Virtual Services Platform

4000 / 8000 / 9000

Engineering

> Management Access Security Technical Configuration Guide

Avaya Networking

Document Date: April 2015

Document Number: NN48500-650

Document Version: 1.1

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http:// www.avaya.com/support.

Abstract

This document provides examples on configuring various items related to accessing the VSP 4000 / 8000 / 9000 securely for management purposes. This document covers accessing the switch using Telnet, HTTP, SSL, SSH, and SNMP.

Revision Control

Version	Date	Revised By	Remarks
Draft 1	3/16/2015	John Vant Erve Jeff Cox	Initial Draft
Draft 2	4/3/2015	Didier Ducarre	Review
Draft 3	4/9/2015	Ludovico Stevens	Review and reworked SSH and SNMP sections
Draft 4	4/13/2015	Rob Tyler	Update SSH section
Draft 5	4/13/2015	John Vant Erve Jeff Cox	Final version
Draft 6	4/16/2015	Ludovico Stevens Rob Tyler	Updates to SSH section 6 and 8.3

Table of Contents

Figures 7
Tables 8
1. Overview 10
2. Enabling or Disabling Access Services via Boot Configuration Flags 10
2.1 Enhanced Secure Mode 11
2.1.1 Enhanced Security Password Requirements 12
2.1.2 Enhanced Security Configuration 12
3. Local password protection 17
3.1 CLI Password Protection 17
3.1.1 User Names and Passwords 18
3.1.2 Enabling or Disabling Access Levels 18
3.3 High Secure (hsecure) Mode 20
3.3.1 Access Level Options – hsecure mode 20
3.4 CLI Logging 21
3.5 CLI Prompt 21
3.6 Login message and password prompt 21
3.7 Telnet Access Configuration Examples using Local Users with hsecure disabled 22
3.7.1 Local Password Configuration - Password Security Disabled 22
3.7.2 Verify Operations 23
4. Password Protection using RADIUS Authentication 24
4.1 Enabling RADIUS globally 26
4.2 Adding RADIUS server for authentication 26
4.3 CLI Profile 27
4.4 Enabling RADIUS accounting globally 27
4.5 Enabling accounting for CLI commands 27
4.6 RADIUS Password Configuration Example 28
4.6.1 Ethernet Routing Switch Configuration 28
4.6.2 VSP Switch: Verify Operations 29
4.6.3 IDE RADIUS Configuration 31
4.6.4 Verify Operations 52
5. Password Protection using TACACS+ Authentication 56
5.1 Enabling TACACS+ globally 58
5.2 Changing TACACS+ user levels 58
5.3 TACACS+ Configuration Example 59

5.3.1 VSP Switch Configuration 59
5.3.2 Verify Operations 59
5.3.3 IDE TACACS+ Configuration 61
5.4 TACACS+ Configuration Example with Command Restrictions 65
5.4.1 VSP Switch Configuration 66
5.4.2 IDE TACACS+ Configuration 67
5.4.3 Verify Operations 76
6. Secure Shell (SSH) and SFTP/SCP 78
6.1 SSH Configuration Example – Password Authentication 82
6.1.1 Configuration 82
6.1.2 Verify Operations 85
6.2 SSH Configuration Example –Public Key Authentication 86
6.2.1 Configuration 86
6.2.2 Verify Operations 94
7. WEB Access – Enterprise Device Manager 95
7.1 EDM configuration Example 96
7.1.1 Configuration 96
7.1.2 Verify Operations 100
8. SNMP 101
8.1 SNMPv3 Overview 101
8.2 Blocking SNMP 102
8.3 Blocking SNMPv1/2 only 102
8.4 Community Strings 103
8.4.1 Displaying the default Community Strings 104
8.5 Adding a new Community String 105
8.6 Deleting Community Strings 105
8.7 Community Strings – Virtual Routers 106
8.8 Community String Configuration Example: Allowing only read-only access using the default community strings 107
8.8.1 Configuration 107
8.8.2 Verify Operations 107
8.9 Configuration Example: Changing the Default SNMP Community Names 108
8.9.1 Configuration 108
8.9.2 Verify Operations 108
8.10 Configuration Example: Adding additional SNMP community strings 109
8.10.1 Configuration 109
8.10.2 Verify Operations 109

8.11 Creating a MIB View 110
8.12 Configuration Example – Adding a new SNMP MIB view 111
8.12.1 Configuration 111
8.12.2 Verify Operations 111
8.13 SNMPv3 Configuration Steps 112
8.13.1 Loading the DES or AES Encryption Module 112
8.13.2 Adding a New SNMPv3 User 112
8.13.3 Adding USM Group 113
8.14 SNMPv3 Configuration Example 115
8.14.1 Configuration 115
8.14.2 Verify Operations 116
8.15 SNMP Traps 119
8.15.1 Trap Receivers 119
8.16 SNMPv1 Trap Configuration Example 120
8.16.1 Configuration 120
8.16.2 Verify Operations 120
9. Access Policy 123
9.1 Enable Access Polices Globally 123
9.2 Adding an Access Policy 124
9.3 Access Policies and SNMP 126
9.4 Access Policy Configuration Example – Adding SNMPv1/2c, SSH, FTP, and TELNET Services 127
9.4.1 Configuration 127
9.4.2 Verify Operations 129
9.5 Access Policy Configuration Example – limit SNMPv3 to specific host and Telnet Access to a specific network 132
9.5.1 Configuration 132
9.5.2 Verify Operations 134
10. Reference Documentation 137

Figures

Figure 1: SNMPv3 USM 101
Figure 2: MIB Structure 110

Tables

Table 1: Enhanced User Levels 11
Table 2: Default User Names and Password 17
Table 3: RADIUS Features 24
Table 4: RADIUS Attributes 24
Table 5: Enhanced Security RADIUS Attributes 25
Table 6: RADIUS Events Logged 25
Table 7: TACACS+ Access Levels 56
Table 8: Enhanced Security TACACS+ Attributes 56
Table 9: SSH clients 78
Table 10: DSA authentication access level and file name 79
Table 11: RSA authentication access level and file name 81
Table 12: Navigation pane buttons 98
Table 13: Navigation tree folders 98

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols

Tip – Highlights a configuration or technical tip.

Note – Highlights important information to the reader.

Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

```
ERS5520-48T# show running-config
```

Output examples from Avaya devices are displayed in a Lucida Console font:

```
ERS5520-48T# show sys-info

Operation Mode:          Switch
MAC Address:             00-12-83-93-B0-00
PoE Module FW:           6370.4
Reset Count:             83
Last Reset Type:         Management Factory Reset
Power Status:            Primary Power
Autotopology:            Enabled
Pluggable Port 45:       None
Pluggable Port 46:       None
Pluggable Port 47:       None
Pluggable Port 48:       None
Base Unit Selection:     Non-base unit using rear-panel switch
sysDescr:                Ethernet Routing Switch 5520-48T-PWR
                         HW:02       FW:6.0.0.10  SW:v6.2.0.009
                         Mfg Date:12042004    HW Dev:H/W rev.02
```

1. Overview

This document provide a guide on how to configure various items related to access security for management purposes on the Virtual Services Platform switch.

2. Enabling or Disabling Access Services via Boot Configuration Flags

You can enable or disable access services by setting boot configuration flags from the Run-Time CLI.

To enable or disabled access services by setting the boot configuration flags, enter the following commands.

```
VSPswitch:1(config)#boot config flags block-snmp
VSPswitch:1(config)#no boot config flags block-snmp
VSPswitch:1(config)#boot config flags ftpd
VSPswitch:1(config)#no boot config flags ftpd
VSPswitch:1(config)#boot config flags rlogind
VSPswitch:1(config)#no boot config flags rlogind
VSPswitch:1(config)#boot config flags sshd
VSPswitch:1(config)#no boot config flags sshd
VSPswitch:1(config)#boot config flags telnetd
VSPswitch:1(config)#no boot config flags telnetd
VSPswitch:1(config)#boot config flags tftpd
VSPswitch:1(config)#no boot config flags tftpd
```

To view the current boot configuration file settings, enter either of the following commands.

```
VSPswitch:1(config)#show boot config flags
VSPswitch:1#more /intflash/config.cfg
```

2.1 Enhanced Secure Mode

The switch supports a configurable flag called enhanced secure. After you enable the new *boot config flags enhancedsecure-mode*, enhanced secure mode allows the system to provide role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use.

The VSP switch does not support the default SNMPv1 and SNMPv2 community strings, and default SNMPv3 user name. The individual in the administrator access level role can configure a non-default value for the community strings, and the VSP switch can continue to support SNMPv1 and SNMPv2. The individual in the administrator access level role can also configure a non-default value for the SNMPv3 user name and the VSP switch can continue to support SNMPv3. If you disable enhanced secure mode, the SNMPv1 and SNMPv2 support for community strings remains the same, and the default SNMPv3 user name remains the same.

After you enable enhanced secure mode, the switch supports role-based authentication levels. With enhanced secure mode enabled, the switch supports the following authentication access levels for local authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+) authentication:

- Administrator
- Privilege
- Operator
- Auditor
- Security

Each username is associated with a certain role in the product and appropriate authorization rights for viewing and executing commands are available for that role.

Table 1: Enhanced User Levels

Access level	Description	Login location
Administrator	The administrator access level permits all read-write access, and can change security settings. The administrator access level can configure ACLI and web-based management user names, passwords, and the SNMP community strings. The administrator access level can also view audit logs.	SSH/Telnet (in band/mgmt)/ console
Privilege	The privilege access level has the same access permission as the administrator; however, the privilege access level cannot use RADIUS or TACACS+ authentication. The system must authenticate the privilege access level within the VSP switch at a console level. The privilege access level is also known as emergency-admin.	Console
Operator	The operator access level can view most switch configurations and status information. The operator access level can change physical port settings at layer 2 and layer 3. The operator	SSH/Telnet (in band/mgmt)/ console/

	access level cannot access audit logs or security settings	
Auditor	The auditor access level can view configuration information, status information, and audit logs.	SSH/Telnet (in band/mgmt)/ console/
Security	The security access level can change security settings only. The security access level also has permission to view configuration and status information.	SSH/Telnet (in band/mgmt)/ console/

2.1.1 Enhanced Security Password Requirements

After enabling enhanced security mode on the switch, you will be able to login for the first time using a user name and password of admin/admin and then will be prompted to change both the user name and password. The password for the admin user must be 15 characters and made up of two of the following characters:

- Two uppercase character, from the range: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Two lowercase character, from the range: abcdefghijklmnopqrstuvwxyz
- Two numeric character, from the range: 1234567890
- Two special character, from the range: `~!@#$%^&*()_-+={[}]|\:;”’<,>.?/

Please note the above requirement applies only to the administrator user.

2.1.2 Enhanced Security Configuration

Enable enhanced secure mode and reboot switch

```
VSPswitch:1(config)#boot config flags enhancedsecure-mode
Warning: Enhancedsecure-mode flag is enabled
Warning: Please save configuration and reboot the switch
         for this to take effect.
VSPswitch:1(config)#save config
VSPswitch:1(config)#reset -y
```

After the switch reboots, login using the initial administrator user name and password of admin/admin and then change user name and use a password made up of 15 characters total using the requirements as outlined in section 2.1.1.

```
Copyright(c) 2010-2015 Avaya, Inc.
All Rights Reserved.
Virtual Services Platform 8200
VSP Operating System Software Build 4.2.0.0_B015 (PRIVATE)
Built: Thu Mar 12 18:18:49 EDT 2015
```

```
Unsupported Software, Internal Use Only

AVAYA COMMAND LINE INTERFACE

Login: admin
Password: admin


        This is an initial attempt using the default user name and password.
        Please change the user name and password to continue.

Enter the new name : rwa
Enter the New password : Admin@!Jvelab123
Re-enter the New password : Admin@!Jvelab123
8202:1>en
8202:1#show cli password
        change-interval 24
        min-passwd-len 8
        password-history 3

        password-rule 1 1 1 1

        pre-expiry-notification-interval 1 7 30
        post-expiry-notification-interval 1 7 30
        access-level
        ACCESS          LOGIN       AGING  MAX-SESSIONS  STATE
        admin           rwa         90     3             ena
        privilege                   90     3             dis
        operator                    90     3             dis
        security                    90     3             dis
        auditor                     90     3             dis
        Default Lockout Time         60
        Lockout-Time:
```

Please note the min-passwd-len and password-rule as shown above applies to all user except for the administrator user

Adding a new temporary user name and password via the administrator access level.

A user in the administrator access role can configure a temporary user name and password. After this user logs in for the first time with the temporary user name and password, the system will force the user to change the temporary user name and password. After you change the temporary user name and password, you cannot use them again in subsequent sessions.

```
VSPswitch:1(config)#password create-user <auditor|operator|privilege|security> <user name>

VSPswitch:1(config)#password create-user operator user1

## After user1 logs in, the user will be prompted to enter a new user name and
password. Note, you cannot use the same user name or password as that temporarily
configured.

Login: user1

Password: **********


        This is an initial attempt using the default user name and password.

        Please change the user name and password to continue.


Enter the new name : userabcd

Enter the New password : ************

Re-enter the New password : ************
```

Please note the privilege user can only be changed via the console port.

Password aging – default is 90 days

```
VSPswitch:1(config)#password aging-time day <1-365> user <user name>
```

Password change interval – default is 24 hours. This is the minimum time before you can change to a new password.

```
VSPswitch:1(config)#password change-interval <1-999>
```

Password length – default is 15 total characters

```
VSPswitch:1(config)#password min-passwd-len <8-32>
```

Password maximum sessions – default is 3 per user name

```
VSPswitch:1(config)#password max-sessions <1-8> user-name <user name>
```

Password history – default is 3 previous passwords remembered

```
VSPswitch:1(config)#password password-history <3-32>
```

Password rule – change between 1 and 2 upper-case, lower-case, numeric-case, and special-case characters. By default, 2 is used for each

```
VSPswitch:1(config)#password password-rule <upper-case: 1-2> <lower-case: 1-2>
<numeric-case: 1-2> <special-characters: 1-2>
```

```
Example: 1 upper case, 2 lower case, 2 numbers, and 1 special character minimum
```

```
VSPswitch:1(config)#password password-rule 1 2 2 1
```

Change default lockout time – default is 60 seconds. This is the length of time a user is locked out if the incorrect user name and/or password is entered

```
VSPswitch:1(config)#password default-lockout-time <61-65000>
```

Password pre-notification and post-notification interval rule

In enhanced security mode, the switch enforces password expiry. To ensure a user does not lose access, the switch offers pre and post notification messages explaining when the password will expire. The administrator can define the pre and post notification interfaces between 1 and 99 days. If you do not change the password before the expiry date, the system locks the account. Once locked, only the administrator can unlock the account. The administrator creates a temporary password that the user will initially have to use to login with and then change the password.

```
VSPswitch:1(config)#password pre-expiry-notification-interval <interval 1: 1-99>
<interval 2: 1-99> <interval 3: 1-99>
```

```
VSPswitch:1(config)#password post-expiry-notification-interval <interval 1: 1-99>
<interval 2: 1-99> <interval 3: 1-99>
```

Factory setting – you can default any password setting by adding default prior to the password setting. Once defaulted, you must save the configuration and reboot the switch

```
VSPswitch:1(config)#default password <setting>
```

```
VSPswitch:1(config)#save config
```

```
VSPswitch:1(config)#reset
```

```
Example: Default the password rule
```

```
VSPswitch:1(config)#default password password-rule
```

```
VSPswitch:1(config)#save config
```

```
VSPswitch:1(config)#reset -y
```

Factory default – reset to factory default plus remove all enhanced user accounts

Only a user with the administrator access role can use this command to return the system back to the factory default defaults and delete all the configured user accounts.

```
VSPswitch:1(config)#sys system-default

WARNING: Executing this command returns the system to factory defaults and deletes all
local configured user accounts.

This command needs system reset to take into effect

Do you want to continue (y/n) ? y

VSPswitch:1(config)# (config)#save config

VSPswitch:1(config)# (config)#reset
```

3. Local password protection

3.1 CLI Password Protection

The following table shows the default values for logon and password for both console and Telnet sessions.

Table 2: Default User Names and Password

Access level	Description	Default logon	Default password
Read-only	Permits view-only configuration and status information. Is equivalent to Simple Network Management Protocol (SNMP) read-only community access.	ro	ro
Layer 1 read/write	View most switch configuration and status information and change physical port settings.	l1	l1
Layer 2 read/write	View and change configuration and status information for Layer 2 (bridging and switching) functions.	l2	l2
Layer 3 read/write	View and change configuration and status information for Layer 2 and Layer 3 (routing) functions.	l3	l3
Read/write	View and change configuration and status information across the switch. You cannot change security and password settings. This access level is equivalent to SNMP read/write community access.	rw	rw
Read/write/all	Permits all the rights of Read/Write access and the ability to change security settings, including the CLI and Web-based management user names and passwords and the SNMP community strings.	rwa	rwa

3.1.1 User Names and Passwords

The default user name and password can be changed by issuing the following command.

```
VSPswitch:1(config)#cli password <login user name> ?
  layer1          Change layer1 read write login/password
  layer2          Change layer2 read write login/password
  layer3          Change layer3 read write login/password
  read-only       Change read only login/password
  read-write      Change read write login/password
  read-write-all  Change read write all login/password
```

For example, assuming you wish to change the read-write-all password, but, still leaving the default user name as *rwa*, enter command shown below. After entering this command, you will be prompted to enter the old password followed by the entering and verifying the new password

```
VSPswitch:1(config)#cli password rwa read-write-all
Enter the old password : rwa
Enter the New password : ******
Re-enter the New password : ******
```

3.1.2 Enabling or Disabling Access Levels

To enable or disable a user level, enter the following command.

```
VSPswitch:1(config)#password access-level <access level>
VSPswitch:1(config)#no password access-level <access level>
```

For example, to disable the read-only access level, enter the following command

```
VSPswitch:1(config)#no password access-level ro
```

To change aging time, lockout time, minimum password length, or password history:

```
VSPswitch:1(config)#password access-level <word> ?
  aging-time            Set age-out time for passwords
  default-lockout-time  Change the default lockout time after three invalid
attempts
  min-passwd-len        Set the minimum length of passwords in hsecure mode
  password-history      Number of previous passwords to remember
<cr>
```

The following command confirms the change.

```
VSPswitch:1#show cli password
        access-level
        aging     90

        min-passwd-len 8
        password-history 3

        ACCESS    LOGIN            STATE
        rwa       rwa              NA
        rw        rw               ena
        l3        l3               ena
        l2        l2               ena
        l1        l1               ena
        ro        ro               dis
        Default Lockout Time       60
        Lockout-Time:
                    IP                  Time
```

3.3 High Secure (hsecure) Mode

The switch supports a configurable flag called high secure (hsecure). High secure mode introduces a protection mechanism to filter invalid source network broadcast IP addresses communicating with the CPU, limitation of failed logon attempts, and two restrictions on passwords: 10-character enforcement and aging time. An example of an invalid source would be an interface in subnet 192.168.168.0/24 where source IP addresses of 192.168.168.0 and 192.168.168.255 are discarded.

After you enable the hsecure flag, the software enforces the 10-character rule for all passwords. This password must contain a minimum of two uppercase characters, two lowercase characters, two numbers, and two special characters.

After you enable hsecure, the system requires you to save the configuration file and reboot the system for hsecure to take effect. If the existing password does not meet the minimum requirements for hsecure, the system prompts you to change the password during the first login.

The default username is rwa and the default password is rwa. In hsecure, the system prompts you to change these during first login because they do not meet the minimum requirements for hsecure.

When you enable hsecure, the system disables Simple Network Management Protocol (SNMP) v1, SNMPv2 and SNMPv3. If you want to use SNMP, you must re-enable SNMP, using the command no boot config flag block-snmp.

After you enable the hsecure flag, you can configure a duration after which you must change your password. You configure the duration by using the aging parameter.

For SNMP and File Transfer Protocol (FTP), after a password expires, access is denied. Before you access the system, you must change a community string to a new string consisting of more than eight characters.

Consider the following after you enable the hsecure flag:

- You cannot enable the Web server for Enterprise Device Manager (EDM) access.
- You cannot enable the Secure Shell (SSH) password authentication.

To enable hsecure mode, enter the following commands. You will be prompted with an error message if telnet or rlogin is enabled.

```
VSPSwitch:1(config)#boot config flags hsecure
Warning: If your CLI session is running over Telnet or Rlogin -
         you will be disconnected and will not be able to reconnect.
Are you sure you want to continue (y/n) ? y
```

3.3.1 Access Level Options – hsecure mode

If High Security (hsecure) is enabled, you can set the aging time, lockout time, mimimum password length, and password history using the following command. By default, the aging time is set for 90 seconds, minimum password length is set for 10 characters, and the password history is set for 3 previous passwords.

```
VSPSwitch:1(config)#password ?
  aging-time            Set age-out time for passwords
  default-lockout-time  Change the default lockout time after three invalid
                        attempts
  min-passwd-len        Set the minimum length of passwords in hsecure mode
  password-history      Number of previous passwords to remember
```

3.4 CLI Logging

If you wish, you can enable CLI logging of ACLI commands executed. The ACLI commands are logged to the system log file using the CLILOG module.

```
VSPswitch:1(config)#clilog enable
VSPswitch:1(config)#show logging file module clilog
```

To disable CLI logging:

```
VSPswitch:1(config)#no clilog enable
```

3.5 CLI Prompt

To change the CLI prompt, enter the following command.

```
VSPswitch:1(config)#prompt <word, 0-255>
```

To change to the default CLI prompt:

```
VSPswitch:1(config)#default prompt
```

3.6 Login message and password prompt

To change the default CLI login prompt, first you must disable the default login prompt (no login-message) and then enter the new prompt.

```
VSPswitch:1(config)#no login-message
VSPswitch:1(config)#login-message {string length 1..1513}
```

To change the default CLI password prompt, first you must disable the default password prompt and then enter the new prompt.

```
VSPswitch:1(config)#no passwordprompt
VSPswitch:1(config)#passwordprompt {string length 1..1510}
```

To change the login-message and password prompt back to the default settings:

```
VSPswitch:1(config)#default login-message
VSPswitch:1(config)#default passwordprompt
```

3.7 Telnet Access Configuration Examples using Local Users with hsecure disabled

3.7.1 Local Password Configuration - Password Security Disabled

For this configuration example, we will configure the following.

- Change the default read-write-all user name from rwa to *user1*
  - For *user1*, use the password *rwaccess*
- Change the default read-only user name from rw to *user2*
  - For *user2*, use the password *readwrite*
- Change the default login and password prompt from *Login:* and *Password:* to *Enter username:* and *Enter your password:*

Step 1 – Add new user names and passwords

```
VSPswitch:1(config)#cli password user1 read-write-all
Enter the old password : *** (rwa)
Enter the New password : ******** (rwaccess)
Re-enter the New password : ********
```

Step 2 – Change default login user and password prompt

```
VSPswitch:1(config)#no login-message
VSPswitch:1(config)#login-message "Enter username: "
VSPswitch:1(config)#no passwordprompt
VSPswitch:1(config)#passwordprompt "Enter your password: "
```

3.7.2 Verify Operations

Step 1 – Verify user names

```
VSPswitch:1(config)#show cli password
        access-level
        aging     90

        min-passwd-len 10
        password-history 3

        ACCESS    LOGIN            STATE
        rwa       user1            NA
        rw        user2            ena
        l3        l3               ena
        l2        l2               ena
        l1        l1               ena
        ro        ro               ena
        Default Lockout Time       60
        Lockout-Time:
                    IP                  Time
```

Step 2 – Verify the login prompt

```
VSPswitch:1(config)#show cli info
cli configuration

more            : true
screen-lines    : 23
telnet-sessions : 8
rlogin-sessions : 8
timeout         : 900 seconds
monitor duration: 300 seconds
monitor interval: 5 seconds

use default login prompt    : false
default login prompt        : Login:
custom login prompt         : Enter username:
use default password prompt : false
default password prompt     : Password:
custom password prompt      : Enter your password:
prompt : 9001
```

4. Password Protection using RADIUS Authentication

Users who access the Avaya switch through Telnet, local console, rlogin, or SSHv2 (password authentication), can be authenticated against a RADIUS server.

RADIUS supports both IPv4 and IPv6 with no differences in functionality or configuration in all but the following case. When you add or update a RADIUS server in Enterprise Device Manager (EDM) you must specify if the address type is an IPv4 or an IPv6 address.

The following table displays the various RADIUS features supported on the VSP switch.

Table 3: RADIUS Features

Feature	Description
Additional user names	You can use additional user names to access the device, in addition to the six existing user names of ro, L1, L2, L3, rw, and rwa. The RADIUS server authenticates the user name and assigns one of the existing access priorities to that name. Unauthenticated user names are denied access to the device. User names ro, L1, L2, L3, rw, and rwa must be added to the RADIUS server if authentication is enabled. Users not added to the server are denied access.
User configurable	• Up to 10 RADIUS servers in each device for fault tolerance (each server is assigned a priority and is contacted in that order). • A secret key for each server to authenticate the RADIUS client • The server UDP port • Maximum retries allowed • Time-out period for each attempt

The following chart displays the outbound attribute values required by the VSP switch for each access level for RADIUS vendor identifier 1584 (Bay Networks) attribute type 192.

Table 4: RADIUS Attributes

Access Level	VSA Attribute 26 – Vendor Identifier 1584 Type 192 value
None-Access	0
Read-Only-Access	1
L1-Read-Write-Access	2
L2-Read-Write-Access	3
L3-Read-Write-Access	4
Read-Write-Access	5
Read-Write-All-Access	6

If enhanced security is enabled, the following chart displays the outbound attribute values required by the VSP switch for each access level for RADIUS vendor identifier 1584 (Bay Networks) attribute type 192.

Table 5: Enhanced Security RADIUS Attributes

Access Level	VSA Attribute 26 – Vendor Identifier 1584 Type 192 value
None-Access	0
Auditor	1
Security	2
Operator	3
Privilege	N/A – Not allowed by RADIUS
Admin	6

If you plan to use RADIUS with enhanced secure mode, please enable RADIUS after the enhanced mode is enabled. If RADIUS is enabled prior to enabling the enhanced secure mode, the RADIUS shared key must be re-entered; one must delete the shared key and re-enter it again.

In addition, you can deny CLI commands for a user. This is done using RADIUS vendor identifier 1584 attribute types 194 and 195. Attribute type 194 needs to be set to a value of 0 while attribute 195 lists the command you wish to deny to a user.

The following table displays the various event and logged information

Table 6: RADIUS Events Logged

Event	Accounting information logged at server
Accounting is turned on at router	• Accounting on request:NAS • IP address
Accounting is turned off at router	• Accounting off request: NAS IP address.
User logs in	• Accounting start request:NAS IP address • Session Id • User Name
More than 40 CLI commands are executed	• Accounting Interim request:NAS IP address • Session Id • CLI commands • User Name
User logs off	• Accounting Stop request:NAS IP Address • Session Id • Session duration • User Name • number of input octets for session • number of octets output for session • number of packets input for session • number of packets output for session • CLI commands

4.1 Enabling RADIUS globally

To use RADIUS, it must be enabled globally using the following command.

```
VSPswitch:1(config)#radius enable
```

If you wish specify and use the source IP address for the RADIUS server configuration, you must also enable the global parameter using the following command

```
VSPswitch:1(config)#radius sourceip-flag
```

4.2 Adding RADIUS server for authentication

To add a RADIUS server, enter the following command with the option of enabling accounting and specifying the source IP address. If you do not specify the source IP, the VSP switch will use the source IP address of the out-going interface. Depending on the number of out-going interfaces, you may have to add two or more RADIUS authenticators on your RADIUS server unless you specify the source IP address. The source IP address should be a circuitless/loopback IP address which is not tied down to a physical interface.

```
VSPswitch:1(config)#radius server host <ip address> key <secret key> ?
  acct-enable  Server acct enabled
  acct-port    Server acct udp port
  enable       Server enabled
  port         Server udp port
  priority     Server priority
  retry        Max number of retries
  source-ip    Source ip address
  timeout      No answer timeout value
  used-by      Use for cli,eapol,snmp or web
  <cr>
```

4.3 CLI Profile

If you wish to restrict CLI commands for a user, simply enable the RADIUS cli-profile setting as shown below. On the RADIUS server, via vendor identifier code 1584 using attributes types 194 and 195, set attribute type 194 to a value of 0 and add the CLI command using attribute 195.

```
VSPswitch:1(config)#radius cli-profile
```

If you wish to change the default CLI access attribute value to another value other than 194, enter the following command.

```
VSPswitch:1(config)#radius command-access-attribute <192-240>
```

If you wish to change the default CLI command attribute value to another value other than 195, enter the following command.

```
VSPswitch:1(config)#radius cli-commands-attribute <192-240>
```

4.4 Enabling RADIUS accounting globally

To use RADIUS accounting, it must also be enabled globally using the following command.

```
VSPswitch:1(config)#radius accounting enable
```

4.5 Enabling accounting for CLI commands

You can specify whether you want CLI commands included in RADIUS accounting requests by issuing the following command.

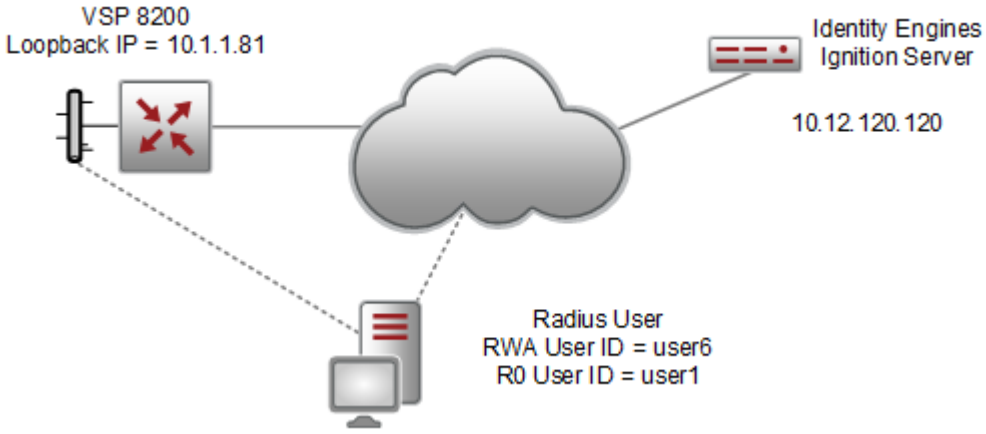
```
VSPswitch:1(config)#radius accounting include-cli-commands
```

You can also specify the number of CLI commands entered prior to the VSP switch sending a CLI accounting record. The default setting is 40. If you wish to change the default value, enter the following command.

```
VSPswitch:1(config)#radius cli-cmd-count <1-40>
```

4.6 RADIUS Password Configuration Example

For this configuration example, we will configure the VSP switch for RADIUS authentication using IPv4 addressing and using the loopback address as the source IP for CLI and EDM authentication. We will also show the configuration steps required using Avaya's Identity Engines Ignition Server.



4.6.1 Ethernet Routing Switch Configuration

Up to ten RADIUS servers are supported on the VSP switch where each server is assigned a priority and is connected according to the assigned priority. For this configuration example we will simply configure one RADIUS server using IPv4 addressing and use the IP loopback address as the source IP address. Please note by default, CLI RADIUS authentication is selected by when adding a RADIUS server – no additional configuration steps are required to enable CLI RADIUS authentication.

Step 1 – Add RADIUS server, enable RADIUS, enable RADIUS accounting, and enable RADIUS accounting to include CLI command with a command count of 5

```
VSPswitch:1(config)#radius server host 10.12.120.120 key avaya priority 1 source-ip 10.1.1.81
VSPswitch:1(config)#radius enable
VSPswitch:1(config)#radius accounting enable
VSPswitch:1(config)#radius accounting include-cli-commands
VSPswitch:1(config)#radius sourceip-flag
VSPswitch:1(config)#radius cli-cmd-count 5
```

Step 2 – Add IP loopback address

```
VSPswitch:1(config)#interface loopback 1
VSPswitch:1(config-if)#ip address 1 10.1.1.81/255.255.255.255
VSPswitch:1(config-if)#exit
```

If you wish to restrict CLI commands for a user, simply enable the RADIUS cli-profile setting as shown below. On the RADIUS server, via vendor identifier code 1584 using attributes types 194 and 195, set attribute type 194 to a value of 0 and add the CLI command using attribute 195.

4.6.2 VSP Switch: Verify Operations

Step 1 – Verify that RADIUS configuration

```
VSPswitch:1#show running-config module radius

#
# RADIUS CONFIGURATION
#

radius server host 10.12.120.120 key ******  priority 1 source-ip 10.1.1.81
radius enable
radius accounting enable
radius accounting include-cli-commands
radius cli-cmd-count 5
radius sourceip-flag
```

Step 2 – Verify that RADIUS has been enabled globally

```
VSPswitch:1#show radius
Sub-Context: clear config dump monitor mplsping mplstrace peer show switchover test
trace
Current Context:

             acct-attribute-value : 193
                      acct-enable : true
         acct-include-cli-commands : true
         access-priority-attribute : 192
              auth-info-attr-value : 91
          command-access-attribute : 194
            cli-commands-attribute : 195
                     cli-cmd-count : 5
                cli-profile-enable : false
                            enable : true
                  igap-passwd-attr : standard
            igap-timeout-log-fsize : 512
                         maxserver : 10
             mcast-addr-attr-value : 90
                     sourceip-flag : true
```

Step 3 – Verify that RADIUS Server Configuration

```
VSPswitch:1#show radius-server
================================================================================================
                                        Radius Server Entries
================================================================================================
                                                                                ACCT ACCT    SOURCE
NAME                      USEDBY SECRET PORT PRIO RETRY TIMEOUT ENABLED PORT ENABLED IP
------------------------------------------------------------------------------------------------
10.12.120.120              cli    ****** 1812 1    1     3       true    1813 true    10.1.1.81
```

4.6.3 IDE RADIUS Configuration

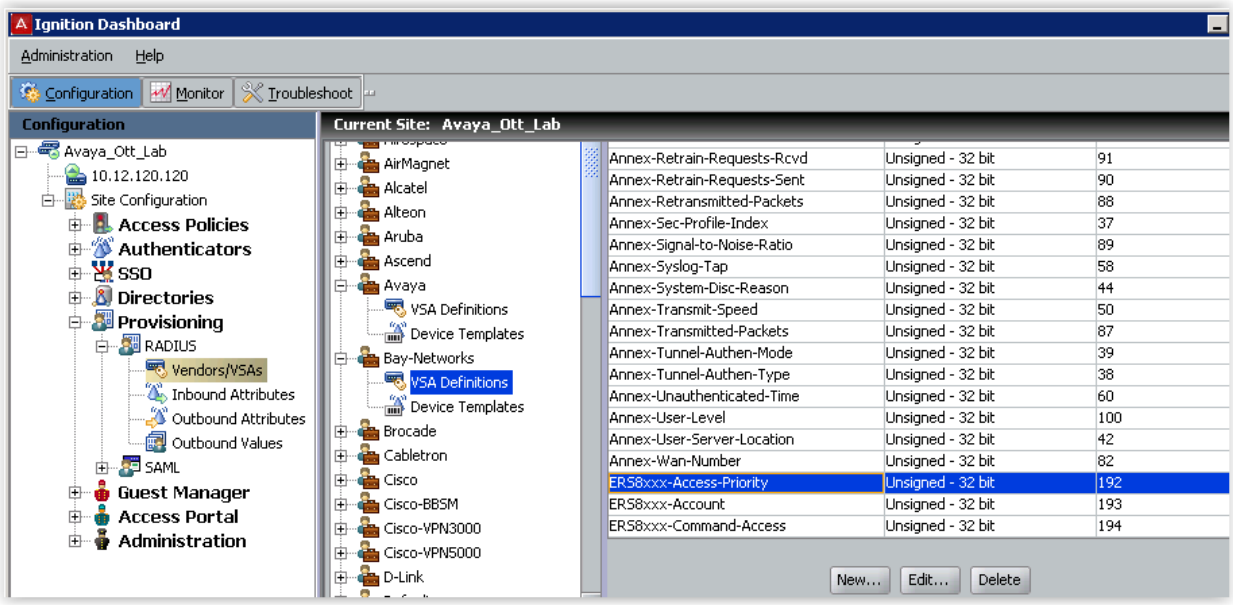
Assuming we are using Identity Engines Ignition Server as the RADIUS server, please follow the configuration steps below.

