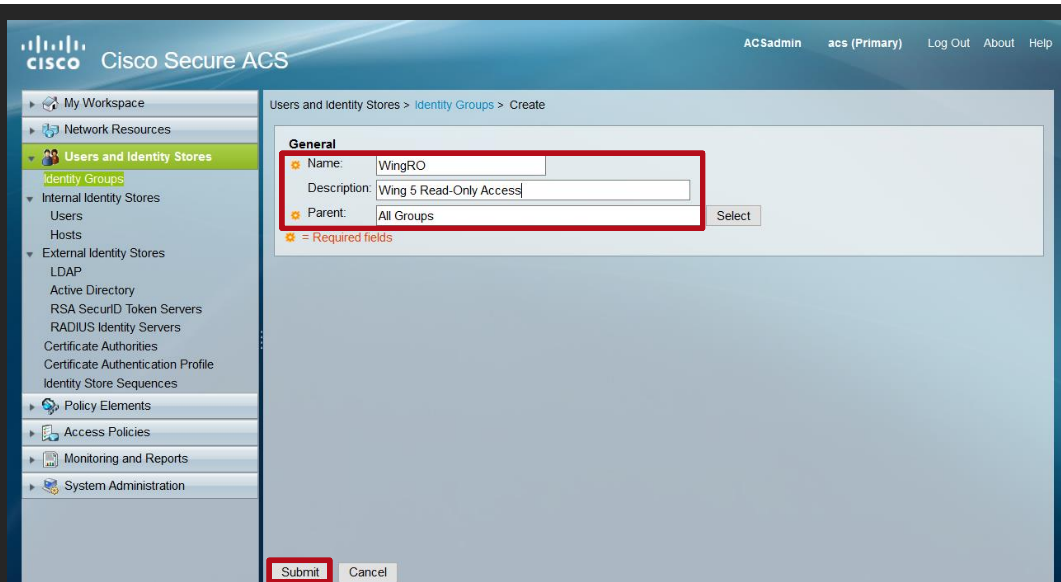
2.2.3 Identity Groups

The following provides an example of how to define identity groups on a Cisco Secure ACS 5.x server. In this example two groups named WingRO and WingRW will be defined. Users assigned to the ***WingRO*** group will be assigned to the ***Monitor*** role and ***Web*** access permissions while users assigned to the ***WingRW*** group will be assigned to the ***Superuser*** role and ***All*** access permissions.

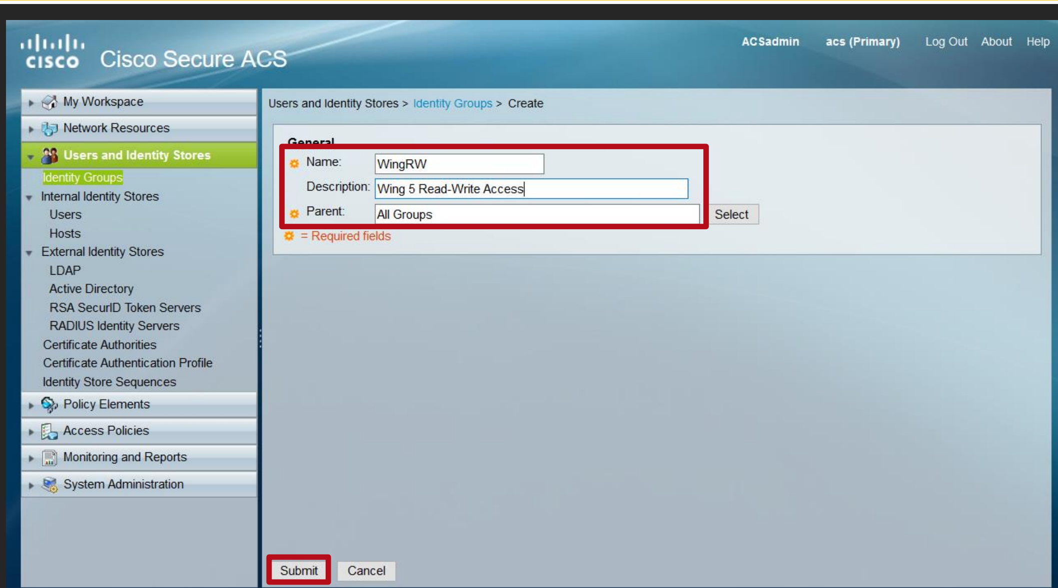
1 Within Cisco Secure ACS select *Users and Identity Stores → Identity Groups → Create*:



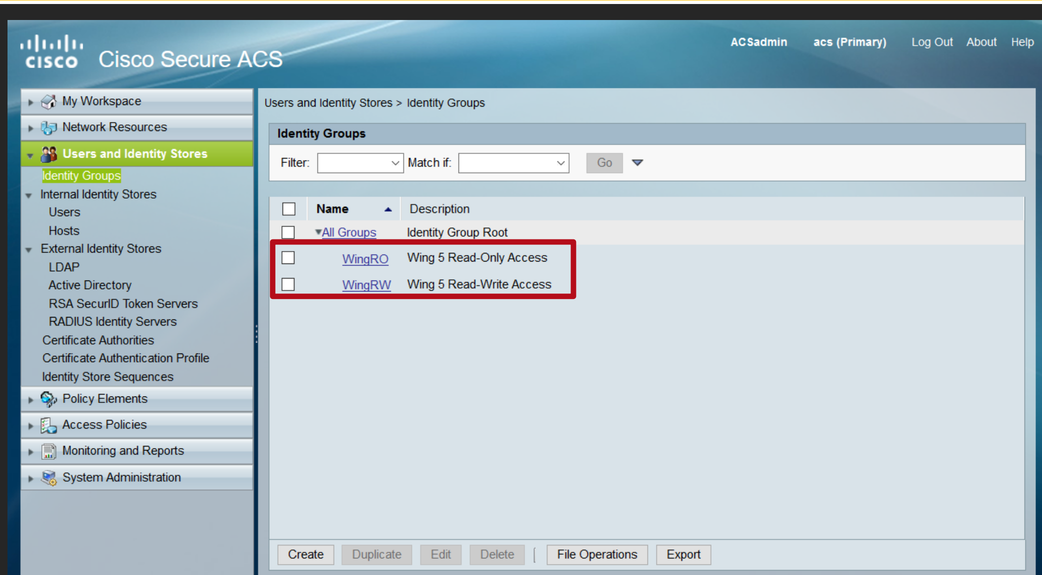
2 Enter a *Name* and *Description* for the *Read Only* access group then click *Submit*:



3 **_Create_ a second group. Enter a _Name_ and _Description_ for the _Read Write_ access group then click _Submit_:**



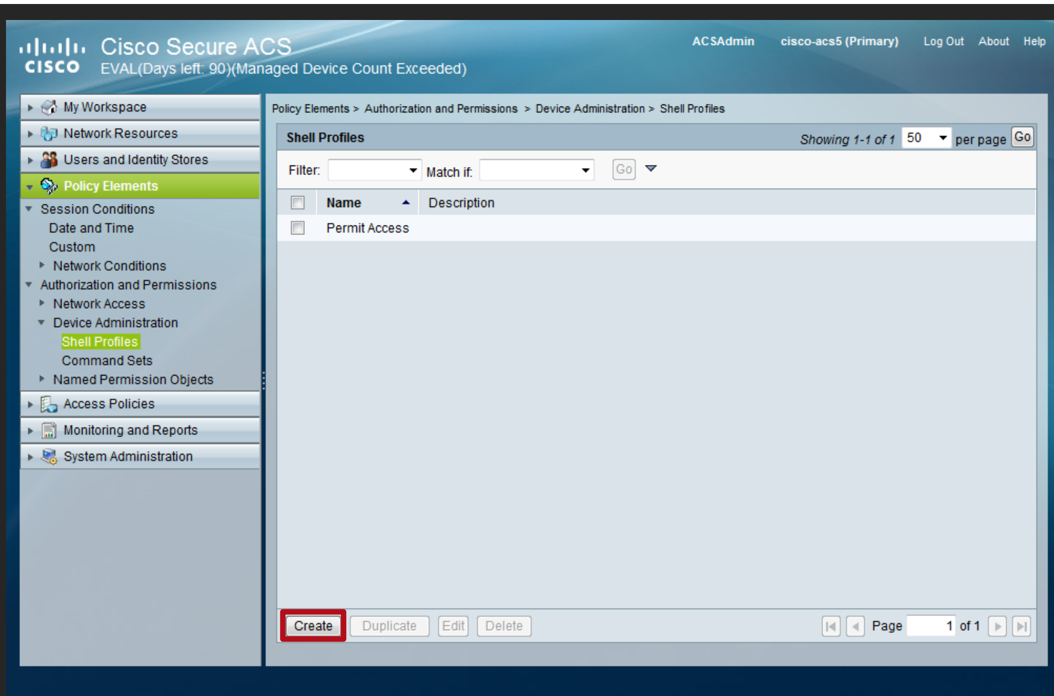
4 **Two _Identity Groups_ have now been created:**



