Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Dorado Software Redcell Enterprise Bundle using SNMP with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration of Dorado Software Redcell Enterprise Bundle using SNMP with Avaya Communication Manager running on various hardware platforms. Information in these Application Notes has been obtained through compliance testing. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration needed to enable Dorado Software Redcell Enterprise Bundle using three modules (Redcell Management Center, Redcell Inventory Manager and Redcell Assure) to be capable of communicating and monitoring Avaya Communication Manager using SNMP. Redcell Enterprise Bundle is a modular application that users can add additional functionality by installing additional Redcell Enterprise Bundle modules. Compliance testing emphasized the capability of Redcell Enterprise Bundle to communicate with Avaya Communication Manager using SNMP version 2c, and the capability of Redcell Enterprise Bundle to receive SNMP traps from Avaya Communication Manager. Redcell Enterprise Bundle was also verified to provide system level information such as software release string, model number, serial number, configured stations, trunk groups and region information. Dorado Software Redcell Enterprise Bundle uses device drivers to communicate with equipment from various manufacturers. For this testing the Avaya Device Driver version 5.1.3.7 was used. Dorado Software Redcell Enterprise Bundle was tested with various Avaya Communication Manager systems.

1.1. Redcell Enterprise Bundle Components

Redcell Management Center (RMC) is an infrastructure administration system for multi-vendor IT environments. RMC is a modular application that provides an integrated system for configuring, monitoring, troubleshooting and managing any infrastructure device, including routers, switches, storage, servers, PCs and security devices. RMC can manage equipment from multiple vendors and serves as a foundation for other Dorado Redcell applications including service assurance and provisioning.

Redcell Inventory Manager is an automated inventory lifecycle management solution that presents the big picture of both physical and logical IT assets - hardware, software and configurations, as well as connections, relationships, and ownership. The product recognizes any IT device with its inherent deep discovery and resynchronization engine and provides sophisticated reporting capabilities.

Redcell Assur**e** provides real-time event management, fault management, service monitoring, syslog monitoring and root cause correlation to ensure uninterrupted operations of multiple services and devices across a heterogeneous infrastructure. Redcell Assure also automates action for rapid and effective response to events.

2. Hardware Configuration

Figure 1 shows the environment used for the compliance testing. The environment consists of an IP based network where several Avaya Communication Manager systems were present. Dorado Software Redcell Enterprise Bundle was part of this IP network with IP connectivity to all the components in the test environment.

The External SNMP Server was used to verify that Redcell could receive SNMP traps, filter traps and forward them to an external SNMP server. The Redcell server was the computer where both the Redcell application and database were housed.

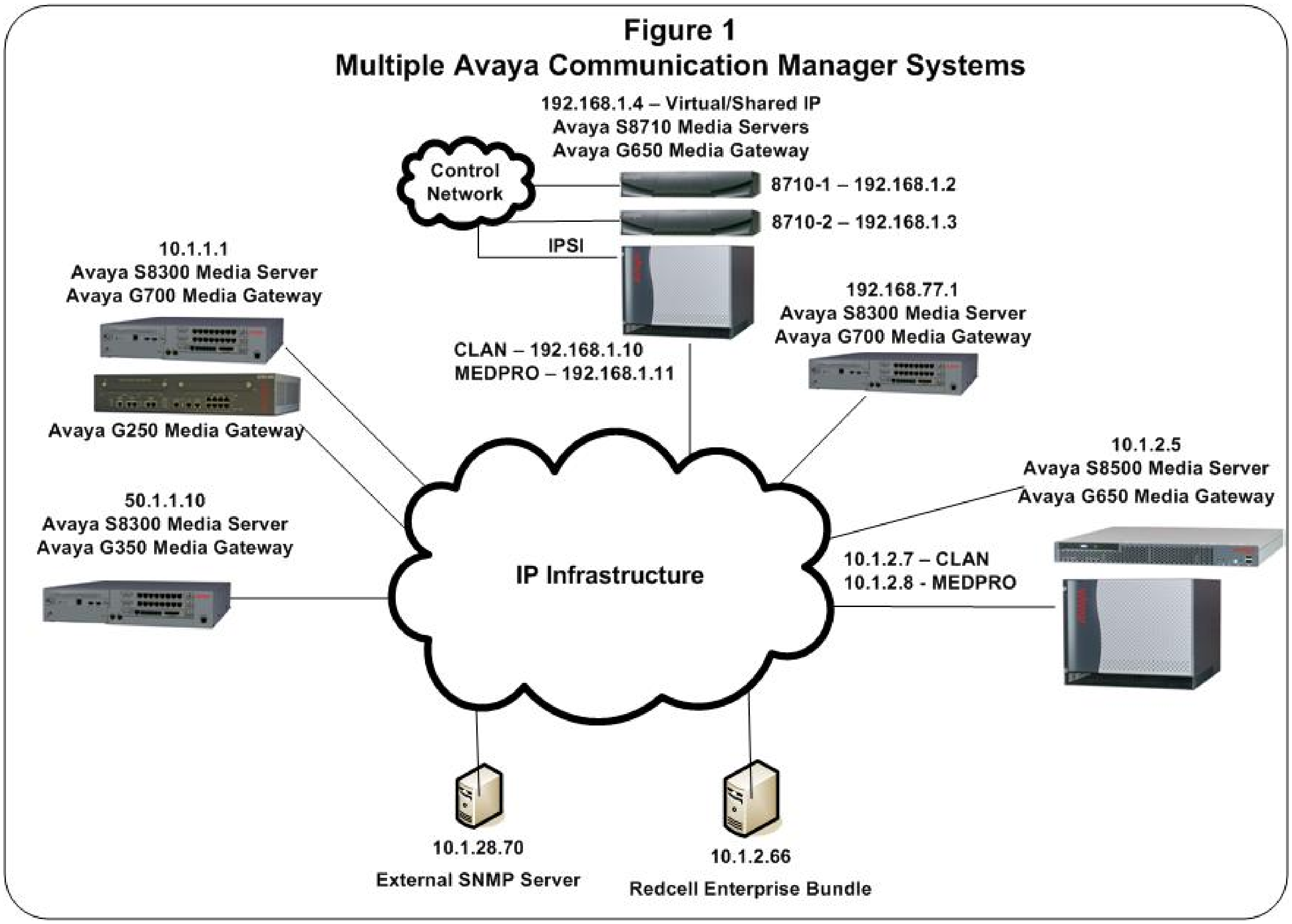
2.1. Figure 1- Multiple Avaya Communication Managers

Inside **Figure 1** are several hardware platforms running Avaya Communication Manager. Three Avaya Media Servers with four Avaya Media Gateways were tested.

- Avaya Media Server 8300 with Avaya G250 Media Gateway.
- Avaya Media Server 8300 with Avaya G350 Media Gateway.
- Avaya Media Server 8300 with Avaya G700 Media Gateway.
- Avaya Media Server 8500 with Avaya G650 Media Gateway.
- Avaya Media Server 8710 with Avaya G650 Media Gateway.

There are no phones shown in the diagram as the purpose of the testing was to prove interoperability between Dorado Software Redcell Enterprise Bundle and Avaya Communication Manager using SNMP. Redcell Enterprise Bundle can manage any IP device (including IP Phones) which responds to PINGs.

Figure 1: Redcell and Avaya Communications Manager Testing Environment



3. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Equipment	Software/Firmware
Avaya Media Server 8300 and Avaya G250 Media Gateway	Avaya Communication Manager 3.1.2.632.1
Avaya Media Server 8300 and Avaya G350 Media Gateway	Avaya Communication Manager 3.1.2.632.1
Avaya Media Server 8300 and Avaya G700 Media Gateway	Avaya Communication Manager 3.1.2.632.1
Avaya Media Server 8500 and Avaya G650 Media Gateway	Avaya Communication Manager 3.1.2.632.1
Avaya Media Server 8710 and Avaya G650 Media Gateway	Avaya Communication Manager 3.1.2.632.1
Redcell Enterprise Bundle	5.3.7.78
Redcell Management Center	5.3
Redcell Inventory Manager	5.3
Redcell Assure	5.3
Redcell Avaya Device Driver	5.3.1.7

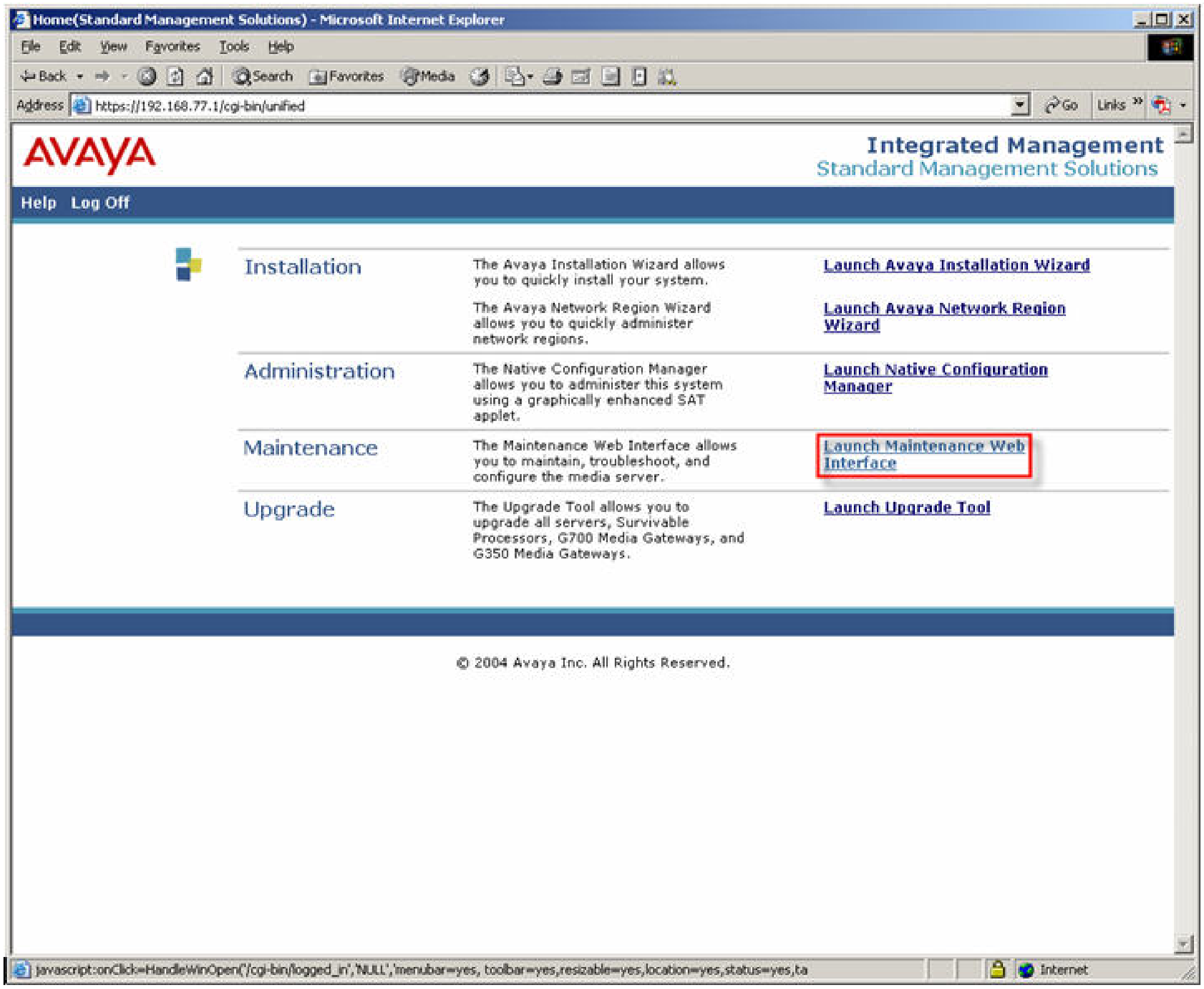
4. Configure Avaya Communication Manager

Enabling an SNMP Management system is a four-step process: configure SNMP agents, configure SNMP traps, enable SNMP to pass through the Avaya Communication Manager firewall and restarting the SNMP agent. This process is the same for the Avaya Media Server 8300, 8500 and 8710. For the Avaya 87XX Media Server series configured in redundancy mode be sure to include the physical address as well as the shared virtual IP address.

Use any web to browser connect to the Avaya Media Server being configured. Place the IP address of the system into the URL. After connecting, log into the Avaya Media Server using appropriate credentials. Click "**Launch Maintenance Web Interface**". This will open up a new window that will allow the user to complete the configuration process.

4.1. Launch the Maintenance Web Interface

This is the web page provided to the user once they have logged into Avaya Communication Manager via a web browser. Click “**Launch Maintenance Web Interface**” to proceed.