The following chart displays the outbound attribute values required by the VSP switch for each access level for RADIUS vendor identifier 1584 (Bay Networks) attribute type 192. For this example, we will configure IDE with attribute values of 1 and 6 for read-only and read-write-all access.

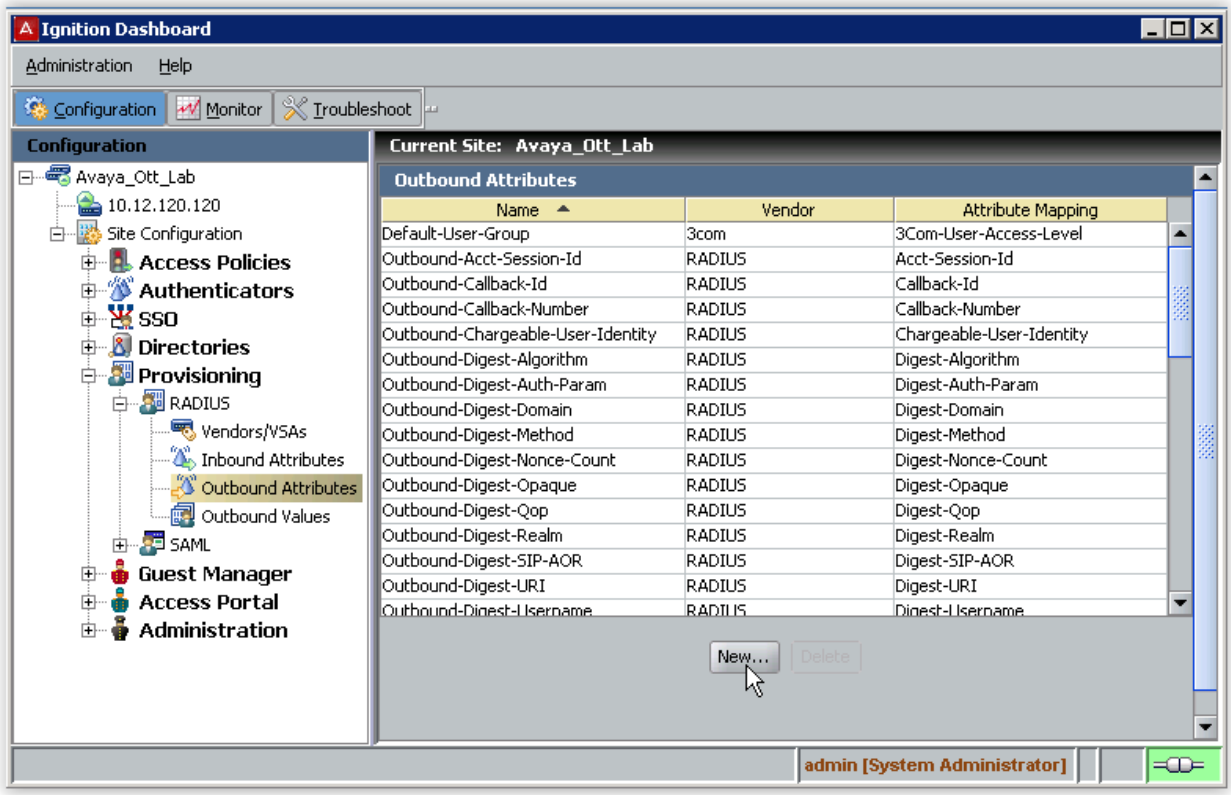
Access Level	Attribute Value	User Name
None-Access	0	
Read-Only-Access	**1**	**user1**
L1-Read-Write-Access	2	
L2-Read-Write-Access	3	
L3-Read-Write-Access	4	
Read-Write-Access	5	
Read-Write-All-Access	**6**	**User6**

4.6.3.1 Add RADIUS Outbound Attribute Access Priority Values for Read-Only and Read-Write-All Access

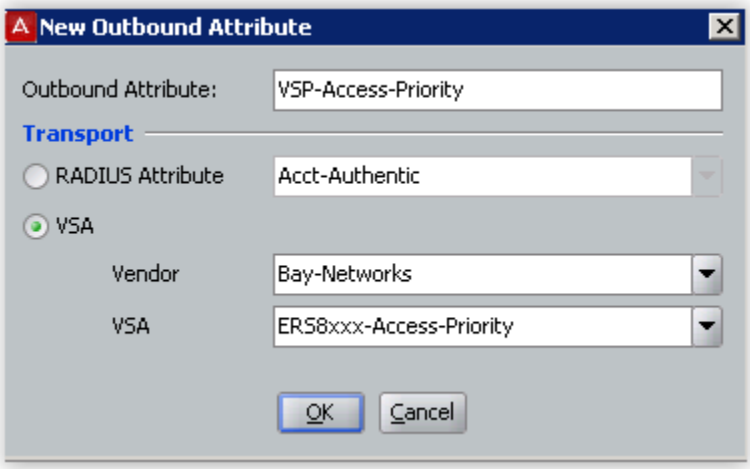
IDE Step 1 – IDE already has the vendor specific attributes defined (Bay Networks vendor code 1584 using attribute type 192) for the VSP switch which can be viewed by going to *Site Configuration -> Provisioning -> RADIUS -> Vendors/VSAs -> Bay-Networks -> VSA Definitions*.



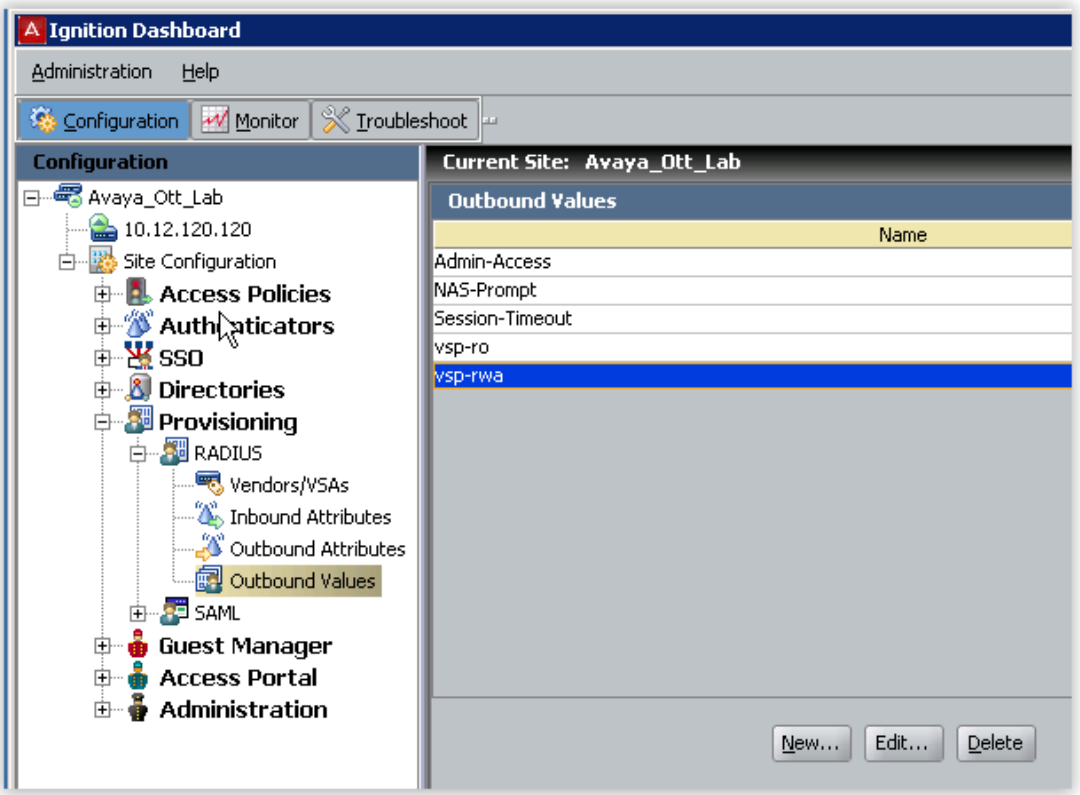
IDE Step 2 – Go to *Site Configuration -> Provisioning -> Outbound Attributes -> New*



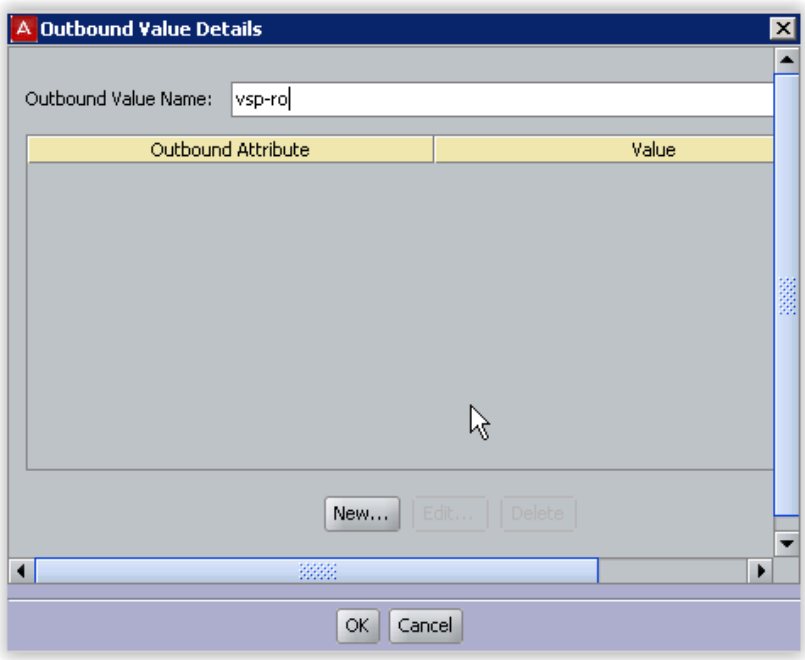
IDE Step 3 – Via the *Outbound Attribute* window, type in a name for the attribute to be used for access priority (i.e. *VSP-Access-Priority* as used in this example), click the *VSA* radio button, select *Bay-Networks* via *Vendor* and *ERS8xxx-Access-Priority* via *VSA.* Click on *OK* when done



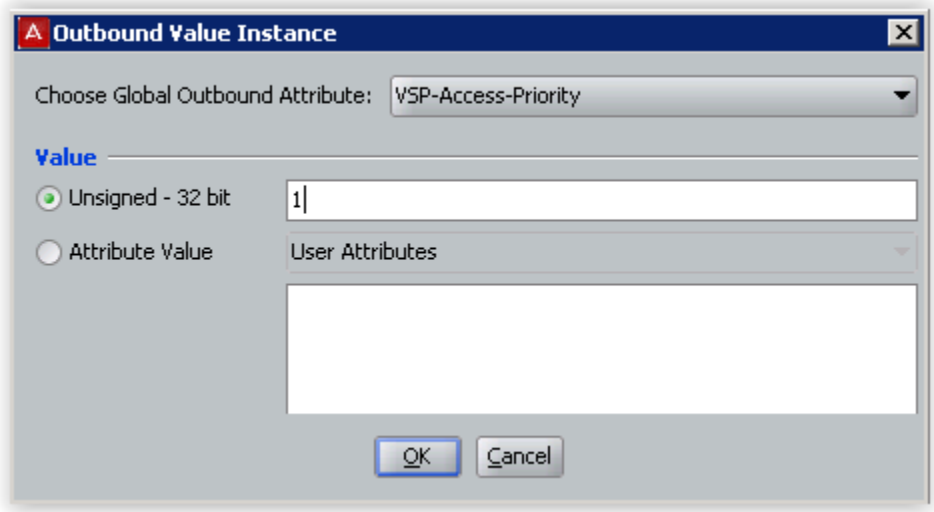
IDE Step 4 – Go to *Site Configuration -> Provisioning -> RADIUS -> Outbound Values -> New*



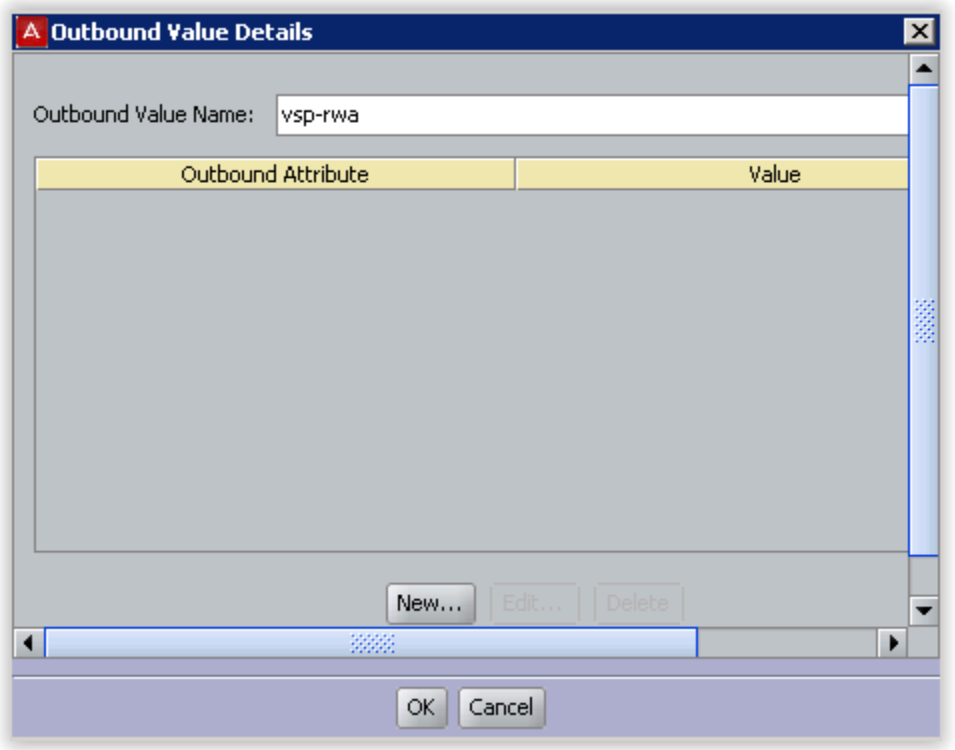
IDE Step 5 – Using the Outbound Attribute created in Step 3, we will first add an attribute value of 1 for read-only-access. Start by entering a name via the Outbound Value Name: window (i.e. *vsp-ro* as used in this example) and click on *New*



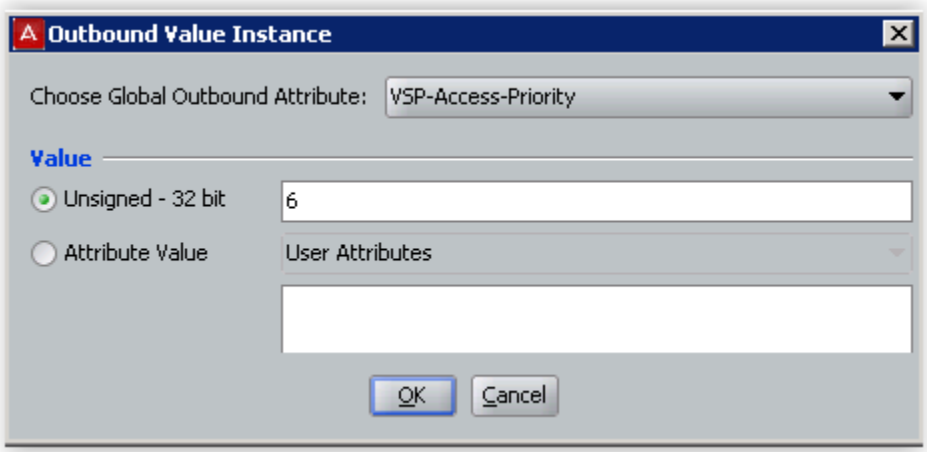
IDE Step 6 – Select the Outbound Attributes name created in Step 3 (i.e. *VSP-Access-Priority* as used in this example) via the *Choose Global Outbound Attribute*: pull down menu. In the Value *Unsigned – 32 bit* window, enter *1* (i.e. value of 1 signifies read-only-access). Click on *OK* twice when done.



IDE Step 7 – Go to *Site Configuration -> Provisioning -> RADIUS -> Outbound Values -> New* again to create the outbound attribute for read-write-all-access. Using the Outbound Attribute created in Step 3, we will add an attribute value of 6 for read-write-all-access. Start by entering a name via the Outbound Value Name: window (i.e. vsp-rwa as used in this example) and click on *New*



IDE Step 8 –Select the Outbound Attributes name created in Step 3 (i.e. *VSP-Access-Priority* as used in this example) via the Choose Global Outbound Attribute: pull down menu. In the *Value Unsigned – 32 bit* window, enter *6* (i.e. value of 6 signifies read-write-all-access). Click on *OK* twice when done.



4.6.3.2 Option – Restrict CLI command

If you wish to restrict a CLI command, you need to set the RADIUS vendor code 1584 attribute type 194 with a value of 0 and enter the CLI command using attribute 195. Ensure that you enable ACLI cli-profile command option on the VSP switch if you wish to use options 194 and 195:

```
VSPswitch:01(config)#radius cli-profile
```

IDE Step 1 – Add attribute 194

- Go to *Site Configuration -> Provisioning -> Outbound Attributes -> New*
  - Via the Outbound Attribute window, type in a name for the attribute to be used to restrict CLI commands, click the *VSA* radio button, select *Bay-Networks* (vendor code 1584) via *Vendor* and *ERS8xxx-Command-Access* (attribute 194) via VSA. Click on *OK* when done

IDE Step 2 – Add attribute 195

- Go to Site *Configuration -> Provisioning -> Outbound Attributes -> New*
  - Via the Outbound Attribute window, type in a name for the attribute to be used to list the CLI command, click the *VSA* radio button, select *Bay-Networks* (vendor code 1584) via *Vendor* and *ERS8xxx-CLI-Commands* (attribute 195) via *VSA*. Click on *OK* when done

IDE Step 3 – Set the attribute 194 value to 0

- Go to Site *Configuration -> Provisioning -> Outbound Values -> New*
  - Enter a name via the Outbound Value Name: and click on *New*
  - Select the Outbound Attributes name created in Step 1 via the *Choose Global Outbound Attribute:* pull down menu. In the *Value Unsigned – 32 bit* window, enter *0* (i.e. value of 0 signifies CLI command restriction). Click on *OK* twice when done.
  - Add this attribute name to the appropriate user when defining the IDE policy

IDE Step 4 – List the CLI command using attribute 195

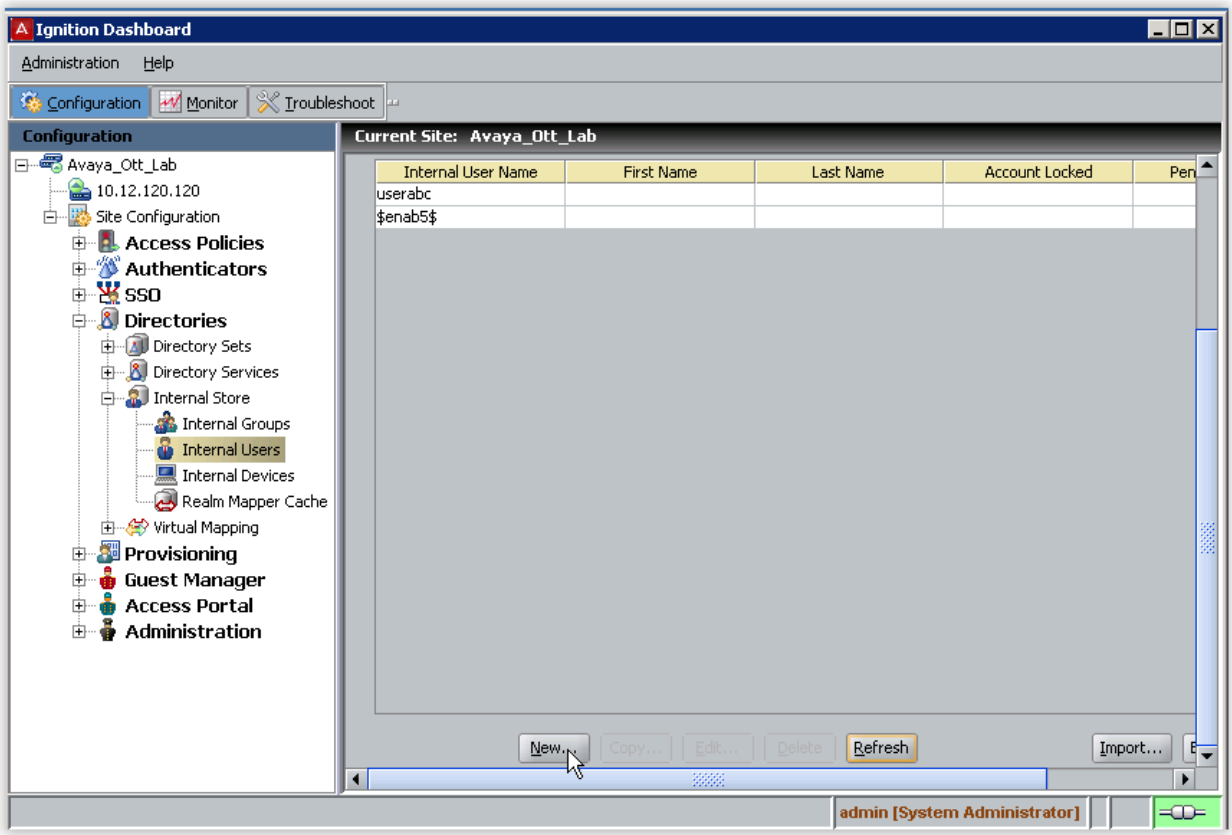
- Go to Site *Configuration -> Provisioning -> Outbound Values -> New*
  - Enter a name via the Outbound Value Name: and click on *New*
  - Select the Outbound Attributes name created in Step 2 via the *Choose Global Outbound Attribute:* pull down menu. In the *String* window, enter the ACLI command you wish to restrict. Click on OK twice when done.
  - Add this attribute name to the appropriate user when defining the IDE policy

4.6.3.3 Add Users

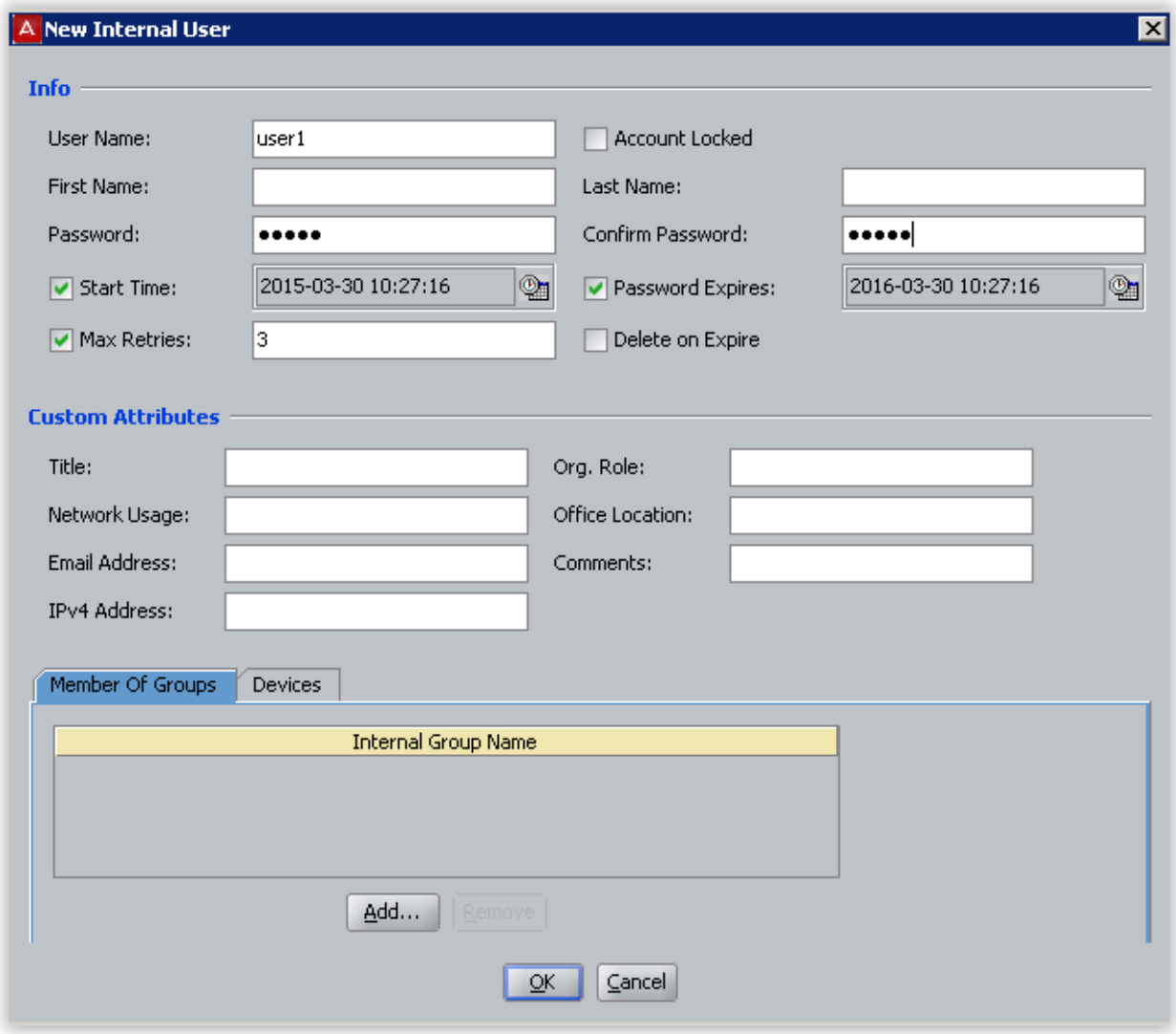
For this configuration example, we will add the following users.

User Name	Access Level
user1	Read-Only-Access
user6	Read-Write-All-Access

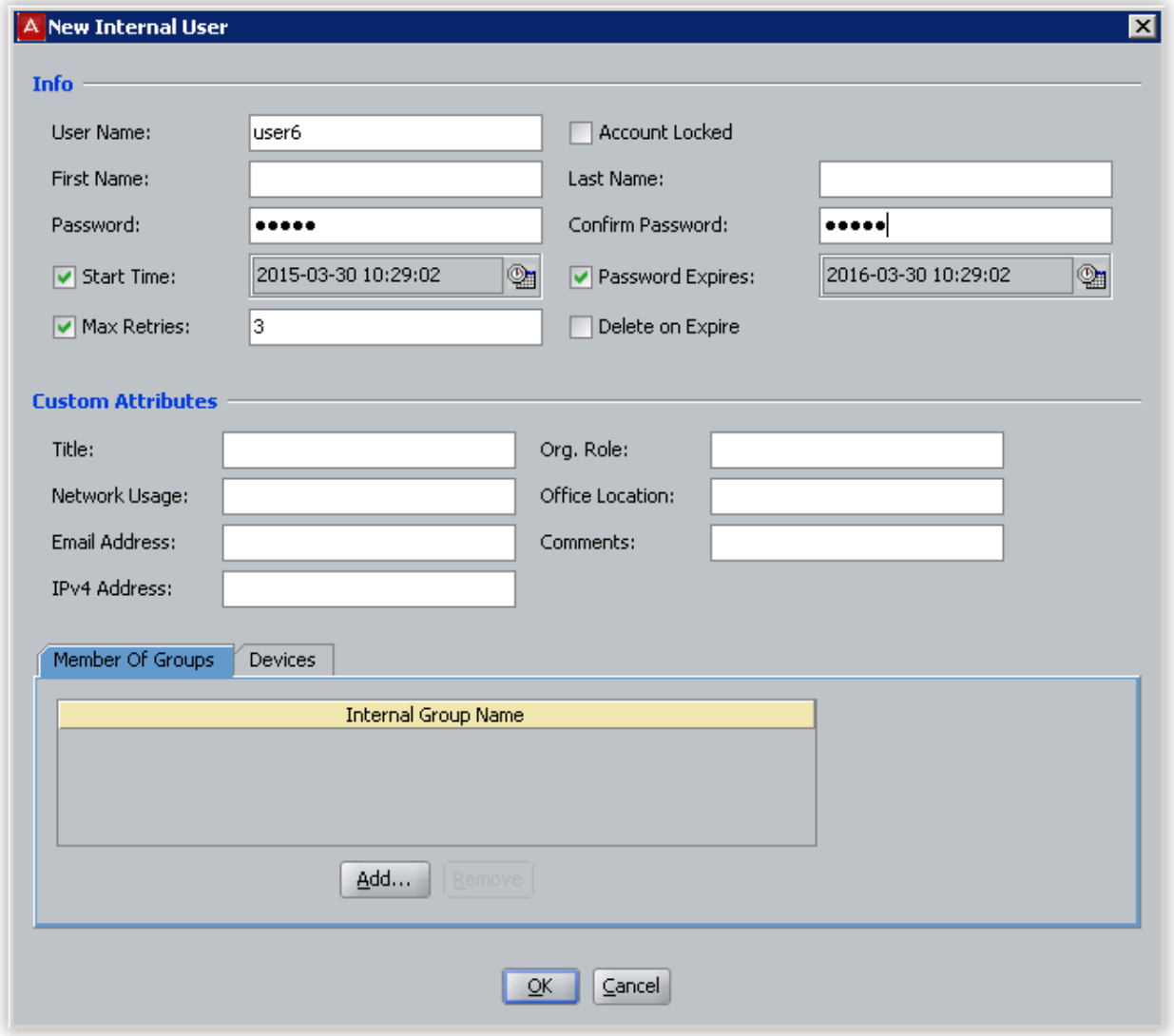
IDE Step 1 – Start by going to *Site Configuration -> Directories -> Internal Store -> Internal Users* and click on *New*



IDE Step 2 – Enter the user name for read-only-access via *User Name:* (i.e. *user1* as used in this example) and enter the password for this user via *Password* and *Confirm Password*. Click on *OK* when done. If you wish, you can also change the expiry date via *Password Expires* if you do not wish to use the default setting of one year

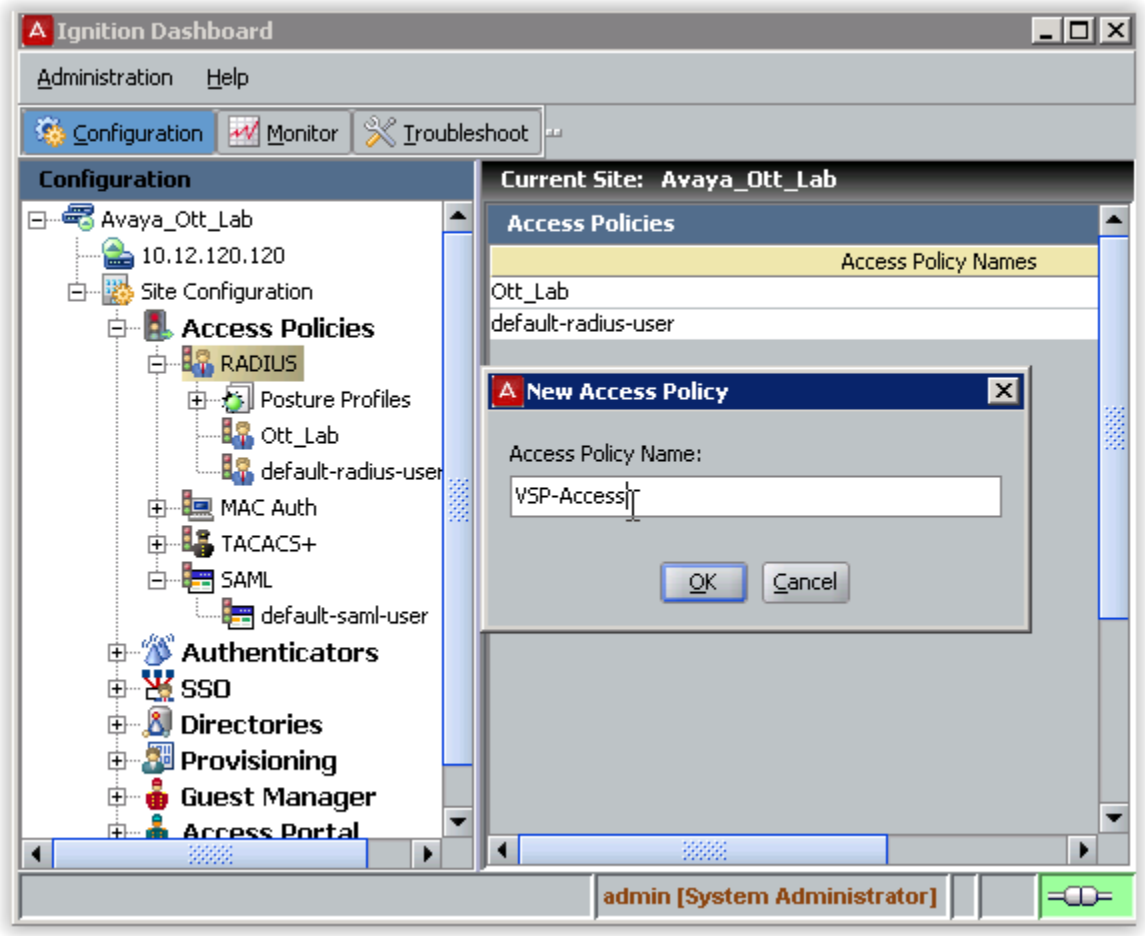


IDE Step 3 – Repeat step 1 again by clicking on New to add the read-write-all-access user. Enter the user name for read-write-all-access via User Name: (i.e. *user6* as used in this example) and enter the password for this user via Password and Confirm Password. Click on OK when done. If you wish, you can also change the expiry date via Password Expires if you do not wish to use the default setting of one year