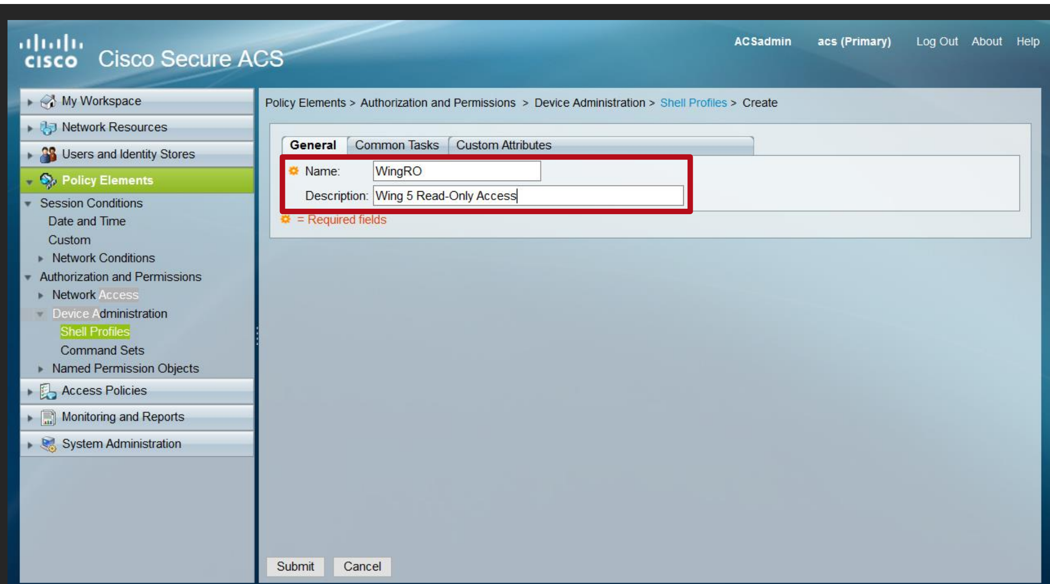
2.2.4 Shell Profiles

The following provides an example of how to define shell profiles on a Cisco Secure ACS 5.x server. In this example two shell profiles named ***WingRO*** and ***WingRW*** will be defined with attributes that determines the role and access permissions each management user is assigned. The name of each shell profile must match the name of the TACACS authentication service defined in the TACACS AAA policy.

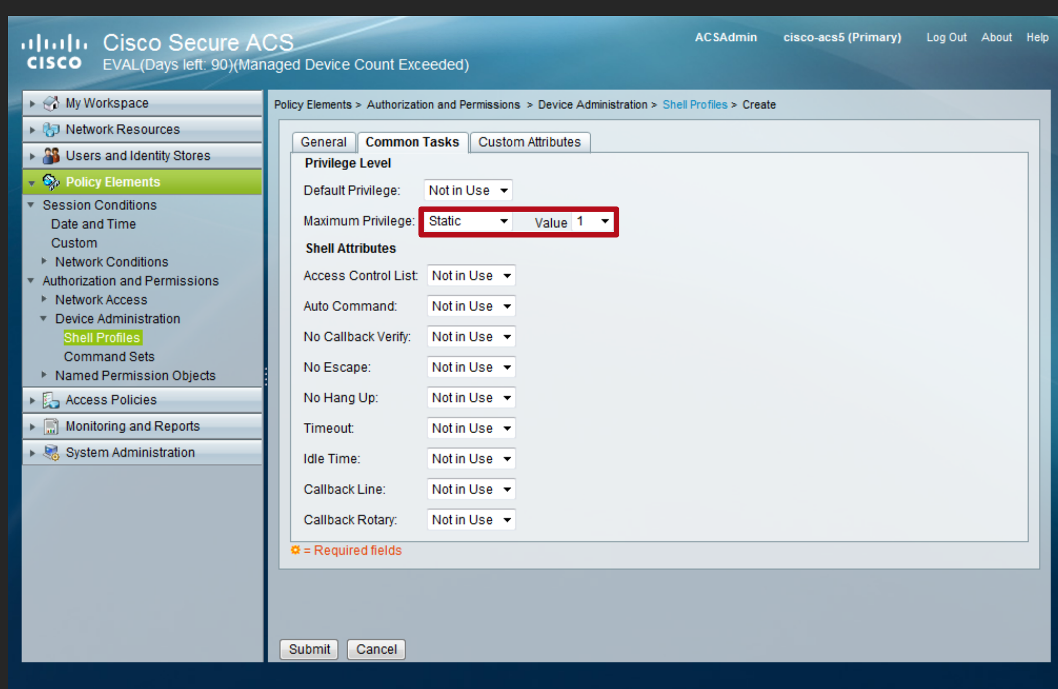
1	**Within Cisco Secure ACS select *Policy Elements → Authorization and Permissions → Device Administration → Shell Profiles → Create*:**



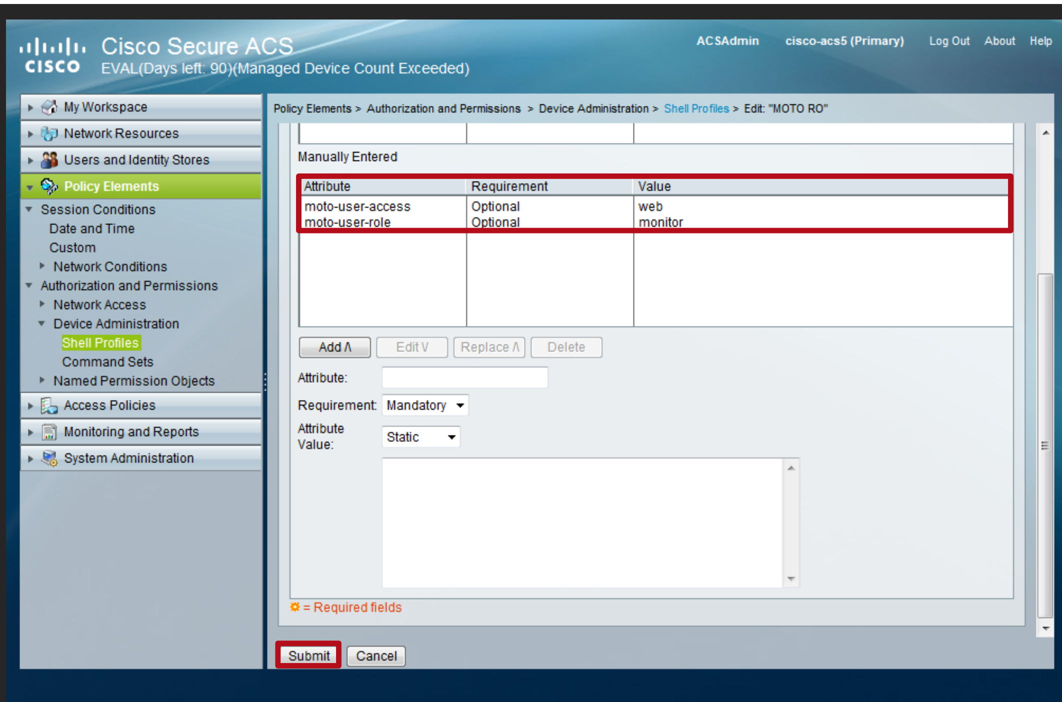
2	**In the *General* tab define the required TACACS+ *services* and *protocols* to add. You can use existing *services* and *protocols* or create your own. The following example defines services and protocol named *WingRO* will be used to provide *Read Only* access into WiNG 5 devices:**