Home(Standard Management Solutions) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://192.168.77.1/cgi-bin/unified
Go Links
AVAYA
Integrated Management
Standard Management Solutions
Help Log Off

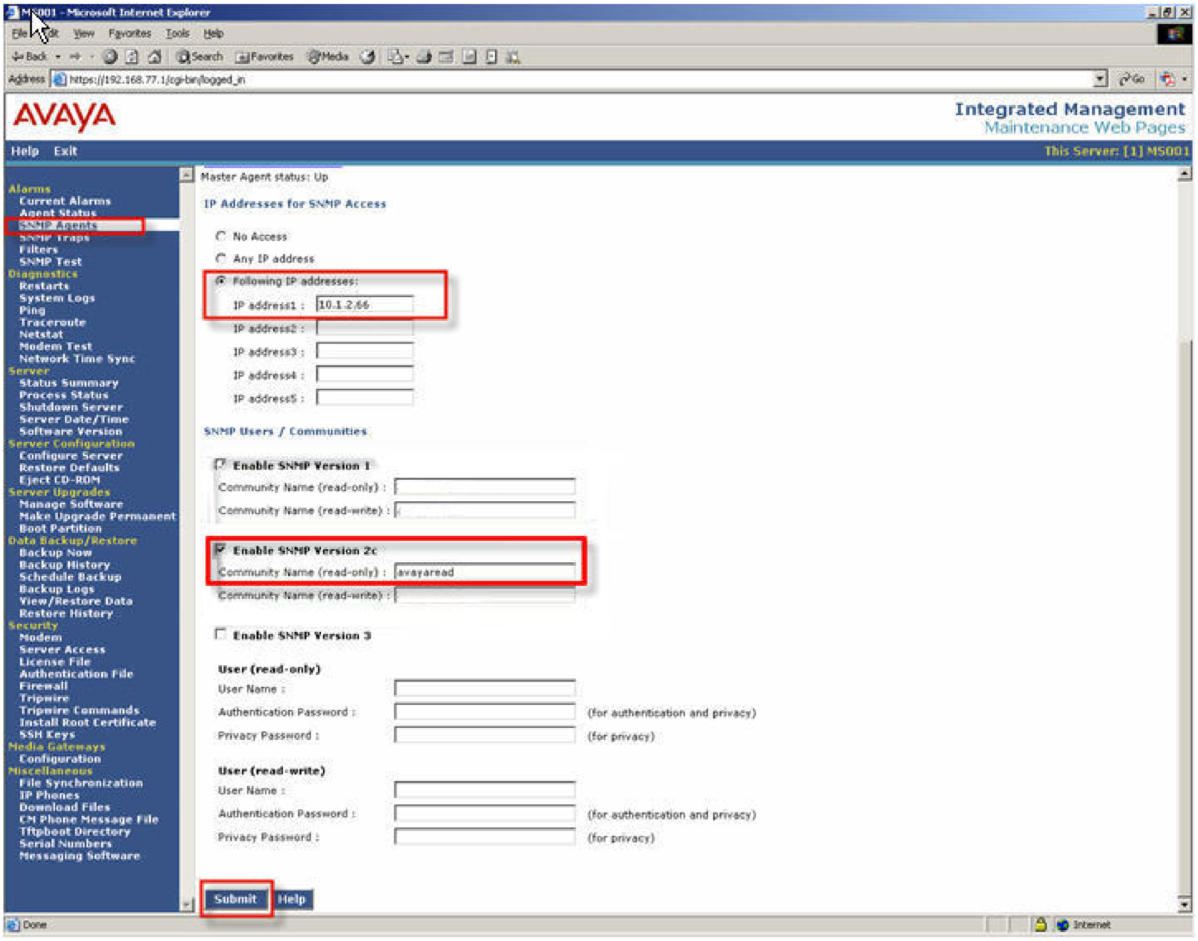
Installation	The Avaya Installation Wizard allows you to quickly install your system.	Launch Avaya Installation Wizard
	The Avaya Network Region Wizard allows you to quickly administer network regions.	Launch Avaya Network Region Wizard
Administration	The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet.	Launch Native Configuration Manager
Maintenance	The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the media server.	Launch Maintenance Web Interface
Upgrade	The Upgrade Tool allows you to upgrade all servers, Survivable Processors, G700 Media Gateways, and G350 Media Gateways.	Launch Upgrade Tool

© 2004 Avaya Inc. All Rights Reserved.

javascript:onClick=HandleWinOpen('/cgi-bin/logged_in','NULL','menubar=yes, toolbar=yes,resizable=yes,location=yes,status=yes,ta

4.2. Configure SNMP Agents

Use the navigation panel on the left side of the web page (colored blue) and select **"Alarms>SNMP Agents"**. Click the "**Following IP addresses**" button and provide the IP address of the Redcell Enterprise Bundle server. Check the check box labeled **"Enable SNMP Version 2c". Configure the "read-only"** community string value. This string can be any value but must match the community string assigned to the Redcell Enterprise Bundle server in Section 5.9. Click "**Submit"**.



Master Agent status: Up

IP Addresses for SNMP Access

○ No Access

○ Any IP address

● Following IP addresses:

IP address1 : 10.1.2.66

IP address2 :

IP address3 :

IP address4 :

IP address5 :

SNMP Users / Communities

□ Enable SNMP Version 1

Community Name (read-only) :

Community Name (read-write) :

☑ Enable SNMP Version 2c

Community Name (read-only) : avayaread

Community Name (read-write) :

□ Enable SNMP Version 3

User (read-only)

User Name :

Authentication Password : (for authentication and privacy)

Privacy Password : (for privacy)

User (read-write)

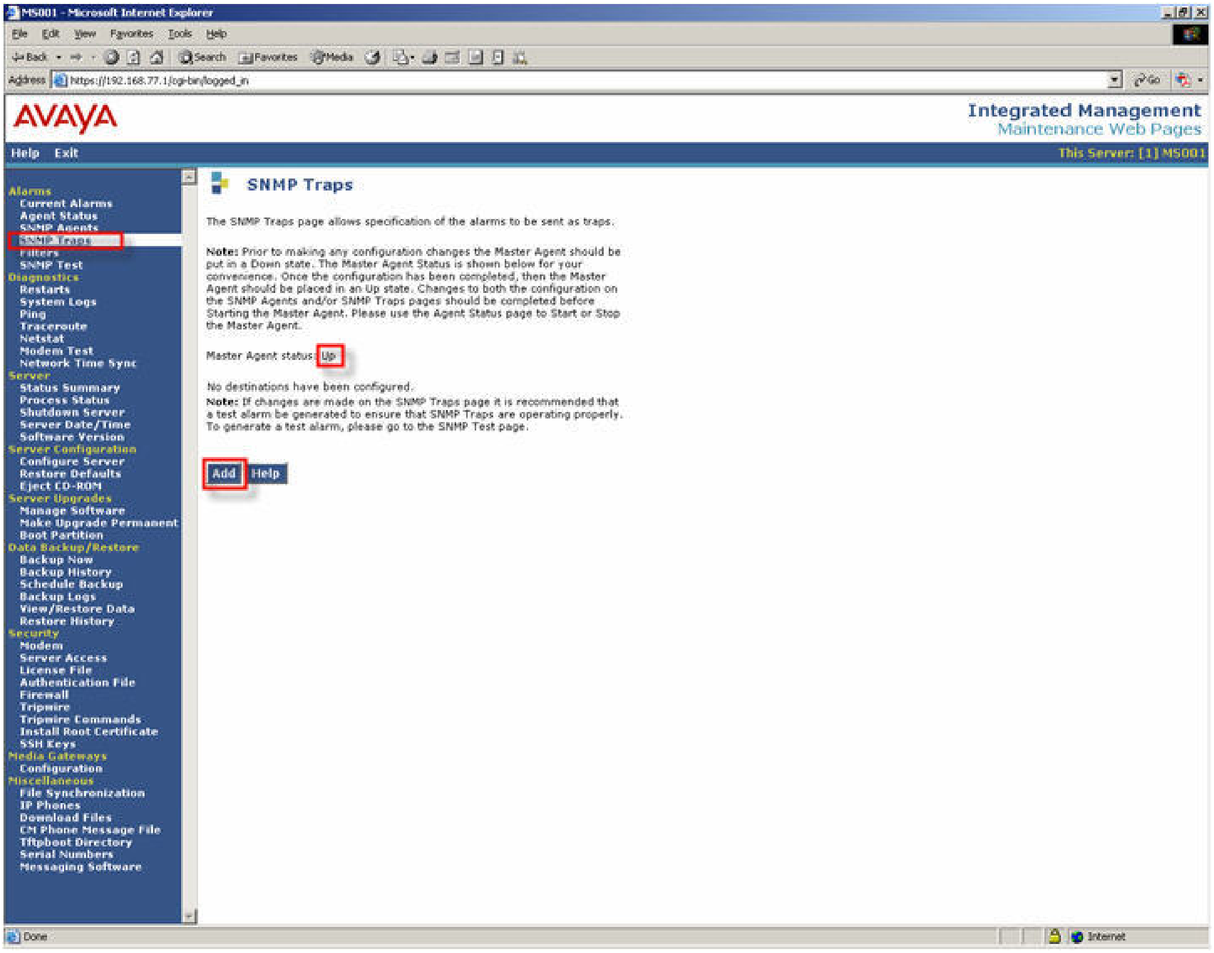
User Name :

Authentication Password : (for authentication and privacy)

Privacy Password : (for privacy)

4.3. Configure SNMP Traps

Use the navigation panel on the left side of the web page (colored blue) and select **"Alarms>SNMP Traps"**. Make sure the Master Agent status indicates **"Up"**. Should the Master Agent status not report up, it can be started using the "**Alarms>Agent Status"** page. Click "**Add"** to add a new SNMP trap recipient.



SNMP Traps

The SNMP Traps page allows specification of the alarms to be sent as traps.

Note: Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages should be completed before Starting the Master Agent. Please use the Agent Status page to Start or Stop the Master Agent.

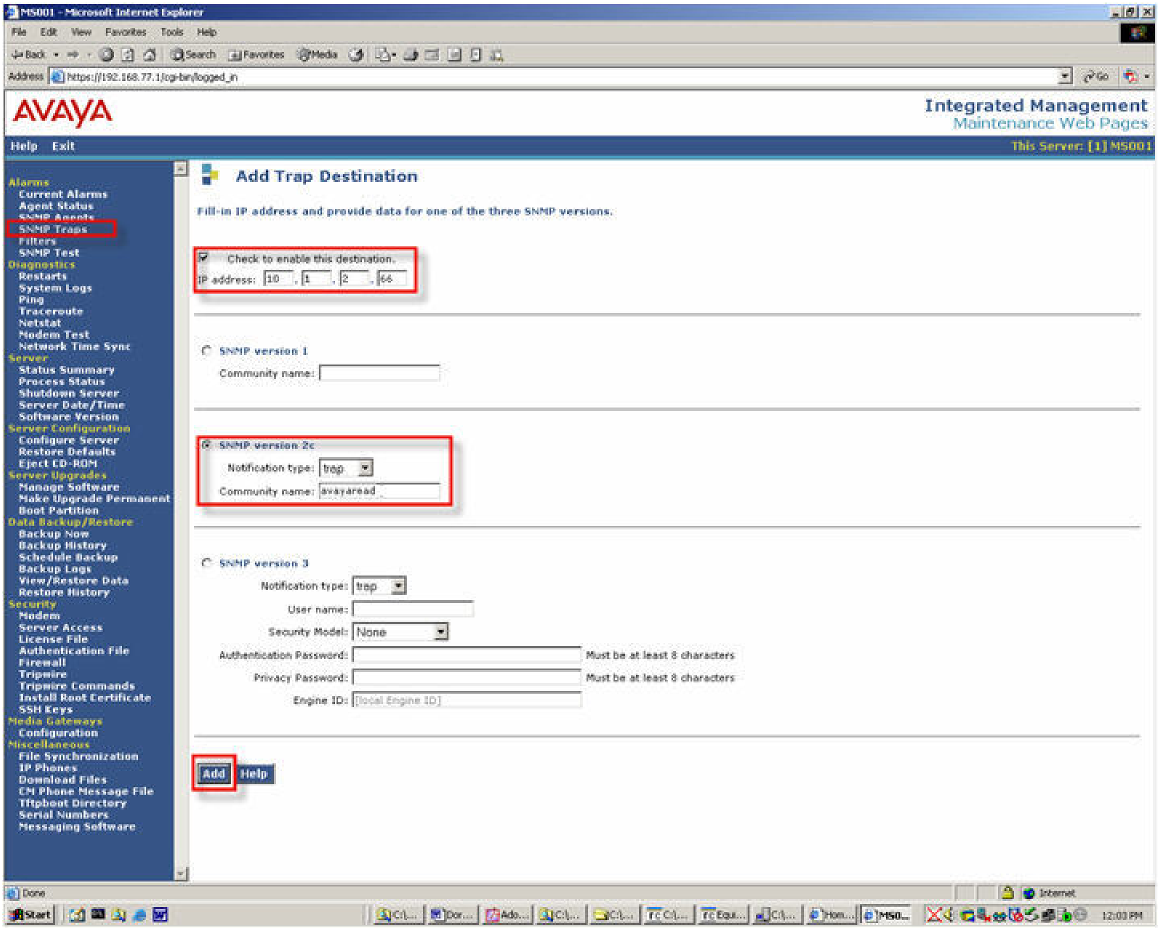
Master Agent status: Up

No destinations have been configured.

Note: If changes are made on the SNMP Traps page it is recommended that a test alarm be generated to ensure that SNMP Traps are operating properly. To generate a test alarm, please go to the SNMP Test page.

4.4. Configure SNMP Traps

Check the check box labeled “**Check to enable this destination**” and provide the IP address of the Redcell Enterprise Bundle server. Click the button labeled “**SNMP Version 2c”** and specify the Notification type of “**trap**” and specify the **“Community name”**. This is the community name where SNMP traps will be sent. This community name does not need to match the previous one defined Section in 4.2. Click “**Add”**.



Add Trap Destination

Fill-in IP address and provide data for one of the three SNMP versions.