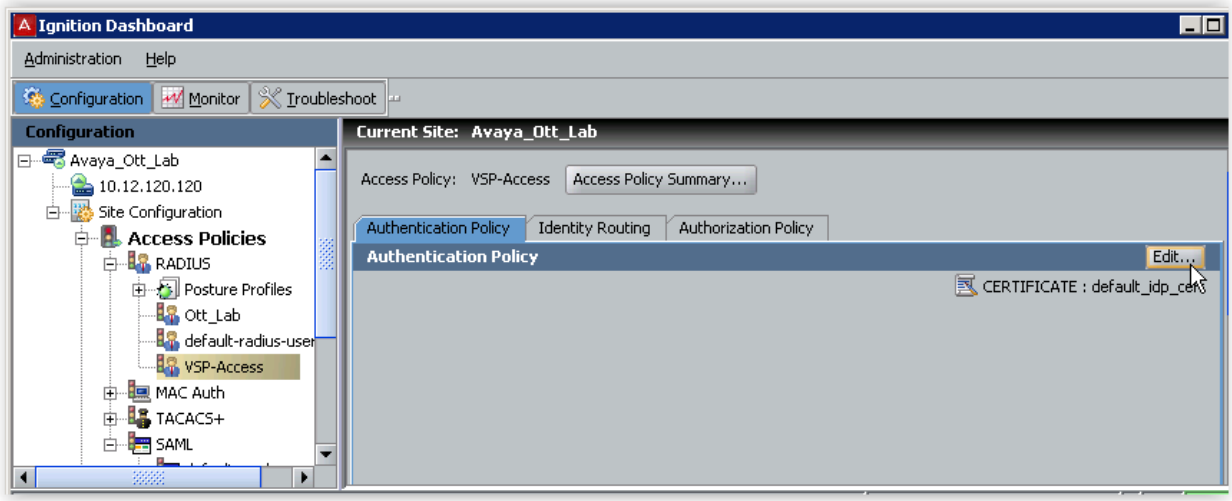


4.6.3.4 Add an Access Policy

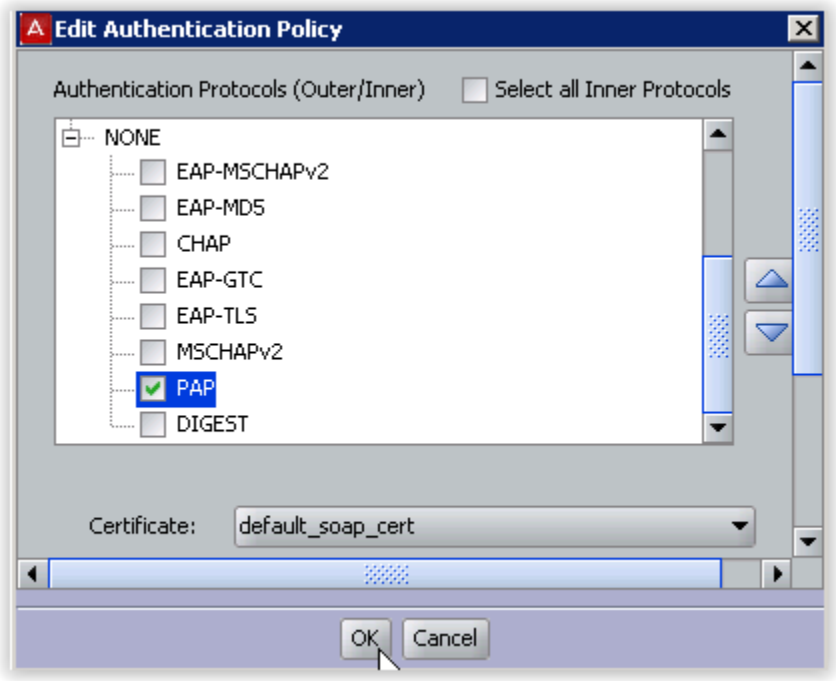
IDE Step 1 – **Go to *Site Configuration -> Access Policies -> RADIUS*. Right-click *RADIUS* and select *New Access Policy*. Enter a policy name (i.e.VSP-Access as used in this example) and click on *OK* when done**



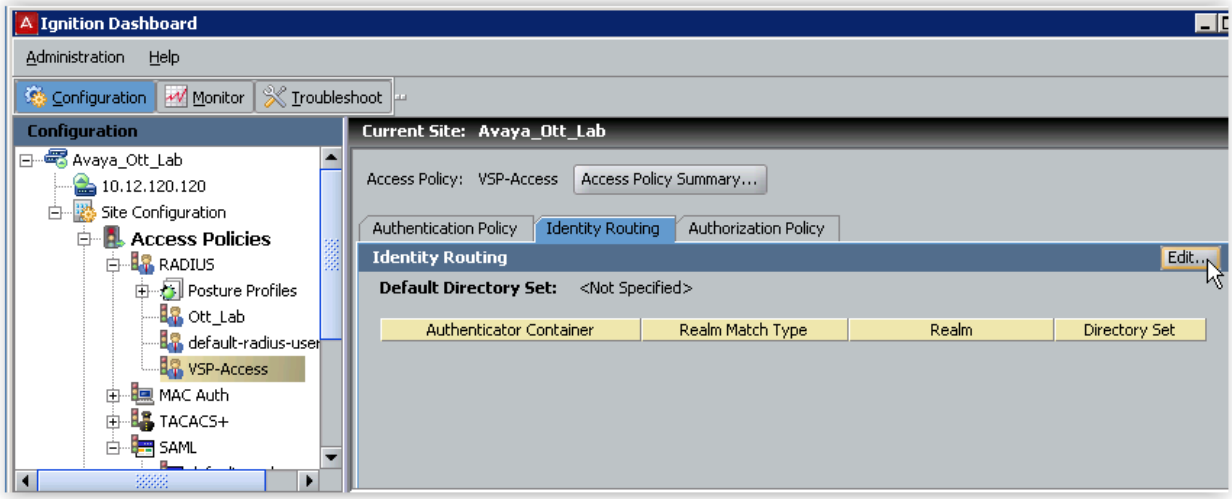
IDE Step 2 – Click on the policy we just created, i.e. ERS8000-Access, and click on *Edit* via the *Authentication Policy* tab



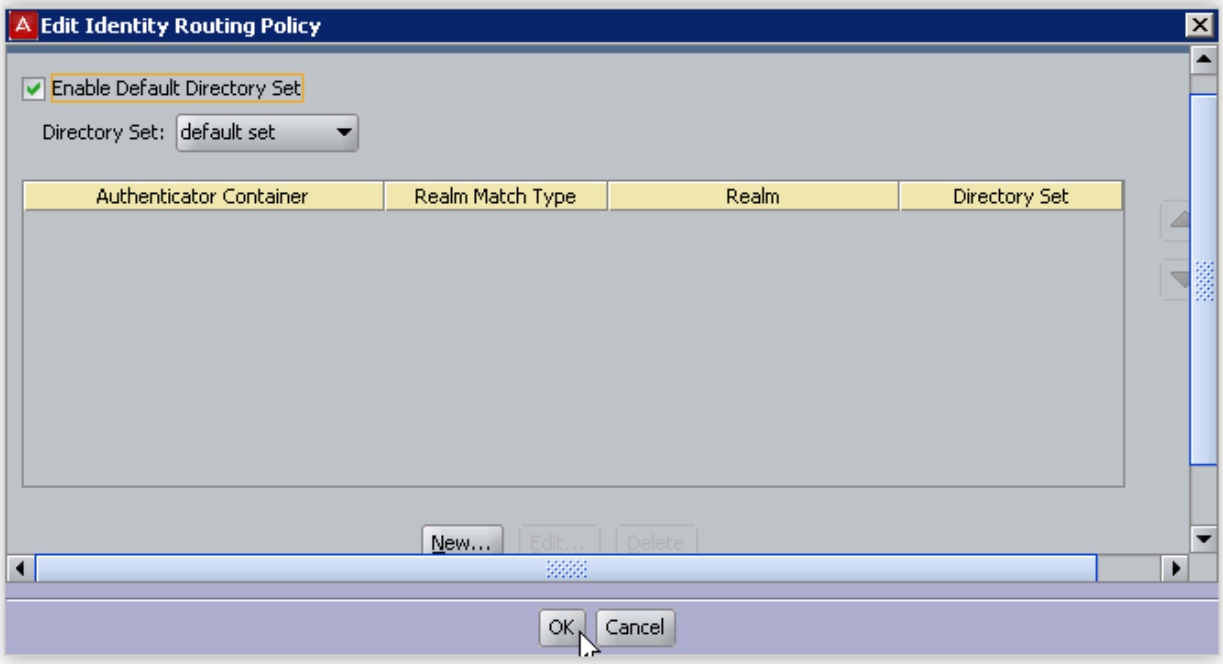
IDE Step 3 – Under *Edit Authentication Policy* window, select *NONE -> PAP* and click on *OK* when done



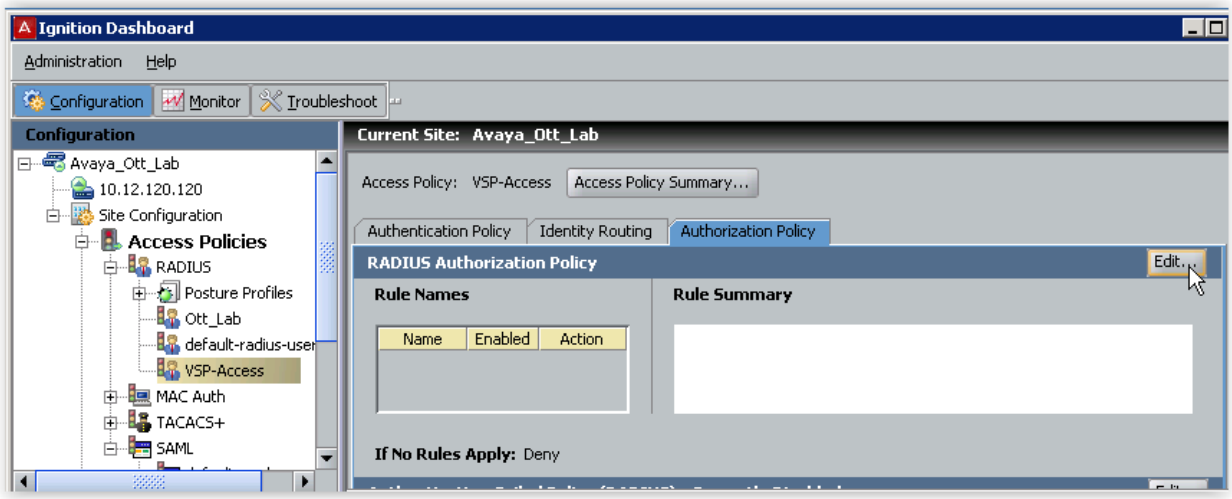
IDE Step 4 – Go to the *Identity Routing tab* and click on *Edit*



IDE Step 5 – Check off the *Enable Default Directory Set* and click on *OK* when done.

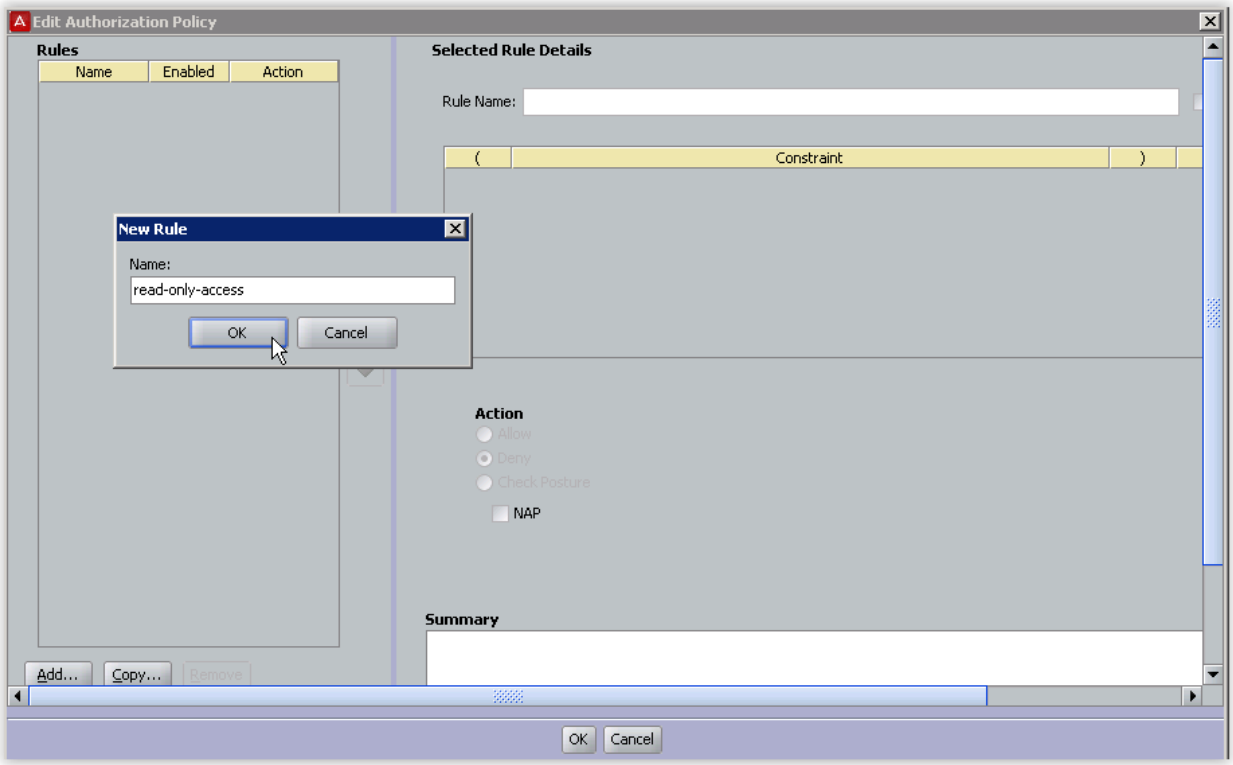


IDE Step 6 – Go to the *Authorization Policy* tab and click on *Edit*



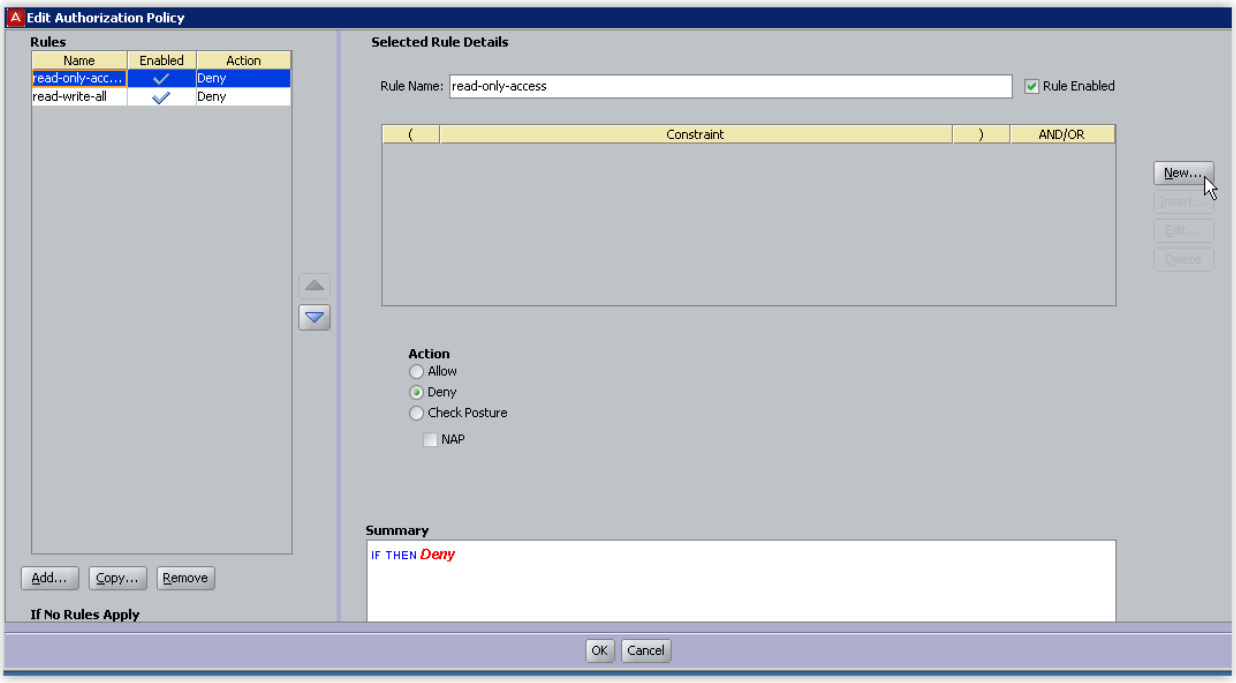
IDE Step 7 – Once the *Edit Authorization Policy* window pops up, click on *Add*

- **Add a rule for read-only-access. When the *New Rule* window pops up, for this example, name the rule *read-only-access***
- **Add a rule for read-write-access. When the *New Rule* window pops up, for this example, name the rule *read-write-access***

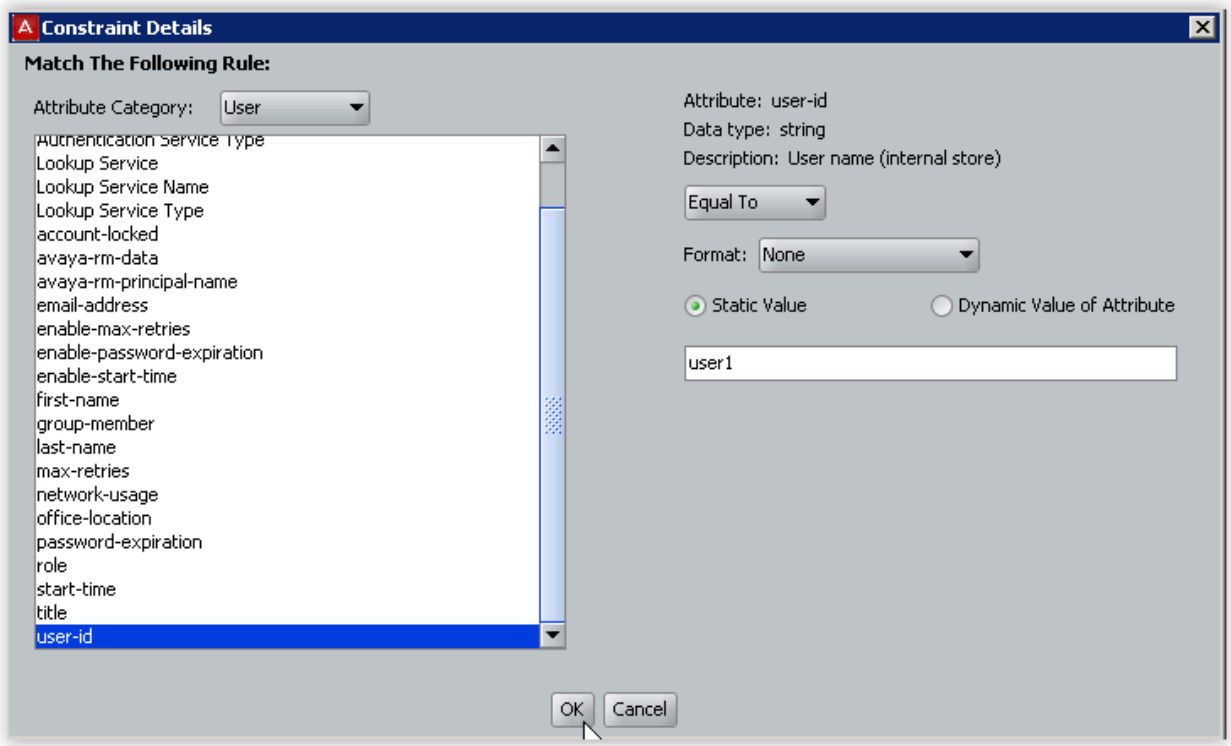


IDE Step 8 – Click on *New* to add a new constraint

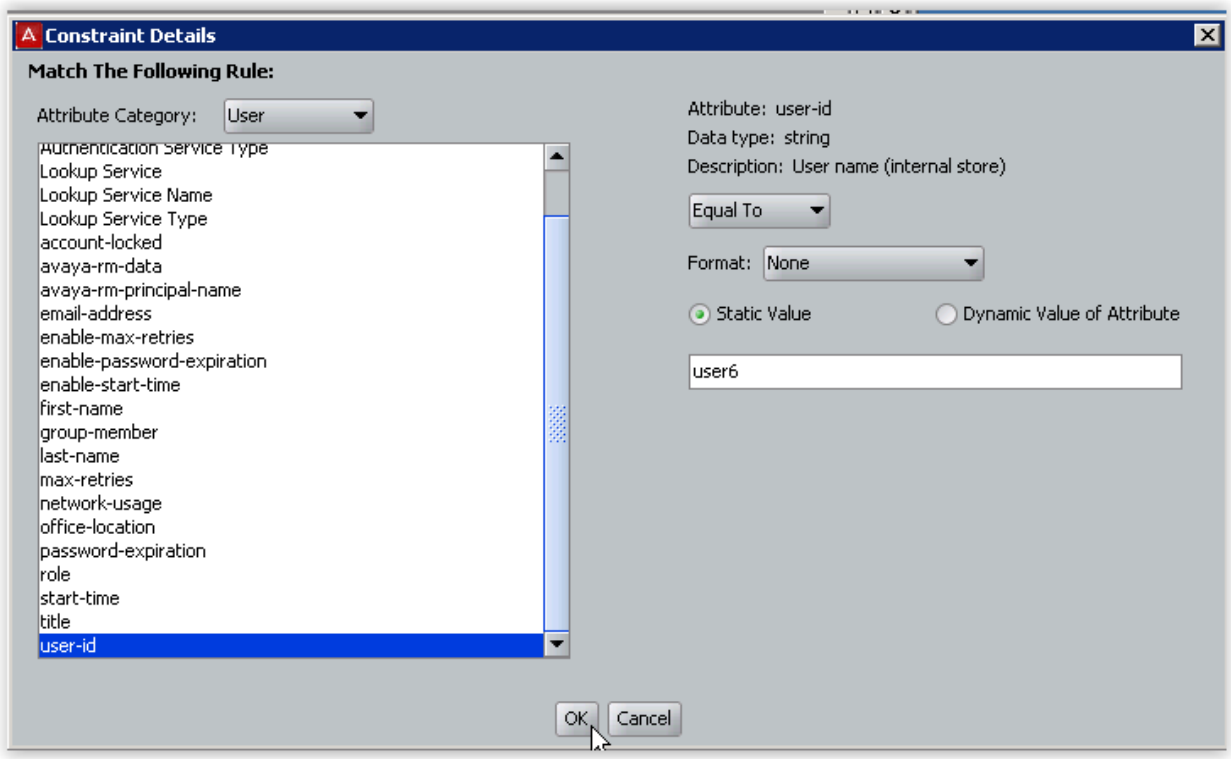
- For the read-only-access rule, we configure the rule to look for a user-id of ***user1***
  - Attribute Category = ***User***, Attribute = ***user-id***, Static Value = ***user1***
- For the read-only-access rule, we configure the rule to look for a user-id of ***user6***
  - Attribute Category = ***User***, Attribute = ***user-id***, Static Value = ***user6***



Select the read-write-all rule and add the following constraint usig the user id's we configured in above:

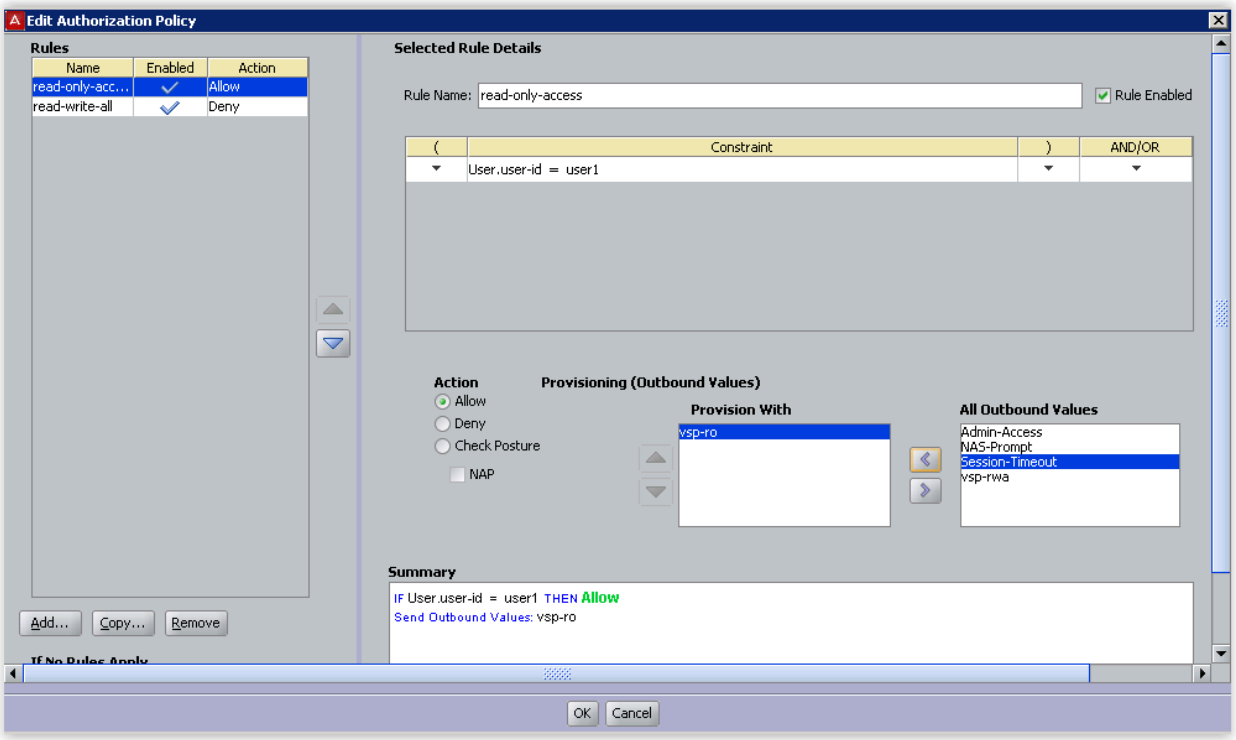


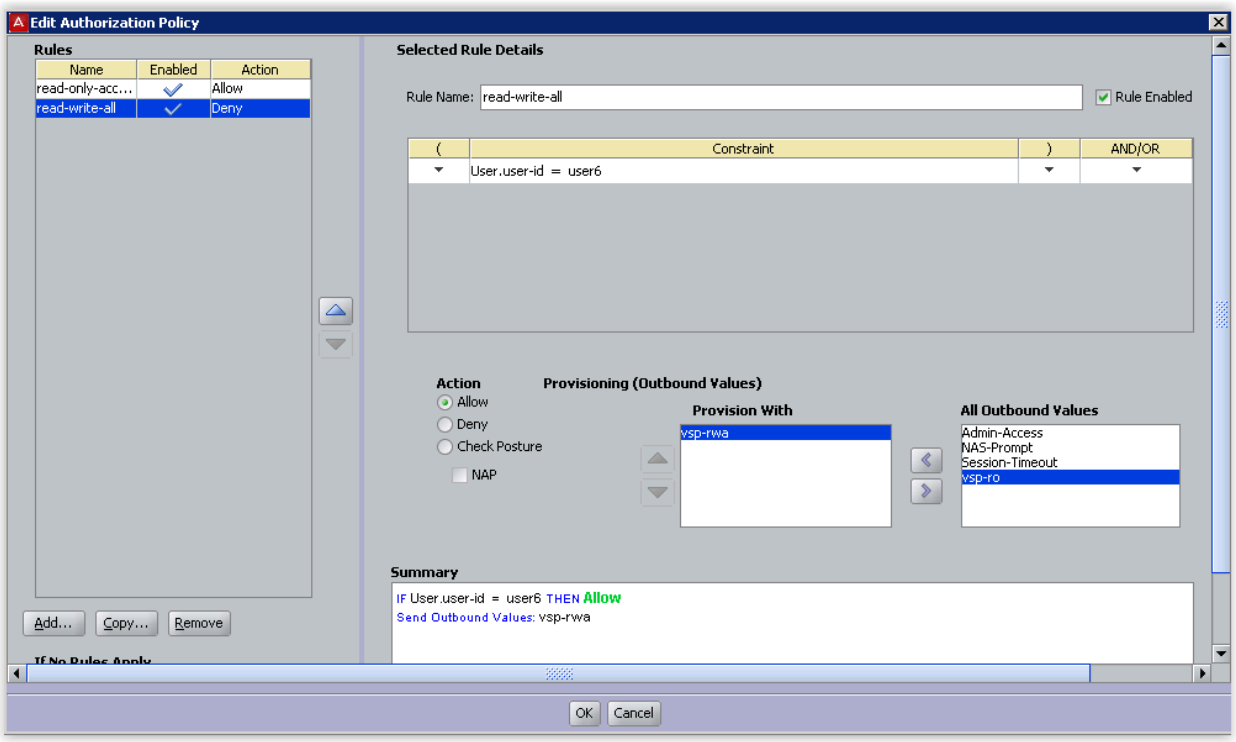
Select the read-write-all rule and add the following constraint:



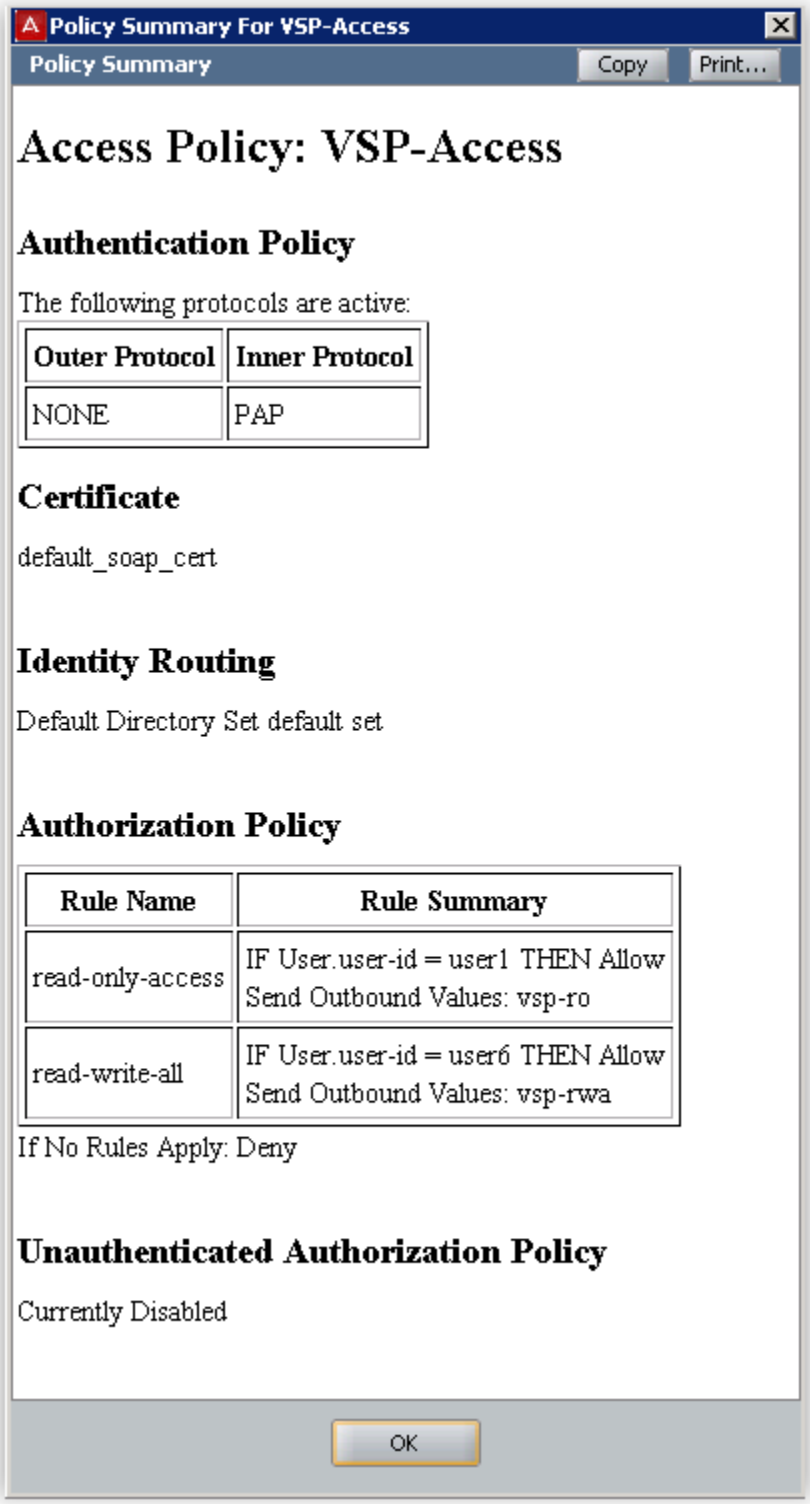
IDE Step 9 – Add the appropriate outbound attribute value for each rule

- **Click on the rule named *read-only-access,***
  - **Select *Action -> Allow.* From the *All Outbound Values* window, select the output attribute we created previously named *vsp-ro* and click on the less-than arrow key to move the attribute to the *Provision With* window**
- **Click on the rule named *read-write-all,***
  - **Select *Action -> Allow*. From the *All Outbound Values* window, select the output attribute we created previously named *vsp-rwa* and click on the less-than arrow key to move the attribute to the *Provision With* window**




Edit Authorization Policy
Rules
Name
Enabled
Action
read-only-acc...
Allow
read-write-all
Deny
Add...
Copy...
Remove
Selected Rule Details
Rule Name:
read-write-all
Rule Enabled
(
Constraint
)
AND/OR
User.user-id = user6
Action
Allow
Deny
Check Posture
NAP
Provisioning (Outbound Values)
Provision With
vsp-rwa
All Outbound Values
Admin-Access
NAS-Prompt
Session-Timeout
vsp-ro
Summary
IF User.user-id = user6 THEN Allow
Send Outbound Values: vsp-rwa
OK
Cancel