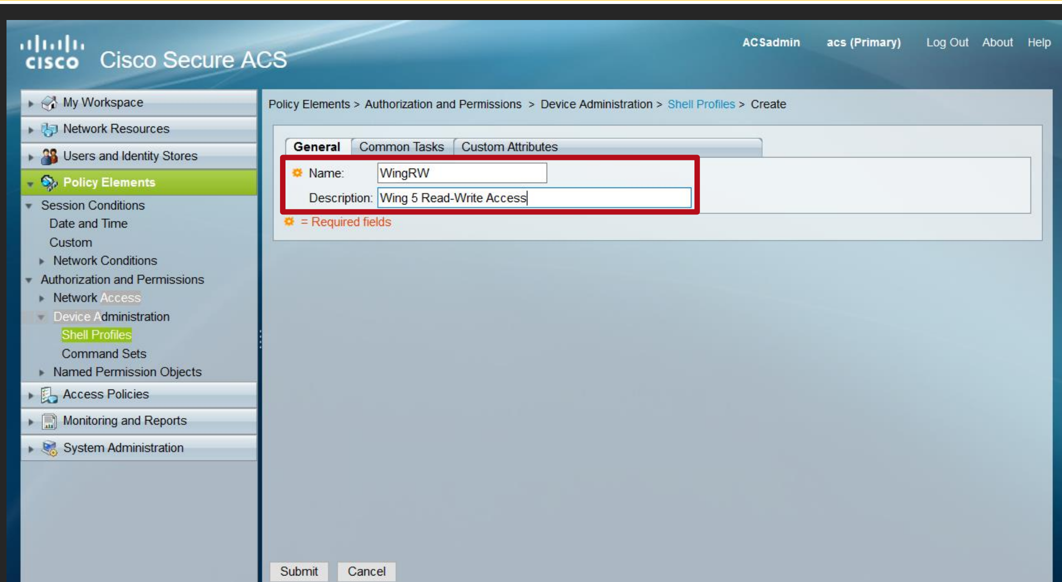
3	**In the *Common Tasks* tab set the *Maximum Privilege* to *Static* and select a value of *1*:**



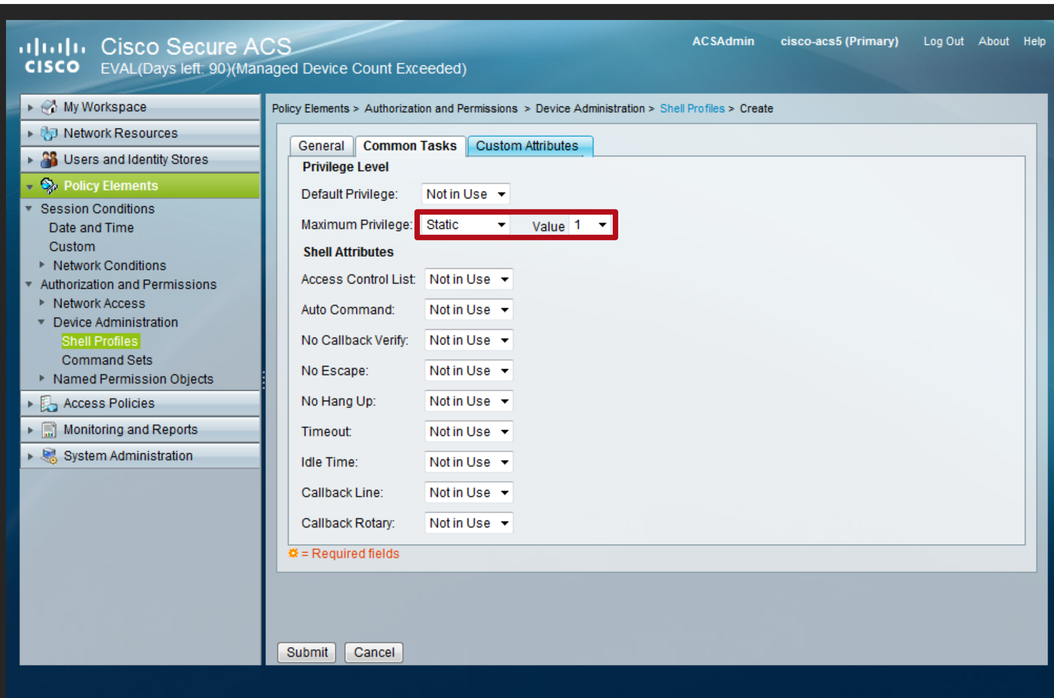
4	**In the *Custom Attributes* tab in the *Attribute* and *Attribute Value* fields, define the attributes to be assigned to the user. In this example Read Only users will be assigned to the *Monitor* role and Web access permissions. Click *Submit*:**



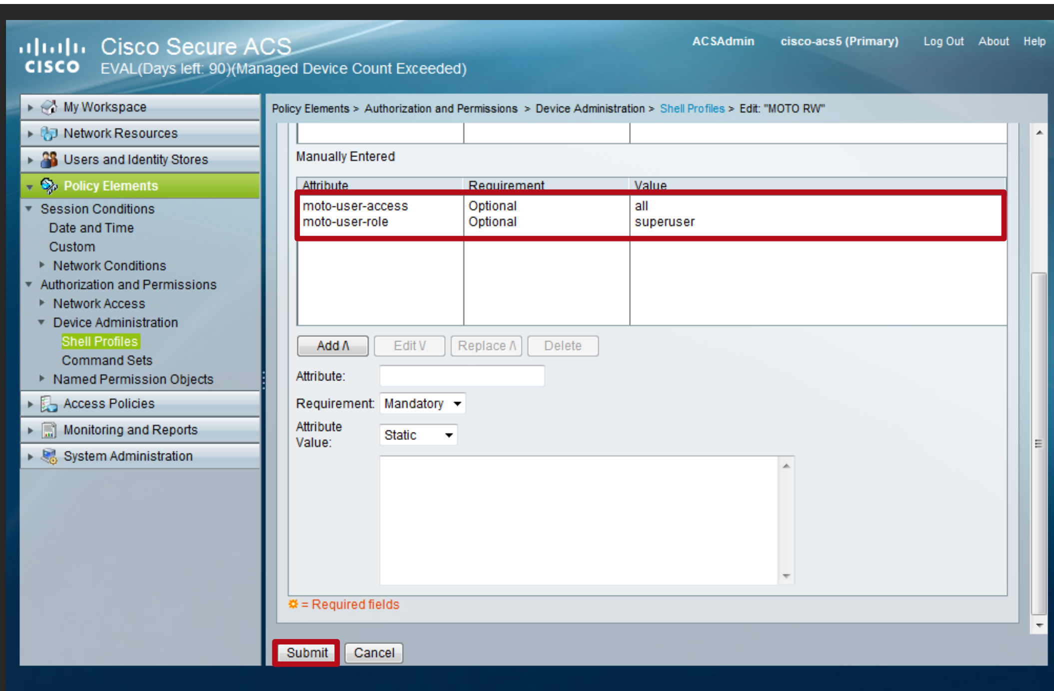
5	**Create a new *Shell Profile*. In the *General* tab define the required TACACS+ *services* and *protocols* to add. You can use existing *services* and *protocols* or create your own. The following example defines services and protocol named *MOTO RW* will be used to provide *Read Write* access into WiNG 5 devices:**



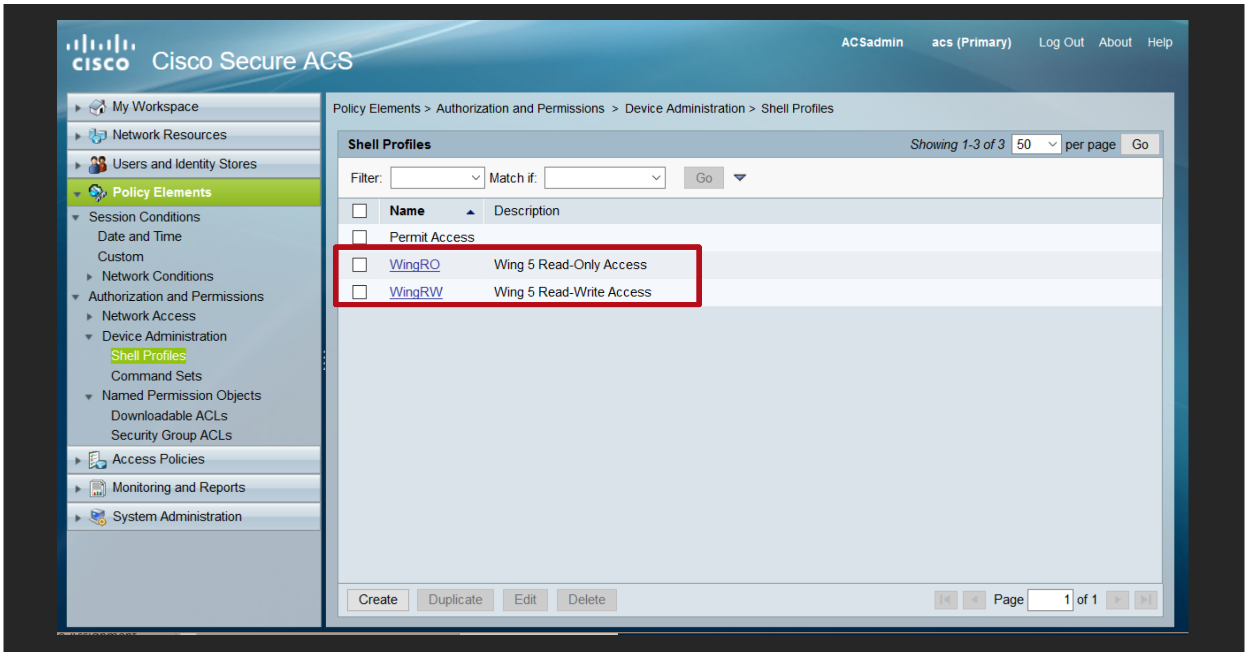
6	In the *Common Tasks* tab set the *Maximum Privilege* to *Static* and select a value of *1*:



7	In the *Custom Attributes* tab in the *Attribute* and *Attribute Value* fields, define the attributes to be assigned to the user. In this example Read Write users will be assigned to the *Superuser* role and *All* access permissions. Click *Submit*:



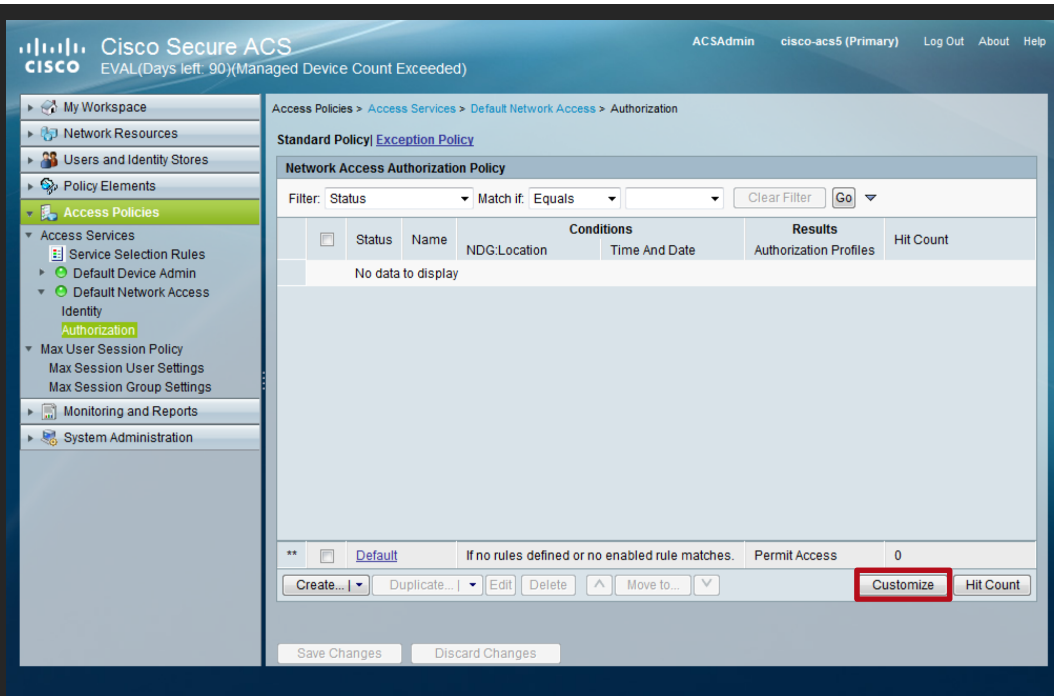
8	***Shell Profiles* named *ZebraRO* and *ZebraRW* have now been created:**



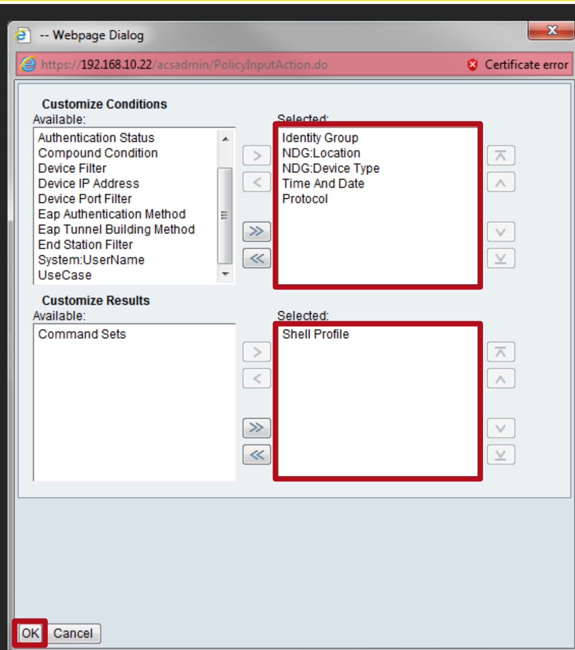
2.2.5 Device Authorization Policies

The following provides an example of how to define device authorization policies on a Cisco Secure ACS 5.x server. Device authorization policies determine the shell profile each management user is assigned based on the device type requesting authentication, location and identity group membership. In this example two device authorization policies named WingRO and WingRW will be defined.

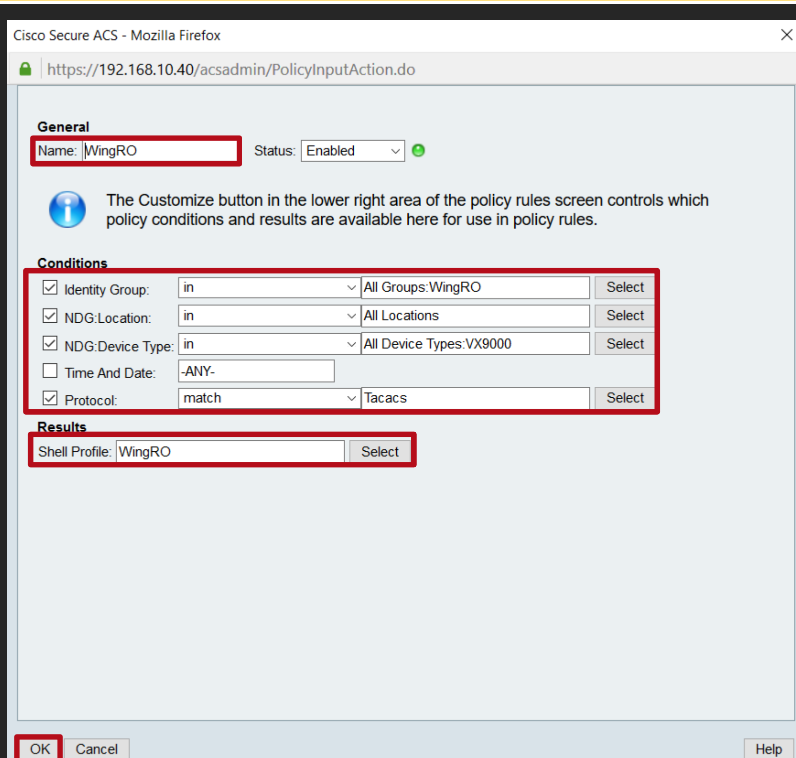
1	**Within Cisco Secure ACS select *Access Policies* → *Default Device Admin* → *Authorization* → *Customize*:**