☑ Check to enable this destination.
IP address: 10 . 1 . 2 . 66

○ SNMP version 1
Community name:

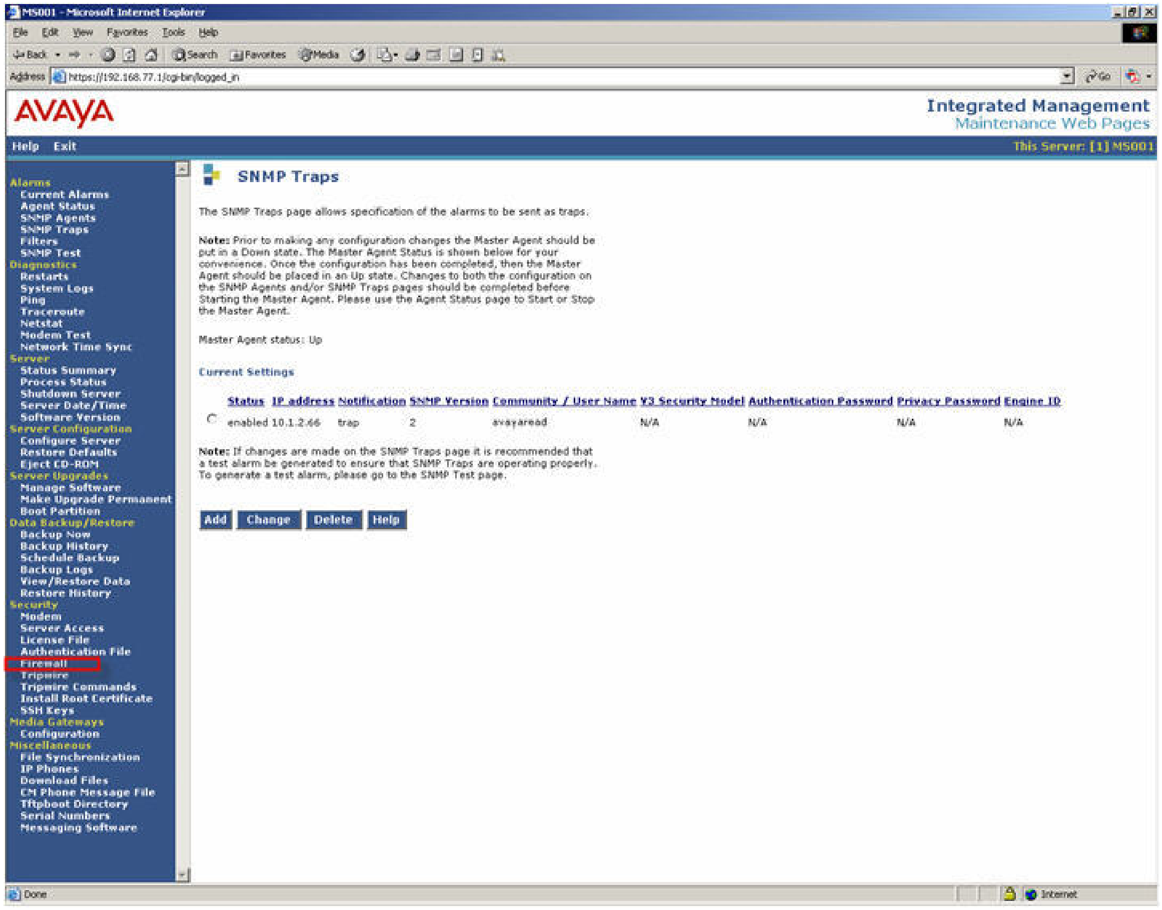
● SNMP version 2c
Notification type: trap
Community name: avayaread

○ SNMP version 3
Notification type: trap
User name:
Security Model: None
Authentication Password: Must be at least 8 characters
Privacy Password: Must be at least 8 characters
Engine ID: [local Engine ID]

Add Help

4.5. Configure SNMP Traps

The SNMP trap recipient has been configured. The Avaya Communication Manager firewall needs to be configured to allow SNMP to pass through the system. Use the navigation panel on the left side of the web page (colored blue) and select **“Security>Firewall”**. The SNMP traps configuration has now been completed and the user is presented with the information. Click “**Firewall”**.



SNMP Traps

The SNMP Traps page allows specification of the alarms to be sent as traps.

Note: Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages should be completed before Starting the Master Agent. Please use the Agent Status page to Start or Stop the Master Agent.

Master Agent status: Up

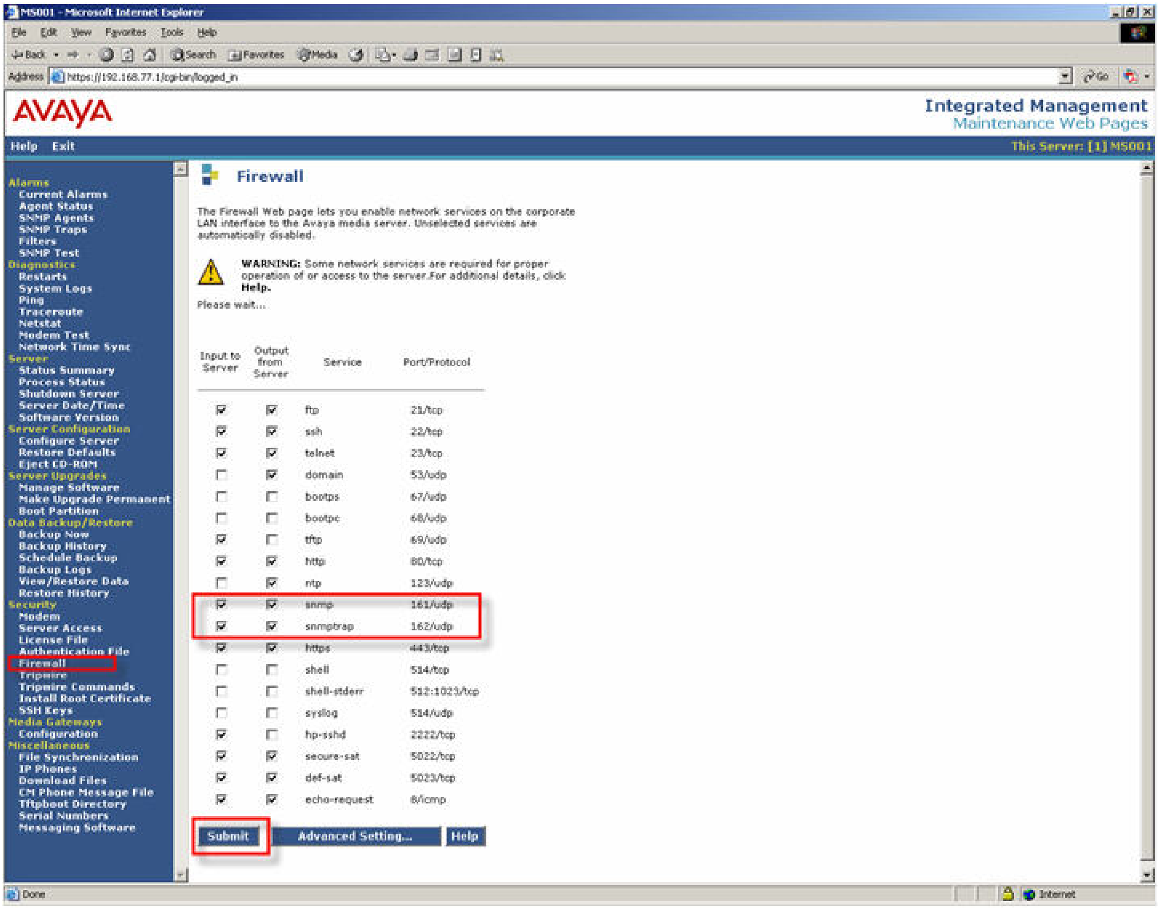
Current Settings

	Status	IP address	Notification	SNMP Version	Community / User Name	V3 Security Model	Authentication Password	Privacy Password	Engine ID
○	enabled	10.1.2.66	trap	2	avayaread	N/A	N/A	N/A	N/A

Note: If changes are made on the SNMP Traps page it is recommended that a test alarm be generated to ensure that SNMP Traps are operating properly. To generate a test alarm, please go to the SNMP Test page.

4.6. Configure Firewall Settings

Check the check boxes for “**snmp**” and “**snmptrap**” for both “**Input to Server**” and “**Output from Server**” to allow the firewall to allow the SNMP traffic. Click **“Submit”**.



Firewall

The Firewall Web page lets you enable network services on the corporate LAN interface to the Avaya media server. Unselected services are automatically disabled.

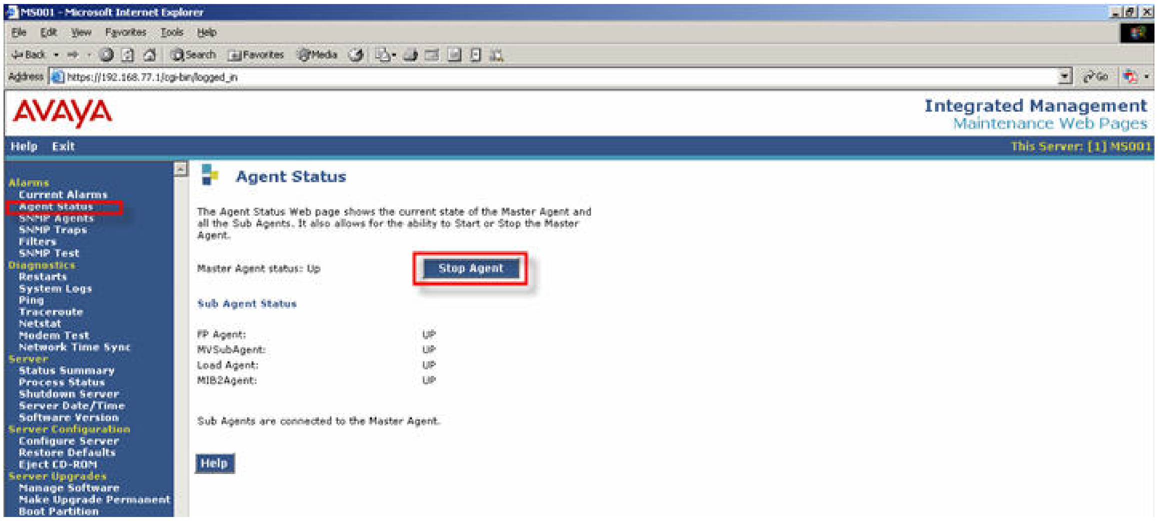
WARNING: Some network services are required for proper operation of or access to the server.For additional details, click **Help.**

Please wait...

Input to Server	Output from Server	Service	Port/Protocol
☑	☑	ftp	21/tcp
☑	☑	ssh	22/tcp
☑	☑	telnet	23/tcp
□	☑	domain	53/udp
□	□	bootps	67/udp
□	□	bootpc	68/udp
☑	□	tftp	69/udp
☑	☑	http	80/tcp
□	☑	ntp	123/udp
☑	☑	snmp	161/udp
☑	☑	snmptrap	162/udp
☑	☑	https	443/tcp
□	□	shell	514/tcp
□	□	shell-stderr	512:1023/tcp
□	□	syslog	514/udp
☑	□	hp-sshd	2222/tcp
☑	☑	secure-sat	5022/tcp
☑	☑	def-sat	5023/tcp
☑	☑	echo-request	8/icmp

4.7. Configure SNMP Agent

Use the navigation section on the left side of the web page (colored blue) and select **"Alarms>Agent Status"**. Using the **Agent Status** web page, stop and then start the agent by clicking on "**Stop Agent**" then "**Start Agent**". This restarts the SNMP agent with the newly configured information which will now be used on the Avaya Media Server.



Agent Status

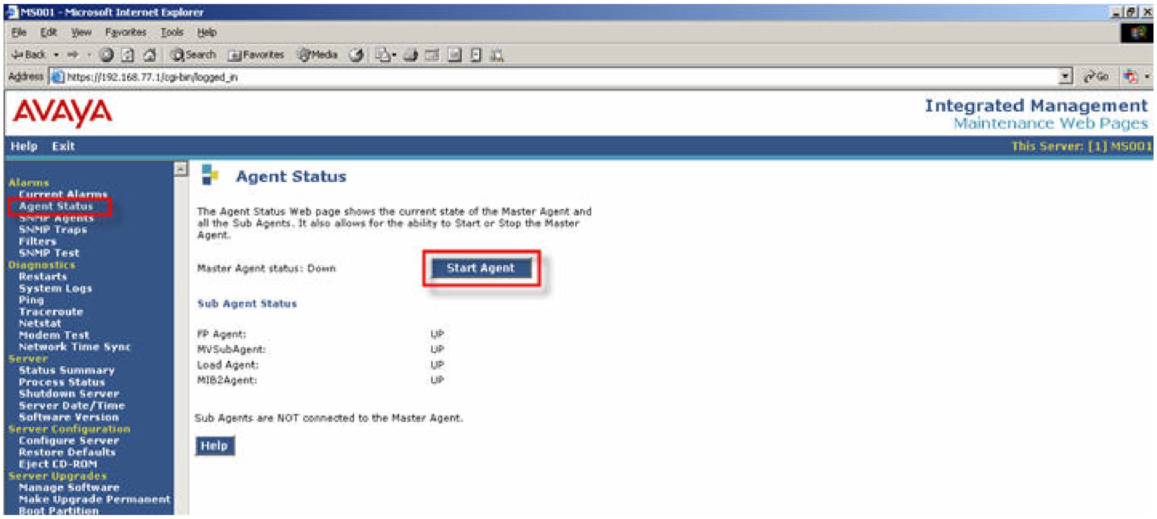
The Agent Status Web page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent.

Master Agent status: Up

Sub Agent Status

FP Agent: UP
MVSubAgent: UP
Load Agent: UP
MIB2Agent: UP

Sub Agents are connected to the Master Agent.



Agent Status

The Agent Status Web page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent.

Master Agent status: Down

Sub Agent Status

FP Agent: UP
MVSubAgent: UP
Load Agent: UP
MIB2Agent: UP

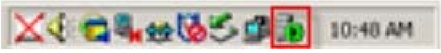
Sub Agents are NOT connected to the Master Agent.