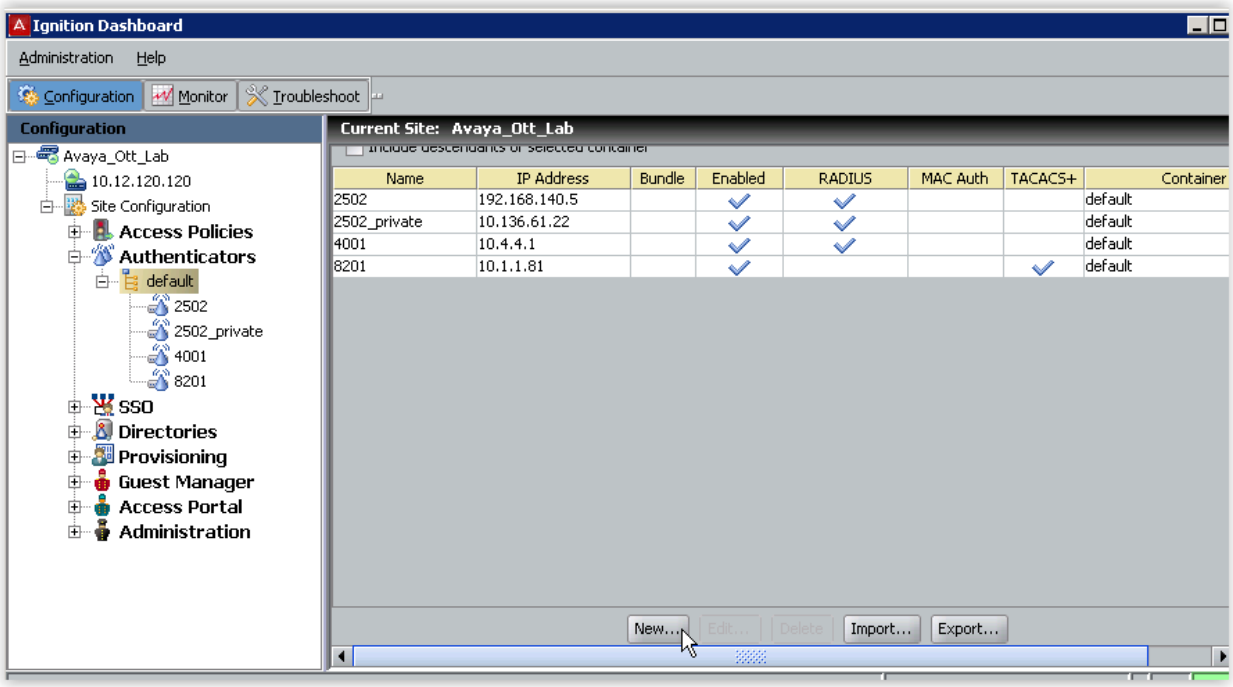
IDE Step 10 – When completed, you can view the complete policy by clicking on the *Access Policy Summary* button



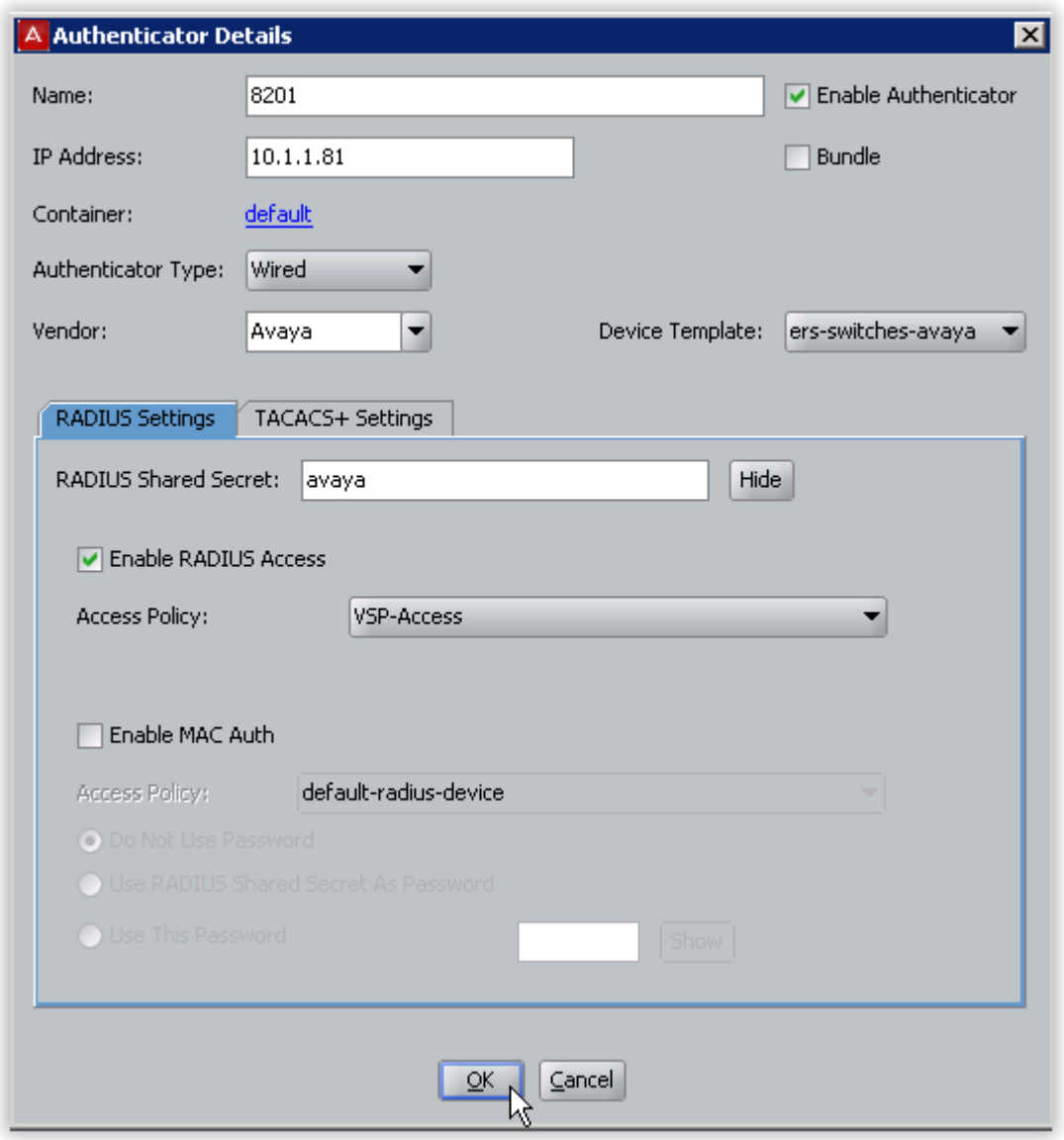
4.6.3.5 Add the Avaya VSP switch as an RADIUS Authenticator

For Ignition Server to process the Avaya switch RADIUS requests, each switch must be added as an Authenticator.

IDE Step 1 – Go to *Site Configuration -> Authenticators -> default* and click on *New*.



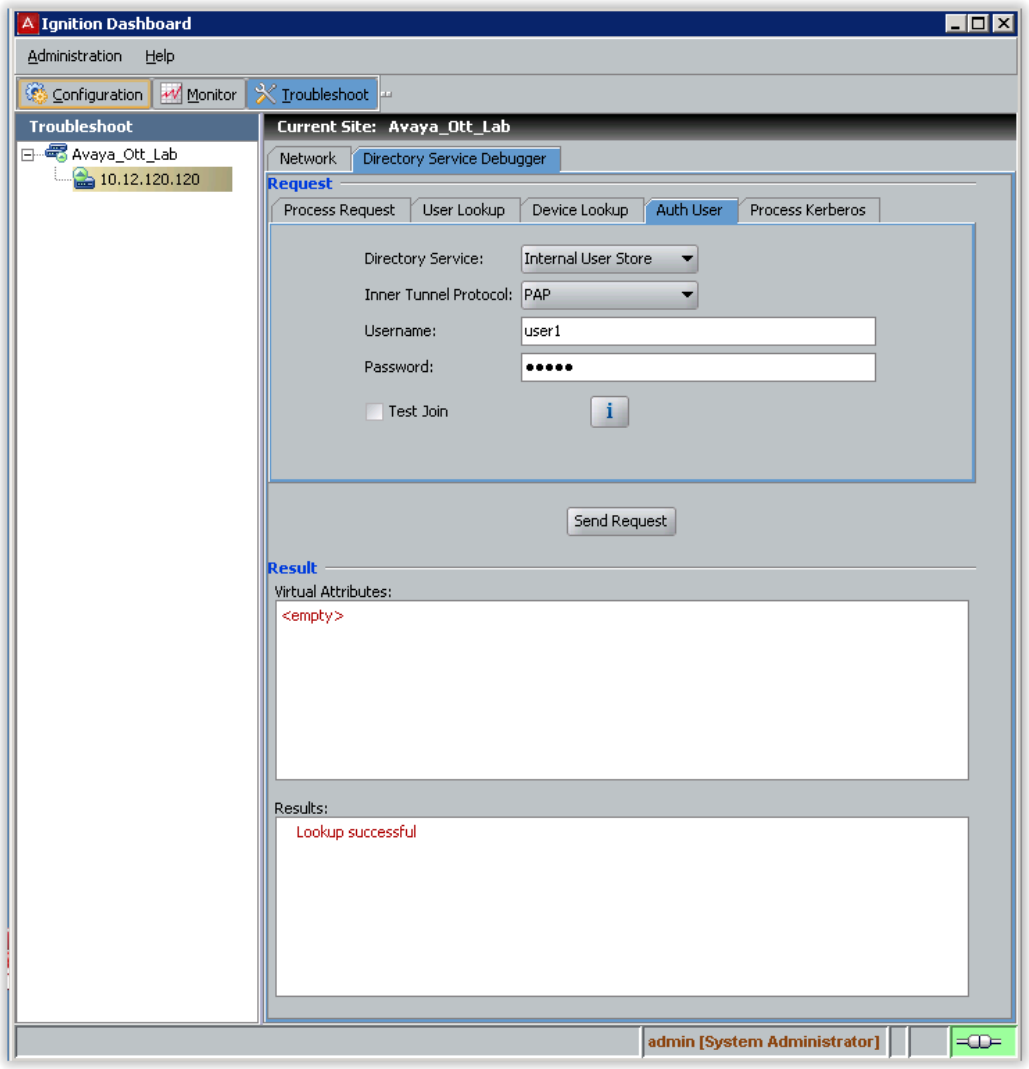
IDE Step 2 – Enter the settings as shown below making sure you select the policy we created previously named *ERS8000-Access* via *Access Policy*. Leave *Enable Authenticator* and *Enable RADIUS Access* checked. Click on *OK* when done.



4.6.4 Verify Operations

You can test user authentication for the VSP switch users configured on IDE by entering the user name and password.

IDE Step 1 – Via Ignition Dashboard, select the IP address of the Ignition Server, click on the *Troubleshoot* tab, go to *Directory Service Debugger* and select the *Auth User* tab. Make you select *Internal User Store* and *PAP* and the enter a valid user name and password configured for the VSP switch and click on *Send Request*. For more details, repeat the same steps but via the *Process Request* tab instead.



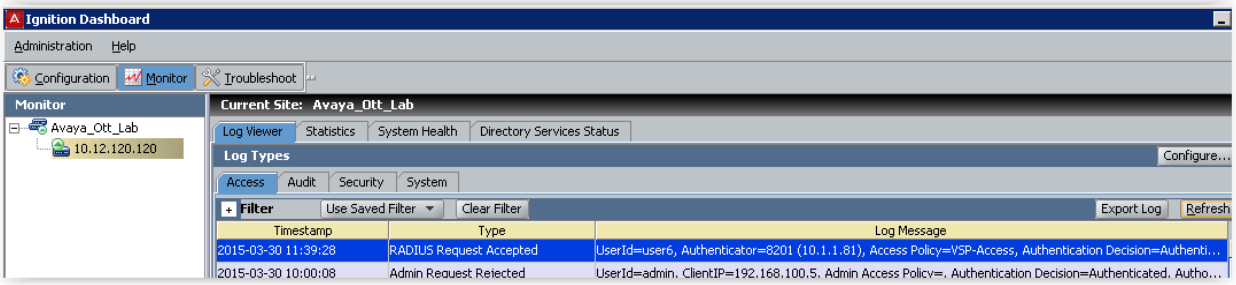
Via Dashboard, verify the following information:

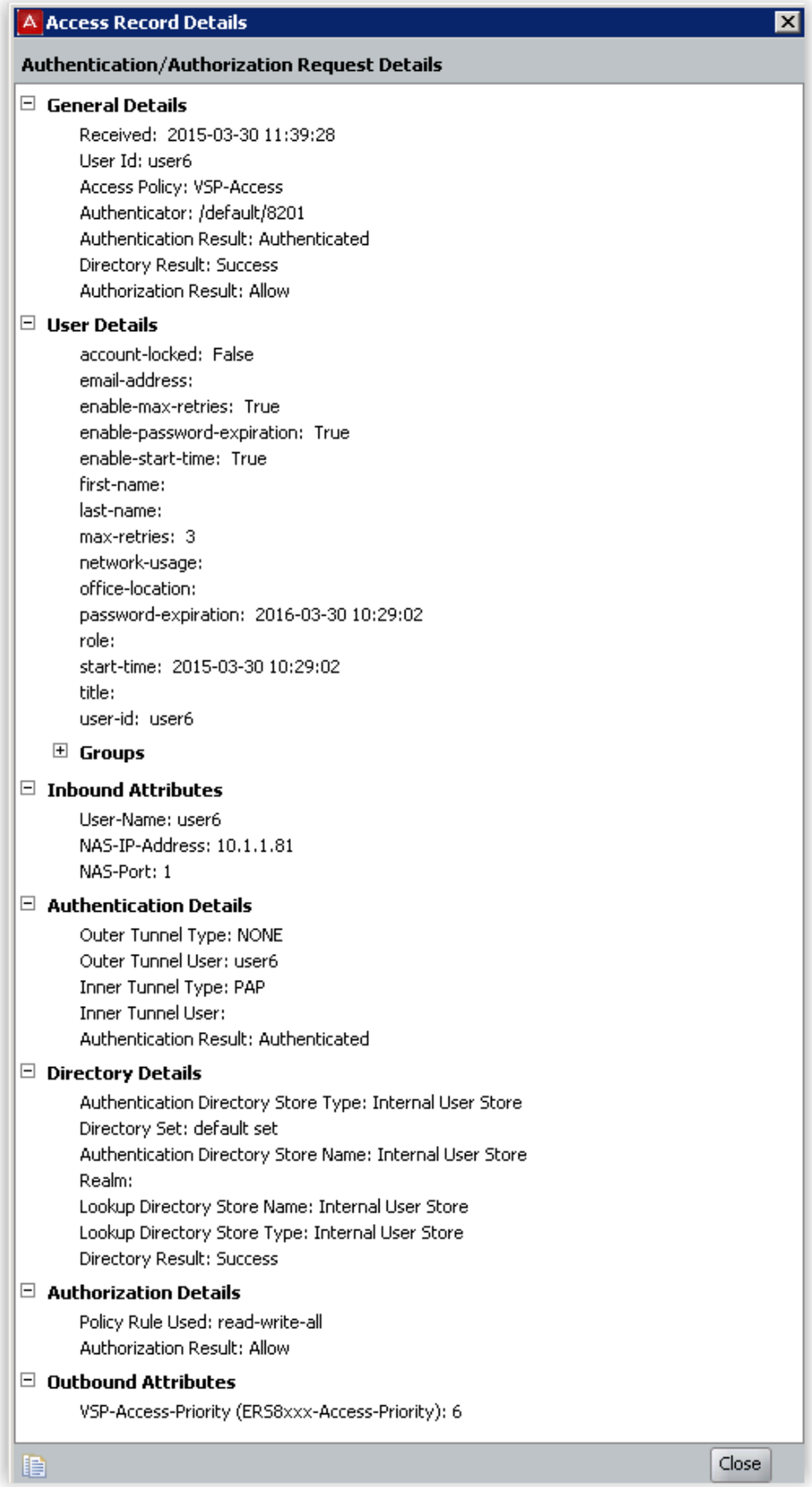
Option	Verify
Results	If successful, ***Authentication successful*** should be displayed

4.6.4.1 Verify user authentication from VSP switch

You can view the authentication details via Ignition Dashboard which provides extensive details about the device or user.

IDE Step 1 – In Dashboard, select the IP address of the Ignition Server and click on the *Monitor* tab, go to *Log Viewer*, and select the *Access* tab. Via the message of a valid user, right-click the message and select *Access Record Details*. Shown before are the results for the read-write-all-access user. Please note you should also see RADIUS accounting records upon a user logging onto and disconnecting from the VSP switch.




Access Record Details
Authentication/Authorization Request Details
General Details
Received: 2015-03-30 11:39:28
User Id: user6
Access Policy: VSP-Access
Authenticator: /default/8201
Authentication Result: Authenticated
Directory Result: Success
Authorization Result: Allow
User Details
account-locked: False
email-address:
enable-max-retries: True
enable-password-expiration: True
enable-start-time: True
first-name:
last-name:
max-retries: 3
network-usage:
office-location:
password-expiration: 2016-03-30 10:29:02
role:
start-time: 2015-03-30 10:29:02
title:
user-id: user6
Groups
Inbound Attributes
User-Name: user6
NAS-IP-Address: 10.1.1.81
NAS-Port: 1
Authentication Details
Outer Tunnel Type: NONE
Outer Tunnel User: user6
Inner Tunnel Type: PAP
Inner Tunnel User:
Authentication Result: Authenticated
Directory Details
Authentication Directory Store Type: Internal User Store
Directory Set: default set
Authentication Directory Store Name: Internal User Store
Realm:
Lookup Directory Store Name: Internal User Store
Lookup Directory Store Type: Internal User Store
Directory Result: Success
Authorization Details
Policy Rule Used: read-write-all
Authorization Result: Allow
Outbound Attributes
VSP-Access-Priority (ERS8xxx-Access-Priority): 6
Close

At minimum, verify the following items:

Option	Verify
Authentication Result	If successful, ***Authenticated*** should be displayed. If not, verify the device using the previous step and if this also fails, verify the Ignition Server configuration.
Authorization Result	If successful, ***Allow*** should be displayed. If not, verify the device using the previous step and if this also fails, verify the Ignition Server configuration.
User Id	Displays the name of the user id, in this example, a user id of ***user6*** was used for the user with read-write-all-access rights.
Access Policy	This field displays the Ignition Server policy used for this user which should be ***VSP-Acess*** as configured for this example.
Policy Rule Used Outbound Attribute	For this user, the Policy rule ***read-write-all*** as configured above should be used which sends an outbound vendor specific attribute value of ***6*** to the VSP switch telling the switch this user has read-write-all-access

5. Password Protection using TACACS+ Authentication

The VSP switch supports the Terminal Access Controller Access Control System plus (TACACS+) client. TACACS+ provides management of users who access the switch through Telnet, console, rlogin, web access through EDM, and SSHv1/v2 (password authentication) connections using Transmission Control Protocol (TCP).

The TACACS+ feature uses Transmission Control Protocol (TCP) for its transport to ensure reliable delivery of packets. TACACS+ provides security by encrypting all traffic between the switch, which acts as the Network Access Server, and the TACACS+ server.

The VSP switch supports level 1 to 6 and level 15 as shown in the table below.

Table 7: TACACS+ Access Levels

Access Level	Privilege Level
None	0 and 7 to 14
Read only	1
Layer 1 read write	2
Layer 2 read write	3
Layer 3 read write	4
Read write	5
Read write all	6
Read write all	15

Table 8: Enhanced Security TACACS+ Attributes

Access Level	VSA Attribute 26 – Vendor Identifier 1584 Type 192 value
None-Access	0, 4, 5, 7 to 14
Auditor	1
Security	2
Operator	3
Privilege	N/A – Not allowed by TACACS+
Admin	6
Admin	15

If you plan to use TACACS+ with enhanced secure mode, please enable TACACS+ after the enhanced mode is enabled. If TACACS+ is enabled prior to enabling the enhanced secure mode, the TACACS+ shared key must be re-entered; one must delete the shared key and re-enter it again.

The current implementation of TACACS+ does not support the following features:

- Point-to-Point Protocol (PPP) authentication and accounting
- IPv6 for TACACS+
- S/KEY (One Time Password) authentication
- PAP/CHAP/MSCHAP authentication methods
- The FOLLOW response of a TACACS+ server, in which the AAA services are redirected to another server. The response is interpreted as an authentication failure.
- User capability to change passwords at runtime over the network. The system administrator must change user passwords locally, on the server.
- TACACS+ command authorization when the user accesses the switch through EDM and SNMP.
- Restriction of command authorization for a specific kind of access. After you enable command authorization, command authorization applies for Telnet, SSH, rlogin, and serial-port access. You cannot restrict command authorization to just one kind of access.

5.1 Enabling TACACS+ globally

Enabling TACACS+ globally

```
VSPswitch(config):1:1#tacacs protocol enable
```

Adding a TACACS+ server

```
VSPswitch(config):1:1#tacacs server <host|secondary-host> <ip address>
VSPswitch(config):1:1#tacacs server <host|secondary-host> <ip address> key <word, 0-128>
VSPswitch:1(config)#tacacs server <host|secondary-host> <ip address> single-connection
VSPswitch:1(config)#tacacs server <host|secondary-host> <ip address> port <1-65535>
VSPswitch:1(config)#tacacs server <host|secondary-host> <ip address> timeout <10-30>
VSPswitch:1(config)#tacacs server <host|secondary-host> <ip address> source <ip address> source-ip-interface enable
```

The single connection parameter maintains a constant connection between the switch and the TACACS+ daemon that must also support this mode. If you do not configure single connenction, the switch uses the default connection type which is per-session or multi-connection mode.

Enabling TACACS+ authentication

```
VSPswitch:1(config)#tacacs authentication <all|cli|web>
```

Enabling TACACS+ authorization of level

```
VSPswitch:1(config)#tacacs authorization level <1-6|all|none>
```

Enabling TACACS+ accounting

```
VSPswitch:1(config)#tacacs accounting <disable|enable> cli
```

To delete or default a setting

```
VSPswitch:1(config)#no tacacs server <host|secondary-host>
VSPswitch:1(config)#no tacacs server <host|secondary-host> <option>
VSPswitch:1(config)#default tacacs server <host|secondary-host> <option>
```

5.2 Changing TACACS+ user levels

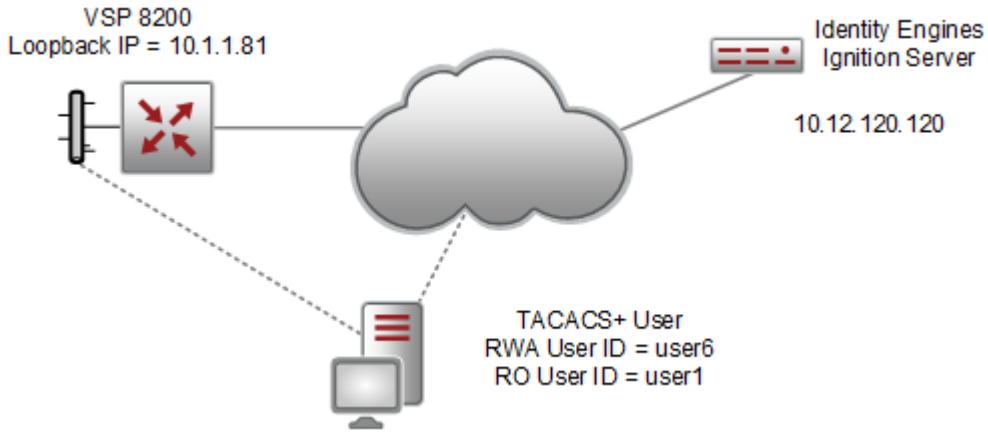
Users can also change their privilege levels when in configuration mode by issuing the following command:

- VSPswitch:1(config)#***tacacs switch level <1-6,15>***

If you do change access levels, the switch will send out an authentication request using a user-id of user-id of *$enab<x>$* will be used where x is in reference to the privilege level. Hence, you will need to add a user name on your TACACS+ server using this naming convention

5.3 TACACS+ Configuration Example

For this configuration example, we will configure the VSP switch for TACACS+ authentication and using the loopback address as the source IP. We will also show the configuration steps required using Avaya's Identity Engines Ignition Server.



5.3.1 VSP Switch Configuration

Step 1: Add loopback interface

```
VSPswitch:1(config)#interface loopback 1
VSPswitch(config-if)#ip address 1 10.1.1.81/255.255.255.255
VSPswitch(config-if)#exit
```

Step 2: Add TACACS+ server, enable TACACS+, and enable TACACS+ accounting

```
VSPswitch:1(config)#tacacs server host 10.12.120.120 key avaya source 10.1.1.81
source-ip-interface enable
VSPswitch:1(config)#tacacs authentication cli
VSPswitch:1(config)#tacacs accounting enable cli
VSPswitch:1(config)#tacacs protocol enable
```

5.3.2 Verify Operations

Step 1: Verify TACACS+ configuration

```
VSPswitch:1(config)#show running-config module tacacs
#
# TACACS CONFIGURATION
#
```

```
tacacs server  host 10.12.120.120 key ****** source 10.1.1.81 source-ip-interface
enable
tacacs protocol enable
tacacs accounting enable cli
```

Step 2: Verify TACACS+ global and server settings

```
VSPswitch:1(config)#show tacacs
Global Status:

   global enable : true

   authentication enabled for : cli

   accounting enabled for : cli

   authorization : disabled

   User privilege levels set for command authorization : None

Server:
                     create :

Prio      Status  Key     Port  IP address     Timeout Single Source     SourceEnabled
Primary   NotConn ******  49    10.12.120.120 10      false  10.1.1.81  true
```

Step 3: Verify TACACS+ users, i.e. assuming a TACACS+ using a user name of user6 via privilege level 6 has successfully been authenticated

```
VSPswitch:1(config)#show users
SESSION   USER                ACCESS    IP ADDRESS
Telnet0   user6               rwa       10.56.86.33 (current)
Console                       none      ----------
```

5.3.3 IDE TACACS+ Configuration

If we are using Identity Engines Ignition Server as the TACAC+ server, please follow the configuration steps below assuming we wish to add the following:

- User Name = user1
  - Privilege Level = 1
  - Read-only access
- User Name = user6
  - Privilege Level = 6
  - Read-write-all access

IDE Step 1 – *Go to Configuration -> <Site name> -> Services -> TACACS+*

Ensure that TACACS+ is enabled, if not, click the *Edit* box and enable TACACS+. The default port, TCP 49, should be left as-is.

IDE Step 2 – Add Users by going to *Configuration -> Site Configuration -> Directories -> Internal Store -> Internal Users* and click on *New*

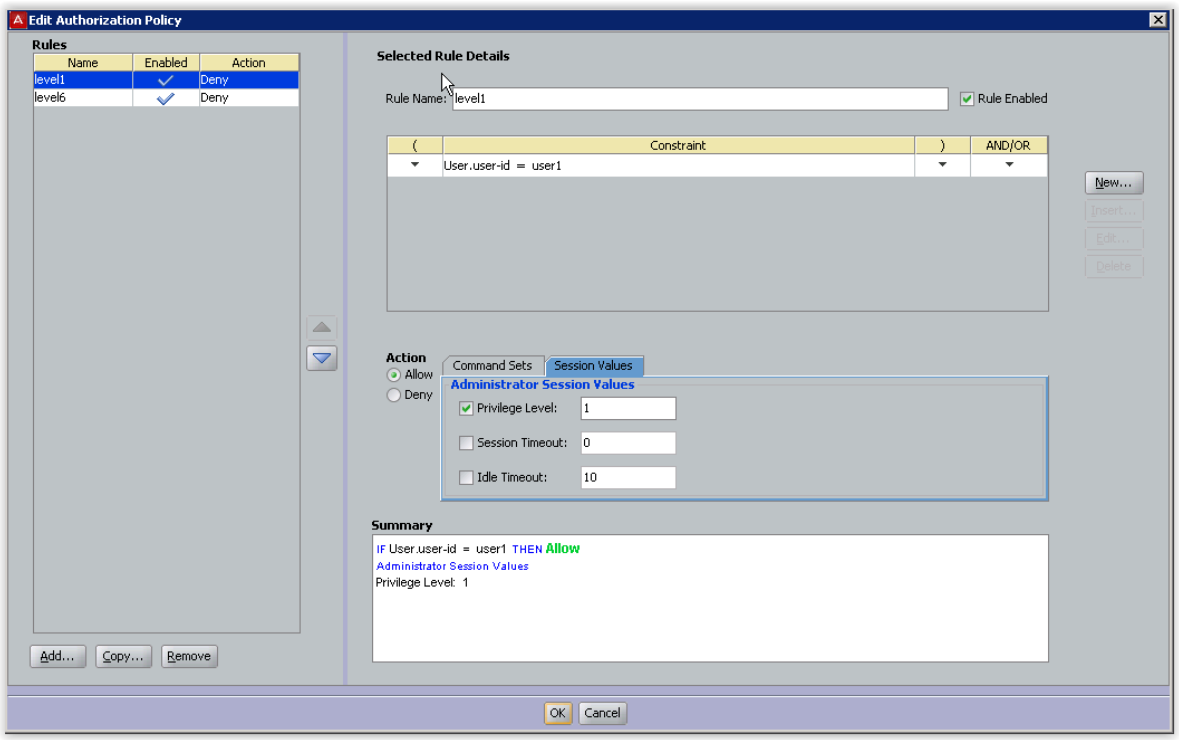
- Enter the user name of *user1* for read-only-access via *User Name*: and enter the password for this user via *Password* and *Confirm Password*. Click on *OK* when done. If you wish, you can also change the expiry date via *Password Expires* if you do not wish to use the default setting of one year.
- Repeat again by clicking on *New* to add *user6*.

IDE Step 3 – Add a new TACACS+ policy by going to *Configuration -> Site Configuration -> Access Policies -> TACACS+*

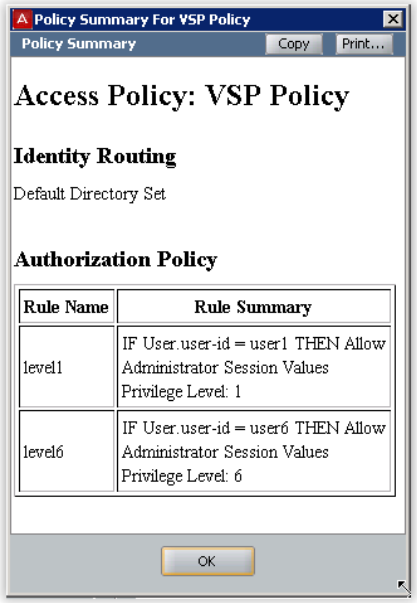
- Right-click *TACACS+* and select *New Access Policy…*
- Via the *New Access Policy* pop-up window, enter a policy name, i.e. *VSP Policy* as used in this example

IDE Step 4 – Go to *Configuration -> Site Configuration -> Access Policies -> TACACS+ -> VSP Policy* (name we configured in Step 3 above)

- Go to the *Authorization Policy* tab and click on *Edit.*
  - Once the *Edit Authorization Policy* window pops up, click on *Add* in the *Rules* window. Add two Rules simply named level1 and level6
  - For the rule named *level1*, click on *New* to add a new constraint. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None*, check *Static Value*, and enter the read-only-access user id of *user1*. Click on *OK* when done. Via *Action*, select *Allow*. Click on the *Session Values* tab, check off *Privilege Level* and enter 1.