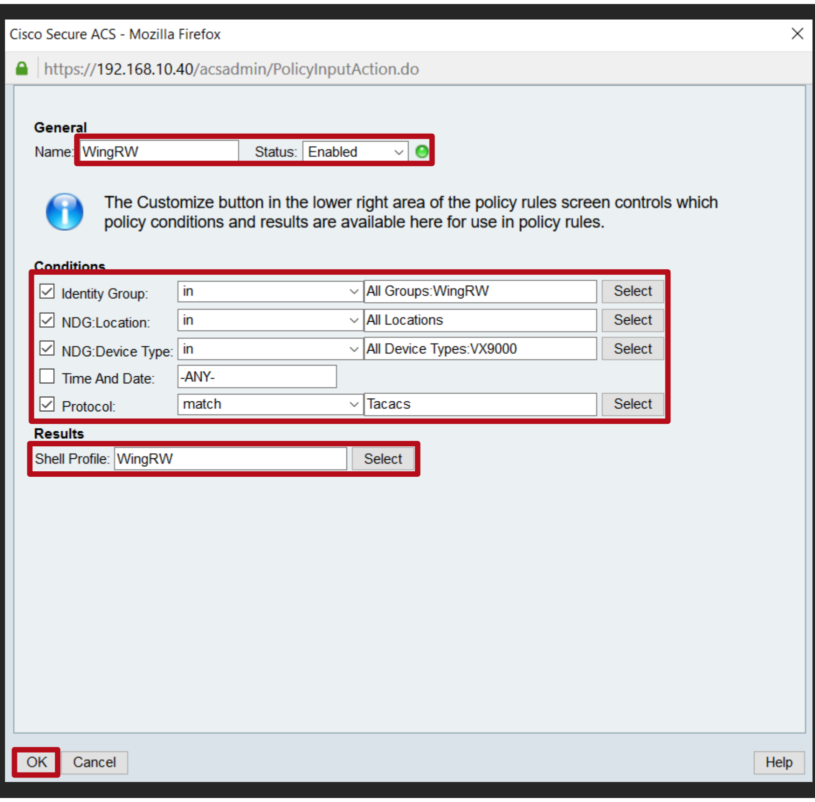
2 ***Add* the *Customize Conditions* named *Identity Group*, *NDG:Location*, *NDG: Device Type* and *Protocol*. Under *Customize Results* add *Shell Profile* then click *OK*:**



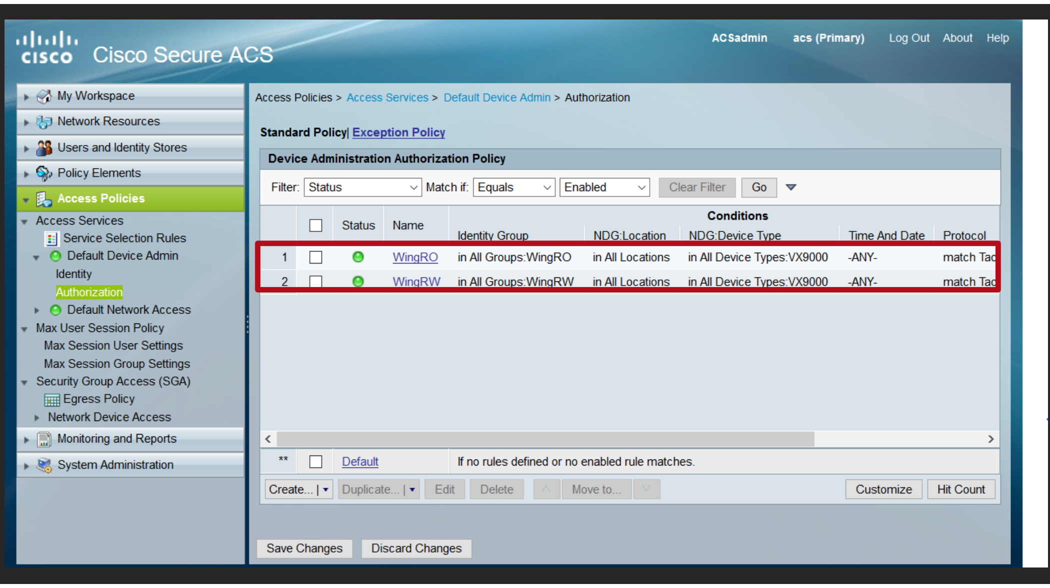
3 **Click *Create*. In the *Name* field enter *WingRO* then select the *Identity Group*, *NDG:Location* and *NDG:Device Type*. Set the *Protocol* to *Tacacs* and select the *Shell Profile* named *WingRO*. Click *OK*:**



4	**Click *Create*. In the *Name* field enter *WingRW* then select the *Identity Group*, *NDG:Location* and *NDG:Device Type*. Set the *Protocol* to *Tacacs* and select the *Shell Profile* named *WingRW*. Click *OK*:**



5	***Device Authorization Policies* named *WingRO* and *WingRW* have now been created:**



2.3 WiNG 5 Configuration

2.3.1 AAA TACACS Policies

The AAA TACACS policy defines the TACACS+ client configuration on a WiNG 5 device. Each AAA TACACS policy can contain up to 2 TACACS+ authentication, authorization and accounting server entries in addition to the names of the TACACS+ authentication service and protocols defined on the Cisco Secure ACS server. The TACACS+ AAA policy also determines the information forwarded to the accounting server.

The following AAA TACACS policy example defines a Cisco Secure ACS server for TACACS+ authentication, accounting and authorization, defines the TACACS+ services and protocols named MOTO RO and MOTO RW and enables CLI command and session accounting:

AAA TACACS Policy Example:

```
!
aaa-tacacs-policy ACS-SERVER
 authentication server 1 host 192.168.10.40 secret 0 wingsecure
 authorization server 1 host 192.168.10.40 secret 0 wingsecure
 accounting server 1 host 192.168.10.40 secret 0 wingsecure
 authentication service Wing protocol RO
 authentication service Wing protocol RW
 accounting commands
 accounting session
!
```

Figure 2.3.1 – AAA TACACS Policy Example

2.3.1.1 Configuration

The following provides the CLI commands required to create or modify a TACACS AAA policy:

aaa-tacacs-policy <policy-name>	
Description	Creates or modifies a TACACS+ authentication, accounting / authorization policy:
Parameters	▪ <policy-name> – AAA TACACS policy name

2.3.1.1.1 TACACS+ Authentication Server(s)

The following provides the supported commands and parameters for TACACS+ authentication:

authentication server <index> host <host> secret <secret> port <port>	
Description	Defines the TACACS+ authentication servers:
Parameters	▪ <index> – Server Index <1 – 2> ▪ <host> – IPv4 Address or Hostname of the server ▪ <secret> – Shared secret to be used for the server ▪ <port> – Port number on which the server is listening for the connection (default 49)
authentication server <index> retry-timeout-factor <retry>	
Description	Defines the scaling of the retry timeout for a TACACS+ authentication server:
Parameters	▪ <retry> – The scaling factor <50 – 200>. 100 implies equal timeouts between retries, smaller values indicate shorter timeouts with each successive attempt, large values indicate longer timeouts after each successive attempt
authentication server <index> timeout <timeout> <attempts>	
Description	Defines the timeout for each request sent to a TACACS+ authentication server:
Parameters	▪ <timeout> – Timeout in seconds <3 – 60> ▪ <attempts> – Number of times a request is send to the TACACS+ server <1 – 10>
authentication directed-request	
Description	Enables users to specify the TACACS+ server to use with @server. Server specified must be present in the configured list of server:
Parameters	▪ None
authentication access-method <method> <method> <method>	
Description	Determines the access methods that require TACACS+ authentication. One or more access methods to be defined:
Parameters	▪ all (default) ▪ console ▪ ssh ▪ telnet ▪ web

2.3.1.1.2 TACACS+ Authentication Service(s)

The following provides the supported commands and parameters to define TACACS+ services and protocols:

authentication service <auth-service-name> protocol <auth-protocol-name>	
Description	Defines the TACACS+ authentication service and protocol names. Note these must match the services and protocols defined on the Cisco Secure ACS server:
Parameters	▪ <auth-service-name> – TACACS+ authentication service name ▪ <auth-protocol-name> – TACACS+ authentication service protocol name

2.3.1.1.3 TACACS+ Authorization Server(s)

The following provides the supported commands and parameters for TACACS+ authorization:

authorization server <index> host <host> secret <secret> port <port>	
Description	Defines the TACACS+ authorization servers:
Parameters	▪ <index> – Server Index <1 – 2> ▪ <host> – IPv4 Address or Hostname of the server ▪ <secret> – Shared secret to be used for the server ▪ <port> – Port number on which the server is listening for the connection (default 49)
authorization server <index> retry-timeout-factor <retry>	
Description	Defines the scaling of the retry timeout for a TACACS+ authorization server:
Parameters	▪ <retry> – The scaling factor <50 – 200>. 100 implies equal timeouts between retries, smaller values indicate shorter timeouts with each successive attempt, large values indicate longer timeouts after each successive attempt
authorization server <index> timeout <timeout> <attempts>	
Description	Defines the timeout for each request sent to a TACACS+ authorization server:
Parameters	▪ <timeout> – Timeout in seconds <3 – 60> ▪ <attempts> – Number of times a request is send to the TACACS+ server <1 – 3>
authorization server preference <preference>	
Description	Defines how an authorization server from the pool is selected:
Parameters	▪ <authenticated-server-host> (default) – Prefer the same server host used for authentication. ▪ <authenticated-server-number> – Prefer the same index / number of the host used for authentication. ▪ <none> – Select an authorization server independent of which server host was used for authentication.