5. Configure Dorado Software Redcell Enterprise Bundle

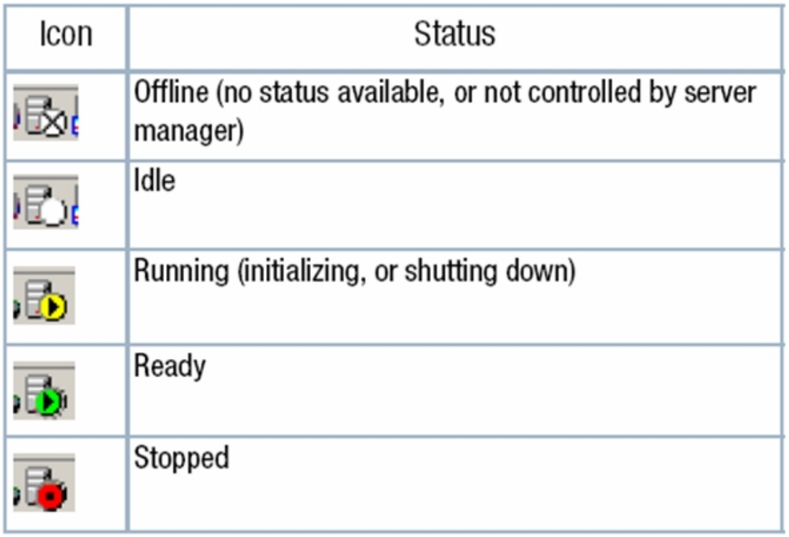
This section details the configuration of Redcell Enterprise Bundle. Redcell Enterprise Bundle can run on a Windows or Solaris platform. For this testing a Windows-based system was chosen, the database and application were installed on the same physical machine but the database does not have to be on the same machine. Redcell has a two step installation process. The first process installs the application and the second process installs the database. Once installed there are additional configurations needed to allow Redcell Enterprise Bundle to communicate with Avaya Communication Manager. This section of the document assumes the user has already installed the database and application and is ready to begin configuring Dorado Software Redcell Enterprise Bundle.

5.1. Verify the Installation of Redcell Enterprise Bundle

With the application and database installed, the software places an icon into the System Tray which can be used to quickly gauge the health of the application. The icon highlighted in the red square is for Redcell Management Center (Redcell Management Center is one of the modules installed into the Redcell Enterprise Bundle). The green symbol indicates the system is healthy.



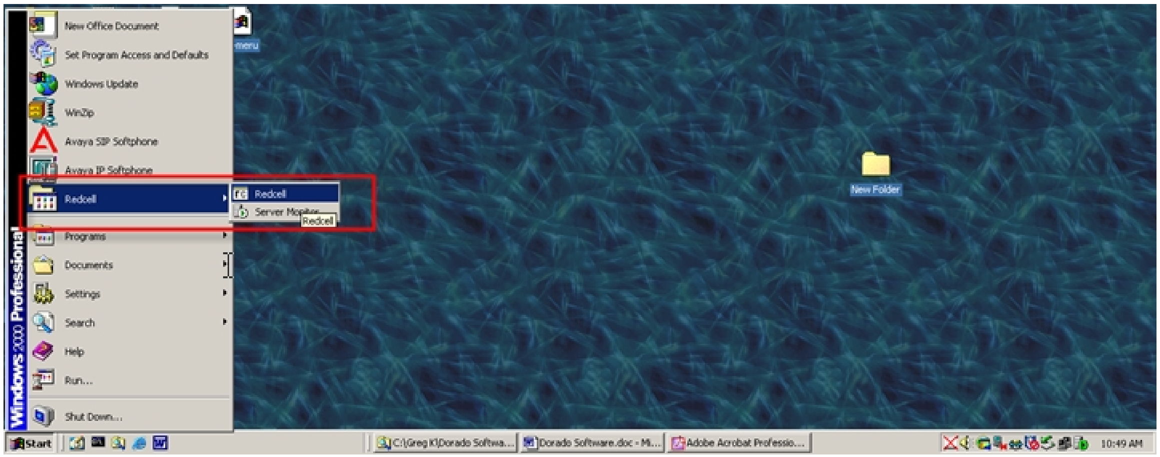
The chart below lists the icons and their respective status.



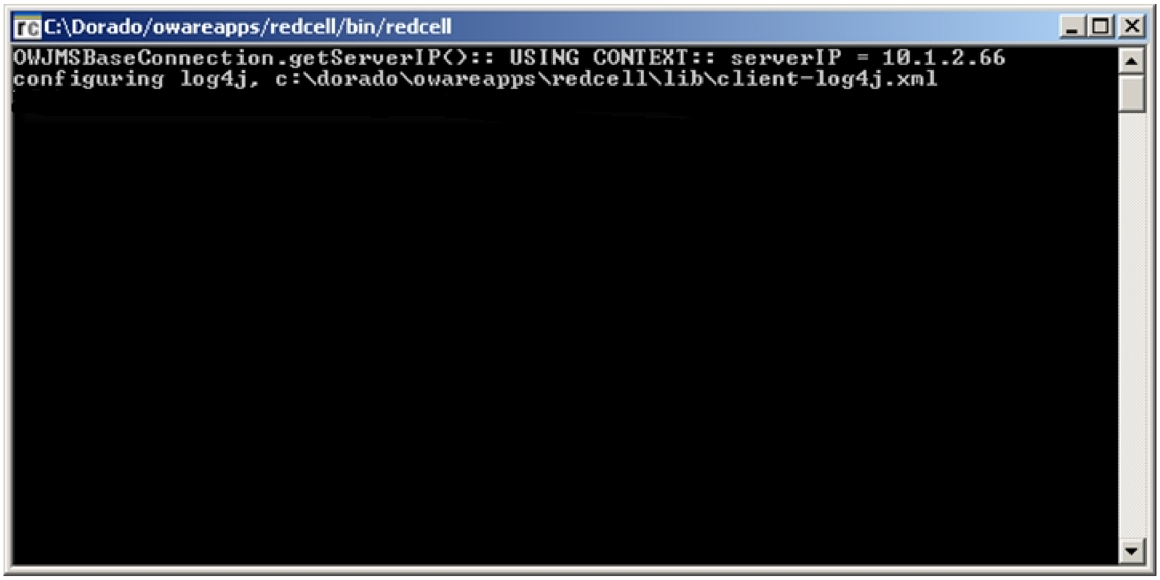
Icon	Status
☒	Offline (no status available, or not controlled by server manager)
○	Idle
▶	Running (initializing, or shutting down)
▶	Ready
●	Stopped

5.2. Start the Application for the First Time

The application installs itself into the “All Users” profile on Windows-based systems and places a shortcut directly into the Start Menu. “**Start>Redcell>Redcell”** is the path to start the application.



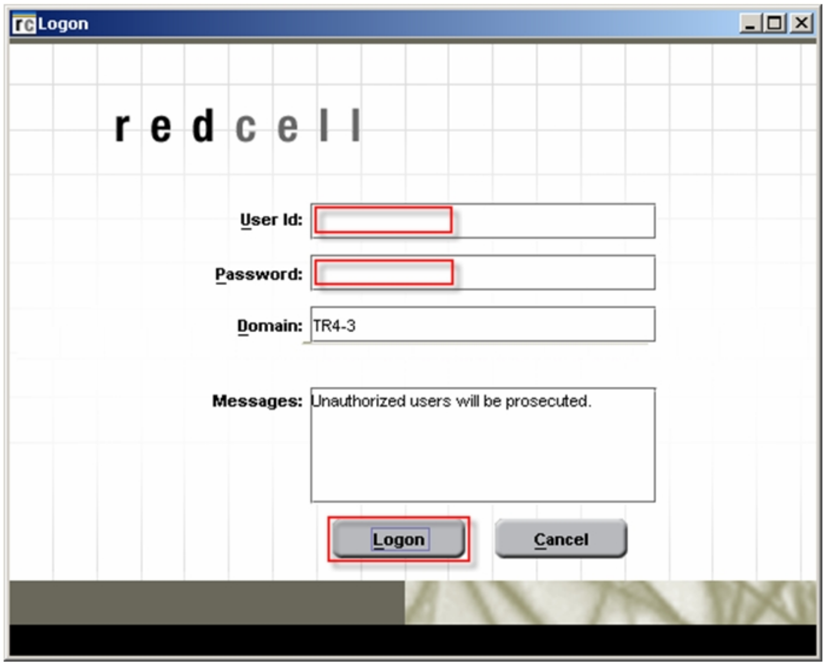
Running the application opens a “Command Prompt” window. This window can be minimized and will remain up while the application is running. Should any errors occur they will be logged to this window.



```
OWJMSBaseConnection.getServerIP():: USING CONTEXT:: serverIP = 10.1.2.66
configuring log4j, c:\dorado\owareapps\redcell\lib\client-log4j.xml
```

5.3. Log into the Application

Log into the application using the default administrator account, this information can be found in the Redcell Enterprise Bundle documentation. The user will be required to change the default administrator password after logging into the system for the first time. Input the appropriate login credentials and click "**Logon**".

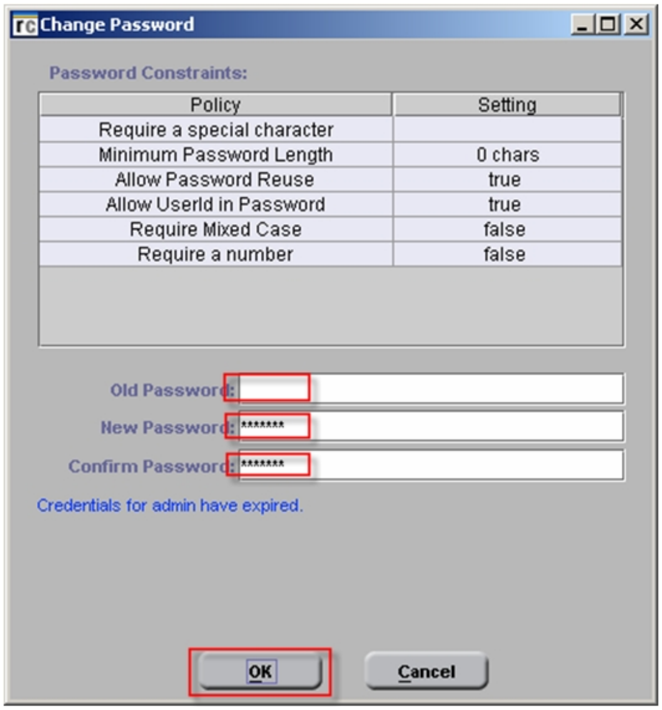


Domain: TR4-3

Messages: Unauthorized users will be prosecuted.

5.4. Change the Default Administrator Login Information

Upon logging in the first time the user has to change the default Administrator login information. Also listed are the criteria necessary for a valid password. Once the new password has been specified which meets the password constraints, click “**OK**”.



Password Constraints:

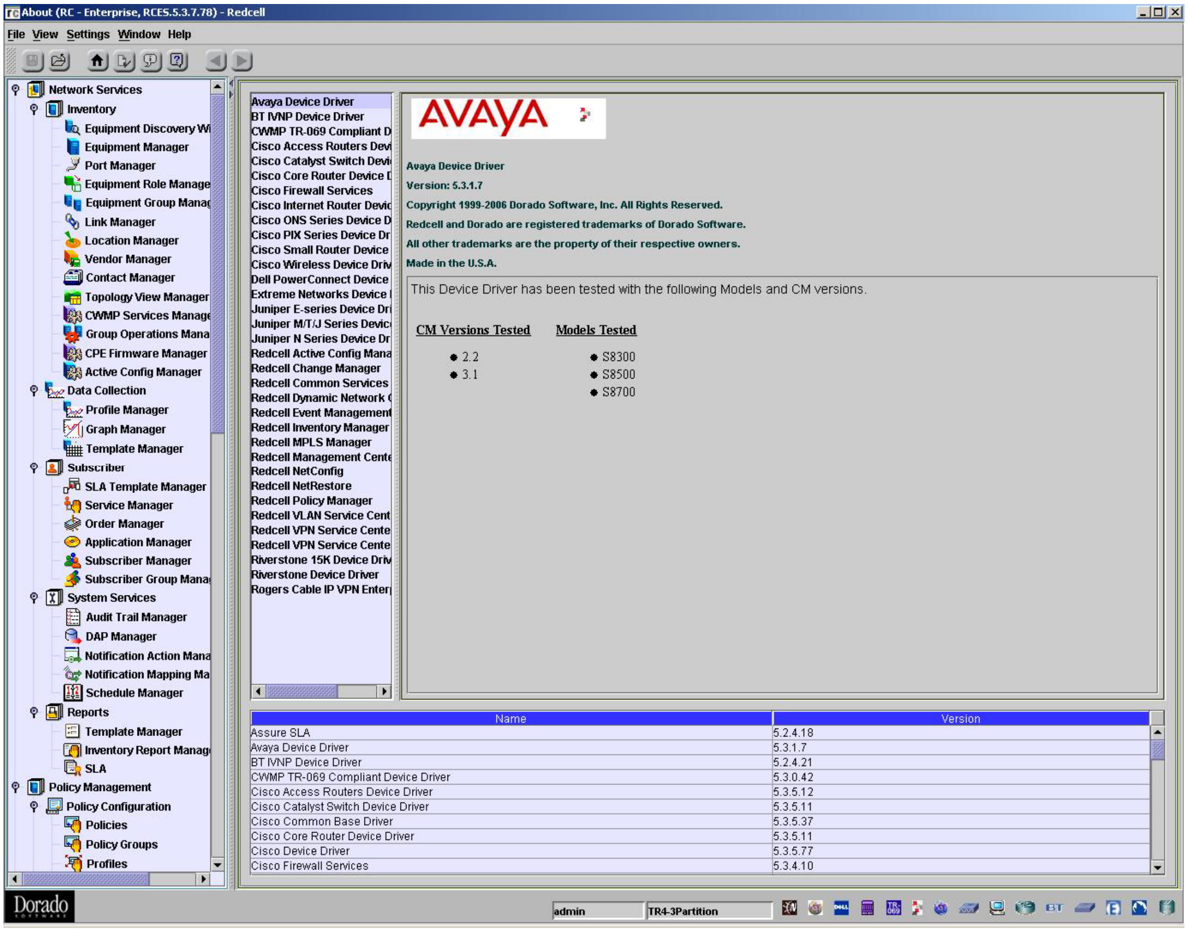
Policy	Setting
Require a special character	
Minimum Password Length	0 chars
Allow Password Reuse	true
Allow UserId in Password	true
Require Mixed Case	false
Require a number	false

Old Password:	
New Password:	*******
Confirm Password:	*******

Credentials for admin have expired.