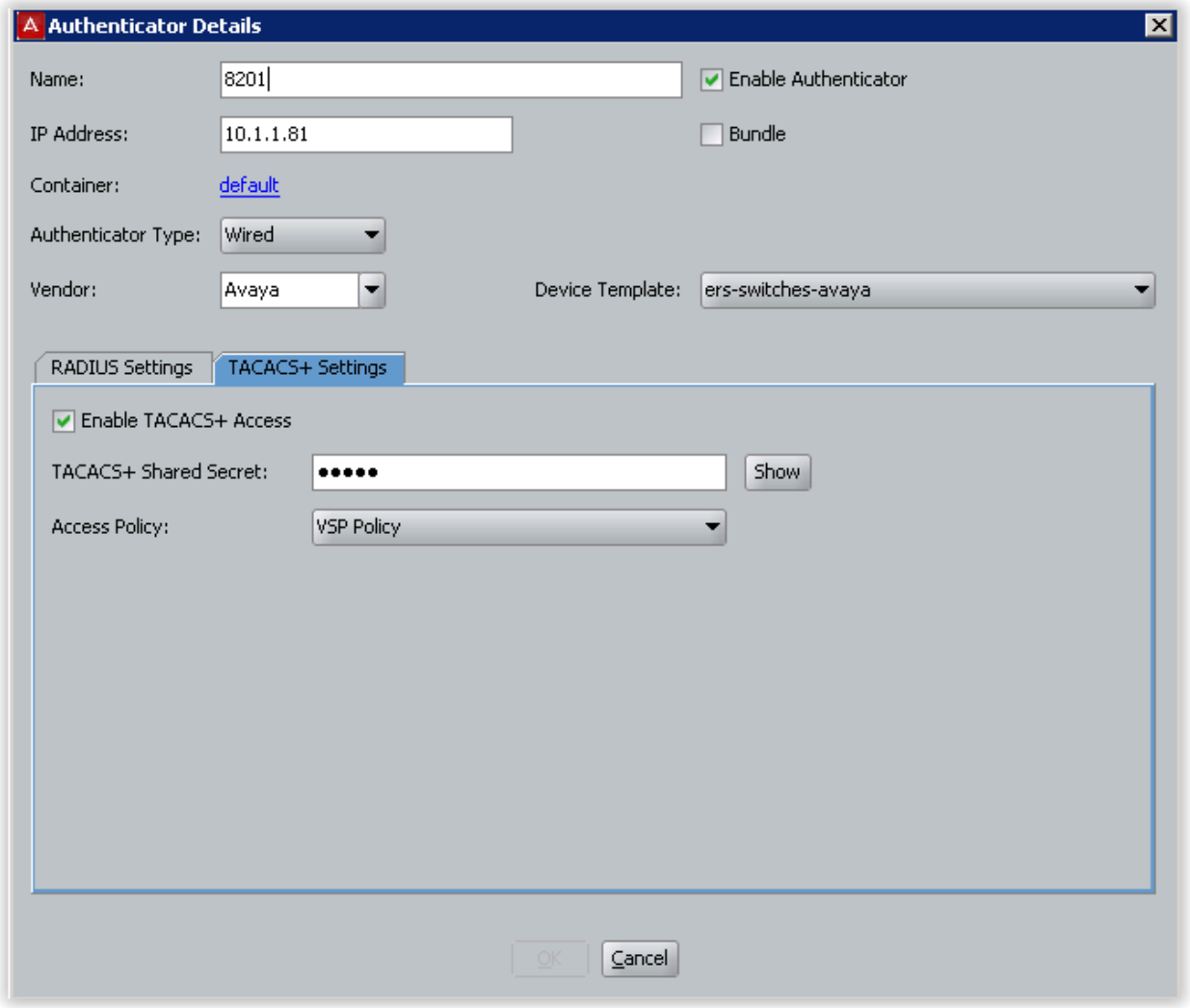


- For the rule named *level6*, click on *New* to add a new constraint. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None*, check *Static Value*, and enter the read-only-access user id of *user6.* Click on *OK* when done. Via *Action*, select *Allow*. Click on the *Session Values* tab, check off *Privilege Level* and enter 6.
- Click on *Ok* when done.
- When completed, you can view the complete policy by clicking on the *Access Policy Summary* button



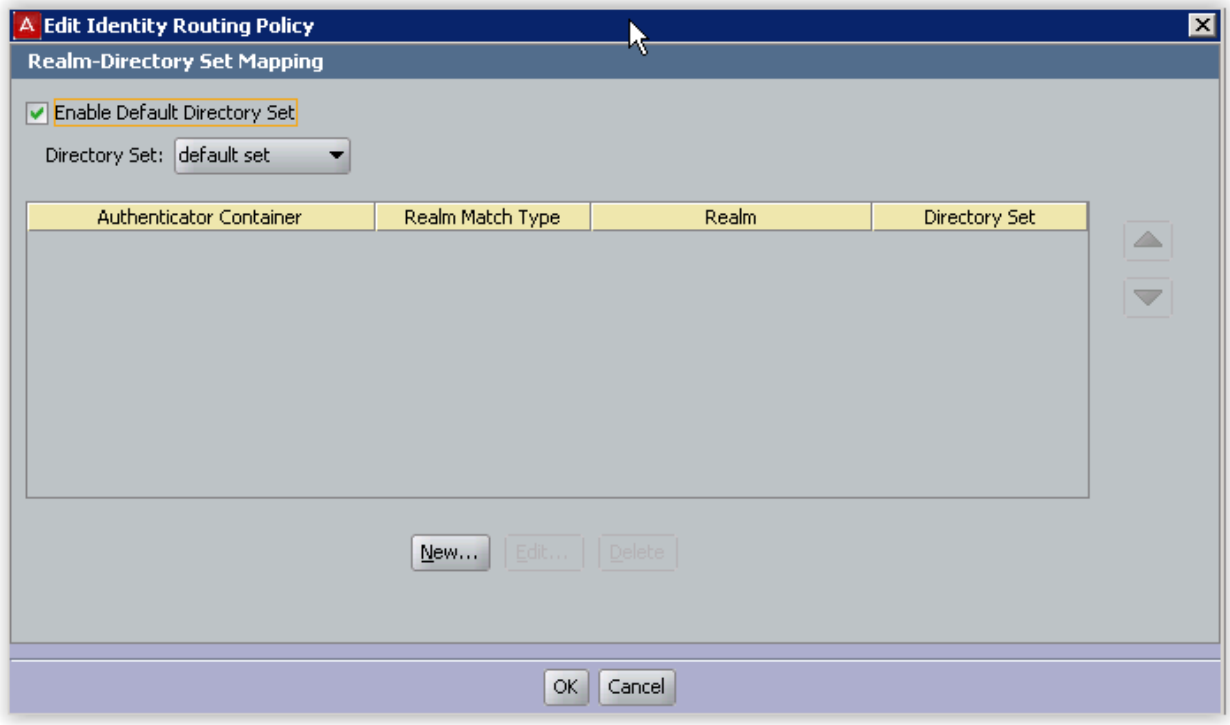
IDE Step 5 – Go to *Configuration ->Site Configuration -> Authenticators -> default*

- Click on *New*
- Enter a name for the switch via *Name*, add the switch IP address via *IP Address*, select *Wired* under *Authenticator Type*, select *Avaya* via *Vendor*, select *ers-switches-avaya* via *Device Template* and remove the default check via *Enable RADIUS Access*.
- Under the RADIUS Setting tab, uncheck the *Enable RADIUS Access* setting to disable RADIUS – this is the default setting
- Next, click on the *TACACS+ Settings* tab and check the *Enable TACACS+ Access* box, add the *TACACS+ Shared Secret*, and select TACACS+ policy name (i.e. *VSP Policy* as used in this example) via *Access Policy*:
- Click on *OK* when done. The configuration should look something like the following

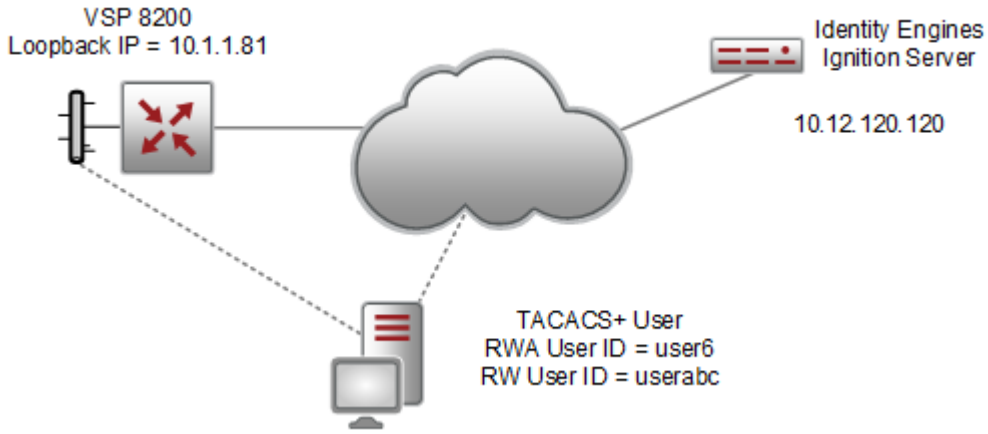


IDE Step 6 – Go to *Configuration ->Site Configuration -> Access Policies -> TACACS+ -> VSP Policy (Name of policy we created in Step 3 above)*

- Go to the *Identity Routing* tab and click on *Edit*
- Check the Enable *Default Directory Set* and then click on *Ok*



5.4 TACACS+ Configuration Example with Command Restrictions



For security reasons, we may wish to restrict users from using certain commands or restricting users from using specific configurable items such as VLAN ranges allowed.

You can enable TACACS+ command authorization for all level or you can select a specific level by adding the following ACLI command to the configuration used from the prevision example:

```
VSPswitch:1(config)#tacacs authorization level ?
   <1-6>  User privilege level
  all     Enable tacacs+ command authorization for all privilege-levels
  none    Disable tacacs+ command authorization for all levels
```

For this configuration example, we will use the same setup as the previous example with the addition of enabling command authorization for levels 3 to 6. Assuming we wish to create a two user accounts with that will allow the following:

- Read-write-all User
  - No command restriction
- Read-write user with the following rules
  - Enable configuration mode
  - Ability to show all parameters
  - Restrict the user to configure create and delete VLAN range 2000 to 2299
  - Restrict the user to add port members only within the VLAN range from 2000 to 2299

5.4.1 VSP Switch Configuration

VSP Switch Configuration

```
#
# TACACS CONFIGURATION
#


tacacs server  host 10.12.120.120 key ****** source 10.1.1.81 source-ip-interface
enable
tacacs protocol enable
tacacs accounting enable cli
tacacs authorization enable
tacacs authorization level 3
tacacs authorization level 4
tacacs authorization level 5
tacacs authorization level 6
```

5.4.2 IDE TACACS+ Configuration

If we are using Identity Engines Ignition Server as the TACAC+ server, please follow the configuration steps below assuming we wish to add the following:

- User Name = user6
  - All commands
- User Name = userabc
  - Privilege Level = 5
  - Read-write access
  - Limit VLAN configuration using VLAN range from 2000 to 2299
  - Limit VLAN port membership using VLAN range from 2000 to 2299

IDE Step 1 – *Go to Configuration -> <Site name> -> Services -> TACACS+*

Ensure that TACACS+ is enabled, if not, click the *Edit* box and enable TACACS+. The default port, TCP 49, should be left as-is.

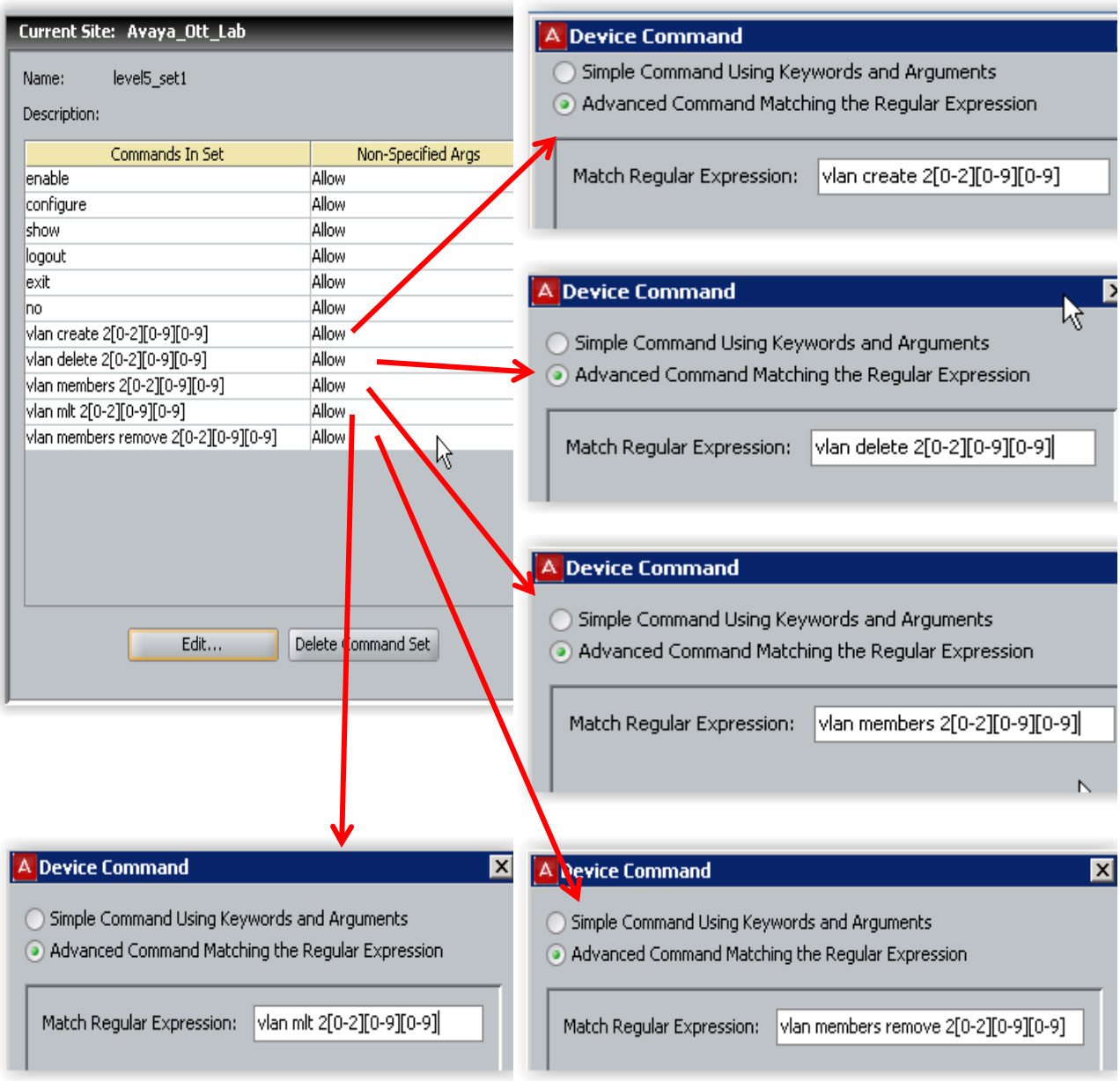
IDE Step 2 – Add Users by going to *Configuration -> Site Configuration -> Directories -> Internal Store -> Internal Users* and click on *New*

- Enter the user name of *user1* for read-only-access via *User Name*: and enter the password for this user via *Password* and *Confirm Password*. Click on *OK* when done. If you wish, you can also change the expiry date via *Password Expires* if you do not wish to use the default setting of one year.
- Repeat again by clicking on *New* to add *userabc*.

IDE Step 3– Add a new device command set by going to *Configuration -> Site Configuration -> TACACS+ -> Device Command Sets* and click on *New*

Via the *New Device Command Set* window, enter a name (***level5_set1*** as used in this example) and click on Add for each ACLI command set:

- For all the normal commands, via the *Device Command* window, select *Simple Command using Keywords and Arguments* and *Allow*
- For the command with ranges, via the *Device Command* window, select *Allow* first via the *Simple Command using Keywords and Arguments* tab and then click on the *Advanced Command Matching the Regular Expression* tab to add the regular expression

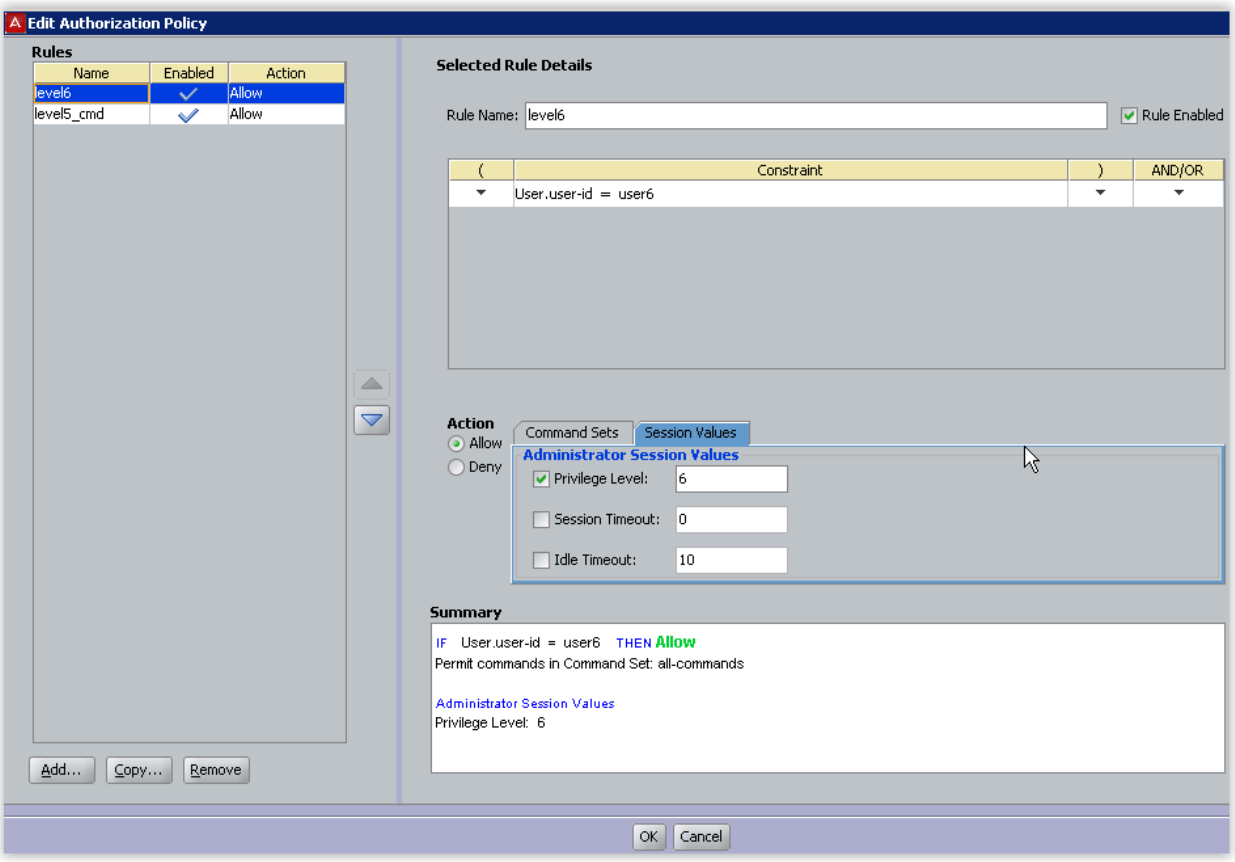


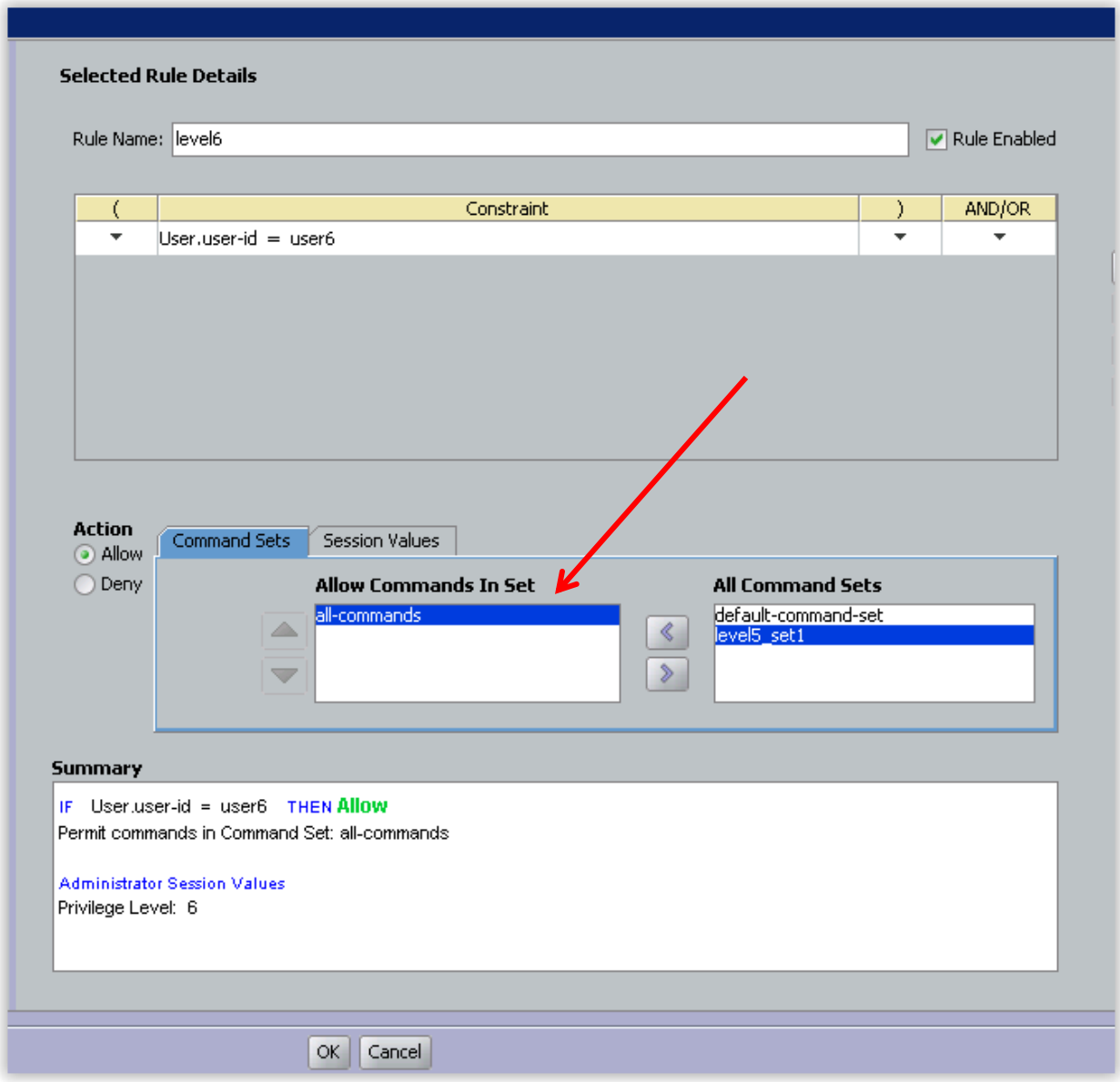
IDE Step 4 – Add a new TACACS+ policy by going to *Configuration* -> *Site Configuration* -> Access *Policies* -> *TACACS+*

- Right-click *TACACS+* and select *New Access Policy…*
- Via the *New Access Policy* pop-up window, enter a policy name, i.e. *VSP Policy* as used in this example

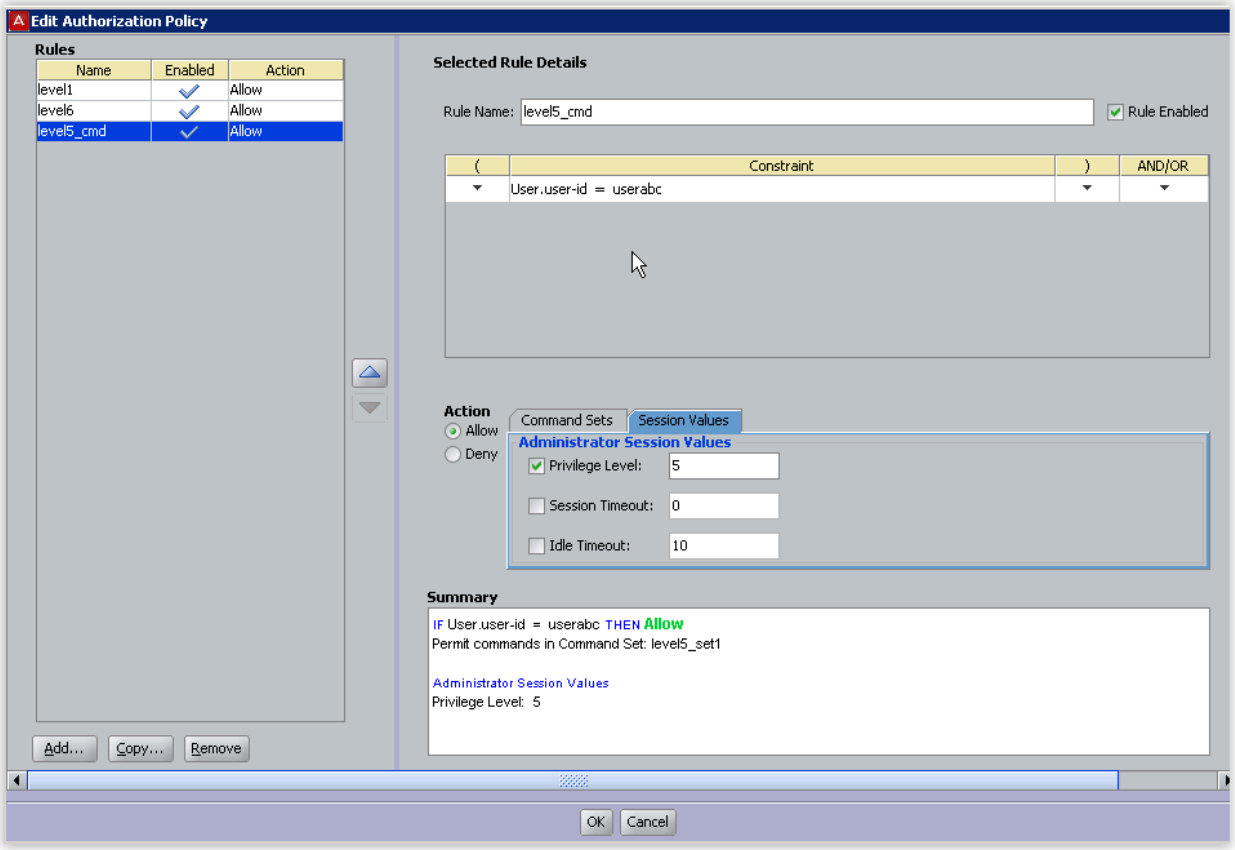
IDE Step 5 – Go to *Configuration* -> *Site Configuration* -> *Access Policies* -> *TACACS+* -> *VSP Policy* (name we configured in Step 4 above)

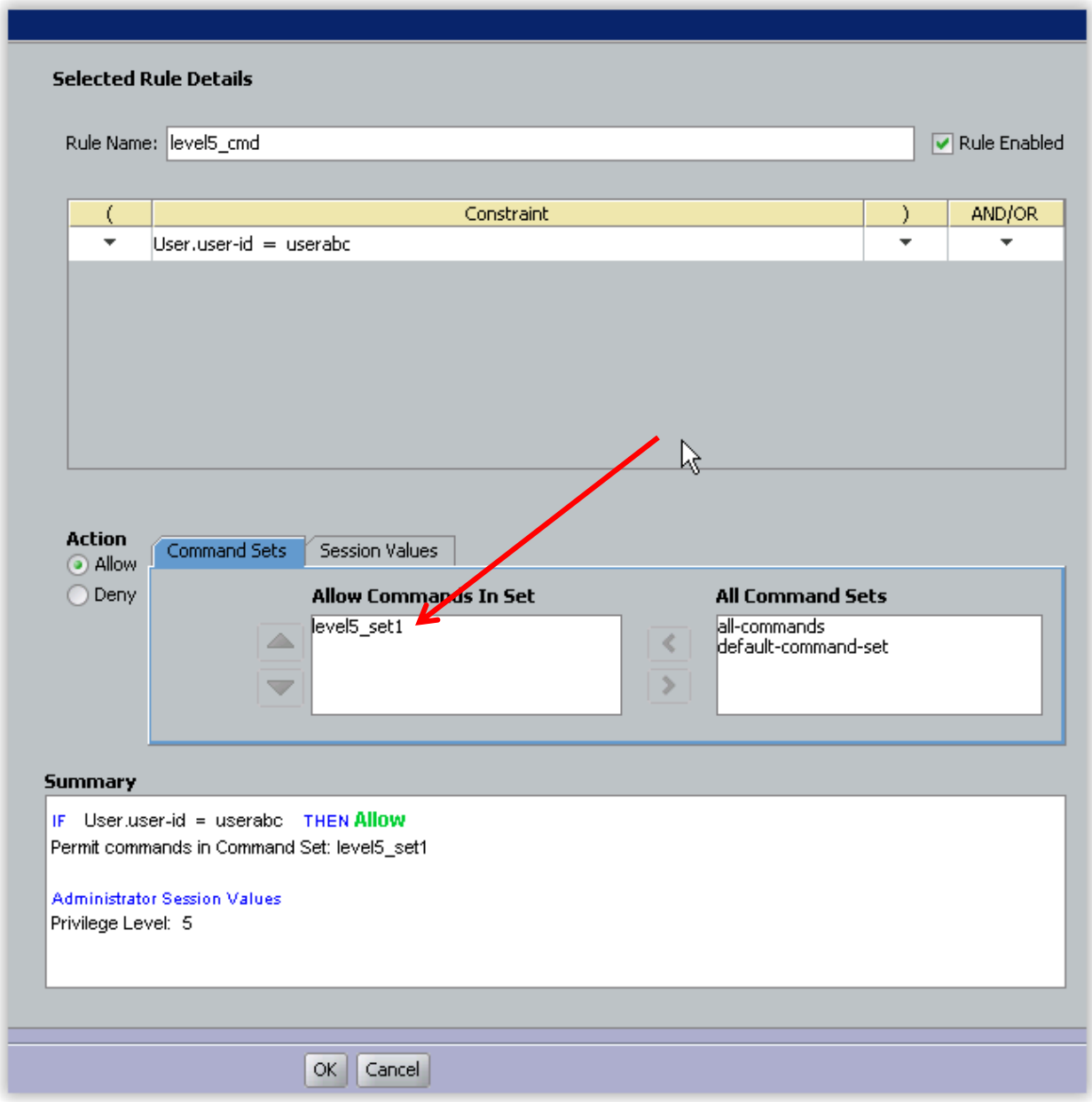
- Go to the *Authorization Policy* tab and click on *Edit.*
  - Once the *Edit Authorization Policy* window pops up, click on *Add* in the *Rules* window. Add two Rules simply named *level6* and *level5_cmd*
  - For the rule named *level6*, click on *New* to add a new constraint. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None*, check *Static Value*, and enter the read-write-all user id of *user6*. Click on *OK* when done. Via *Action*, select *Allow*. Click on the *Session Values* tab, check off *Privilege Level* and enter *6*. Via the *Command Sets tab*, select *all-commands* to move it to the *Allow Command in Set* window.



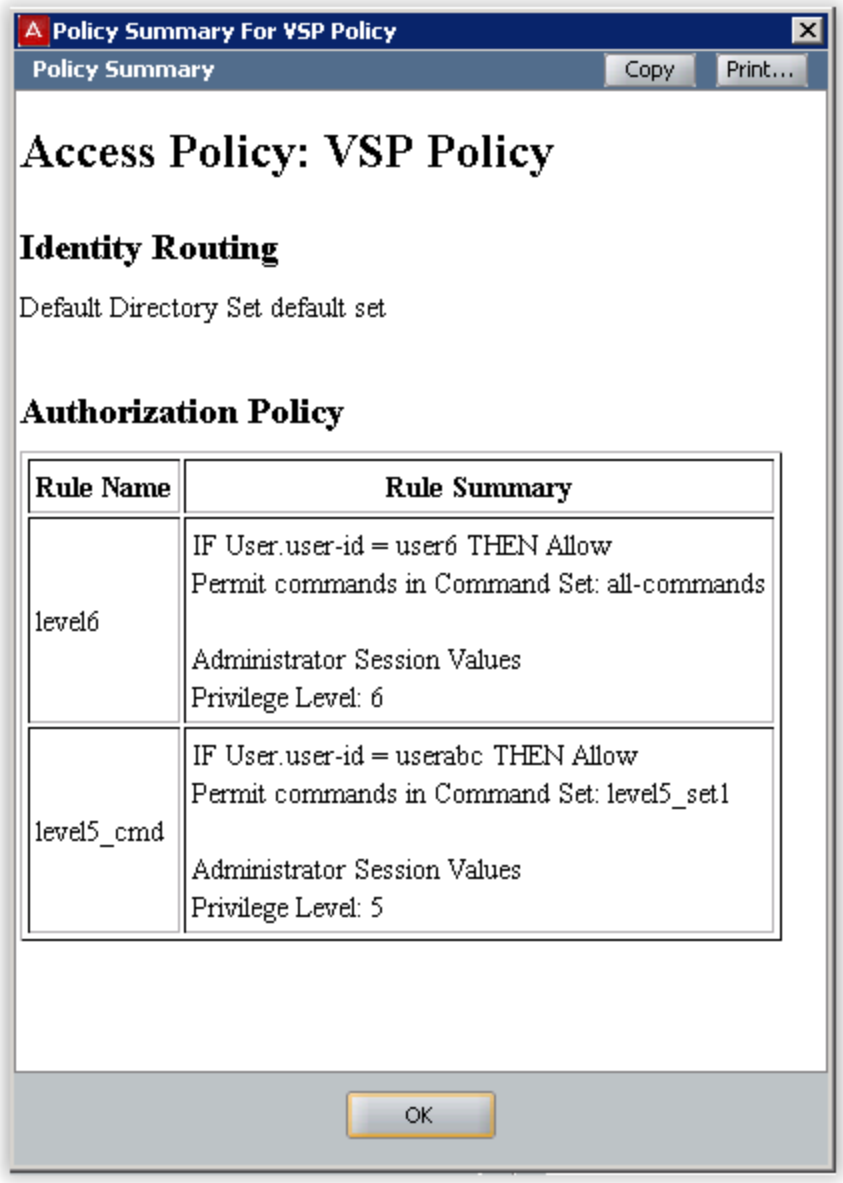

Selected Rule Details
Rule Name: level6
Rule Enabled
(Constraint) AND/OR
User.user-id = user6
Action
Allow
Deny
Command Sets
Session Values
Allow Commands In Set
all-commands
All Command Sets
default-command-set
level5_set1
Summary
IF User.user-id = user6 THEN Allow
Permit commands in Command Set: all-commands
Administrator Session Values
Privilege Level: 6
OK
Cancel

- For the rule named *level5_cmd*, click on *New* to add a new constraint. From *Attribute Category*, select *User* and scroll down and select *user-id*. Select *Equal To* with *Format* of *None*, check *Static Value*, and enter the read-only-access user id of *userabc.* Click on *OK* when done. Via *Action*, select *Allow*. Click on the *Session Values* tab, check off *Privilege Level* and enter *5*. Via the *Command Sets tab*, select *level5_set1* (name of device command rule used in step 3) to move it to the *Allow Command in Set* window.