`authorization access-method <method>`	
Description	Determines the access methods that require TACACS+ command authorization. One or more access methods to be defined:
Parameters	▪ all ▪ console ▪ ssh ▪ telnet (default)

`authorization allow-privileged-commands`	
Description	Allows privileged commands to be executed without command authorization:
Parameters	▪ None

2.3.1.1.4 TACACS+ Accounting Server(s)

The following provides the supported commands and parameters for TACACS+ accounting:

`accounting server <index> host <host> secret <secret> port <port>`	
Description	Defines the TACACS+ accounting servers:
Parameters	▪ <index> – Server Index <1 – 2> ▪ <host> – IPv4 Address or Hostname of the server ▪ <secret> – Shared secret to be used for the server ▪ <port> – Port number on which the server is listening for the connection (default 49)

`accounting server <index> retry-timeout-factor <retry>`	
Description	Defines the scaling of the retry timeout for a TACACS+ accounting server:
Parameters	▪ <retry> – The scaling factor <50 – 200>. 100 implies equal timeouts between retries, smaller values indicate shorter timeouts with each successive attempt, large values indicate longer timeouts after each successive attempt

`accounting server <index> timeout <timeout> <attempts>`	
Description	Defines the timeout for each request sent to a TACACS+ accounting server:
Parameters	▪ <timeout> – Timeout in seconds <3 – 60> ▪ <attempts> – Number of times a request is send to the TACACS+ server <1 – 3>

accounting server preference <preference>	
Description	Defines how an accounting server from the pool is selected:
Parameters	▪ <authenticated-server-host> (default) – Prefer the same server host used for authentication. ▪ <authenticated-server-number> – Prefer the same index / number of the host used for authentication. ▪ <authorized-server-host> – Prefer the same server host used for authorization. ▪ <authorized-server-number> – Prefer the same index / number of the host used for authorization. ▪ None – Select an accounting server independent of which server host was used for authentication or authorization.
accounting access-method <method>	
Description	Determines the access methods that require TACACS+ accounting. One or more access methods to be defined:
Parameters	▪ all (all) ▪ console ▪ ssh ▪ telnet
accounting auth-fail	
Description	Enables accounting for authentication fail details:
Parameters	▪ None
accounting commands	
Description	Enables accounting for CLI commands:
Parameters	▪ None
accounting session	
Description	Enables accounting for session start and stop details:
Parameters	▪ None

2.3.2 Management Polices

Once an AAA TACACS policy has been defined, it must be assigned to one or more Management policies before TACACS+ can be utilized. Management policies determine the management interfaces that are enabled on each WiNG 5 device, local administrative users, roles and access permissions and external RADIUS or TACACS+ servers used to authenticate administrative users.

By default each WiNG 5 device is assigned to a Management policy named ***default*** which is assigned using profiles. TACACS+ can be enabled on the default Management policy or any user defined Management policy.

Most typical deployments will include separate Management policies for Wireless Controllers and Access Points. Separate Management policies are recommended as the management requirements and interfaces for each device differ. In this case to enable TACACS+ on both Wireless Controllers and Access Points, TACACS+ will need to be enabled on each Management policy.

The following Management policy examples enable TACACS+ authentication, authorization and accounting on user defined Management policies assigned to Wireless Controllers and Access Points. TACACS+ fallback to local authentication is also enabled in the event of a WiNG 5 device cannot reach any defined TACACS+ servers for authentication:

Management Policy Examples:

```
!
management-policy CONTROLLER-MANAGEMENT
 no http server
 https server
 ssh
 user admin password 0 wingsecure role superuser access all
 snmp-server user snmptrap v3 encrypted des auth md5 0 wingsecure
 snmp-server user snmpoperator v3 encrypted des auth md5 0 wingsecure
 snmp-server user snmpmanager v3 encrypted des auth md5 0 wingsecure
 aaa-login tacacs fallback
 aaa-login tacacs authorization
 aaa-login tacacs accounting
 aaa-login tacacs policy ACS-SERVER
!
```

```
!
management-policy AP-MANAGEMENT
 ssh
 user admin password 0 wingsecure role superuser access all
 aaa-login tacacs fallback
 aaa-login tacacs authorization
 aaa-login tacacs accounting
 aaa-login tacacs policy CISCO-ACS-SERVER
!
```

Figure 2.3.2 – Management Policy Examples

2.3.2.1 Configuration

The following provides the CLI commands required to create or modify a Management Policy:

Management-policy <policy-name>	
Description	Creates or modifies a Management policy:
Parameters	▪ <policy-name> – Management policy name

2.3.2.1.1 AAA Login

The following provides the supported commands and parameters to enable TACACS authentication, authorization and accounting within a Management policy:

aaa-login tacacs accounting	
Description	Enables TACACS+ accounting for WiNG 5 devices assigned to the Management Policy:
Parameters	▪ None
aaa-login tacacs authentication	
Description	Enables TACACS+ authentication for WiNG 5 devices assigned to the Management Policy:
Parameters	▪ None
aaa-login tacacs authorization	
Description	Enables TACACS+ authorization for WiNG 5 devices assigned to the Management Policy:
Parameters	▪ None
aaa-login tacacs fallback	
Description	Enables fallback to local authentication if TACACS+ authentication fails.
Parameters	▪ None
aaa-login tacacs policy <aaa-tacacs-policy>	
Description	Assigns the AAA TACACS policy to the Management policy.
Parameters	▪ None

2.4 Verification

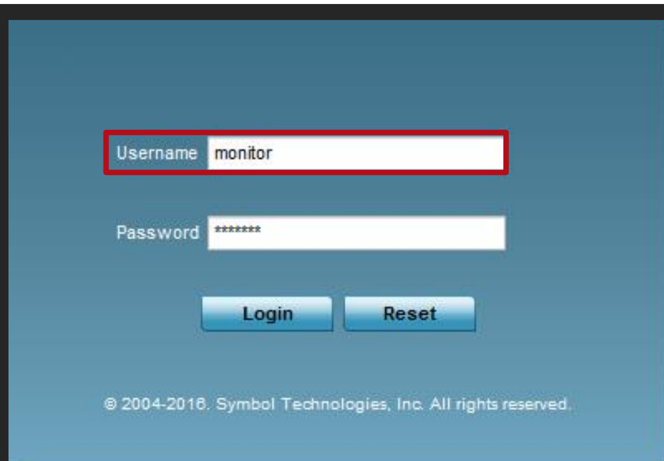
The following provides the necessary steps required to validate TACACS+ authentication, authorization and accounting. In this example two user accounts have been defined on each Cisco Secure ACS server and assigned to the appropriate groups. The users group membership determines the role and access permissions assigned to the management user.