5.5. Administer Redcell

This is the main window for the Redcell Management Center application.



Avaya Device Driver

Version: 5.3.1.7

Copyright 1999-2006 Dorado Software, Inc. All Rights Reserved.

Redcell and Dorado are registered trademarks of Dorado Software.

All other trademarks are the property of their respective owners.

Made in the U.S.A.

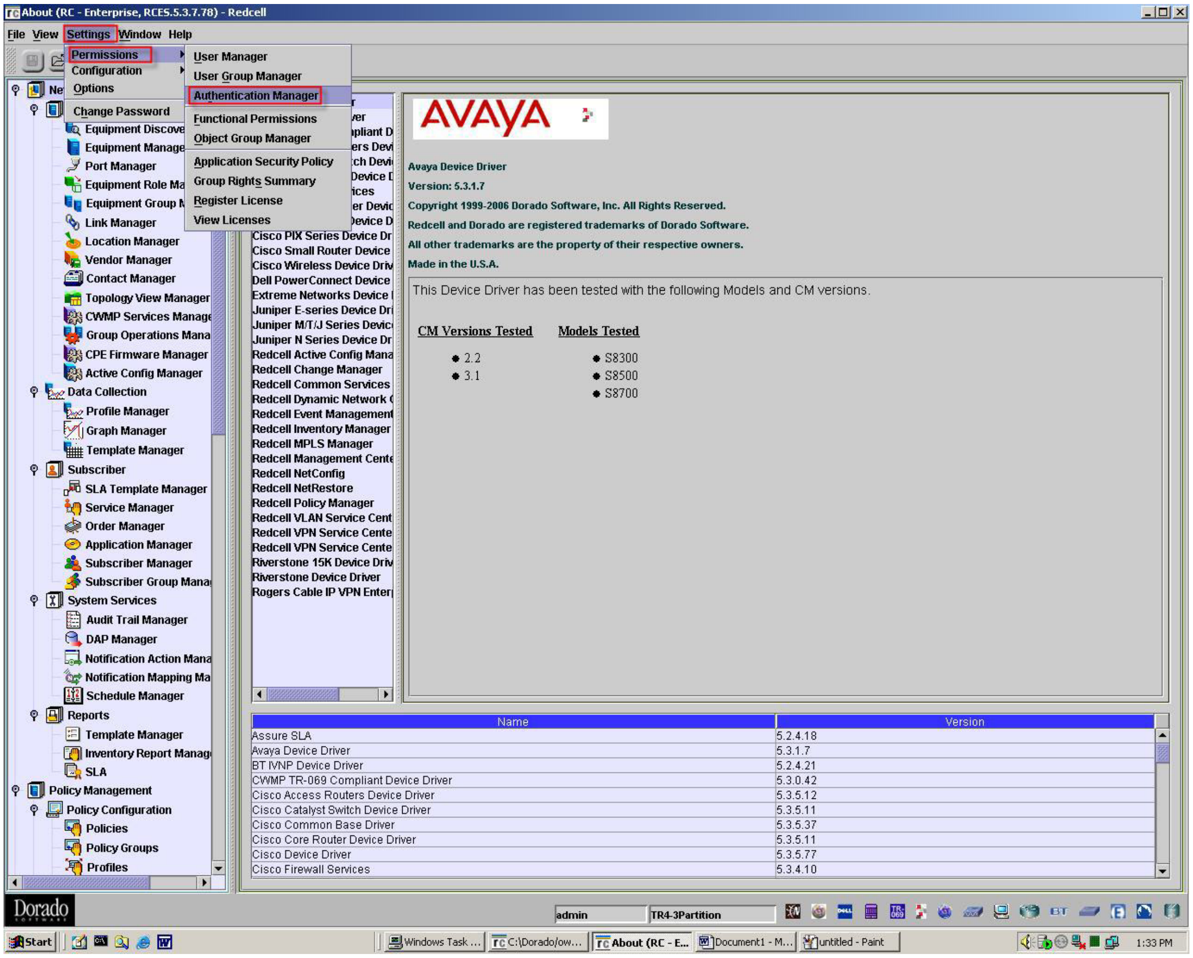
This Device Driver has been tested with the following Models and CM versions.

CM Versions Tested	Models Tested
● 2.2	● S8300
● 3.1	● S8500
	● S8700

Name	Version
Assure SLA	5.2.4.18
Avaya Device Driver	5.3.1.7
BT IVNP Device Driver	5.2.4.21
CWMP TR-069 Compliant Device Driver	5.3.0.42
Cisco Access Routers Device Driver	5.3.5.12
Cisco Catalyst Switch Device Driver	5.3.5.11
Cisco Common Base Driver	5.3.5.37
Cisco Core Router Device Driver	5.3.5.11
Cisco Device Driver	5.3.5.77
Cisco Firewall Services	5.3.4.10

5.6. Configure Authentication Manager

Define the community string values used by Redcell for Avaya Communication Manager. This is where the user will match the community string values assigned to Avaya Communications Manager in Section 4.2. Use the menu commands to select “**Settings>Permissions>Authentication Manager”**.



Avaya Device Driver

Version: 5.3.1.7

Copyright 1999-2006 Dorado Software, Inc. All Rights Reserved.

Redcell and Dorado are registered trademarks of Dorado Software.

All other trademarks are the property of their respective owners.

Made in the U.S.A.

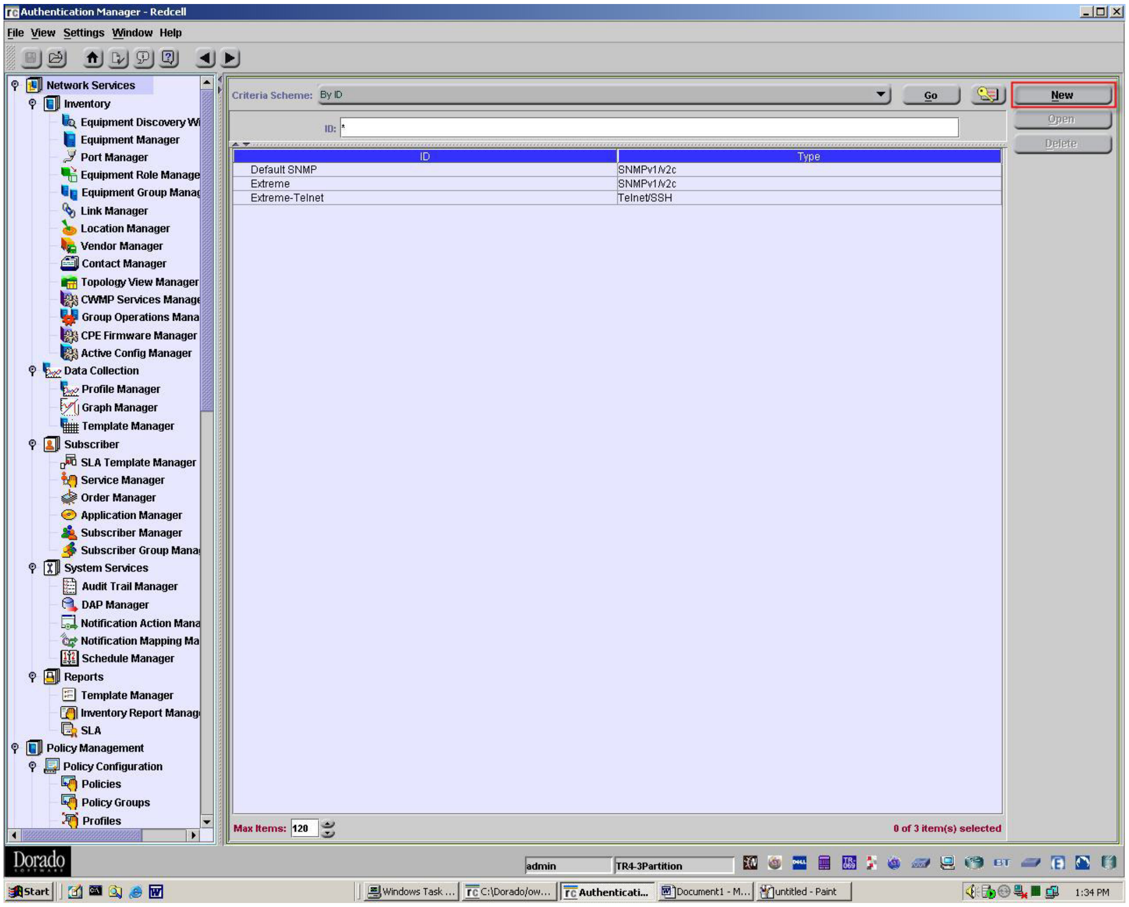
This Device Driver has been tested with the following Models and CM versions.

CM Versions Tested	Models Tested
• 2.2	• S8300
• 3.1	• S8500
	• S8700

Name	Version
Assure SLA	5.2.4.18
Avaya Device Driver	5.3.1.7
BT IVNP Device Driver	5.2.4.21
CWMP TR-069 Compliant Device Driver	5.3.0.42
Cisco Access Routers Device Driver	5.3.5.12
Cisco Catalyst Switch Device Driver	5.3.5.11
Cisco Common Base Driver	5.3.5.37
Cisco Core Router Device Driver	5.3.5.11
Cisco Device Driver	5.3.5.77
Cisco Firewall Services	5.3.4.10

5.7. Configure Authentication Manager

Click “**New**” to create a new authentication schema which will be used for Avaya Communication Manager.