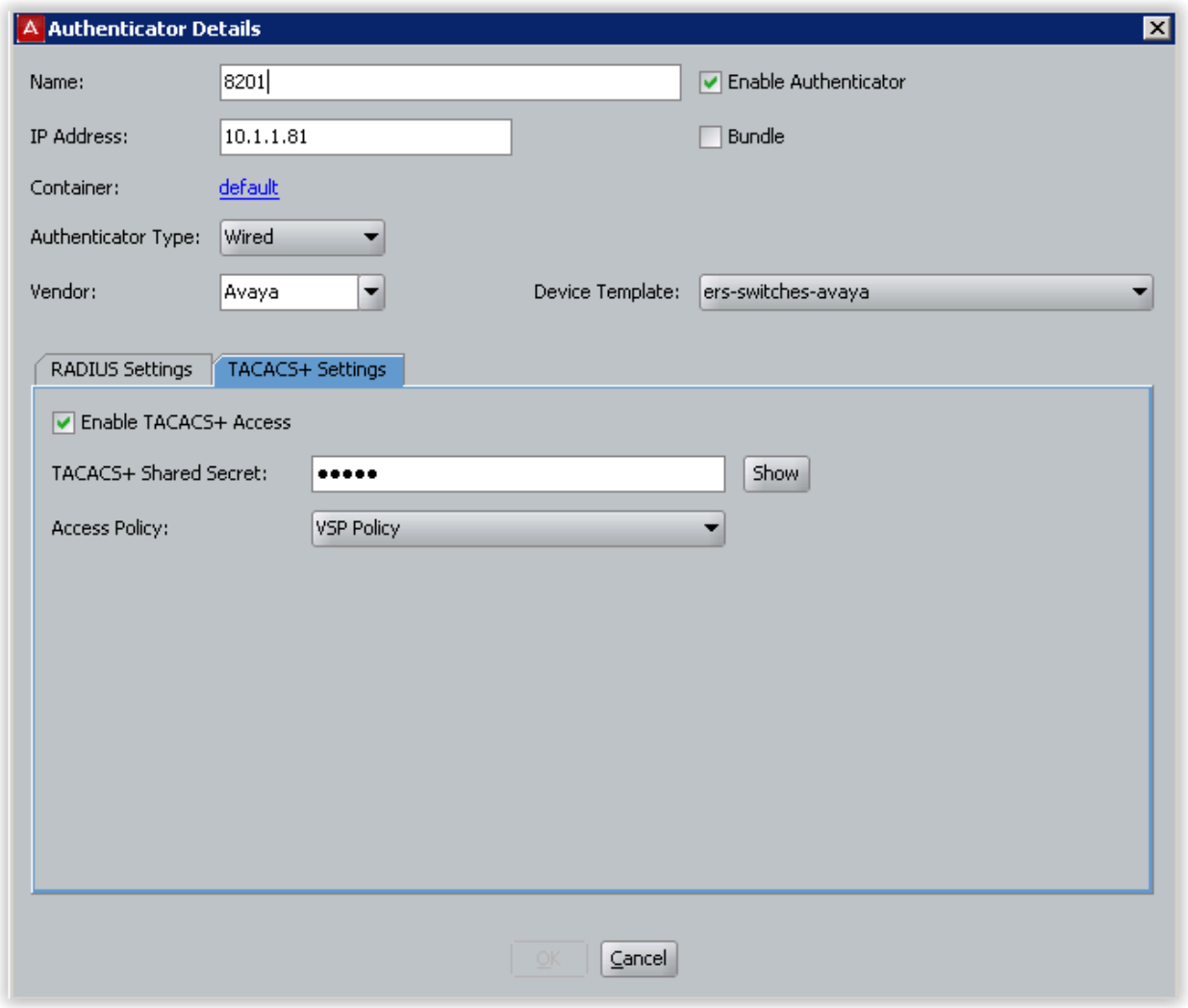
- When completed, you can view the complete policy by clicking on the *Access Policy Summary* button



IDE Step 6 – Go to *Configuration ->Site Configuration -> Authenticators -> default*

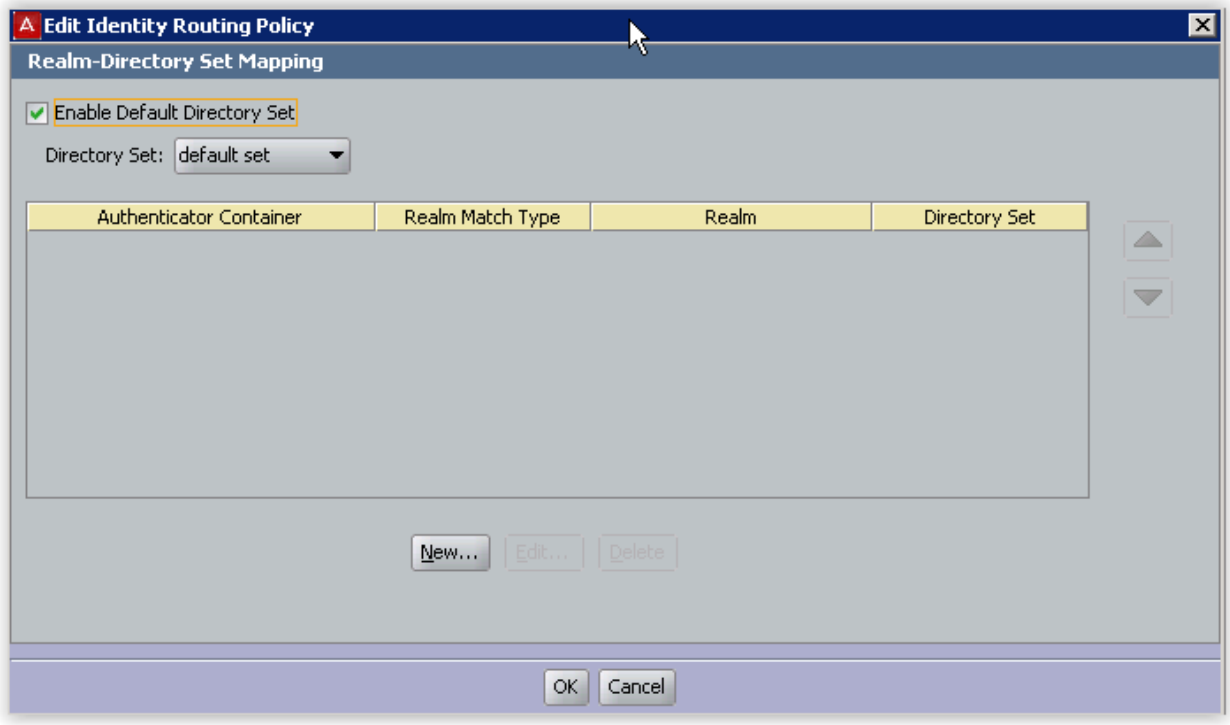
- Click on *New*
- Enter a name for the switch via *Name*, add the switch IP address via *IP Address*, select *Wired* under *Authenticator Type*, select *Avaya* via *Vendor*, select *ers-switches-avaya* via *Device Template* and remove the default check via *Enable RADIUS Access*.
- Under the RADIUS Setting tab, uncheck the *Enable RADIUS Access* setting to disable RADIUS – this is the default setting
- Next, click on the *TACACS+ Settings* tab and check the *Enable TACACS+ Access* box, add the *TACACS+ Shared Secret*, and select TACACS+ policy name (i.e. *VSP Policy* as used in this example) via *Access Policy*:

- Click on *OK* when done. The configuration should look something like the following



IDE Step 6 – Go to *Configuration ->Site Configuration -> Access Policies -> TACACS+ -> VSP Policy (Name of policy we created in Step 3 above)*

- Go to the *Identity Routing* tab and click on *Edit*
- Check the Enable *Default Directory Set* and then click on *Ok*



5.4.3 Verify Operations

Step 1: Verify TACACS+ global and server settings

```
VSPswitch:1(config)#show tacacs
Global Status:

   global enable : true

   authentication enabled for : cli

   accounting enabled for : cli

   authorization : enabled

   User privilege levels set for command authorization : l2 l3 rw rwa

Server:
                     create :

Prio      Status  Key     Port  IP address     Timeout Single Source     SourceEnabled
Primary   NotConn ******  49    10.12.120.120 10      false  10.1.1.81  true
```

Step 2: Verify TACACS+ users, i.e. assuming a TACACS+ using a user name of user6 via privilege level 6 has successfully been authenticated

```
VSPswitch:1(config)#show users
ESSION   USER                ACCESS    IP ADDRESS
Telnet0   user6                rwa       10.56.86.33 (current)
Console                       none      ----------
```

Step 3: Verify TACACS+ user userabc can only create/delete VLAN 2000-2299 and add port member

```
VSPswitch:1#show users
SESSION   USER                ACCESS    IP ADDRESS
Telnet0   userabc             rw        10.56.86.56 (current)
Console                       none      ----------
VSPswitch:1(config)#vlan create 1099 type port-mstprstp 0
                   ^
% Permission denied.
VSPswitch:1(config)#vlan create 2300 type port-mstprstp 0
```

```
                ^
% Permission denied.
VSPswitch:1(config)#vlan create 2000 type port-mstprstp 0
VSPswitch:1(config)#vlan members 2000 1/18
8201:1(config)#vlan members 1900 1/19
                ^
% Permission denied.
```

6. Secure Shell (SSH) and SFTP/SCP

The SSH protocol supports the following security features:

- Authentication. This feature determines, in a reliable way, the SSH client. During the login process, the SSH client is queried for a digital proof of identity.

  Supported authentications are public key (either RSA or DSA) and password

- Encryption. The SSHv2 server uses encryption algorithms to scramble data and render it unintelligible except to the receiver. Supported encryption and ciphers are:
  - VSP9000 and VOSS versions prior to 4.2: aes128-cbc, aes192-cbc, aes256-cbc, and 3des-cbc,3des
  - VOSS 4.2 or higher: aes128-cbc, aes256-cbc,3des-cbc, aes128-ctr,aes256-ctr, and aes192-ctr,aes192-cbc
- Integrity. This feature guarantees that the data is transmitted from the sender to the receiver without any alteration. If any third party captures and modifies the traffic, the SSH server detects this alteration. Supported hash algorithms are:
  - VSP9000 and VOSS versions prior to 4.2: hmac-md5,hmac-sha1,aead-aes-128-gcm-ssh,aead-aes-256-gcm-ssh,hmac-sha1-96,hmac-md5-96
  - VOSS 4.2 or higher: hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96

Secure Copy (SCP) and/or Secure File Transfer (SFTP) are off by default and enabled when SSH is enabled using the *boot config flags ssh* command. Please note the VSP 9000 and VOSS 4.1 or lower for the VSP 4000 or VSP 8000 only supports SCP while in the VOSS 4.2 release SFTP is supported.

SSH client is supported on the VSP switch. Authentication via password and DSA is supported; RSA is not supported. DSA keys can be generated, but, only equal to or less than 1024 bits.

The following table describes the third-party SSH and SFTP client software that have been tested with the VSP switch.

Table 9: SSH clients

SSH Client	Secure Shell (SSH)	SFTP or SCP

SecureCRT	• Supports SSHv2 client.
	• Authentication:
	  ○ RSA
	  ○ DSA
	  ○ Password
		• SecureFX distribution support SCP and SFTP
		Note: To display doted directory, in SecureFX, go to *Options -> Global Options* and via the Global Options popup window, go *to File Transfer -> View* and make sure *Do not show dot files* is not checked

Putty	• Supports SSH-2 client.
	• Authentication:
	  ○ RSA
	  ○ DSA
	  ○ Password
		• Client distribution includes both a SFTP and SCP client

OpenSSH	• Supports SSHv2 clients.	• Client distribution includes SCP

Linux/Unix/Cygwin	• Authentication:
	  ○ RSA
	  ○ DSA
	  ○ Password
		and SFTP

FileZilla		• Includes SFTP support

After you install one of the SSHv2 clients you must generate a client and server key using the RSA or DSA algorithms if you wish to use public key authentication. Please note that the VSP switch when acting as an SSH server can only support one PKI key per access level, i.e. one key file per rwa, rw, ro, etc. access level.

The VSP switch generates a DSA server and client keys stored in the following location respectively:

```
/intflash/.ssh/ssh_dsa.key
/intflash/.ssh/id_dsa_rwa (private key for DSA client)
/intflash/.ssh/id_dsa_rwa.pub (public key for DSA client)
```

If a DSA key pair does not exist, then the VSP modular switch automatically generates one when you enable the SSHv2 server.

To authenticate an SSHv2 client using DSA, the administrator must copy the public part of the client DSA key to /intflash/.ssh directory on the VSP switch that is acting as the SSHv2 server. That file that is copied over to the SSHv2 server must be named according to Table 10 shown below.

Table 10: DSA authentication access level and file name

Client key format	Access Level	File name VSP 9000 and VOSS 4.1 or lower (VSP 4000/8000)
Client key in IETF format (SSHv2)	RWA	*/intflash/.ssh/dsa_key_rwa_ietf*
	RW	*/intflash/.ssh/dsa_key_rw_ietf*
	RO	*/intflash/.ssh/dsa_key_ro_ietf*
	L3	*/intflash/.ssh/dsa_key_rwl3_ietf*
	L2	*/intflash/.ssh/dsa_key_rwl2_ietf*
	L1	*/intflash/.ssh/dsa_key_rwl1_ietf*
Client key in non IETF format	RWA	*/intflash/.ssh/dsa_key_rwa*
	RW	*/intflash/.ssh/dsa_key_rw*
	RO	*/intflash/.ssh/dsa_key_ro*
	L3	*/intflash/.ssh/dsa_key_rwl3*
	L2	*/intflash/.ssh/dsa_key_rwl2*
	L1	*/intflash/.ssh/dsa_key_rwl1*

Please note that for the VSP 9000 only, the client keys in IEFT format requires the key to end with “ietf.

Client key format	Access Level	File name VSP 4000 & VSP 8000 – VOSS 4.2 or higher
Client key in non IETF and IETF format with enhanced secure mode disabled	RWA	*/intflash/.ssh/dsa_key_rwa*
	RW	*/intflash/.ssh/dsa_key_rw*
	RO	*/intflash/.ssh/dsa_key_ro*
	L3	*/intflash/.ssh/dsa_key_rwl3*
	L2	*/intflash/.ssh/dsa_key_rwl2*
	L1	*/intflash/.ssh/dsa_key_rwl*
Client key with enhanced secure mode enabled	Administrator	*/intflash/.ssh/dsa_key_admin*
	Operator	*/intflash/.ssh/dsa_key_operator*
	Security	*/intflash/.ssh/dsa_key_security*
	Privilege	*/intflash/.ssh/dsa_key_priv*
	Auditor	*/intflash/.ssh/dsa_key_auditor*

The VSP switch support IETF and non-IETF for DSA.

The VSP switch generates a RSA only server key stored in the following location respectively:

```
/intflash/.ssh/ssh_rsa.key
```

If a RSA key pair does not exist, then the VSP modular switch automatically generates one when you enable the SSHv2 server.

The following table lists the access levels and file names you can use for storing the SSH client authentication information using RSA.

Table 11: RSA authentication access level and file name

Client key format	Access level	File name
Client key in IETF format with enhanced secure mode disabled	RWA	*/intflash/.ssh/rsa_key_rwa*
	RW	*/intflash/.ssh/rsa_key_rw*
	RO	*/intflash/.ssh/rsa_key_ro*
	L3	*/intflash/.ssh/rsa_key_rwl3*
	L2	*/intflash/.ssh/rsa_key_rwl2*
	L1	*/intflash/.ssh/rsa_key_rwl1*
Client key in IETF format with enhanced secure mode enabled	administrator	*/intflash/.ssh/rsa_key_admin*
	operator	*/intflash/.ssh/rsa_key_operator*
	privilege	*/intflash/.ssh/rsa_key_priv*
	auditor	*/intflash/.ssh/rsa_key_auditor*

6.1 SSH Configuration Example – Password Authentication

6.1.1 Configuration

The following is a configuration example showing how to configure SSH password authentication. The user credentials can either be the local user passwords stored on the switch or you could use an external server such as RADIUS to authenticate the users. This example only covers the SSH configuration and not the user password configuration.

If you are using RADIUS or TACACS+ for password authentication, please setup the RADIUS or TACACS+ server referring to the sections titled *Password Protection using RADIUS Authentication* and *Password Protection using TACACS+ Authentication*.

Step 1: Enable the SSH boot flag

```
VSPswitch:1(config)#boot config flags sshd
VSPswitch:1(config)#save config
```

Step 2: Enable SSH globally

```
VSPswitch:1(config)#ssh
```

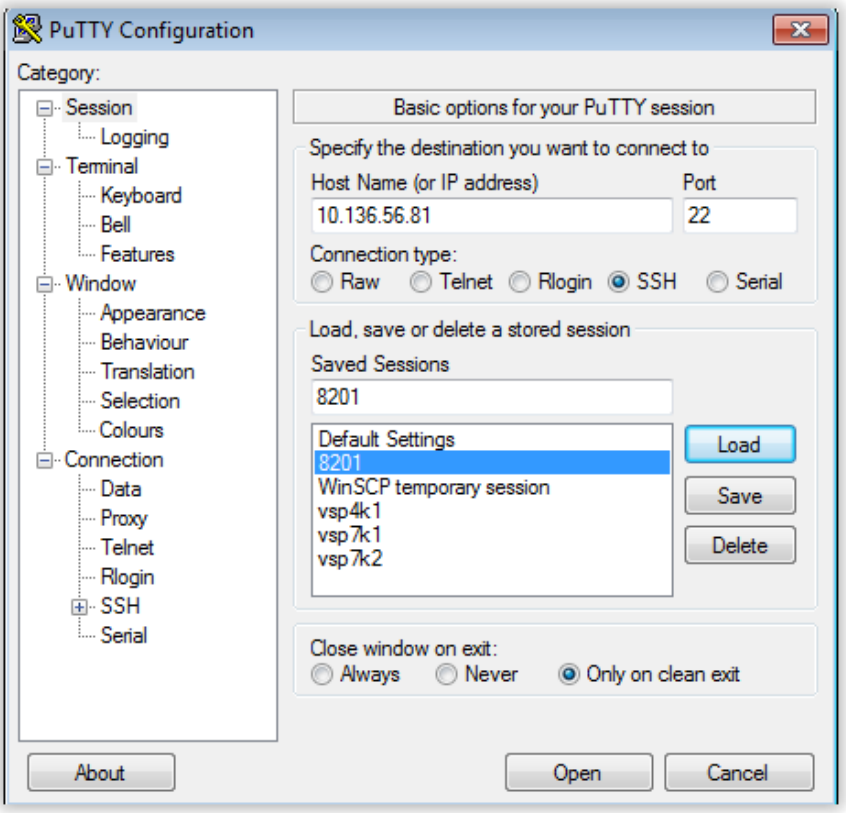
Step 3: Enable SSH password authentication – enabled by default

```
VSPswitch:1(config)#ssh pass-auth
```

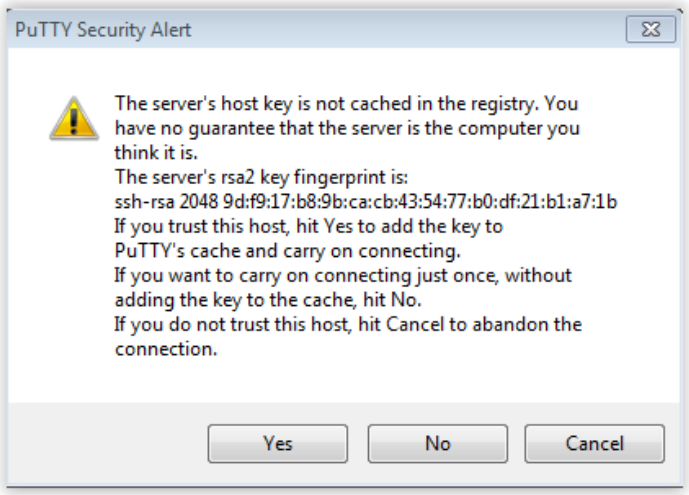
Step 4: Enable SSH secure mode

```
VSPswitch:1(config)#ssh secure
Securely enable SSH; set boot flags of telnet/rlogin/ftp/tftp/snmp daemon to false,
continue? (y/n) ? y
```

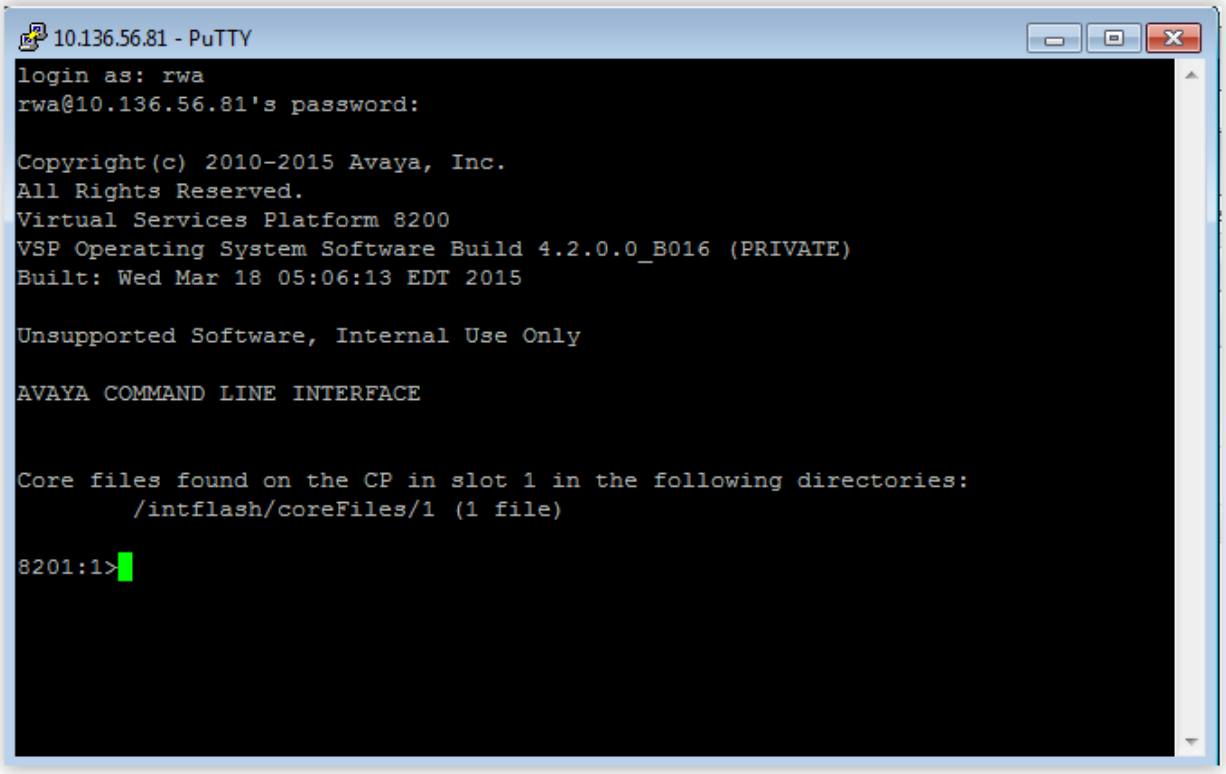
Step 5: Open up Putty and go to Session -> Host Name (or IP address), enter the IP address of the switch, select SSH, and click on Open when done



Step 6: Click on Yes when prompted with the public key fingerprint. You will only be prompted with this message once, unless, you select No to accept to accept this fingerprint, but, not save it.



Step 4: Enter login credentials



Step 5: Using SSH to connect to another switch

```
VSPswitch(config):1:1#exit
VSPswitch:1#ssh 10.136.56.82 -l rwa
Trying 10.136.56.82 ...
Are you sure you want to continue?  (y/n) ? y
rwa@10.136.56.82's password: ******
```

6.1.2 Verify Operations

Step 1: Verify SSH session

```
VSPswitch:1#show ssh session
        SSH Session ID : 0
        User Name      : rwa
        Host           : 10.55.72.46
```

Step 2: Verify SSH configuration

```
VSPswitch:1(config)#show ssh global
Total Active Sessions  : 1
        version            : v2only
        port               : 22
        max-sessions       : 4
        timeout            : 60
        action rsa-keygen  : rsa-keysize 2048
        action dsa-keygen  : dsa-keysize 2048
        rsa-auth           : true
        dsa-auth           : true
        pass-auth          : true
        enable             : secure
```

Step 3: Verify SSH session via log file

```
VSPswitch:1#show logging file module SSH
CP1  [03/26/15 11:32:19.436:EDT] 0x000d8602 00000000 GlobalRouter SSH INFO SSH CLI
session start: user rwa on host 10.55.72.46
CP1  [03/26/15 11:32:19.365:EDT] 0x000d8602 00000000 GlobalRouter SSH INFO SSH user
authentication succeeded for user rwa on host 10.55.72.46
```

6.2 SSH Configuration Example –Public Key Authentication

6.2.1 Configuration

Using Public Key Authentication is more involved than using SSH password authentication. On the Client, a set of keys (i.e. public/private) must be generated. The client's public key must then be transferred to the switch using SCP, SFTP, ftp, or tftp. Note that if SSH secure mode is enabled, ftp and tftp will be disabled by default, but, you have to choice to re-enable both or either of these features again.

Putty will be used as the SSH Client while Puttygen will be used to generate the DSA key pairs. We will use the DSA key names of *dsa_key_rwa* and *vsppriv.ppk* for the public and private key names. The DSA public key generated by Puttygen must be transferred to the VSP switch using the naming convention shown in table 10 above.

Step 1: Enable the SSH boot flag

```
VSPswitch:1(config)#boot config flags sshd
VSPswitch:1(config)#save config
```

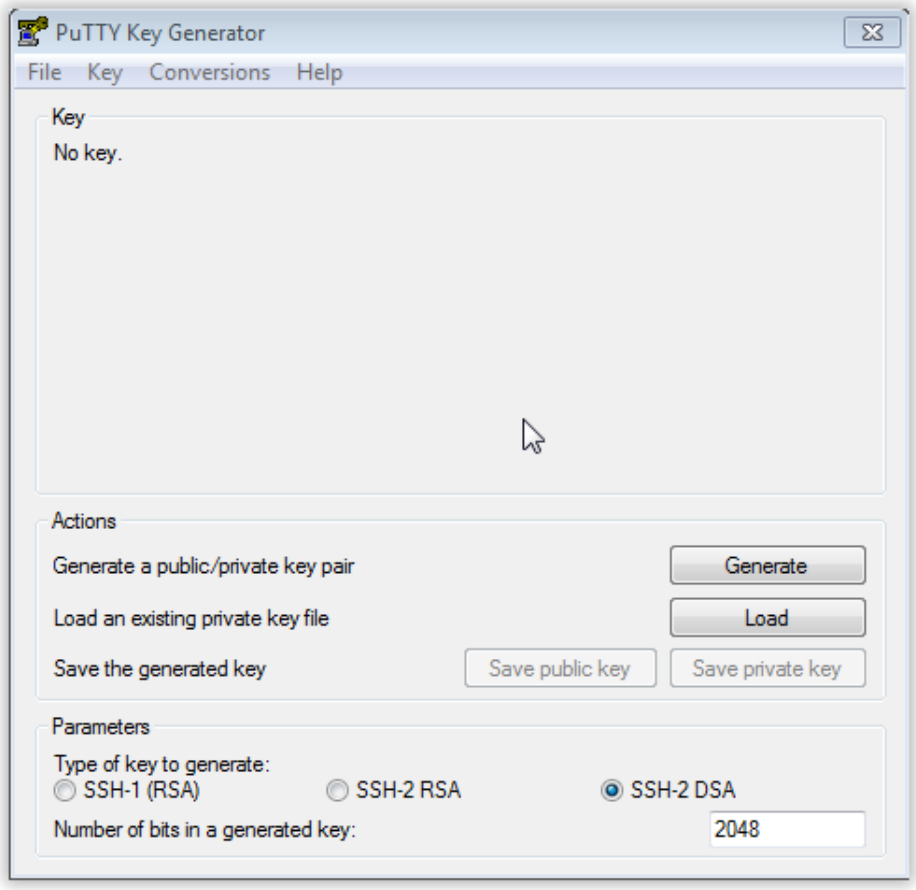
Step 2: Enable SSH globally

```
VSPswitch:1(config)#ssh
```

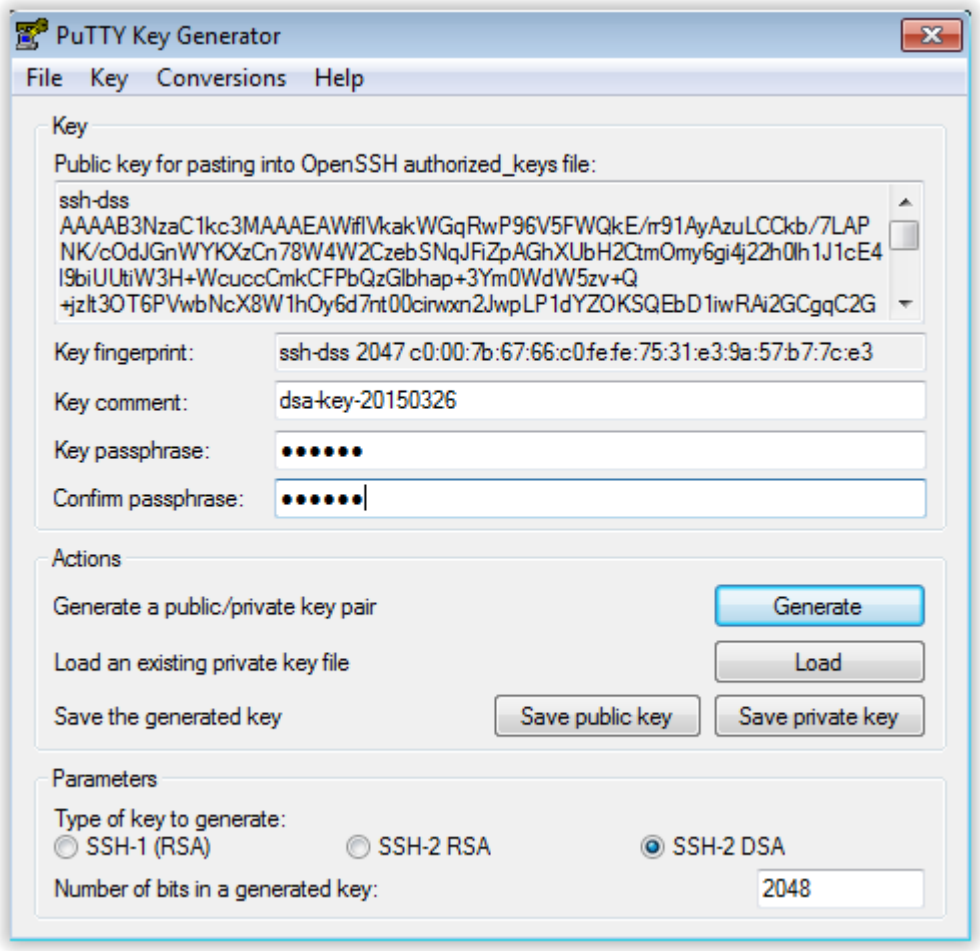
Step 3: Enable SSH secure mode

```
VSPswitch:1(config)#ssh secure
Securely enable SSH; set boot flags of telnet/rlogin/ftp/tftp/snmp daemon to false,
continue? (y/n) ? y
```

Step 4: Run Puttygen and select SSH-2 DSA key with 2048 bits and click on Generate to create both a public and private key. The public key will be uploaded to the switch. You will be prompted to move your mouse to create the key



Step 5: Enter a Key passphrase to be used with this key and click on both Save public key and private key. You will be prompted to enter a file name; i.e. for this example, *dsa_key_rwa* was used for the public key and *vsppriv.ppk* was used for the private key



Step 6: Assuming we are using PSCP, SFTP, or Filezilla, copy the public key (dsa_key_rwa in this example) over to the VSP switch. If you have two CPU cards, then this process must repeated twice, once for each CPU card. In this example, the PSCP and SFTP program is located via the directory c:\putty. Please note, the file name must use the file naming as shown in table 10 above. The file name will be */intflash/.ssh/dsa_key_rwa_ietf* if an VSP9000 or */intflash/.ssh/dsa_key_rwa* for all other VSP models using VOSS 4.2 or higher

SCP using Putty (VSP9000):

```
Go to the directory where PSCP is installed and then enter the following command and
assuming the remote switch is a VSP 8200:

pscp c:\putty\vspkey.pub rwa@10.136.56.81:/intflash/.ssh/dsa_key_rwa

rwa@10.136.56.81's password: <enter rwa password>

vspkey.pub                |          1 kB |   1.2 kB/s | ETA: 00:00:00 | 100%

Fatal: Server unexpectedly closed network connection
```

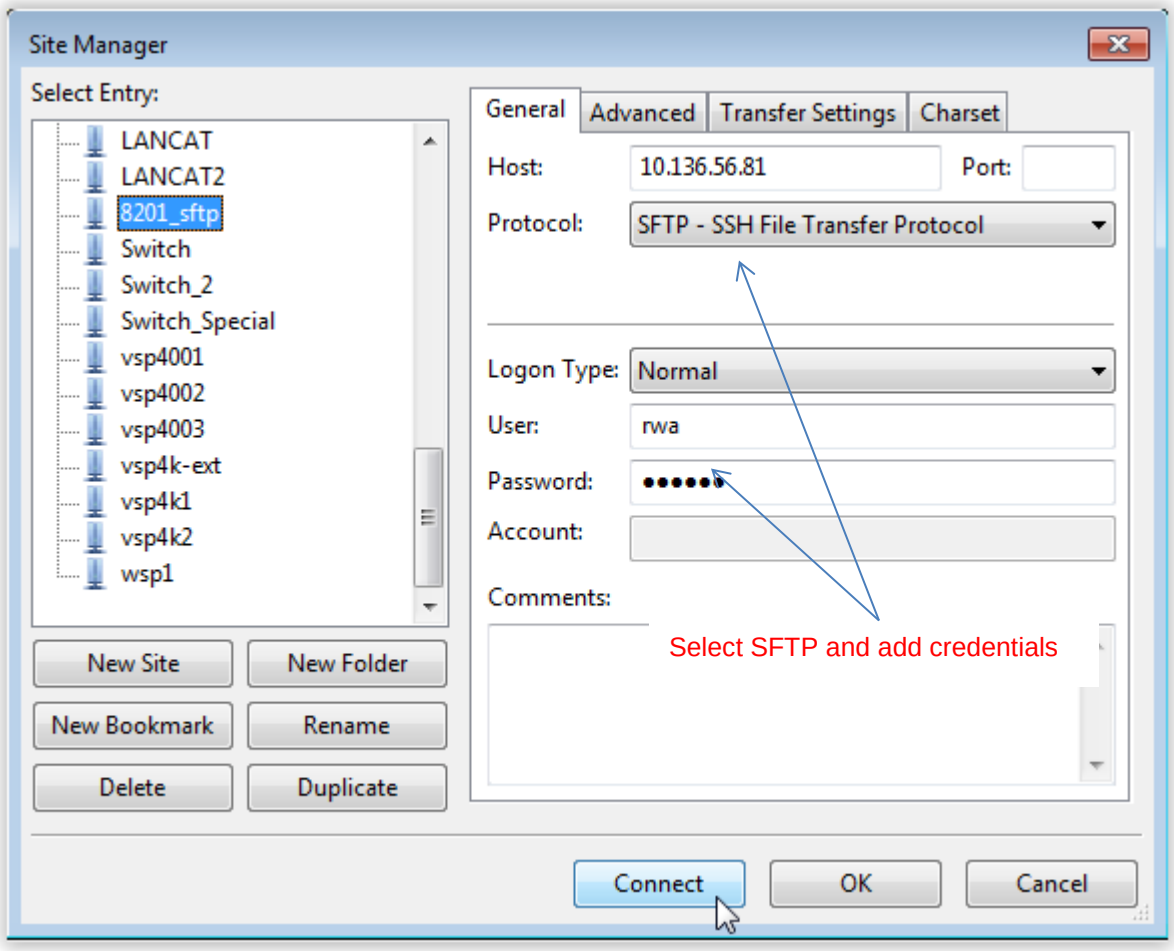
SFTP using Putty: VOSS 4.2 (VSP4000 or VSP8000):

Go to the directory where SFTP is installed and then enter the following command and assuming the remote switch is a VSP 8200:

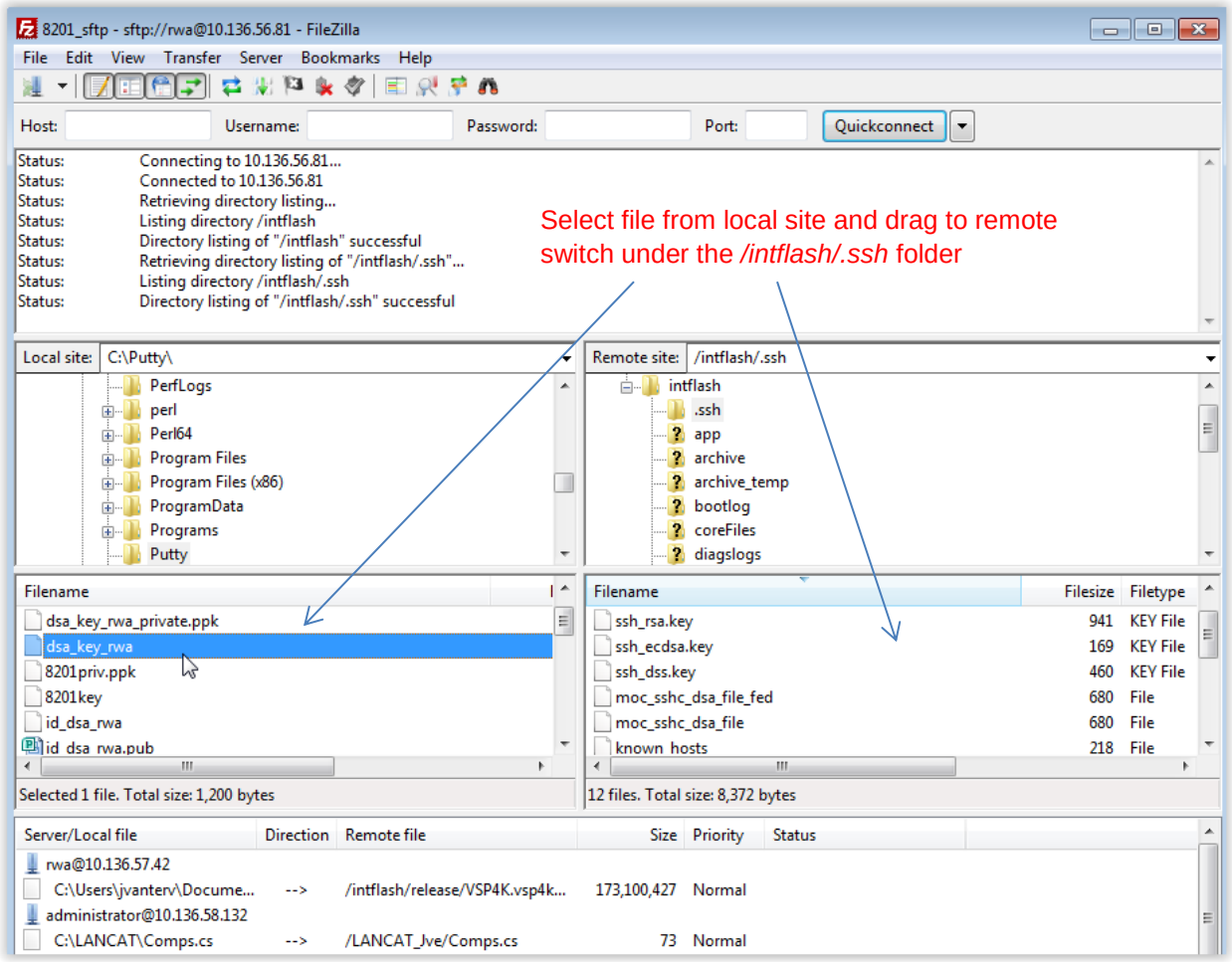
```
psftp> open  rwa@10.136.56.81
Using username "rwa".
rwa@10.136.56.81's password: ********
Remote working directory is /intflash
psftp> cd .ssh
Remote directory is now /intflash/.ssh
psftp> put c:\putty\dsa_key_rwa
local:c:\putty\ dsa_key_rwa => remote:/intflash/.ssh/dsa_key_rwa
psftp> exit
```

Filezilla:

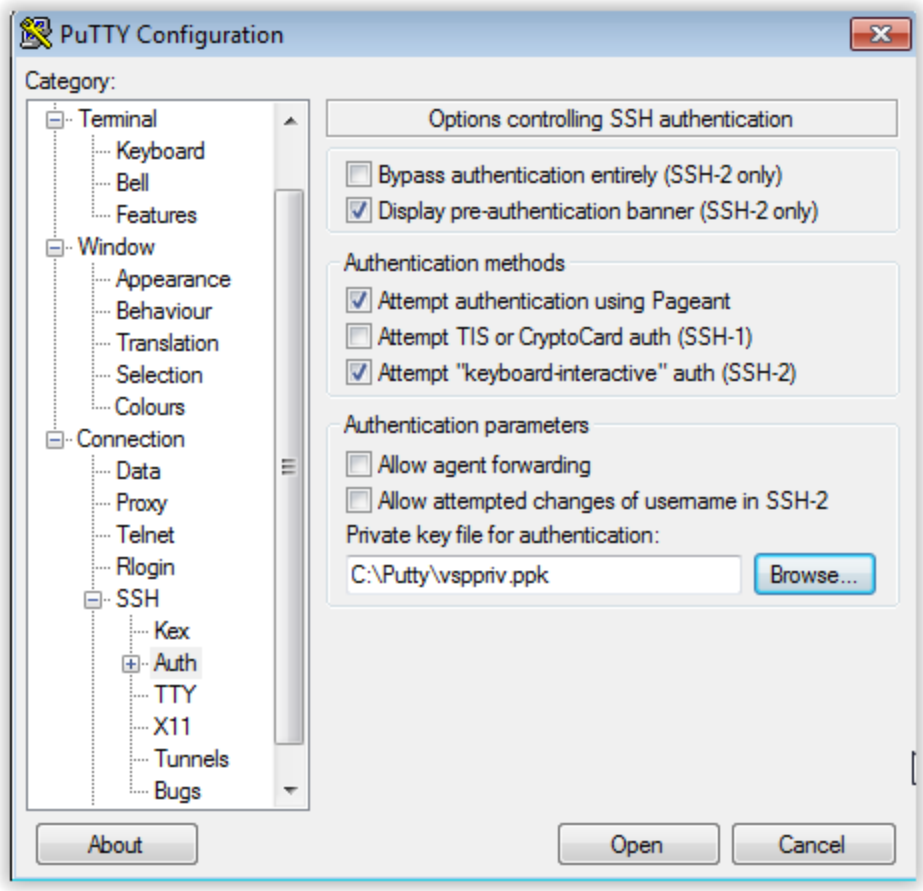
a) Open Filezilla and open an SFTP session



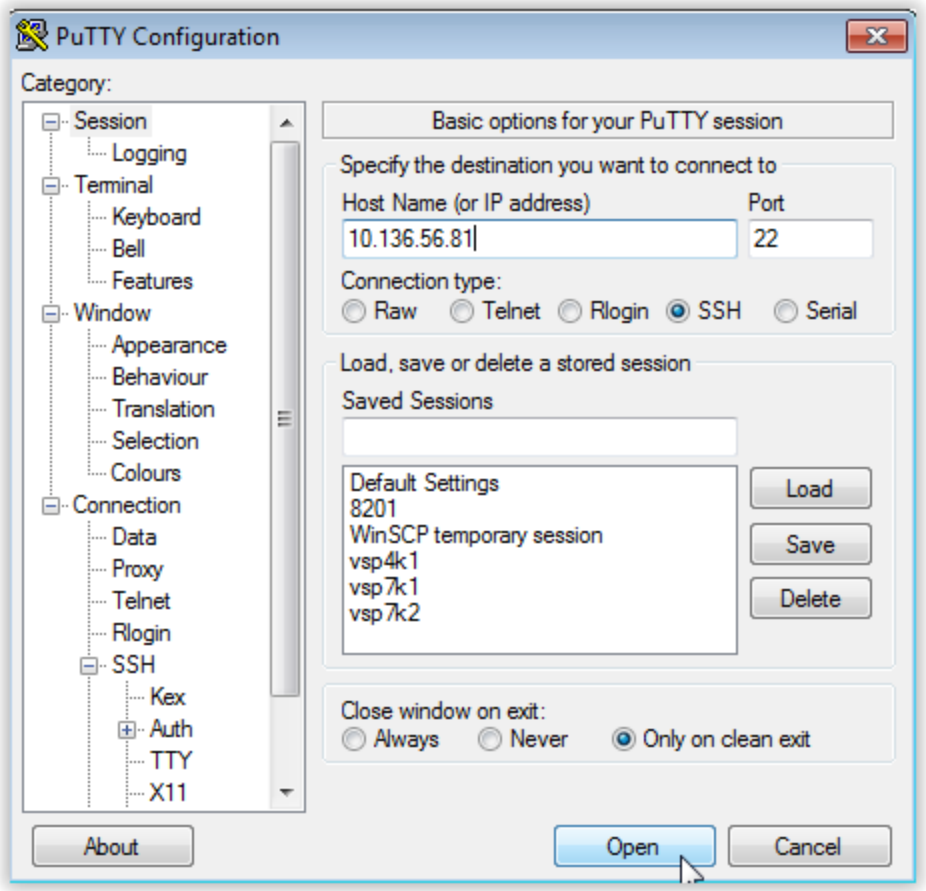
b) Once connected to the switch, copy the public key to the */intflash/.ssh* directory on the VSP switch



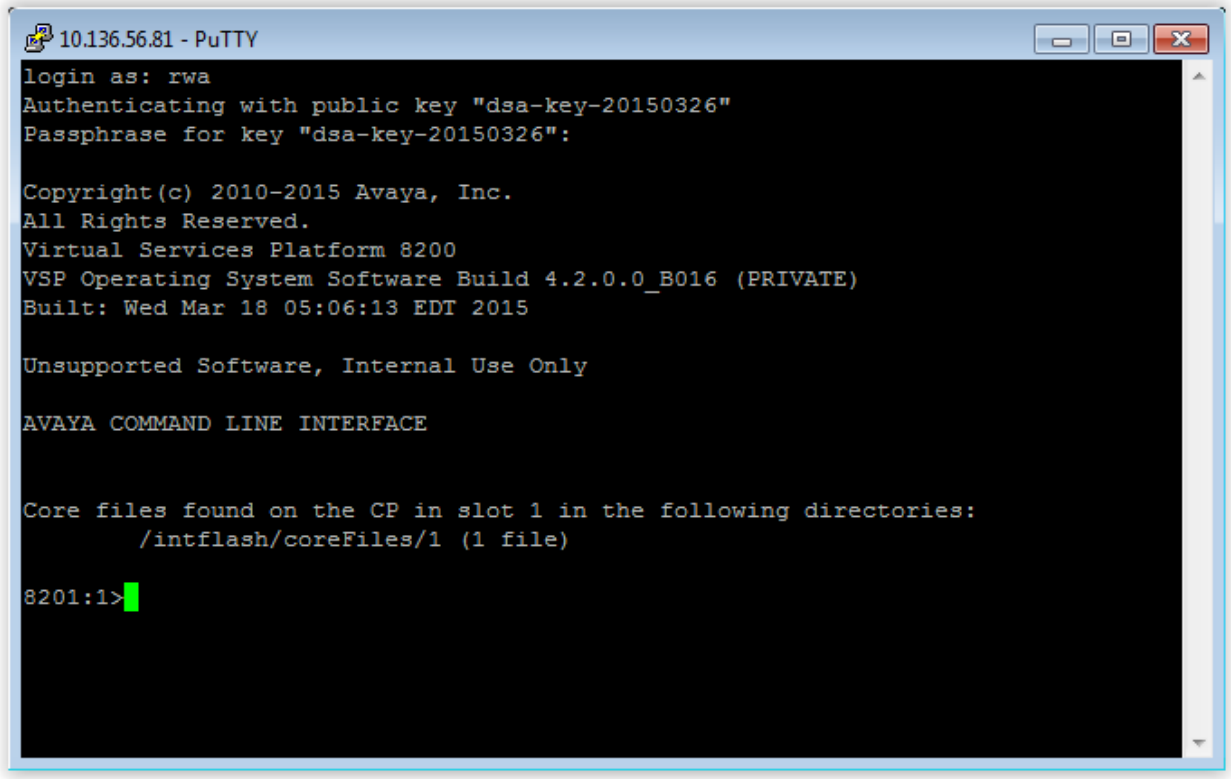
Step 7: Open up Putty, scroll down to *SSH -> Auth* and select the private key generated above by clicking on the *Browse* icon and then click on *Open*



Step 8: Go to Session -> Host Name (or IP address) , enter the IP address of the switch, select SSH, and click on Open when done



Step 9: Enter any user name you like when prompted with the login as prompt and enter the DSA Key passphrase from the DSA key you generated above



6.2.2 Verify Operations

Step 1: Verify SSH session

```
VSPswitch:1#show ssh session
        SSH Session ID : 0
        User Name      : rwa
        Host           : 10.55.72.46
```

Step 2: Verify SSH configuration

```
VSPswitch:1#show ssh global
Total Active Sessions  : 1
        version            : v2only
        port               : 22
        max-sessions       : 4
        timeout            : 60
        action rsa-keygen  : rsa-keysize 2048
        action dsa-keygen  : dsa-keysize 2048
        rsa-auth           : true
        dsa-auth           : true
        pass-auth          : true
        enable             : true
```

Step 3: Verify DSA download public key

```
VSPswitch:1(config)#ls /intflash/.ssh
drwxr-xr-x  2 0       0             4096 Mar 26 13:34  ./
drwxr-xr-x 20 0       0             4096 Mar 24 13:22  ../
-rw-r--r--  1 0       0              887 Jun 25  2014  host.key
-rw-r--r--  1 0       0              899 Jun 25  2014  host.cert
-rw-r--r--  1 0       0              460 Mar 26 12:49  ssh_dss.key
-rw-r--r--  1 0       0              941 Mar 26 11:16  ssh_rsa.key
-rw-r--r--  1 0       0              169 Mar 26 11:16  ssh_ecdsa.key
-rw-r--r--  1 0       0              680 Mar 26 13:04  moc_sshc_dsa_file
-rw-r--r--  1 0       0              458 Mar 26 13:04  id_dsa_rwa
-rw-r--r--  1 0       0              590 Mar 26 13:04  id_dsa_rwa.pub
-rw-r--r--  1 0       0             1195 Mar 26 13:34  dsa_key_rwa
```

7. WEB Access – Enterprise Device Manager

The WEB management interface can be enabled to support Enterprise Device Manager (EDM). Enterprise Device Manager (EDM) is a Web-based graphical user interface (GUI) between you and your VSP switch. EDM makes retrieval of configuration information from a device a point-and-click operation. To access EDM, you must enable the Web server on the VSP switch. By default, the Web server is disabled.

EDM is built-in to the VSP switch, and the EDM Web server is the switch itself. You do not have to install any additional client software and there is no operating system dependency.

EDM comes with each VSP switch and enables you to directly manage that switch. If you want to manage the switch from a centralized location.

For EDM to display and function correctly, use one of the following Web browsers:

- Mozilla Firefox, version 26
- Microsoft Internet Explorer, version 8.0

You cannot open two HTTP sessions from the same IP address to the same switch using the same browser. To open two simultaneous sessions to the same switch, you must open one session in Internet Explorer and another in Firefox.

This is important in cases where you open a switch in one VRF (for example, VRF 1), and then open a subsequent session for the same switch to a second VRF (for example, VRF 2). In this case, the device physical view in the first session does not change (showing VRF 1), but any configurations made in this first session will be applied to the VRF shown in the second session (VRF 2).

The WEB server demon can either be enabled or disabled by issuing the following command.

```
VSPswitch:1(config)#web-server ?
  def-display-rows     Set web server default display row width
  enable               Enable web-server
  help-tftp            Set web server html directories
  http-port            Set web server HTTP port
  https-port           Set web server HTTPS port
  inactivity-timeout   Change web-server login session inactivity timeout
  password             Set web server password
  secure-only          Enables secure-only on webserver
```

7.1 EDM configuration Example

The following is an example using a Firefox browser to log into a VSP switch to the global router instance using EDM. For this example, we will change the default setting as follows.

- Change default user name of rwa to user1234
- Add password of pswd1234
- Add TFTP server address of 192.168.50.100 for the EDM help files assuming the files are stored in a folder named */help/VOSSc420_HELP_EDM*

7.1.1 Configuration

Step 1: Enable EDM on the VSP switch

```
VSPswitch:1(config)#web-server enable
VSPswitch:1(config)#web-server password <ro|wr|rwa> <user name> <password>
VSPswitch:1(config)#web-server password rwa admin AdminUser@!1234
```

By default the Web server is configured with the secure-only option that requires you to use https://<ip_address> to access the switch. To access EDM using http, you must disable the secure-only option using the ACLI command *no web-server secure-only*.

The default EDM user name and password is *admin* and *password*.

Step 2: Optional help files

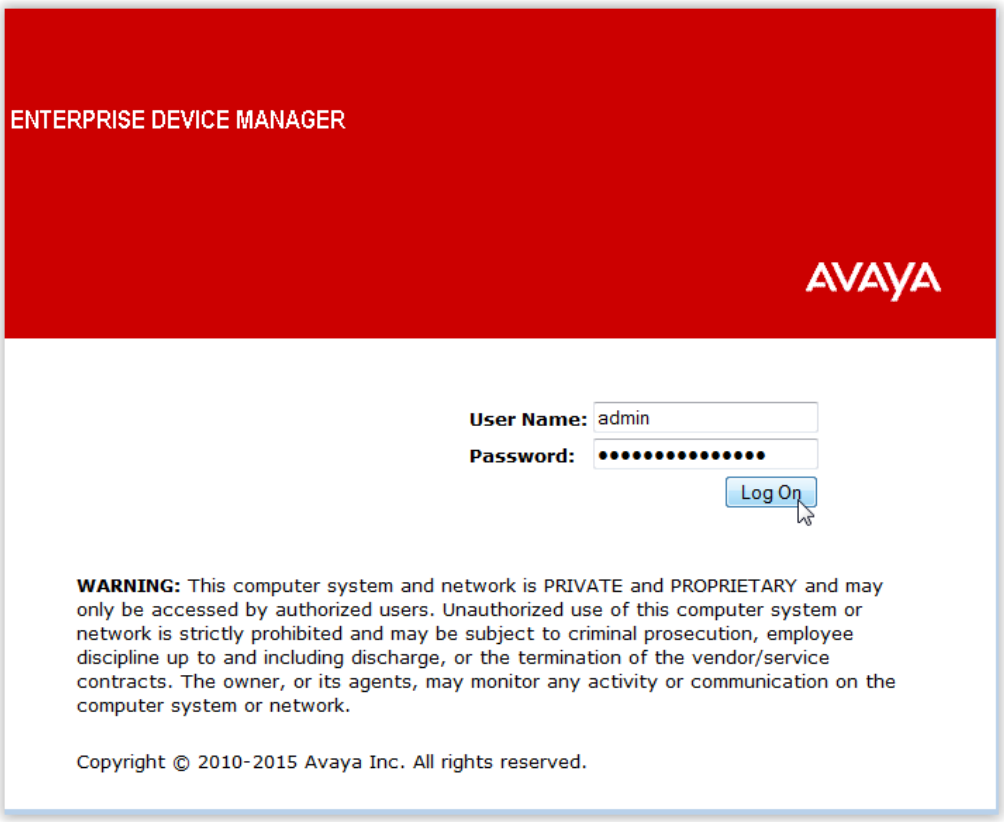
```
VSPswitch:1(config)#web-server help-tftp 10.136.61.50:/help/VOSSv420_HELP_EDM
```

Configures the TFTP or FTP directory for the help files in the format of a.b.c.d:/ or a.b.c.d:/<directory>.

If you are using FTP to get the help files, make sure you add the host user credentials:

```
VSPswitch:1(config)#boot config host user <user name>
VSPswitch:1(config)#boot config host password <password>
```

Step 3: Login using the credential from step 1



Step 4: EDM Main Menu

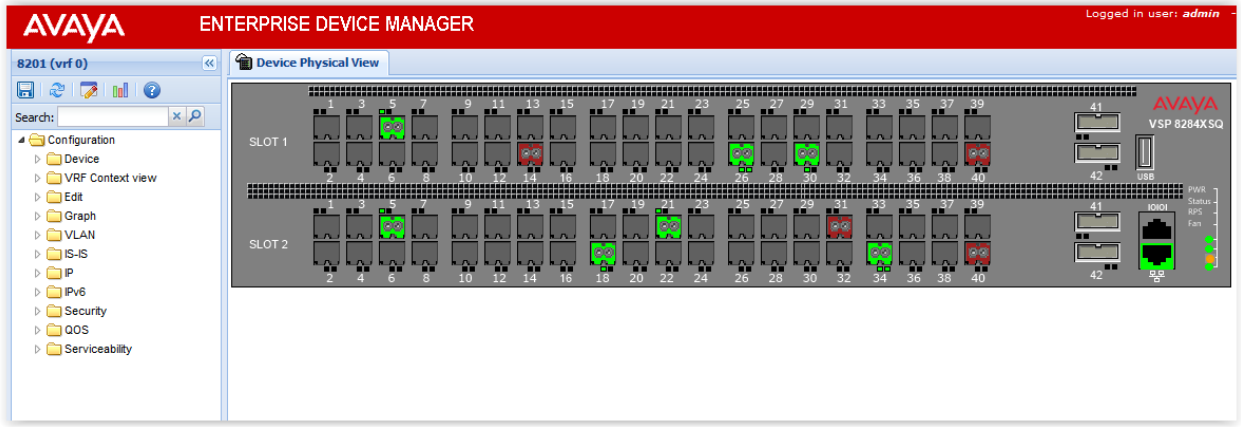


Table 12: Navigation pane buttons

Button	Name	Description
	Save Config	Saves the running configuration
	Refresh Status	Refreshes the Device Physical View.
	Edit	Edits the selected item in the Device Physical View.
	Graph	Opens the graph options for the selected item in the Device Physical View.

Table 13: Navigation tree folders

Menu	Description
Device	Use the Device menu to refresh and update device information or enable polling. Preference Setting — Enable polling or hot swap detection. Configure the frequency to poll the device. Refresh Status — Use this option to refresh the device view. Rediscover Device — Use this to trigger a rediscovery to update all of the device information.
VRF Context view	Use the VRF Context view to switch to another VRF context view when you use the embedded EDM. GlobalRouter is the default view at log in. You can configure both Global Router (GRT) and Virtual Routing and Forwarding (VRF) instances when you launch a VRF context view. You can open only five tabs

	for each EDM session.
Edit	Use the Edit menu to view and configure parameters for the chassis or for the currently selected object. The selected object can be a module or a port. You can also use the Edit menu to perform the following tasks: check and update security settings for the device run diagnostic tests change the configuration of the file system, NTP, service delivery, and SNMPv3 settings for the device
Graph	Use the Graph menu to view and configure EDM statistics and to produce graphs of the chassis or port statistics.
VLAN	Use the VLAN menu to view and configure VLANs, spanning tree groups (STG), MultiLink Trunks/LACP, MAC Learning, Global MAC Filtering, SMLT, and SLPP.
IS-IS	Use the IS-IS menu to view and configure IS-IS and Shortest Path Bridging MAC (SPBM).
IP	Use the IP menu to view and configure IP routing functions for the system, including IP routing protocols, IP-VPN, IP-MVPN, IGMP, Multicast, TCP/UDP, VRRP, RSMLT, DHCP, PIM, UDP forwarding, and policies.
IPv6	Use the IPv6 menu to view and configure IPv6 routing functions, including TCP/UDP, tunnels, and OSPF.
Security	Use the Security menu to view and configure policies, filters, and protocols such as RADIUS, SSH,and EAPoL.
QOS	Use the QOS menu to view and configure QoS mapping tables, filters, profiles, and policy statistics.
Serviceability	Use the Serviceability menu to configure RMON alarms and the SLAMon application. You can also use the Serviceability menu to view the RMON alarm log and history log, and to enable or disable RMON history or statistics on all ports.

7.1.2 Verify Operations

Step 1: Enable EDM on the VSP switch

```
VSPswitch:1(config)#show web-server
Web Server Info :

        Status                    : on
        Secure-only               : enabled
        RWA Username               : admin
        RWA Password               : ***************
        Def-display-rows          : 30
        Inactivity timeout        : 900 sec
        Html help tftp source-dir : 10.136.61.50:/help/VOSSv420_HELP_EDM
        HttpPort                  : 80
        HttpsPort                 : 443
        NumHits                   : 7
        NumAccessChecks           : 1
        NumAccessBlocks           : 0
        NumRxErrors               : 6
        NumTxErrors               : 0
        NumSetRequest             : 0
        Last Host Access Blocked  : 0.0.0.0
```

8. SNMP

8.1 SNMPv3 Overview

SNMPv3 is the third version of the Internet-Standard Management Framework and is derived from and builds upon both the original Internet-Standard Management Framework (SNMPv1) and the second Internet-Standard Management Framework (SNMPv2). SNMPv3 is not a stand-alone replacement for SNMPv1 and/or SNMv2. It defines security capabilities to be used in conjunction with SNMPv2 (preferred) or SNMPv1. As shown in the Figure 1 below, SNMPv3 specifies a User Security Model (USM) that uses a payload of either a SNMPv1 or a SNMPv2 protocol data unit (PDU).

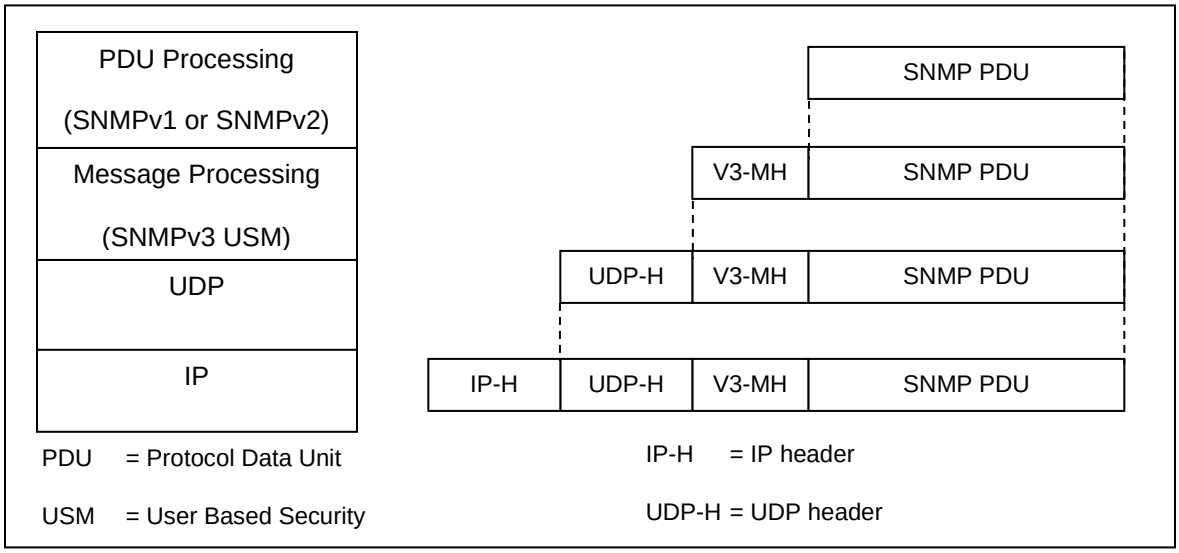


Figure 1: SNMPv3 USM

Authentication within the User-based Security Model (USM) allows the recipient of the message to verify whom the message is from and whether the message has been altered. As per RFC 2574, if authentication is used, the entire message is checked for the integrity. Authentication uses a secret key to produce a fingerprint of the message, which is included in the message. The receiving entity uses the same secret key to validate the fingerprint. VSP9000 and VOSS versions prior to 4.2 support two authentication protocols: HMAC-MD5 and HMAC-SHA-96 for use with USM. VOSS 4.2 and later versions support MD5, SHA-1 and SHA-2

While the USM provides the user-name/password authentication and privacy services, control access to management information (MIB) must be defined. The View-based Access Control Module (VACM) is used to define a set of services that an application can use for checking access rights (read, write, notify) to a particular object. VACM uses the ASN.1 notation (3.6.1.4) or the name of the SNMP MIB branch, i.e. Org.Dod.Internet.Private. The administrator can define a MIB group view for a user to allow access to an appropriate portion of the MIB matched to an approved security level. The three security levels are:

- ***NoAuthNoPriv***-Communication without authentication and privacy
- ***AuthNoPriv***-Communication with authentication (MD5 or SHA) and without privacy
- ***AuthPriv***-Communication with authentication (MD5 or SHA) and privacy (DES or AES)

8.2 Blocking SNMP

By default, SNMP access is enabled. You can disable SNMP; this includes SNMPv1/v2 and SNMPv3, access to the VSP switch by using the following commands:

```
VSPswitch(config)#boot config flags block-snmp
VSPswitch(config)#save boot
```

To re-enable SNMP access, type in the following command:

```
VSPswitch(config)#no boot config flags block-snmp
```

8.3 Blocking SNMPv1/2 only

If you wish to allow only SNMPv3 access, you can disable SNMPv1/2 only by entering the following commands:

To disable SNMPv1/v2 only, enter the following commands:

```
VSPswitch(config)#no snmp-server community-by-index first
VSPswitch(config)#no snmp-server community-by-index second
```

At this point, SNMPv1/v2 will be disabled and only SNMPv3 will be allowed.

8.4 Community Strings

For security reasons, the SNMP agent validates each request from an SNMP manager before responding to the request. This is accomplished by verifying that the manager belongs to a valid SNMP community. An SNMP community is a logical relationship between an SNMP agent and one or more SNMP managers (the manager software implements the protocols used to exchange data with SNMP agents). You define communities locally at the agent.

The agent establishes one community for each combination of authentication and access control characteristics that you choose. You assign each community a unique name (community string), and all members of a community have the same access privileges, The default VACM group tables provide either read-only or read-write:

- Read-only: members can view configuration and performance information.
- Read-write: members can view configuration and performance information, and also change the configuration.

By defining a community, an agent limits access to its MIB to a selected set of management stations. By using more than one community, the agent can provide different levels of MIB access to different management stations.

SNMP community strings are required for access to the switch using SNMP-based management software. You set the SNMP community strings using the CLI. If you have read/write/all access authority, you can modify the SNMP community strings for access to the device through Enterprise Device Manager.

When saving the configuration file, a hidden and encrypted file is created that contains the SNMP community table information. The SNMP community strings are not referenced in the VSP switch configuration file.

8.4.1 Displaying the default Community Strings

The following command displays the two default community strings. By default, for the index named *first*, a community string of *public* is used and for the index named *second*, a community string name of *private* is used. As you can see, the community strings names of *public* and *private* string names are not displayed and shown as multiple asterisks. The community strings are encrypted using the blowfish algorithm and are stored in a hidden file – please see section titled hidden files for more details. The access rights are determined by the Security Name from the VACM table.

```
VSPswitch#show snmp-server community
================================================================================
                                    Community Table
================================================================================
Index           Name            Security Name   Transport Tag
--------------------------------------------------------------------------------
first           ********        readview
second          ********        initialview
```

To view the SNMP security name VACM group details, enter the CLI command shown below. You can also use EDM to view the VACM details by going to *Configuration -> Edit -> SnmpV3 -> VACM Table -> Group Membership and Group Access Right.*

```
VSPswitch#show snmp-server group
================================================================================
                     VACM Group Membership Configuration
================================================================================
Sec Model  Security Name                 Group Name
--------------------------------------------------------------------------------
snmpv1     readview                      readgrp
snmpv1     initialview                   v1v2grp
snmpv2c    readview                      readgrp
snmpv2c    initialview                   v1v2grp

4 out of 4 Total entries displayed
--------------------------------------------------------------------------------



================================================================================
                       VACM Group Access Configuration
================================================================================
Group      Prefix Model    Level        ReadV      WriteV     NotifyV
--------------------------------------------------------------------------------
initial           usm      noAuthNoPriv root       root       root
initial           usm      authPriv     root       root       root
readgrp           snmpv1   noAuthNoPriv v1v2only              org
```

```
readgrp           snmpv2c noAuthNoPriv v1v2only              org
v1v2grp           snmpv1  noAuthNoPriv v1v2only   v1v2only   v1v2only
v1v2grp           snmpv2c noAuthNoPriv v1v2only   v1v2only   v1v2only

6 out of 6 Total entries displayed
--------------------------------------------------------------------------------
```

The community string names are always hidden and never displayed when issuing the show community CLI command. Also, the SNMP community strings are not displayed in the configuration file and are instead stored in a hidden file named *snmp_comm.txt*. You can view the contents of this file by issuing the ACLI command *ls /intflash/snmp_comm.txt*. It is also important to backup this file to an external server.

8.5 Adding a new Community String

To add a new community strings, enter the following command:

```
VSPswitch(config)#snmp-server community <name> index <Comm Idx> secname <security name>
```

Where:

Parameter	Description
Comm Idx	The unique index value of a row in this table. The range is 1-32 characters.
name	The community string for which a row in this table represents a configuration
security name	Maps community string to the security name in the VACM Group Member Table.

8.6 Deleting Community Strings

To delete a community string, enter the following command:

```
VSPswitch(config)#no snmp-server community-by-index <Comm Idx>
```

Where:

Parameter	Description
Comm Idx	The unique index value of a row in this table. The range is 1-32 characters.

Since the above command uses the Community Index that is not hidden, it can be used to delete entries for which the actual community string has been forgotten.

8.7 Community Strings – Virtual Routers

If you wish to enable SNMP at a VRF level for SMNPv1/2, access is controlled via community strings. The default read community string is *public::x* while the default read-write community string is *private::x* where x equals the VRF instance, a number from 1 to 255. This allows access to the switch only at the VRF level.

VRF level community strings are automatically generated by the system whenever a new VRF is created.

8.8 Community String Configuration Example: Allowing only read-only access using the default community strings

8.8.1 Configuration

Assuming we are using default settings, read-only access uses the VACM table security name of *readview* referenced to a SNMP community security name of *first*. Read-write access uses the VACM table security name of *initialview* referenced to a SNMP community security name of *second*. Hence, all we have to do is change the VACM table security name from *initialview* to *readview* for the SNMP Community security name of *second*. The end result, if a user attempts to connect to an VSP switch using SNMPv1 or SNMPv2c using the default community strings of public and private, the user will only get read-only access.

Change the default read-write community name with the read-only VACM security name

```
VSPswitch:1(config)#snmp-server community private secname readview
```

8.8.2 Verify Operations

Verify SNMP community

```
VSPswitch:1#show snmp-server community
================================================================================
                                    Community Table
================================================================================
Index           Name            Security Name   Transport Tag
--------------------------------------------------------------------------------
first           ********        readview
second          ********        readview

4 out of 4 Total entries displayed
```

8.9 Configuration Example: Changing the Default SNMP Community Names

8.9.1 Configuration

The following commands changes the default community strings from the default names of public/private to public1234/private1234. Please note, you must delete the default community string indexes first.

Step 1 – Change the read-only access default community string from *public* to *public1234.* You must first delete the default read-only community string and then add the new community string

```
VSPswitch:1(config)#no snmp-server community public
VSPswitch:1(config)#snmp-server community public1234 group readgrp index first secname readview
```

Step 2 – Change the write-right access default community string from *private* to *private1234*. You must first delete the default read-write community string and then add the new community string

```
VSPswitch:1(config)#no snmp-server community private
VSPswitch:1(config)# snmp-server community private1234 group v1v2grp index second secname initialview
```

8.9.2 Verify Operations

Verify settings

```
VSPswitch:1#show snmp-v3 community
================================================================================
                                    Community Table
================================================================================
Index           Name            Security Name   Transport Tag
--------------------------------------------------------------------------------
first           ********        readview
second          ********        initialview

4 out of 4 Total entries displayed
```

At this time, there is no ACLI command available to change the community string name. However, you can use EDM to change the default SNMP community strings by going to *Configuration -> Edit -> SnmpV3 -> Community Table* and double-click the box via the Name column via Index row named *first* and *second*.

8.10 Configuration Example: Adding additional SNMP community strings

8.10.1 Configuration

Assuming we wish to leave the default community strings intact and add an additional read-only and read-write community string.