Username	Role	Access Permissions
monitor	monitor	Web
superuser	superuser	All

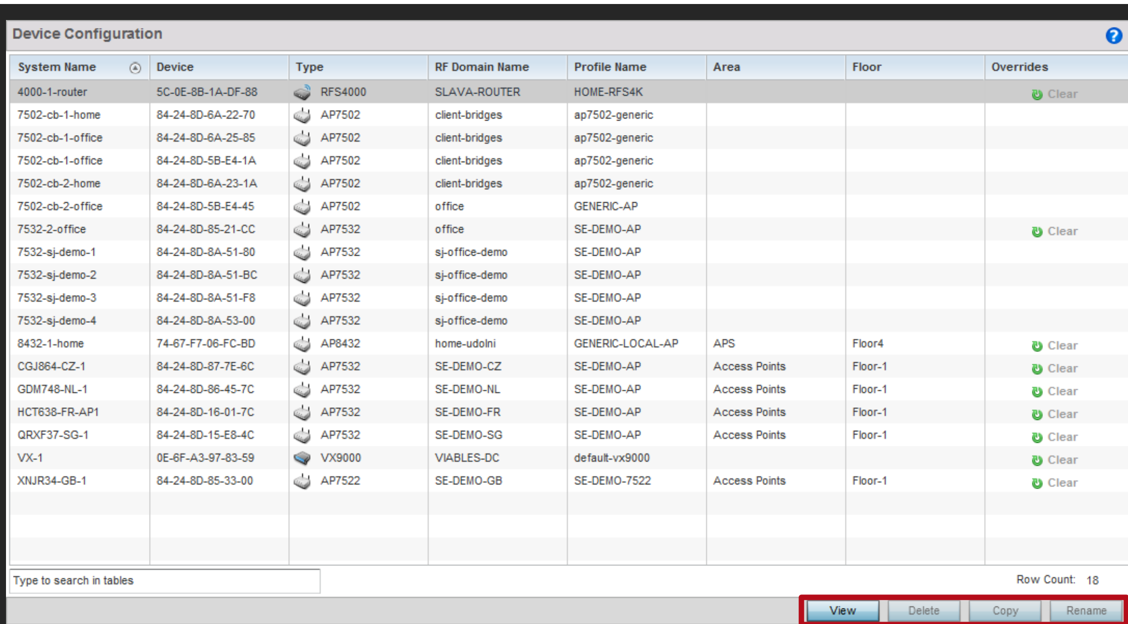
2.4.1 Role Assignment

The following provides the verification steps required to verify authentication and role assignments:

1	Using the Web UI, login to the Wireless Controller using the *monitor* username and password:



2	**The user will be authenticated, authorized and assigned to the *Monitor* role which provides read-only access on the Wireless Controller. Select *Configuration* → *Devices* and attempt to edit a device. Notice no edit functionality is available as the user is only permitted read-only access on the device:**

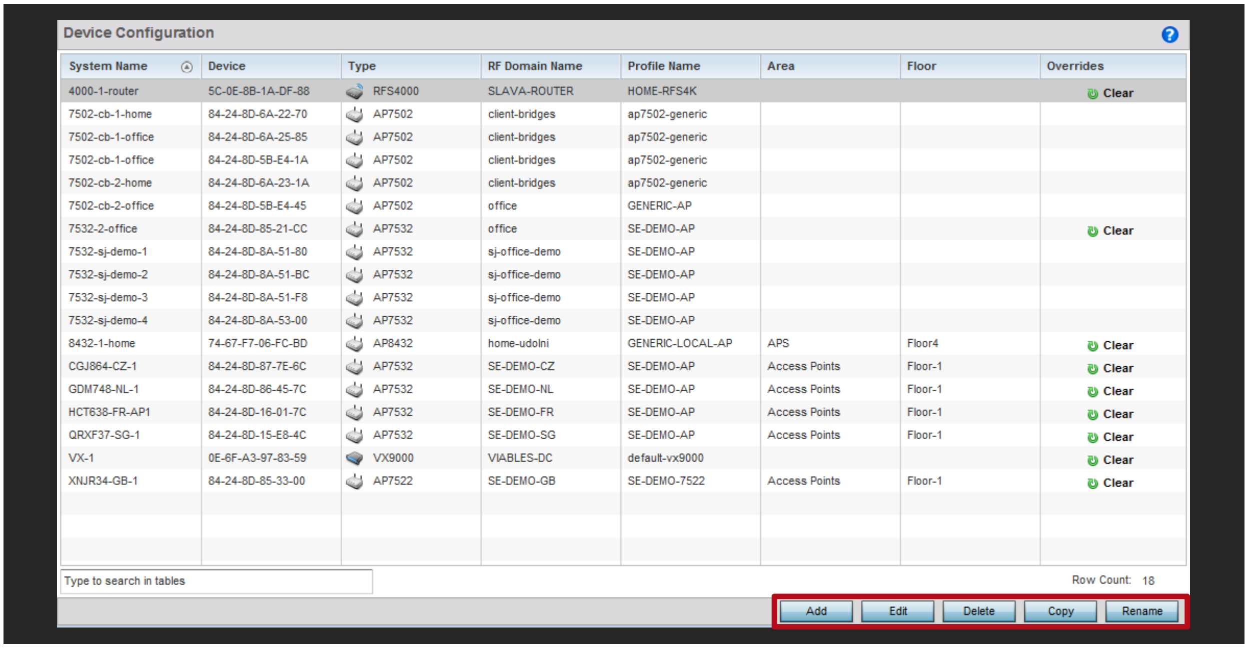


Device Configuration

System Name	Device	Type	RF Domain Name	Profile Name	Area	Floor	Overrides
4000-1-router	5C-0E-8B-1A-DF-88	RFS4000	SLAVA-ROUTER	HOME-RFS4K			Clear
7502-cb-1-home	84-24-8D-6A-22-70	AP7502	client-bridges	ap7502-generic			
7502-cb-1-office	84-24-8D-6A-25-85	AP7502	client-bridges	ap7502-generic			
7502-cb-1-office	84-24-8D-5B-E4-1A	AP7502	client-bridges	ap7502-generic			
7502-cb-2-home	84-24-8D-6A-23-1A	AP7502	client-bridges	ap7502-generic			
7502-cb-2-office	84-24-8D-5B-E4-45	AP7502	office	GENERIC-AP			
7532-2-office	84-24-8D-85-21-CC	AP7532	office	SE-DEMO-AP			Clear
7532-sj-demo-1	84-24-8D-8A-51-80	AP7532	sj-office-demo	SE-DEMO-AP			
7532-sj-demo-2	84-24-8D-8A-51-BC	AP7532	sj-office-demo	SE-DEMO-AP			
7532-sj-demo-3	84-24-8D-8A-51-F8	AP7532	sj-office-demo	SE-DEMO-AP			
7532-sj-demo-4	84-24-8D-8A-53-00	AP7532	sj-office-demo	SE-DEMO-AP			
8432-1-home	74-67-F7-06-FC-BD	AP8432	home-udolni	GENERIC-LOCAL-AP	APS	Floor4	Clear
CGJ864-CZ-1	84-24-8D-87-7E-6C	AP7532	SE-DEMO-CZ	SE-DEMO-AP	Access Points	Floor-1	Clear
GDM748-NL-1	84-24-8D-86-45-7C	AP7532	SE-DEMO-NL	SE-DEMO-AP	Access Points	Floor-1	Clear
HCT638-FR-AP1	84-24-8D-16-01-7C	AP7532	SE-DEMO-FR	SE-DEMO-AP	Access Points	Floor-1	Clear
QRXF37-SG-1	84-24-8D-15-E8-4C	AP7532	SE-DEMO-SG	SE-DEMO-AP	Access Points	Floor-1	Clear
VX-1	0E-6F-A3-97-83-59	VX9000	VIABLES-DC	default-vx9000			Clear
XNJR34-GB-1	84-24-8D-85-33-00	AP7522	SE-DEMO-GB	SE-DEMO-7522	Access Points	Floor-1	Clear

3	**Using the Web UI, login to the Wireless Controller using the *superuser* username and password:**

4	**The user will be authenticated, authorized and assigned to the *Superuser* role which provides full access on the Wireless Controller. Select *Configuration → Devices* and attempt to edit a device. Notice the edit functionality is now available as the user is only permitted full access on the device:**



Device Configuration

System Name	Device	Type	RF Domain Name	Profile Name	Area	Floor	Overrides
4000-1-router	5C-0E-8B-1A-DF-88	RFS4000	SLAVA-ROUTER	HOME-RFS4K			Clear
7502-cb-1-home	84-24-8D-6A-22-70	AP7502	client-bridges	ap7502-generic			
7502-cb-1-office	84-24-8D-6A-25-85	AP7502	client-bridges	ap7502-generic			
7502-cb-1-office	84-24-8D-5B-E4-1A	AP7502	client-bridges	ap7502-generic			
7502-cb-2-home	84-24-8D-6A-23-1A	AP7502	client-bridges	ap7502-generic			
7502-cb-2-office	84-24-8D-5B-E4-45	AP7502	office	GENERIC-AP			
7532-2-office	84-24-8D-85-21-CC	AP7532	office	SE-DEMO-AP			Clear
7532-sj-demo-1	84-24-8D-8A-51-80	AP7532	sj-office-demo	SE-DEMO-AP			
7532-sj-demo-2	84-24-8D-8A-51-BC	AP7532	sj-office-demo	SE-DEMO-AP			
7532-sj-demo-3	84-24-8D-8A-51-F8	AP7532	sj-office-demo	SE-DEMO-AP			
7532-sj-demo-4	84-24-8D-8A-53-00	AP7532	sj-office-demo	SE-DEMO-AP			
8432-1-home	74-67-F7-06-FC-BD	AP8432	home-udolni	GENERIC-LOCAL-AP	APS	Floor4	Clear
CGJ864-CZ-1	84-24-8D-87-7E-6C	AP7532	SE-DEMO-CZ	SE-DEMO-AP	Access Points	Floor-1	Clear
GDM748-NL-1	84-24-8D-86-45-7C	AP7532	SE-DEMO-NL	SE-DEMO-AP	Access Points	Floor-1	Clear
HCT638-FR-AP1	84-24-8D-16-01-7C	AP7532	SE-DEMO-FR	SE-DEMO-AP	Access Points	Floor-1	Clear
QRXF37-SG-1	84-24-8D-15-E8-4C	AP7532	SE-DEMO-SG	SE-DEMO-AP	Access Points	Floor-1	Clear
VX-1	0E-6F-A3-97-83-59	VX9000	VIABLES-DC	default-vx9000			Clear
XNJR34-GB-1	84-24-8D-85-33-00	AP7522	SE-DEMO-GB	SE-DEMO-7522	Access Points	Floor-1	Clear