Criteria Scheme: By ID

ID: *

ID	Type
Default SNMP	SNMPv1/v2c
Extreme	SNMPv1/v2c
Extreme-Telnet	Telnet/SSH

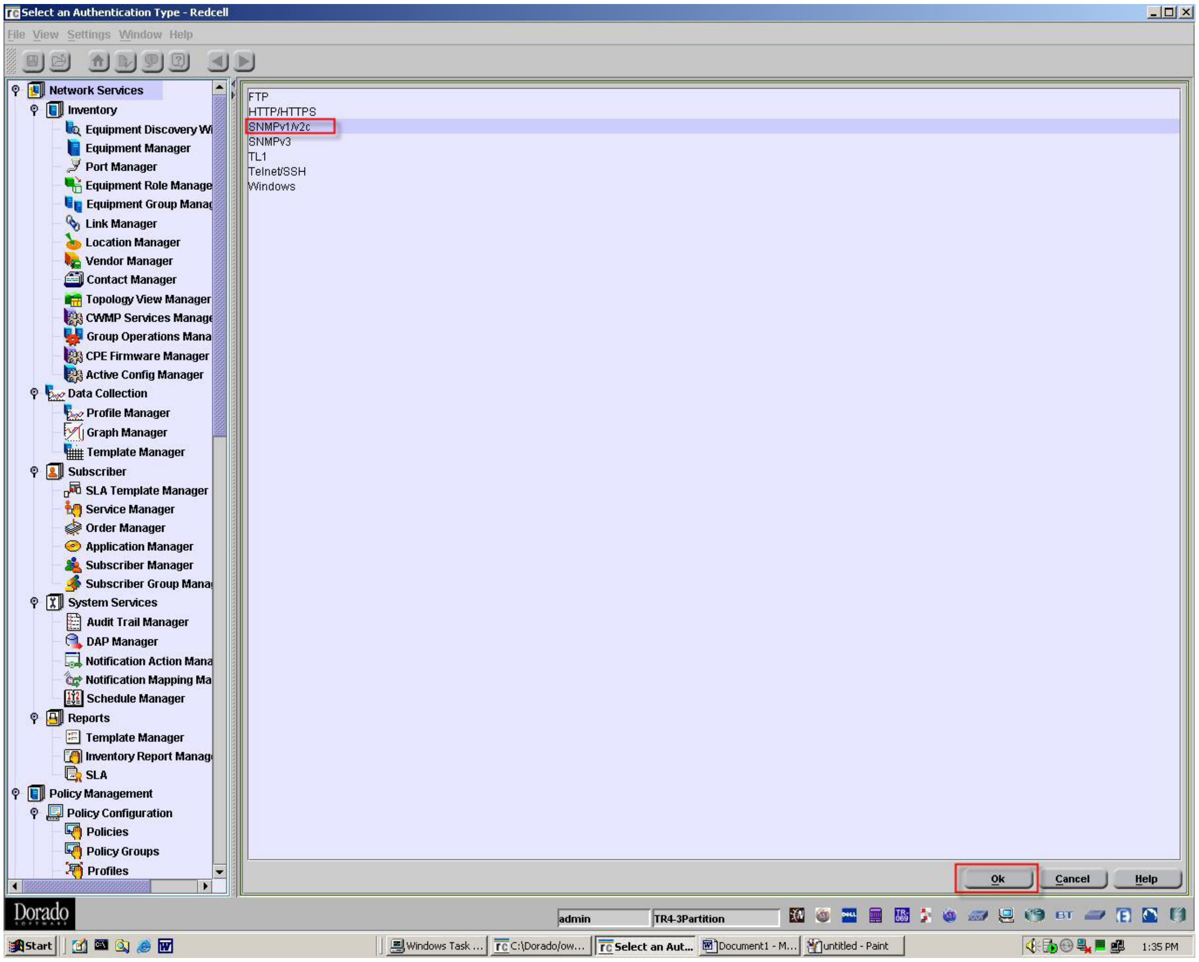
Max Items: 120

0 of 3 item(s) selected

admin TR4-3Partition

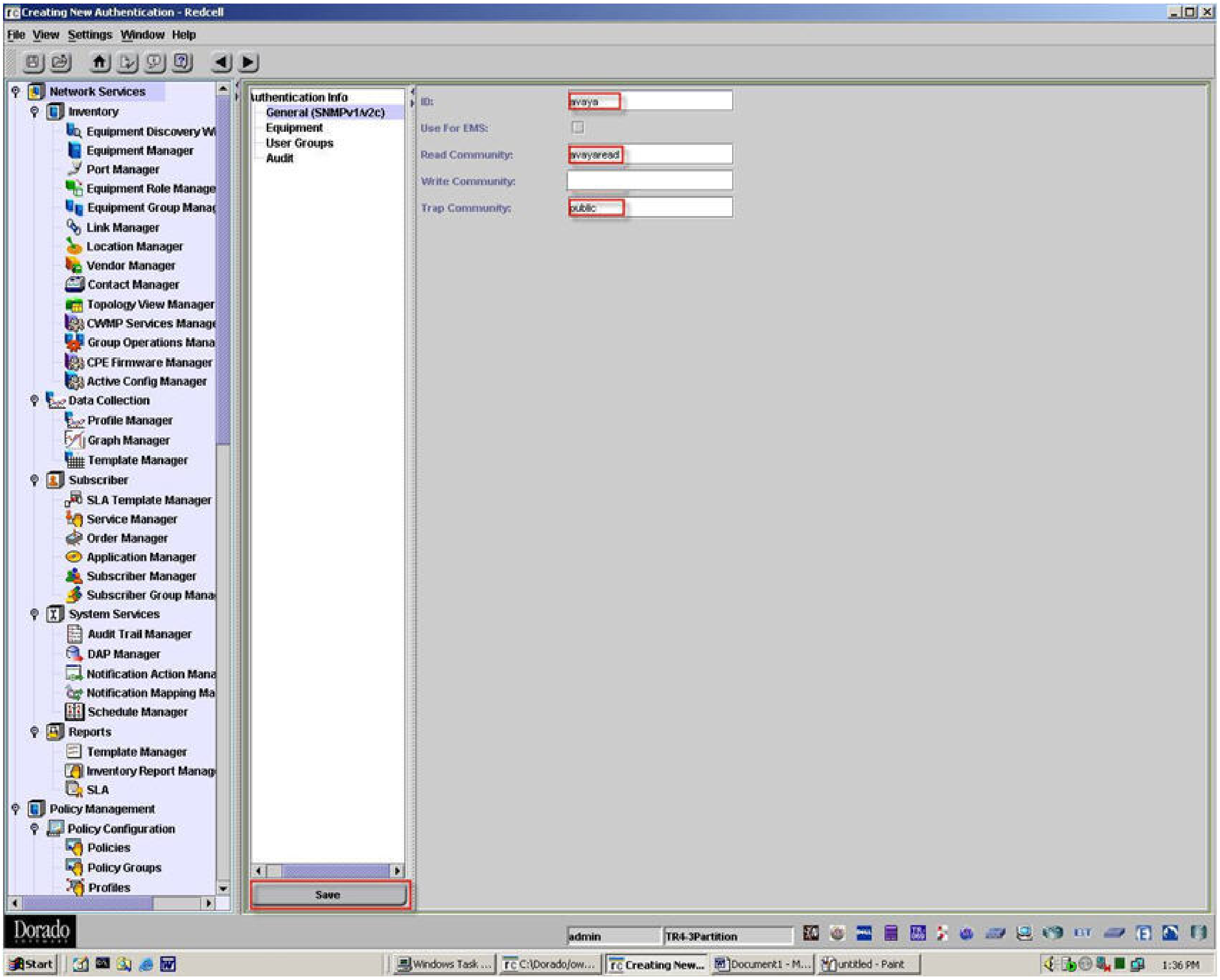
5.8. Configure Authentication Manager

Select “**SNMPv1/v2c**” then click “**Ok**”.



5.9. Configure Authentication Manager

Specify the **ID** of this new SNMP schema. This can be any name defined by the user as long as it is unique. Specify the "**Read Community**" and "**Trap Community**". The read community value needs to match those configured on Avaya Communication Manger in Section 4.2. Click "**Save".**



ID: avaya

Use For EMS: □

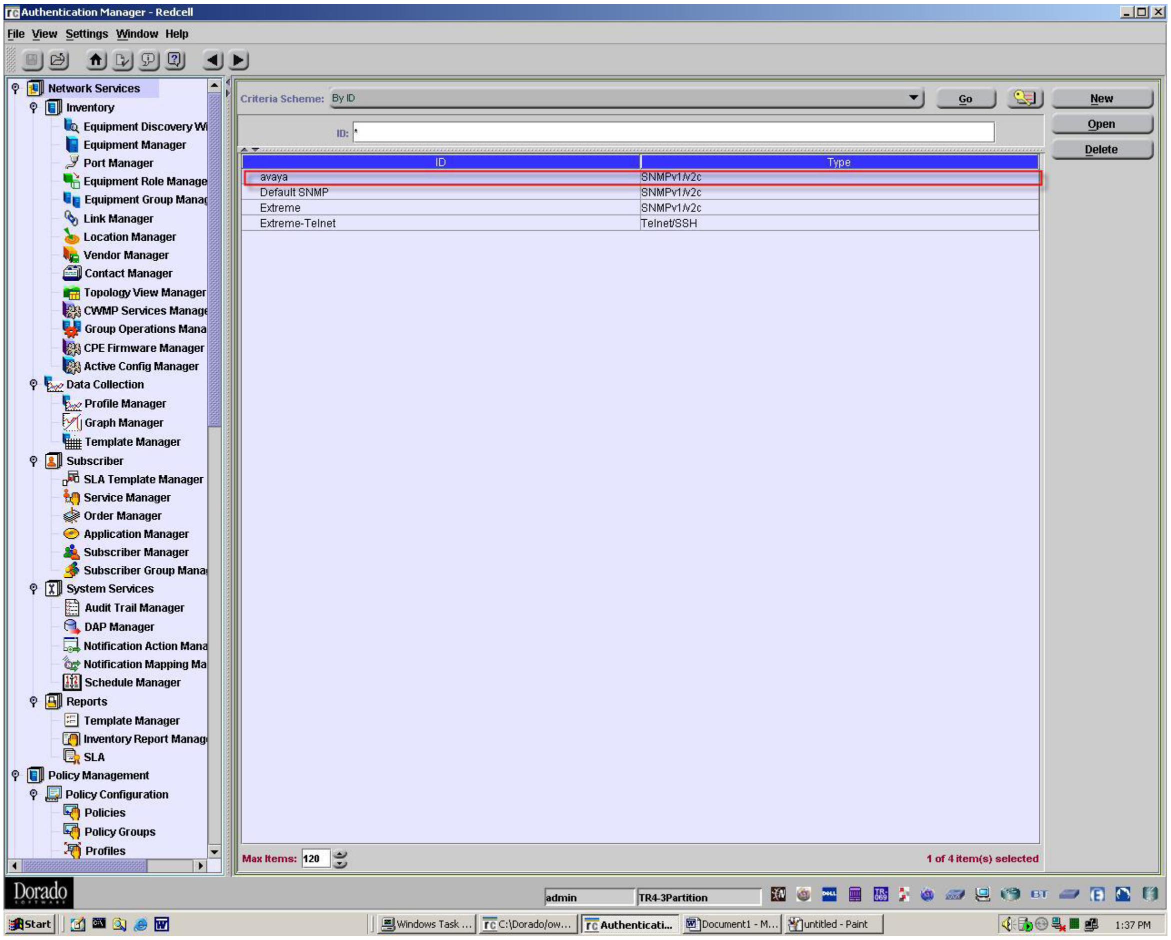
Read Community: avayaread

Write Community:

Trap Community: public

5.10. Configure Authentication Manager

The newly created schema now appears in the list and can now be used for Device Discovery.



Criteria Scheme: By ID

ID: *

ID	Type
avaya	SNMPv1/v2c
Default SNMP	SNMPv1/v2c
Extreme	SNMPv1/v2c
Extreme-Telnet	Telnet/SSH

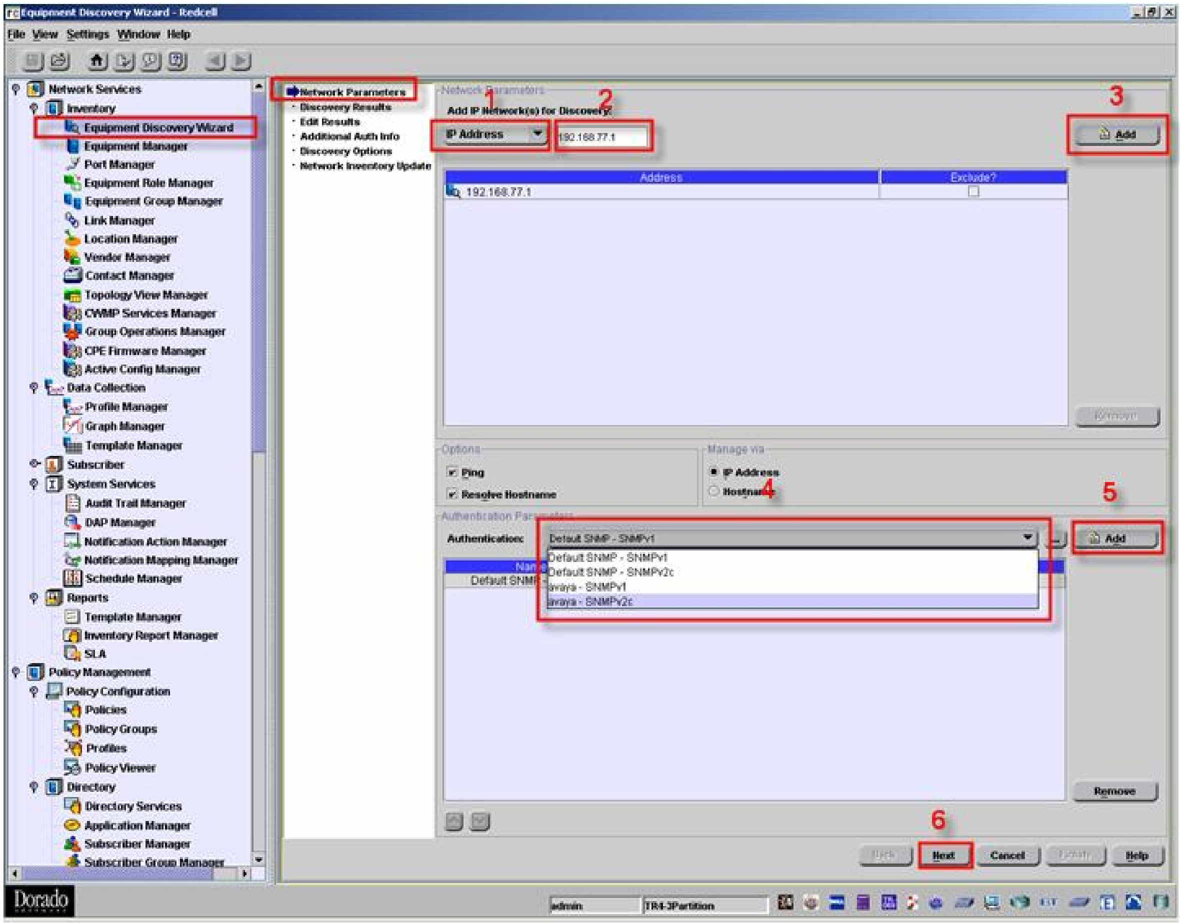
Max Items: 120

1 of 4 item(s) selected

5.11. Configure Equipment Discovery Wizard – Network Parameters

Using the menu on the left and select “**Network Services>Inventory>Equipment Discovery Wizard**”. Once selected the user is presented with the following interface where the basic information can be input into the system.

1 – Select the Method for Discovery. Using the pull down menu select “**IP Address”**
2 – Specify the **IP Address** of the Avaya Communication Manger to be discovered.
3 – Click **Add** to place the newly specified IP Address into table for identification. Repeat this step for each device being discovered, see **Figure 1** for the network diagram.
4 – Select the method of Authentication – Specify **“SNMPv2c”** to be used as the Authentication. This is the SNMP authentication ID that was created in Section 5.9.
5 – Click **Add** to add this new authentication method.
6 – Click “**Next”.**



Add IP Network(s) for Discovery: IP Address 192.168.77.1

Address	Exclude?
192.168.77.1	□

☑ Ping
☑ Resolve Hostname

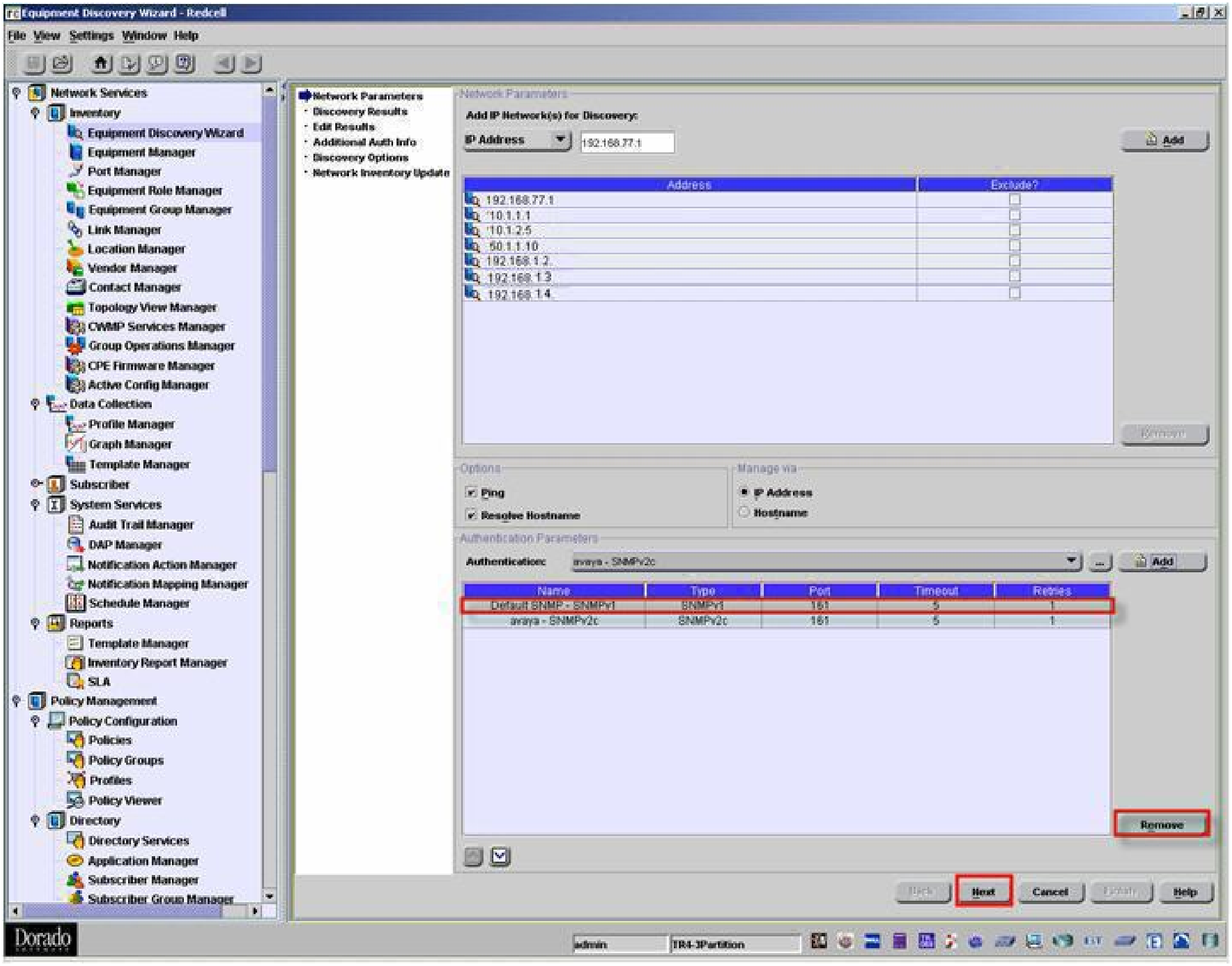
● IP Address
○ Hostname

Authentication: Default SNMP - SNMPv1
Default SNMP - SNMPv1
Default SNMP - SNMPv2c
avaya - SNMPv1
avaya - SNMPv2c