Step 1 – Create the new read-only community using an index name of *third*, add the community string of *readonly*, and add the read-only VACM security name of *readview*

```
VSPswitch:1(config)#snmp-server community readonly index third secname readview
```

Step 2 – Create the new read-write community using an index name of *forth*, add the community string of *readwrite*, and add the read-only VACM security name of *initialview*

```
VSPswitch:1(config)#snmp-server community readwrite index fourth secname initialview
```

8.10.2 Verify Operations

Verify configuration

```
VSPswitch:1#show snmp-server community
================================================================================
                              Community Table
================================================================================
Index           Name            Security Name   Context Name    Transport Tag
--------------------------------------------------------------------------------
first           ********        readview
forth           ********        initialview
second          ********        initialview
third           ********        readview
```

8.11 Creating a MIB View

As mentioned in the previous step, the VSP switch has a number of default MIB views. The MIB view configures the branches of the SNMP MIB tree that are permitted or not permitted for a particular user or group. The VSP switch MIB tree follows the ASN.1 hierarchical structure for both private and enterprise (private) MIBs.

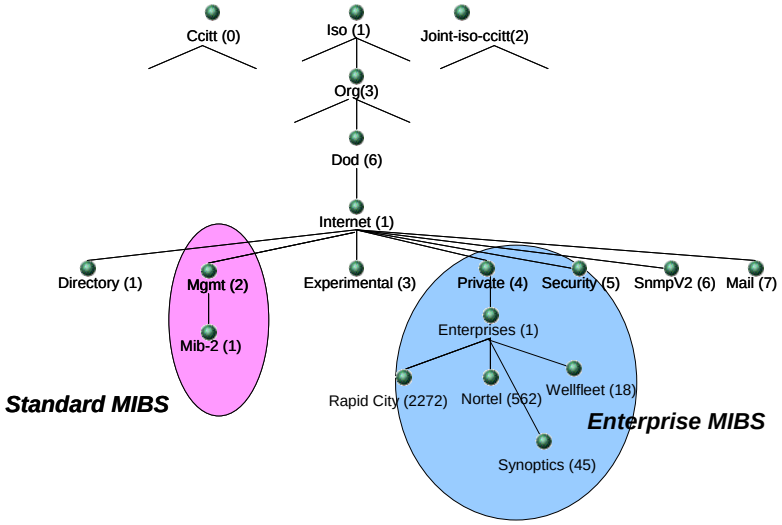


Figure 2: MIB Structure

To create a new MIB view, enter the following command:

```
VSPswitch(config)#snmp-server view <view name> <subtree oid>
```

8.12 Configuration Example – Adding a new SNMP MIB view

8.12.1 Configuration

For example, to add a new MIB view named *ro_private* to exclude the Private branch, enter the following.

Step 1 – Create the new MIB view named *ro_private*

```
VSPswitch:1(config)#snmp-server view ro_private -1.3.6.1.4
```

8.12.2 Verify Operations

Verify configuration

```
VSPswitch:1(config)#show snmp-server view
================================================================================
                                   MIB View
================================================================================
View Name                       Subtree                         Mask

--------------------------------------------------------------------------------
org                             +1.3
vrf                             -1.3
  .    .
v1v2only                        -1.3.6.1.6.3.18
ro_private                      -1.3.6.1.4
```

8.13 SNMPv3 Configuration Steps

The following are the configuration steps required to enable SNMPv3:

- Load the DES or AES Encryption Module
- Setting SNMPv3 security level option
- Adding a SNMP User USM
- Assigning the USM as a member to a SNMPv3 USM group
- Assigning the USM group access level of either authPriv, authNoPriv, or noAuthNoPriv
- Assigning a MIB view to the USM group

8.13.1 Loading the DES or AES Encryption Module

In order to use SNMPv3 USM group access level authPriv, the DES or AES encryption module must be loaded. The DES or AES module is required in order to provide secure communications (encryption) between the user and the VSP switch.

The AES standard is the current encryption standard (FIPS-197) intended to be used by the U.S. Government organizations to protect sensitive information. It is also becoming a global standard for commercial software and hardware that uses encryption or other security features.

Once the DES or AES encryption module is uploaded to the VSP switch (on VSP900 and VOSS prior to 4.2, the encryption module file VSPxxxx_modules.tgz must be added to the primary software load). It can be loaded by typing the following command:

For single DES:

```
VSPswitch(config)#load-encryption-module DES
```

For AES:

```
VSPswitch(config)#load-encryption-module AES
```

In VOSS release 4.2 for the VSP 4000 and VSP 8000, the encryption modules are automatically linked with the application image, thus there is no need to manually load them via the ACLI commands shown above.

8.13.2 Adding a New SNMPv3 User

The first step is to add a user to the USM (User-based Security Model) table. You can add a new user to the USM table by typing in the following command:

```
VSPswitch(config)#snmp-server user <user name> <md5|sha> [authentication
password<1-32>] <des|aes> [privacy password<1-32>]
```

8.13.3 Adding USM Group

The USM group is used to define the access level and MIB view given to a user and assigning it to one of three USM access levels.

One of following three USM access levels must be assigned to a USM group:

- ***NoAuthNoPriv***-Communication without authentication and privacy
- ***AuthNoPriv***-Communication with authentication (MD5 or SHA) and without privacy
- ***AuthPriv***-Communication with authentication (MD5 or SHA) and privacy (DES or AES)

We can assign the USM group to either an existing MIB view or we could create a new MIB view and then assign it to the USM group. The next section will describe how to add a new MIB view.

To view the default MIB views, enter command shown below:

```
VSPswitch#show snmp-server view

================================================================================
                                  MIB View
================================================================================
View Name            Subtree                        Mask                Type

--------------------------------------------------------------------------------
org                  1                                                  include
root                 1                                                  include
snmp                 1.3.6.1.6.3                                        include
snmp                 1.3.6.1.2.1.1                                      include
layer1               1.3                                                exclude
  . .       .
  . .       .
v1v2only             1.0                                                include
v1v2only             1.2                                                include
v1v2only             1.3                                                include
v1v2only             1.3.6.1.6.3.15                                     exclude
v1v2only             1.3.6.1.6.3.16                                     exclude
v1v2only             1.3.6.1.6.3.18                                     exclude
```

The VSP switch has a number of default groups, with one default USM group named *initial*. The default groups can be examined by typing in commands shown below:

```
VSPswitch#show snmp-server group

================================================================================
                        VACM Group Access Configuration
================================================================================
Group       Prefix Model   Level         ReadV       WriteV      NotifyV
--------------------------------------------------------------------------------
initial            usm     noAuthNoPriv  root        root        root
initial            usm     authPriv      root        root        root
readgrp            snmpv1  noAuthNoPriv  v1v2only                org
readgrp            snmpv2c noAuthNoPriv  v1v2only                org
v1v2grp            snmpv1  noAuthNoPriv  v1v2only    v1v2only    v1v2only
v1v2grp            snmpv2c noAuthNoPriv  v1v2only    v1v2only    v1v2only

================================================================================
                      VACM Group Membership Configuration
================================================================================
Sec Model  Security Name                   Group Name
--------------------------------------------------------------------------------
snmpv1     readview                        readgrp
snmpv1     sBladeUser                      sBladeGrp
snmpv1     initialview                     v1v2grp
snmpv2c    readview                        readgrp
snmpv2c    sBladeUser                      sBladeGrp
snmpv2c    initialview                     v1v2grp
usm        initial                         initial
```

The default USM level, named *initial*, has both authentication and encryption (authPriv) with full read-write views. You can use this group for initial SNMPv3 access to the VSP switch. The name of the read-write view starts at *root* – please see next step in regards to setting up the MIB view.

You can add a new USM Group by entering the following commands:

```
VSPswitch(config)#snmp-server group <group access name> <context name> < auth-no-priv|auth-priv|no-auth-no-priv> read-view <value> write-view <value> notifiy-view <value>
```

8.14 SNMPv3 Configuration Example

For this configuration example, we wish to accomplish the following:

- Add User 1 to USM table with authentication protocol of MD5 and privacy protocol of DES, i.e. authPriv)
  - Use a user name of *user1*, a MD5 authentication password of *user1234*, and a DES privacy password of *userpriv*
  - Allow User 1 full MIB views with full permission starting the existing view “org”
- Add User 2 to USM table authentication protocol of MD5 with no privacy protocol, i.e. authNoPriv
  - Use a user name of *user2* with a MD5 authentication password of *user2abcd*
  - Allow User 2 full MIB read permission starting from the exiting “org” level, but exclude write permission from all Private Enterprise MIB’s

To accomplish the above, please follow the steps below.

8.14.1 Configuration

Step 1 – Make sure the DES file is loaded on the switch and then issue the following command – note this step is not required for VOSS release 4.2 or higher

```
VSPswitch:1(config)#load-encryption-module DES
```

Step 2 – Add SNMPv3 authPriv User. In this example, we will use a user name of *user1*, a MD5 password of *user1234*, and a DES privacy password of *userpriv*

```
VSPswitch:1(config)#snmp-server user user1 group group_1 md5 user1234 des userpriv
```

Step 3 – Add SNMPv3 authNoPriv User. In this example, we will use a user name of *user2* and a MD5 password of *user2abcd*

```
VSPswitch:1(config)#snmp-server user user2 group group_1 md5 user2abcd
```

Step 4 – Add USM group using a name of *group_1* with an access level of authPriv and read & write view to *org*. For the PPCLI, we will need to add the user name to the group; in our example, this is *user1*

```
VSPswitch:1(config)#snmp-server group group_1 "" auth-priv read-view org write-view
org
```

Step 5 – Using USM created above, *group_1*, add an access level of authNoPriv with read view to *org* and write to *private* where we will use this level to setup the MIB view in the next step. For the PPCLI, we will need to add the user name to the group; in our example, this is *user2*

```
VSPswitch:1(config)#snmp-server group group_1 "" auth-no-priv read-view org write-view
private
```

Step 6 – Create a new MIB view to exclude the private MIB for User 2

```
VSPswitch:1(config)#snmp-server view private +1
```

```
VSPswitch:1(config)#snmp-server view private -1.3.6.1.4
```

8.14.2 Verify Operations

Step 1 – Verify SNMPv3 Users

```
VSPswitch:1(config)#show snmp-server user
Engine ID = 80:00:08:E0:03:00:80:2D:BE:20:00

================================================================================
                                USM Configuration
================================================================================
User/Security Name    Engine Id                          Protocol
--------------------------------------------------------------------------------
user1                 0x80:00:08:E0:03:00:80:2D:BE:20:00 HMAC_MD5, DES PRIVACY,
user2                 0x80:00:08:E0:03:00:80:2D:BE:20:00 HMAC_MD5, NO  PRIVACY
initial               0x80:00:08:E0:03:00:80:2D:BE:20:00 NO AUTH,  NO  PRIVACY
```

Step 2 – Verify SNMP VACM group and access configuration

```
VSPswitch:1(config)#show snmp-server group
================================================================================
                      VACM Group Membership Configuration
================================================================================
Sec Model  Security Name                  Group Name
--------------------------------------------------------------------------------
snmpv1     readview
snmpv1     sBladeUser                     sBladeGrp
snmpv1     initialview
snmpv2c    readview
snmpv2c    sBladeUser                     sBladeGrp
snmpv2c    initialview
usm        user1                          group_1
usm        user2                          group_1
usm        initial                        initial

9 out of 9 Total entries displayed
--------------------------------------------------------------------------------
```

```
================================================================================
                        VACM Group Access Configuration
================================================================================

Group       Prefix Model    Level         ReadV       WriteV      NotifyV
--------------------------------------------------------------------------------
group_1             usm     authNoPriv    org         private
group_1             usm     authPriv      org         org
initial             usm     noAuthNoPriv  root        root        root
initial             usm     authPriv      root        root        root
readgrp             snmpv1  noAuthNoPriv  v1v2only                org
readgrp             snmpv2c noAuthNoPriv  v1v2only                org
v1v2grp             snmpv1  noAuthNoPriv  v1v2only    v1v2only    v1v2only
v1v2grp             snmpv2c noAuthNoPriv  v1v2only    v1v2only    v1v2only
sBladeGrp           snmpv1  noAuthNoPriv  sBladeView  sBladeView  sBladeView
sBladeGrp           snmpv2c noAuthNoPriv  sBladeView  sBladeView  sBladeView
```

Step 2 – Verify SNMP MIB view

```
VSPswitch:1(config)#show snmp-server group
================================================================================
                                   MIB View
================================================================================
View Name                        Subtree                          Mask

--------------------------------------------------------------------------------
org                              +1.3
|
private                          -1.3.6.1.4

private                          +1

v1v2only                         +1.0

v1v2only                         +1.2

v1v2only                         +1.3

v1v2only                         -1.3.6.1.6.3.15
```

```
v1v2only                        -1.3.6.1.6.3.16

v1v2only                        -1.3.6.1.6.3.18
```

8.15 SNMP Traps

8.15.1 Trap Receivers

The SNMP target address is configured using the following command:

Please note, the port and filter parameter is optional in all cases.

- SNMPv1

```
VSPswitch(config)#snmp-server host <ipv4|ipv6 addr> port <1-65535> v1
<security name> filter <filter profile name>
```

- SNMPv2c

```
VSPswitch (config)#snmp-server host <ipv4|ipv6 addr> port <1-65535>  v2c
<security name> inform timeout <value> retries <value> mms <value> filter
<filter profile name>
```

- SNMPv3

```
VSPswitch(config)#snmp-server host <ipv4|ipv6 addr> port <1-65535>  v3
<noAuthNoPriv| authNoPriv|authPriv> <user name> inform timeout <value>
retries <value> mms <value> filter <filter profile name>
```

Where:

Variable	Value
ipv4|ipv6 addr	Specifies either an IPv4 or IPv6 address.
<security name>	<security name 1-32> specifies the security name, which identifies the principal that generates SNMP messages.
inform	inform indicates that SNMP notifications should be sent as inform (rather than trap). Inform PDUs are ACKed, Traps PDUs are not
mms	mms <0-2147483647> specifies the maximum message size as an integer with a range of 1 to 2147483647.
Retries	retries <0-255> specifies the retry count value with a range of 0 to 255.
timeout	timeout <0-2147483647> specifies the timeout value in seconds with a range of 0 to 214748364.
filter	filter <WORD 1-32> specifies the filter profile to use.
target-name	target-name <WORD 1-32> is the target name with a string length of 1 to 32.

8.16 SNMPv1 Trap Configuration Example

8.16.1 Configuration

In this example, we will configure the following

- Add a SNMPv1 trap-receiver with a host address of 192.168.50.100
- Add a SNMPv2c trap-receiver with a host address of 192.168.50.101
- Add a SNMPv3 trap-receiver with a host address of 192.168.50.102
- Use an IP loopback address as the SNMP trap source address

Note: when using Avaya Visualization Performance & Fault Manager (VPFM), if you discover the managed VSP switches using SNMPv3, you must ensure that the VSP switches will generate SNMP Traps back to VPFM using the same SNMP version, otherwise VPFM will not perform any correlation with the Traps it receives

Step 1 – Add an SNMPv1 trap receiver with an target address of 192.168.50.100 using the default notification tag *trapTag* for SNMPv1 traps

```
VSPswitch:1(config)#snmp-server host 192.168.50.100 v1 readview
VSPswitch:1(config)#snmp-server host 192.168.50.101 v2c readview
VSPswitch:1(config)#snmp-server host 192.168.50.102 v3 authNoPriv operator
```

Step 2 – Add the Loopback address

```
VSPswitch:1(config)#interface loopback 1
VSPswitch:1(config-if)#ip address 1 10.55.1.1/32
VSPswitch:1(config-if)#exit
```

Step 3 – Set the SNMP trap sender IP address using the Loopback address

```
VSPswitch:1(config)#snmp-server sender-ip 192.168.50.100 10.55.1.1
VSPswitch:1(config)#snmp-server sender-ip 192.168.50.101 10.55.1.1
VSPswitch:1(config)#snmp-server sender-ip 192.168.50.102 10.55.1.1
VSPswitch:1(config)#snmp-server force-trap-sender enable
VSPswitch:1(config)#snmp-server force-iphdr-sender enable
```

8.16.2 Verify Operations

Step 1 – Verify configuration

```
VSPswitch:1(config)#show running-config module sys
#
```

```
# SNMP V3 GLOBAL CONFIGURATION
#

snmp-server force-iphdr-sender enable
snmp-server sender-ip 192.168.50.100 10.55.1.1
snmp-server sender-ip 192.168.50.101 10.55.1.1
snmp-server sender-ip 192.168.50.102 10.55.1.1
snmp-server force-trap-sender enable

#
# SNMP V3 TARGET ADDRESS CONFIGURATION
#

snmp-server host 192.168.50.100 v1 readview
snmp-server host 192.168.50.101 v2c readview
snmp-server host 192.168.50.103 v3 authNoPriv operator
```

Step 2 – Verify SNMP trap receiver

```
VSPswitch:1(config)#show snmp-server host
================================================================================================
                              Target Address Configuration
================================================================================================

Target Name                       TDomain   TAddress                TMask
------------------------------------------------------------------------------------------------
4f99cb74d471bada1dc572fa85a1fe51 ipv4      192.168.50.102:162
c0c5053151fc2c2528f09ef8dea9ae40 ipv4      192.168.50.100:162
e3db3c46aee813fc6fd46acccf54bca4 ipv4      192.168.50.101:162


================================================================================================================
                                              Target Address Configuration
================================================================================================================
Target Name                       Timeout Retry TagList       Params                              MMS
----------------------------------------------------------------------------------------------------------------
4f99cb74d471bada1dc572fa85a1fe51 1500    3     trapTag       4f99cb74d471bada1dc572fa85a1fe51 484
c0c5053151fc2c2528f09ef8dea9ae40 1500    3     trapTag       c0c5053151fc2c2528f09ef8dea9ae40 484
e3db3c46aee813fc6fd46acccf54bca4 1500    3     trapTag       e3db3c46aee813fc6fd46acccf54bca4 484
```

```
================================================================================================
                                Target Params Configuration
================================================================================================
Target Name                          MP Model  Security Name                     Sec Level
------------------------------------------------------------------------------------------------
4f99cb74d471bada1dc572fa85a1fe51 usm       operator                          authNoPriv
TparamV1                             snmpv1    readview                          noAuthNoPriv

TparamV2                             snmpv2c   readview                          noAuthNoPriv
c0c5053151fc2c2528f09ef8dea9ae40 snmpv1    readview                          noAuthNoPriv
e3db3c46aee813fc6fd46acccf54bca4 snmpv2c   readview                          noAuthNoPriv
```

9. Access Policy

You can control access to the switch by creating an access policy. Presently, management access to a VSP switch is only allowed to an IP interface in VRF zero (GRT). Management access is not allowed to an IP interface in any other VRF. An access policy specifies the hosts or networks that can access the device through various services, such as Telnet, SNMP, Hypertext Transfer Protocol (HTTP), Remote Shell (RSH), and remote login (rlogin). Overall, the Access Policy feature on the VSP switch supports the following feature:

- ***Access level:*** Specifies the access level of the trusted as hostreadOnly (ro), readWrite (rw), or readWriteAll (rwa)
- ***Mode:*** Indicates whether a packet having a source IP address that matches this entry should be permitted to enter the device or denied access.
- ***Service***: Indicates the protocol to which this entry should be applied. Choices are telnet, snmp, tftp, ftp, http, rlogin, and/or ssh.
- ***Precedence:*** Indicates the precedence of the policy. The lower the number, the higher the precedence (1 to 128).
- ***Network Address and Network Mask:*** Indicates the source network IP address and mask. An address of 0.0.0.0 specifies any address on the network.
- ***Host:*** Indicates the trusted IP address of the host performing rlogin or rsh into the device. Applies only to rlogin and rsh.
- ***Access-strict:*** Sets the access level strictly.

Enterprise Device Manager does not provide SNMPv3 support for an access policy. If you modify an access policy with Device Manager, ensure SNMPV3 is disabled.

9.1 Enable Access Polices Globally

To enable or disable access policy globally, enter the following command.

```
VSPswitch(config)#access-policy
VSPswitch(config)#no access-policy
```

9.2 Adding an Access Policy

To add a new access policy, enter the following command.

a) Add a new policy

```
VSPswitch(config)#access-policy <1..65535>
```

b) After entering the above command, enter the appropriate parameters and services:

```
VSPswitch(config)#access-policy <1..65535> ?
  access-strict   Set access level strictly
  accesslevel     Set policy access level
  enable          Enables accesspolicy in global configuration
  ftp             Enable ftp
  host            Set access policy trusted host addr
  http            Enable http
  mode            Access policy mode {allow|deny}
  name            Set access policy name
  network         Set access policy netaddr/netmask
  precedence      Set access policy precedence
  rlogin          Enable rlogin
  snmp-group      Add snmpV3 group under this access policy
  snmpv3          Enable snmp
  ssh             Enable ssh
  telnet          Enable telnet
  tftp            Enable tftp
  username        Set access policy trusted host user name
```

where:

Variable	Value
Id	Specifies the policy ID.
name	Specifies the name of the policy.
mode	Indicates whether a packet with a source IP address matching this entry is permitted to enter the device or is denied access.
precedence	Indicates the precedence of the policy expressed in a range from 1–128. The lower the number, the higher the precedence.
network	Specifies whether the designated IP address and subnet mask are permitted or denied access through the specified access service. IPv4 is expressed in the format a.b.c.d. IPv6 is expressed in the format a:b:c:d:e:f:g:h.

host	Indicates the trusted address of a host performing a remote login to the device. You cannot use wildcard entries
username	Specifies the user name assigned to the trusted host. The trusted host name applies only to rlogin and rsh. Ensure that the trusted host user name is the same as your network logon user name; do not use the switch user name, for example, rwa. You cannot use wildcard entries. The user must already be logged in with the user name to be assigned to the trusted host. For example, using "rlogin -l newusername xx.xx.xx.xx" does not work from a UNIX workstation.
accesslevel	Specifies the access level of the trusted host as one of the following: • ro (readOnly) • rw (readWrite) • rwa (readWriteAll)
accessstrict	Enables or disables strict access criteria for remote users. If unchecked, a user must use an access level identical to the one you selected in the dialog box to use this service. true: remote login users can use only the currently configured access level false: remote users can use any access Level If you do not select true or false, user access is governed by criteria specified in the policy table. For example, a user with an rw access level specified for a policy ID in the policy table is allowed rw and rw access, and ro is denied access.
snmp-group	Adds snmp-v3 group under the access policy. `group-name` is the snmp-v3 group name expressed in a range from 1–32 characters. `model` is the security model: either snmpv1, snmpv2c, or usm.

9.3 Access Policies and SNMP

A policy can be added to allow an administrator to specify a group or groups from the View-based Access Control Module (VACM) for SNMPv1, SNMPv2c, or USM. This allows the administrator to create separate policies for SNMP users based on USM (SNMPv3) or community (SNMPv1 or SNMPv2c) and associate them to groups.

The following command is used to add a SNMP group to a policy.

```
VSPswitch(config)#access-policy <1-65535> snmp-group <group name> <
snmpv1|snmpv2c|usm>
```

```
VSPswitch(config)#access-policy <1-65535> snmpv3
```

In regards to the SNMP group name, use the following command to display the SNMP VACM group access configuration. The default SNMPv1 and SNMPv2c read group name is *readgrp* while the default read-write group is *v1v2grp* which can be found under the snmpv1 and snmpv2c VACM model as shown below. All SNMPv3 groups are shown under the USM model. Please refer to the SNMPv3 section above for more details.

```
VSPswitch#show snmp-server group
================================================================================
                      VACM Group Access Configuration
================================================================================
Group       Prefix Model    Level         ReadV      WriteV     NotifyV
group_1            usm      authPriv      org        org
|
readgrp            snmpv1   noAuthNoPriv v1v2only              org
readgrp            snmpv2c noAuthNoPriv v1v2only              org
|
v1v2grp            snmpv1   noAuthNoPriv v1v2only   v1v2only   v1v2only
v1v2grp            snmpv2c noAuthNoPriv v1v2only   v1v2only   v1v2only
```

9.4 Access Policy Configuration Example – Adding SNMPv1/2c, SSH, FTP, and TELNET Services

9.4.1 Configuration

For this example, we demonstrate how to limit SNMPv1 and SNMPv2c read-write access to a single host and read-only access to a single network. We will also demonstrate show to limit HTTP and Telnet services with read-only and write-write access to separate networks. Overall, we will configure the following

- Policy 1 (default policy)
  - Allow only read-only access to network 172.30.0.0/16 for Telnet and HTTP
- Policy 2
  - Limit SNMPv1 and SNMPv2c read-write access to host 172.30.20.21
- Policy 3
  - Limit SNMPv1 and SNMPv2c read-only access to network 172.0.0.0/8
- Policy 4
  - Allow read-write access to network 172.30.20.0/24 for Telnet and HTTP

The default SNMPv1 and SNMPv2c VACM read group name is *readgrp* while the default read-write group is *v1v2grp*. For this example we will simple use these VACM groups. This can be verified using ACLI command *show snmp-server group*

Step 1 –Setup the default policy, policy 1, to allow for read-only access to network 172.30.0.0/16 for telnet and HTTP services

```
VSPswitch:1(config)#access-policy 1 network 172.30.0.0 16
VSPswitch:1(config)#access-policy 1 access-strict
VSPswitch:1(config)#access-policy 1 accesslevel ro
VSPswitch:1(config)#no access-policy 1 ssh
VSPswitch:1(config) no access-policy 1 ftp
```

Step 2 – Setup policy 2 to allow for read-write SNMPv1 & SNMPv2c access to host 172.30.20.21

```
VSPswitch:1(config)#access-policy 2
VSPswitch:1(config)#access-policy 2 name policy2
VSPswitch:1(config)#access-policy 2 host 172.30.20.21
VSPswitch:1(config)#access-policy 2 snmpv3
VSPswitch:1(config)#access-policy 2 snmp-group v1v2grp snmpv1
VSPswitch:1(config)#access-policy 2 snmp-group v1v2grp snmpv2c
```

Step 3 - Setup policy 3 to allow for read-only SNMPv1 & SNMPv2c access to network 172.0.0.0/8

```
VSPswitch:1(config)#access-policy 3
VSPswitch:1(config)#access-policy 3 name policy3
VSPswitch:1(config)#access-policy 3 network 172.0.0.0 255.0.0.0
VSPswitch:1(config)#access-policy 3 snmpv3
VSPswitch:1(config)#access-policy 3 snmp-group readgrp snmpv1
VSPswitch:1(config)#access-policy 3 snmp-group readgrp snmpv2c
```

Step 4 - Setup policy 4 to allow for read-write to network 172.30.20.0/24 for telnet and HTTP services

```
VSPswitch:1(config)#access-policy 4
VSPswitch:1(config)#access-policy 4 name policy4
VSPswitch:1(config)#access-policy 4 network 172.30.20.0 24
VSPswitch:1(config)#access-policy 4 accesslevel rwa
VSPswitch:1(config)#access-policy 4 access-strict
VSPswitch:1(config)#access-policy 4 http telnet
```

Step 5 - Enable access-policies globally

```
VSPswitch:1(config)#access-policy
```

9.4.2 Verify Operations

Step 1 - Verify Access Policy Configuration

```
VSPswitch:1#show running-config module sys
#
# ACCESS-POLICY CONFIGURATION
#

access-policy
access-policy 1 network 172.30.0.0 16
access-policy 1 access-strict
no access-policy 1 ssh
access-policy 2
access-policy 2 name "policy2" host 172.30.20.21
access-policy 2 snmpv3
access-policy 2 snmp-group v1v2grp snmpv1
access-policy 2 snmp-group v1v2grp snmpv2c
access-policy 3
access-policy 3 name "policy3" network 172.0.0.0 8
access-policy 3 snmpv3
access-policy 3 snmp-group readgrp snmpv1
access-policy 3 snmp-group readgrp snmpv2c
access-policy 4
access-policy 4 name "policy4" network 172.30.20.0 24 accesslevel rwa
access-policy 4 access-strict
access-policy 4 http telnet
```

Step 2 - Verify Access Policy Settings

```
VSPswitch:1#show access-policy
AccessPolicyEnable: on

                Id: 1
              Name: default
      PolicyEnable: true
              Mode: allow
           Service: http|telnet
        Precedence: 128
```

```
         NetAddrType: ipv4
             NetAddr: 172.30.0.0
             NetMask: 255.255.0.0
    TrustedHostAddr: 0.0.0.0
TrustedHostUserName: none
         AccessLevel: readOnly
        AccessStrict: true
               Usage: 143

                  Id: 2
                Name: policy2
        PolicyEnable: true
                Mode: allow
             Service: snmpv3
          Precedence: 10
         NetAddrType: ipv4
             NetAddr: 0.0.0.0
             NetMask: 0.0.0.0
    TrustedHostAddr: 172.30.20.21
TrustedHostUserName: none
         AccessLevel: readOnly
        AccessStrict: false
               Usage: 0


                  Id: 3
                Name: policy3
        PolicyEnable: true
                Mode: allow
             Service: snmpv3
          Precedence: 10
         NetAddrType: ipv4
             NetAddr: 172.0.0.0
             NetMask: 255.0.0.0
    TrustedHostAddr: 0.0.0.0
TrustedHostUserName: none
         AccessLevel: readOnly
        AccessStrict: false
               Usage: 478
```

```
                  Id: 4
                Name: policy4
        PolicyEnable: true
                Mode: allow
             Service: http|telnet
          Precedence: 10
         NetAddrType: ipv4
             NetAddr: 172.30.20.0
             NetMask: 255.255.255.0
     TrustedHostAddr: 0.0.0.0
 TrustedHostUserName: none
         AccessLevel: readWriteAll
        AccessStrict: true
               Usage: 7597
```

Step 3 - Verify Access Policy Configuration

```
VSPswitch:1#show access-policy snmp-group
         snmpv3-groups :

Policy 1 snmpv3-groups:
                        Group Name      Snmp-Model

Policy 2 snmpv3-groups:
                        Group Name      Snmp-Model
                        v1v2grp          snmpv1
                        v1v2grp         snmpv2c

Policy 3 snmpv3-groups:
                        Group Name      Snmp-Model
                        readgrp          snmpv1
                        readgrp         snmpv2c

Policy 4 snmpv3-groups:
                        Group Name      Snmp-Model
```

9.5 Access Policy Configuration Example – limit SNMPv3 to specific host and Telnet Access to a specific network

9.5.1 Configuration

A policy can be added to allow administrator to specify a group or groups for SNMPv3 access. This allows the administrator to create separate policies for SNMP users based on USM.

For this example, we wish setup a policy to limit SNMPv3 to a specific host and allow Telnet access to a network. Overall, we wish to configure the following:

- Create SNMPv3 AuthPriv User
  - Add an SNMPv3 AuthPriv user using MD5 authentication and DES privacy protocol
  - User name = user1, MD5 authentication password = user1234, and DES privacy password = userpric
  - Use SNMP USM group name of group_1
- Create access policy 2
  - Limit SNMP USM group_1 only to host 172.30.20.21
- Create access policy 3
  - Limit Telnet access only to network 172.30.0.0/16

Step 1 - Add SNMPv3 user

```
VSPswitch:1(config)#load-encryption-module DES
VSPswitch:1(config)#snmp-server user user1 group group_1 md5 user1234 des userpriv
VSPswitch:1(config)#snmp-server group group_1 "" auth-priv read-view org write-view org
```

Note, in VOSS 4.2 and later, it is not necessary to manually load the encryption modules. In these releases, the encryption modules are loaded automatically with the run-time image.

Step 2 - Assuming no access policies have been created and we wish to leave the default, policy 1 intact (which allows for ftp, http, telnet and ssh access), we can start with policy 2 and name the policy policy2 for SNMPv3 access

```
VSPswitch:1(config)#access-policy 2
VSPswitch:1(config)#access-policy 2 name policy2
VSPswitch:1(config)#access-policy 2 host 172.30.20.21
VSPswitch:1(config)#access-policy 2 accesslevel rwa
VSPswitch:1(config)#access-policy 2 snmp-group group_1 usm
VSPswitch:1(config)#access-policy 2 access-strict
VSPswitch:1(config)#access-policy 2 snmpv3
```

Step 3 - Create policy 3 for Telnet acccess and name the policy policy3

```
VSPswitch:1(config)#access-policy 3
VSPswitch:1(config)#access-policy 3 name policy3
VSPswitch:1(config)#access-policy 3 network 172.30.0.0 255.255.0.0
VSPswitch:1(config)#access-policy 3 accesslevel rwa
VSPswitch:1(config)#access-policy 3 access-strict
VSPswitch:1(config)#access-policy 3 ssh telnet
```

Step 4 - Enable access-policies globally

```
VSPswitch:1(config)#access-policy
```

If SNMPv3 access is denied even if the criterion for the access policy is valid, ensure that SNMP is not blocked by the block-snmp boot configuration flag. The setting should be set to false to allow SNMP (flags block-snmp false).

Depending if policy 1 is used or not, you may wish to ensure it is disabled by issuing the ACLI command *no access-policy 1 enable*.

9.5.2 Verify Operations

Step 1 - Verify Access Policy Configuration

```
VSPswitch:1#show running-config module sys
#
# ACCESS-POLICY CONFIGURATION
#

access-policy
no access-policy 1 enable
access-policy 1 ftp
access-policy 2
access-policy 2 name "policy2" host 172.30.20.21 accesslevel rwa
access-policy 2 access-strict
access-policy 2 snmpv3
access-policy 2 snmp-group group_1 usm
access-policy 3
access-policy 3 name "policy3" network 172.30.0.0 16 accesslevel rwa
access-policy 3 access-strict
access-policy 3 ssh telnet
```

Step 2 - Verify Access Policy Settings

```
VSPswitch:1#show access-policy
AccessPolicyEnable: on

                  Id: 1
                Name: default
        PolicyEnable: false
                Mode: allow
             Service: ftp|http|telnet|ssh
          Precedence: 128
         NetAddrType: any
             NetAddr: N/A
             NetMask: N/A
     TrustedHostAddr: N/A
 TrustedHostUserName: none
         AccessLevel: readOnly
        AccessStrict: false
```

```
                Usage: 0


                   Id: 2
                 Name: policy2
         PolicyEnable: true
                 Mode: allow
              Service: snmpv3
           Precedence: 10
          NetAddrType: ipv4
              NetAddr: 0.0.0.0
              NetMask: 0.0.0.0
     TrustedHostAddr: 172.30.20.21
 TrustedHostUserName: none
         AccessLevel: readWriteAll
        AccessStrict: true
                Usage: 0


                   Id: 3
                 Name: policy3
         PolicyEnable: true
                 Mode: allow
              Service: telnet|ssh
           Precedence: 10
          NetAddrType: ipv4
              NetAddr: 172.30.0.0
              NetMask: 255.255.0.0
     TrustedHostAddr: 0.0.0.0
 TrustedHostUserName: none
         AccessLevel: readWriteAll
        AccessStrict: true
                Usage: 772
```

Step 3 - Add SNMPv3 user

```
VSPswitch:1#show access-policy snmp-group
           snmpv3-groups :

Policy 1 snmpv3-groups:
                         Group Name      Snmp-Model

Policy 2 snmpv3-groups:
                         Group Name      Snmp-Model
                         group_1             usm

Policy 3 snmpv3-groups:
                         Group Name      Snmp-Model
```

10. Reference Documentation

Document Title	Publication Number	Description