Type to search in tables

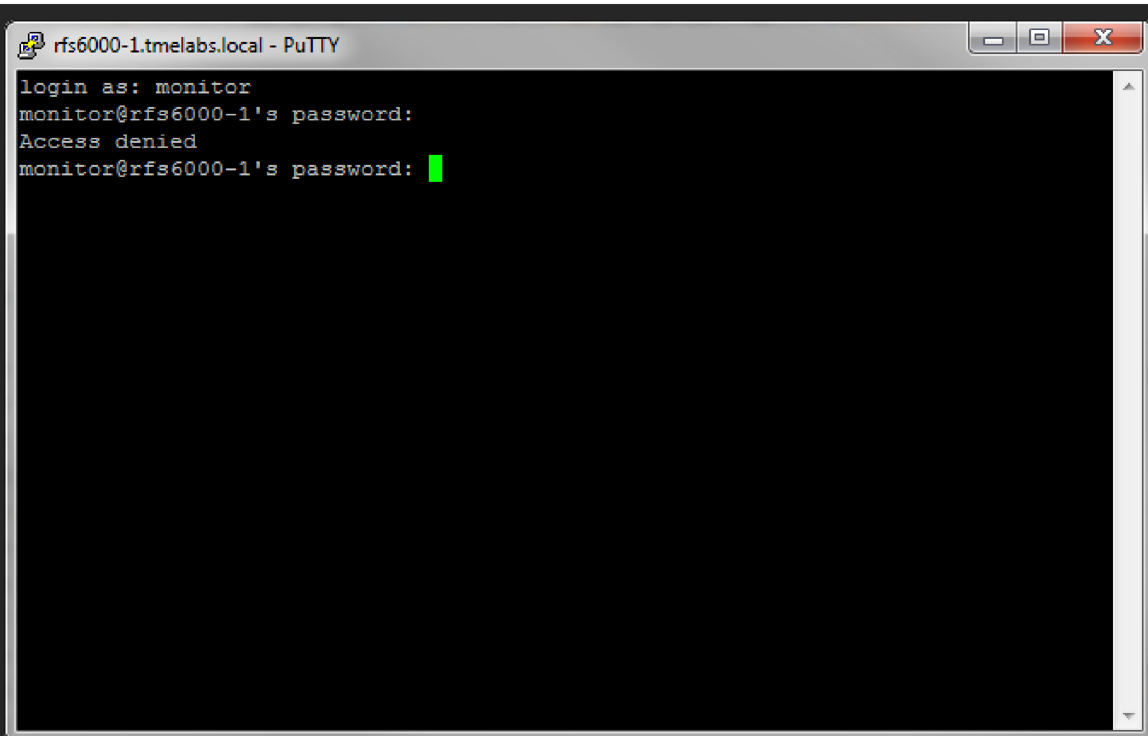
Row Count: 18

Add Edit Delete Copy Rename

2.4.2 Access Permissions

The following provides the verification steps required to verify access permissions:

1	**Using PuTTy initiate a SSH session to the Wireless Controller and attempt to login using the *monitor* username and password. You will see an Access denied message from the Wireless Controller:**



2	**Using the CLI on the Wireless Controller, issue a *show event-history* command. This will display details the login events and will provide the reason for why the connection was refused. In this example the connection was refused due to the monitor user not being permitted access from the SSH management interface:**

```
rfs6000-1# show event-history
```

```
2012-04-17 15:23:27     rfs6000-1  SYSTEM     LOGIN_FAIL            Log-in failed for User:
'monitor' from 'ssh'
2012-04-17 15:23:27     rfs6000-1  SYSTEM     LOGIN_FAIL_ACCESS     Log-in failed - User:
'monitor' is not allowed access from 'ssh'
2012-04-17 15:23:20     rfs6000-1  SYSTEM     LOGIN_FAIL            Log-in failed for User:
'monitor' from 'ssh'
2012-04-17 15:23:20     rfs6000-1  SYSTEM     LOGIN_FAIL_ACCESS     Log-in failed - User:
'monitor' is not allowed access from 'ssh'
```

2.4.3 CLI Command Accounting

The following provides the verification steps required on the Cisco Secure ACS server to verify TACACS+ CLI command accounting.

2.4.3.1 Cisco Secure ACS 4.X

1	**Within Cisco Secure ACS select *Reports and Activity → TACACS+ Administration*. TACACS+ CLI command accounting records forwarded from the Wireless Controller will be displayed. Accounting records can also be exported to CSV:**

Date	Time	User-Name	Group-Name	cmd	priv-lvl	service	NAS-Portname	task_id	NAS-IP-Address	reason
04/17/2012	14:39:31	superuser	Motorola - ReadWrite	show running-config <cr>	1	shell	con	18	192.168.20.22	..
04/17/2012	14:39:28	superuser	Motorola - ReadWrite	end <cr>	1	shell	con	18	192.168.20.22	..
04/17/2012	14:14:26	superuser	Motorola - ReadWrite	show context <cr>	1	shell	con	18	192.168.20.22	..
04/17/2012	14:14:25	superuser	Motorola - ReadWrite	management-policy tmelabs <cr>	1	shell	con	18	192.168.20.22	..
04/17/2012	14:14:23	superuser	Motorola - ReadWrite	configure terminal <cr>	1	shell	con	18	192.168.20.22	..
04/17/2012	14:14:22	superuser	Motorola - ReadWrite	enable <cr>	1	shell	con	18	192.168.20.22	..
04/17/2012	13:21:10	superuser	Motorola - ReadWrite	rf-domain tmelabs <cr>	1	shell	con	17	192.168.20.22	..
04/17/2012	13:21:06	superuser	Motorola - ReadWrite	configure terminal <cr>	1	shell	con	17	192.168.20.22	..
04/17/2012	13:21:05	superuser	Motorola - ReadWrite	enable <cr>	1	shell	con	17	192.168.20.22	..
04/17/2012	12:41:54	admin	Default Group	exit <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	12:41:53	admin	Default Group	show context include-factory <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	12:34:16	admin	Default Group	show context <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	12:34:14	admin	Default Group	exit <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	12:34:12	admin	Default Group	rf-domain tmelabs <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	12:10:32	admin	Default Group	exit <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	11:57:21	admin	Default Group	show context include-factory <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	11:33:58	admin	Default Group	show context include-factory <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	11:33:57	admin	Default Group	aaa-tacacs-policy CISCO-ACS-SERVER <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	11:33:54	admin	Default Group	configure terminal <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	11:33:52	admin	Default Group	end <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	11:15:17	admin	Default Group	show context <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	11:11:37	admin	Default Group	exit <cr>	1	shell	con	12	192.168.20.22	..
04/17/2012	11:11:35	admin	Default Group	help search aaa-tacacs-policy <cr>	1	shell	con	12	192.168.20.22	..

2.4.3.2 Cisco Secure ACS 5.X

1	**Within Cisco Secure ACS 5.X select *Monitoring and Reports* → *Launch Monitoring & Report Viewer*. Select *Reports* → *Catalog* → *AAA Protocol* → *TACACS Accounting* → *Run*. TACACS+ CLI command accounting records forwarded from the Wireless Controller will be displayed. Accounting records can also be exported to CSV:**