Name
Default SNMP

5.12. Configure Equipment Discovery Wizard – Network Parameters

By default Redcell Enterprise Bundle uses SNMP version 1, in this testing SNMP version 2c was used. Therefore, SNMP version 1 authentication needs to be removed from the configuration. Select “**Default SNMP – SNMPv1**” inside the authentication window then click “**Remove**” to remove it for this device. Click “**Next”**.



Network Parameters

Add IP Network(s) for Discovery:

IP Address 192.168.77.1

Address	Exclude?
192.168.77.1	□
10.1.1.1	□
10.1.2.5	□
50.1.1.10	□
192.168.1.2	□
192.168.1.3	□
192.168.1.4	□

Options

☑ Ping

☑ Resolve Hostname

Manage via

● IP Address

○ Hostname

Authentication Parameters

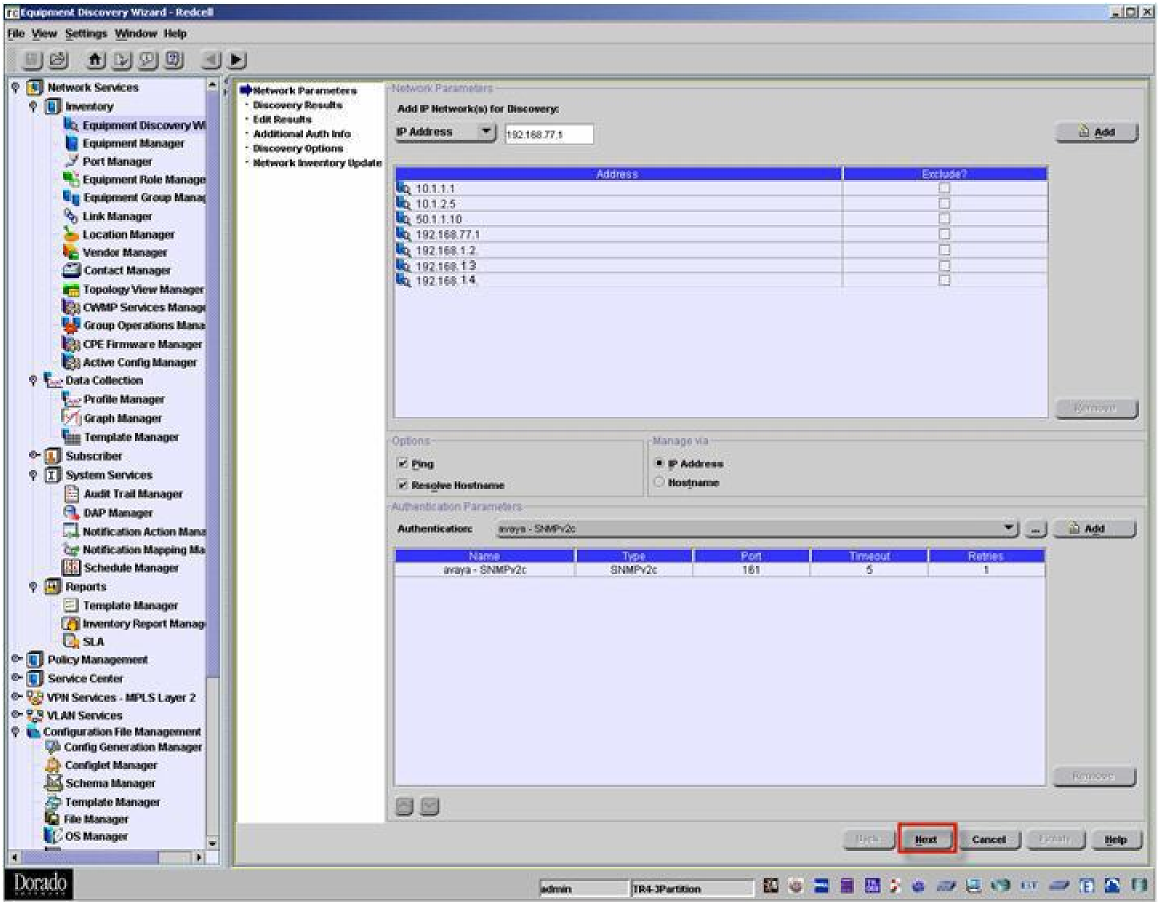
Authentication: avaya - SNMPv2c

Name	Type	Port	Timeout	Retries
Default SNMP - SNMPv1	SNMPv1	161	5	1
avaya - SNMPv2c	SNMPv2c	161	5	1

admin TR4-3Partition

5.13. Configure Equipment Discovery – Network Parameters

Once the IP addresses and authentication method have been specified the user can begin the discovery. Click “**Next**” to start the discovery.



Network Parameters

Add IP Network(s) for Discovery:

IP Address: 192.168.77.1

Address	Exclude?
10.1.1.1	□
10.1.2.5	□
50.1.1.10	□
192.168.77.1	□
192.168.1.2	□
192.168.1.3	□
192.168.1.4	□

Options

☑ Ping

☑ Resolve Hostname

Manage via

● IP Address

○ Hostname

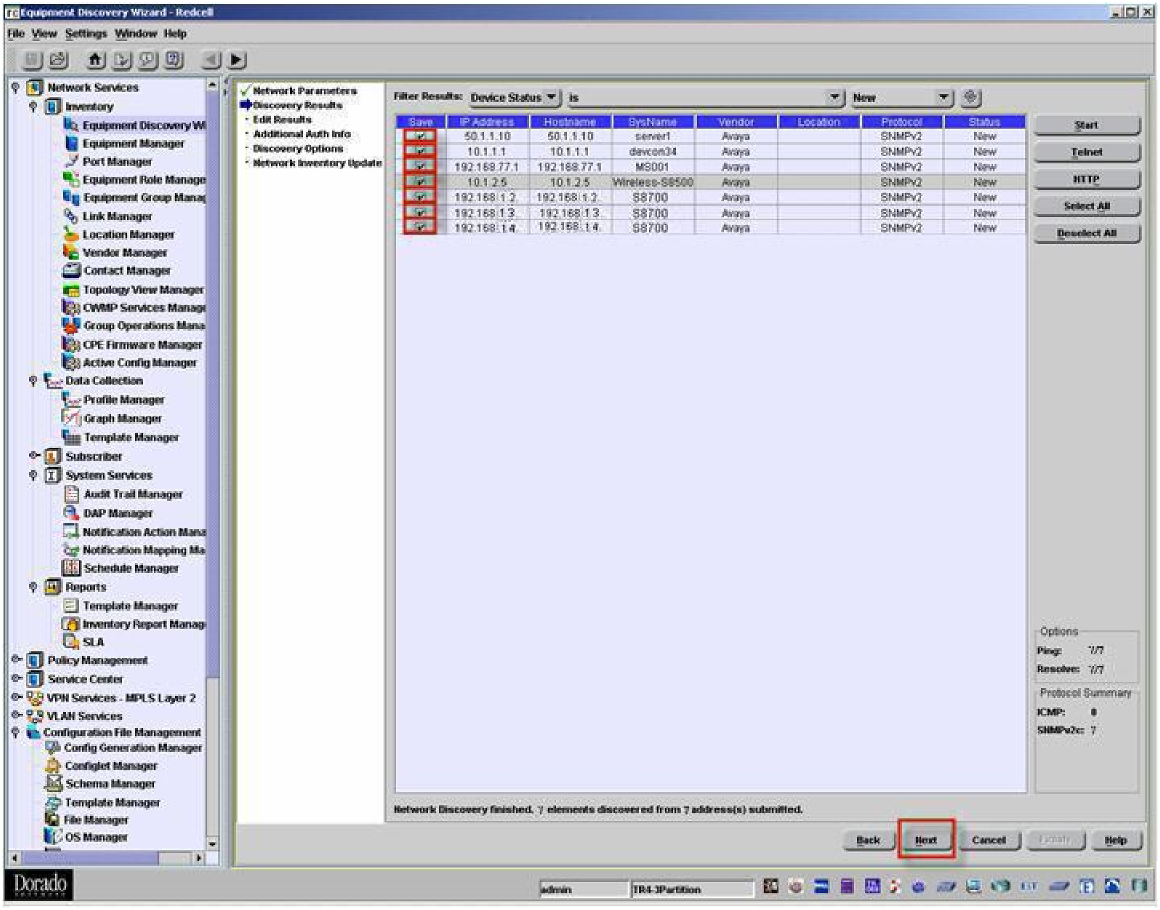
Authentication Parameters

Authentication: avaya - SNMPv2c

Name	Type	Port	Timeout	Retries
avaya - SNMPv2c	SNMPv2c	161	5	1

5.14. Configure Equipment Discovery Wizard – Discovery Results

For each discovered object, check the check box in the corresponding **“Save”** column, click “**Next**”. This creates the database entries for the discovered object.



Filter Results: Device Status is New

Save	IP Address	Hostname	SysName	Vendor	Location	Protocol	Status
☑	50.1.1.10	50.1.1.10	server1	Avaya		SNMPv2	New
☑	10.1.1.1	10.1.1.1	devcon34	Avaya		SNMPv2	New
☑	192.168.77.1	192.168.77.1	MS001	Avaya		SNMPv2	New
☑	10.1.2.5	10.1.2.5	Wireless-S8500	Avaya		SNMPv2	New
☑	192.168.1.2	192.168.1.2	S8700	Avaya		SNMPv2	New
☑	192.168.1.3	192.168.1.3	S8700	Avaya		SNMPv2	New
☑	192.168.1.4	192.168.1.4	S8700	Avaya		SNMPv2	New

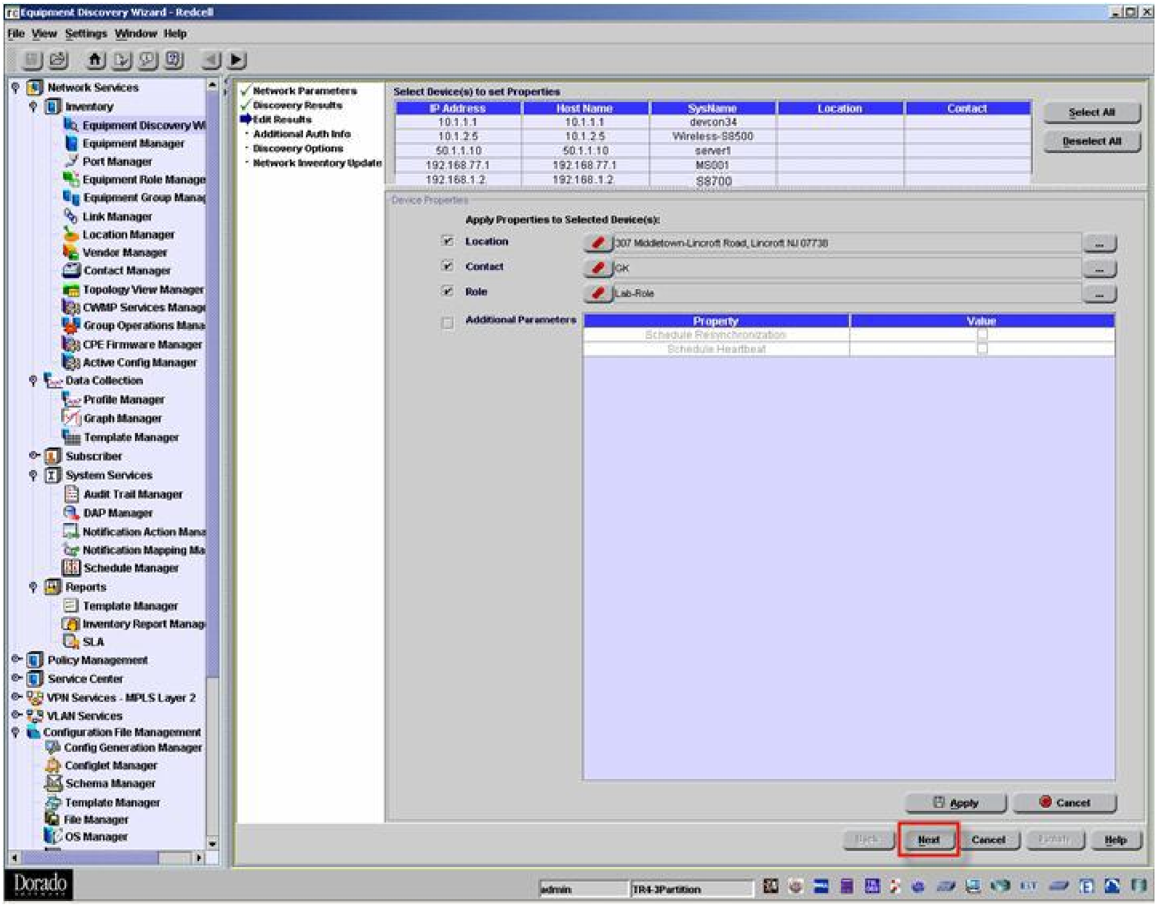
Options
Ping: 7/7
Resolve: 7/7

Protocol Summary
ICMP: 0
SNMPv2c: 7

Network Discovery finished, 7 elements discovered from 7 address(s) submitted.

5.15. Configure Equipment Discovery Wizard – Edit Results

This is the screen where Location, Contact and Roles can be assigned to equipment. Assigning these parameters is not a requirement. Click “**Next**”.



Select Device(s) to set Properties

IP Address	Host Name	SysName	Location	Contact
10.1.1.1	10.1.1.1	devcon34		
10.1.2.5	10.1.2.5	Wireless-S8500		
50.1.1.10	50.1.1.10	server1		
192.168.77.1	192.168.77.1	MS001		
192.168.1.2	192.168.1.2	S8700		

Apply Properties to Selected Device(s):

☑ Location: 307 Middletown-Lincroft Road, Lincroft NJ 07738

☑ Contact: GK

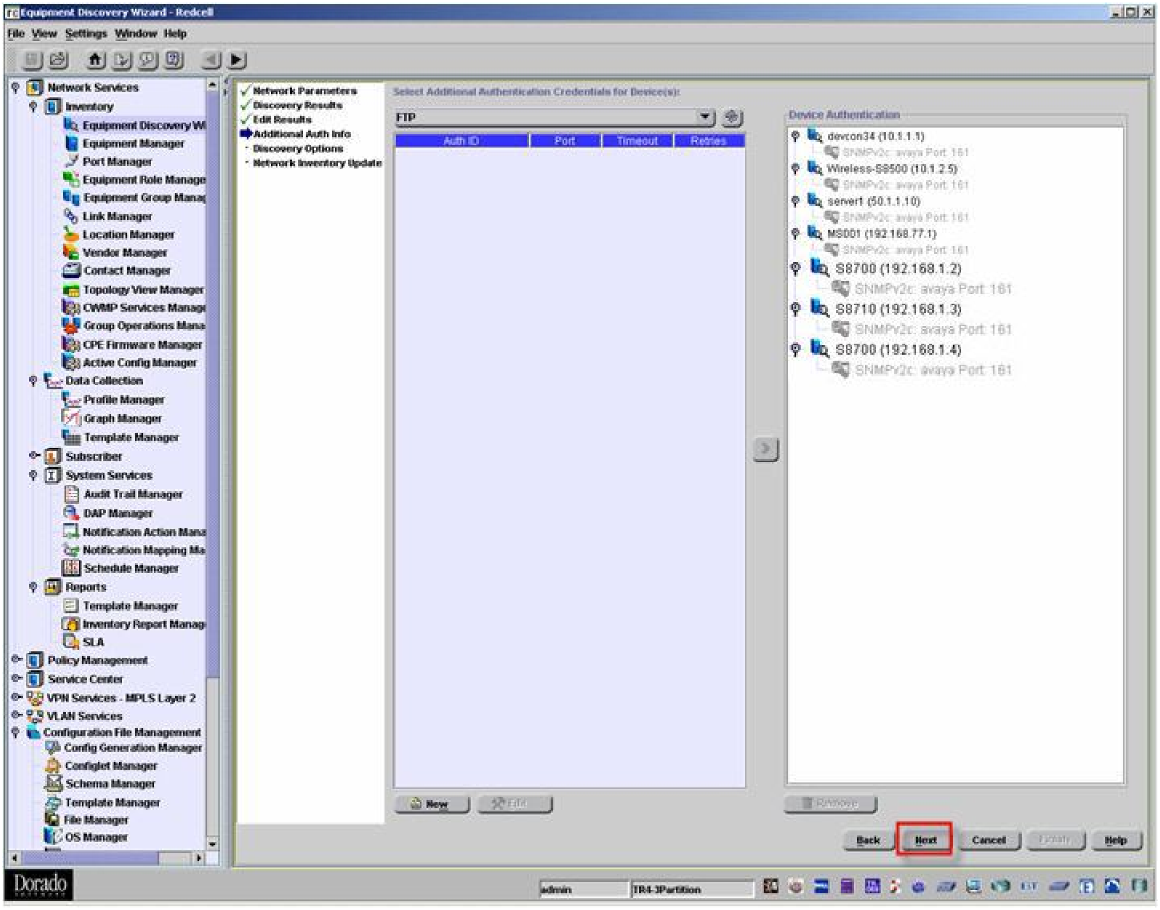
☑ Role: Lab-Role

☐ Additional Parameters

Property	Value
Schedule Resynchronization	☐
Schedule Heartbeat	☐

5.16. Configure Equipment Discovery Wizard – Additional Auth Info

This screen presents the user with the option of specifying additional access methods and authentication credentials for devices that have been discovered. Click "**Next**"



Select Additional Authentication Credentials for Device(s):

FTP

Auth ID	Port	Timeout	Retries

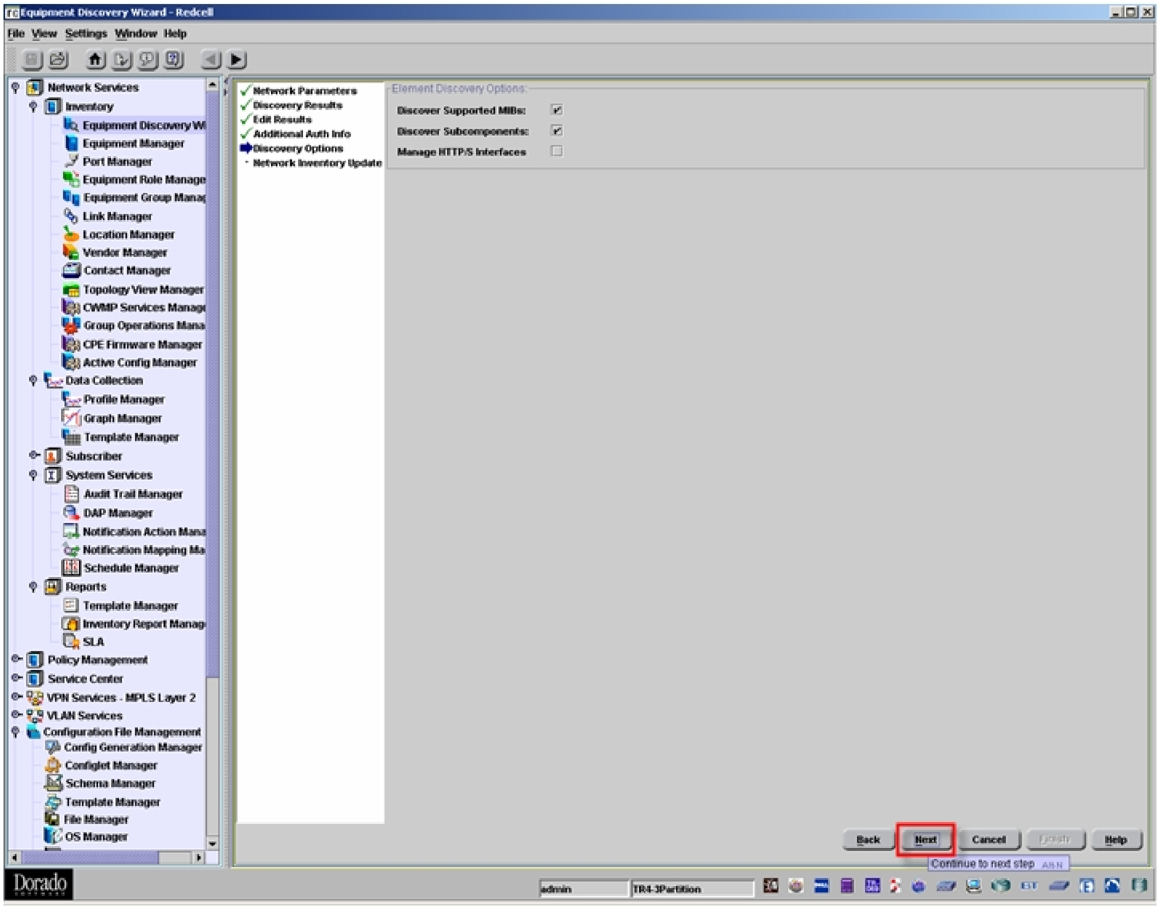
Device Authentication

- devcon34 (10.1.1.1)
  - SNMPv2c: avaya Port: 161
- Wireless-S8500 (10.1.2.5)
  - SNMPv2c: avaya Port: 161
- server1 (50.1.1.10)
  - SNMPv2c: avaya Port: 161
- MSD01 (192.168.77.1)
  - SNMPv2c: avaya Port: 161
- S8700 (192.168.1.2)
  - SNMPv2c: avaya Port: 161
- S8710 (192.168.1.3)
  - SNMPv2c: avaya Port: 161
- S8700 (192.168.1.4)
  - SNMPv2c: avaya Port: 161

admin TR4-3Partition

5.17. Configure Equipment Discovery Wizard – Discovery Options

These options are enabled by default. Click “**Next**” to continue.



Element Discovery Options:

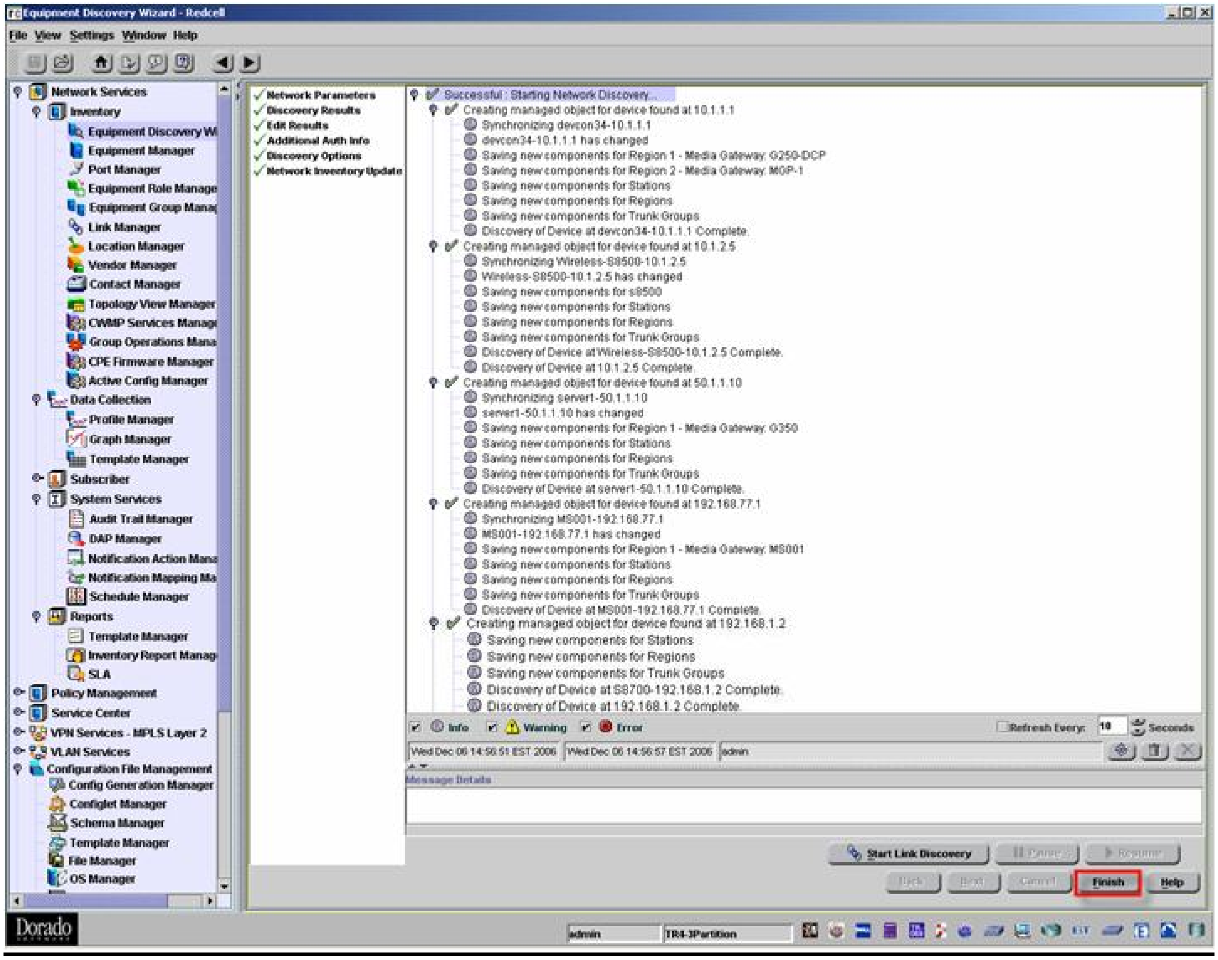
Discover Supported MIBs: ☑

Discover Subcomponents: ☑

Manage HTTP/S Interfaces ☐

5.18. Configure Equipment Discovery Wizard – Network Inventory Update

Click “**Finish**” to complete the discovery.



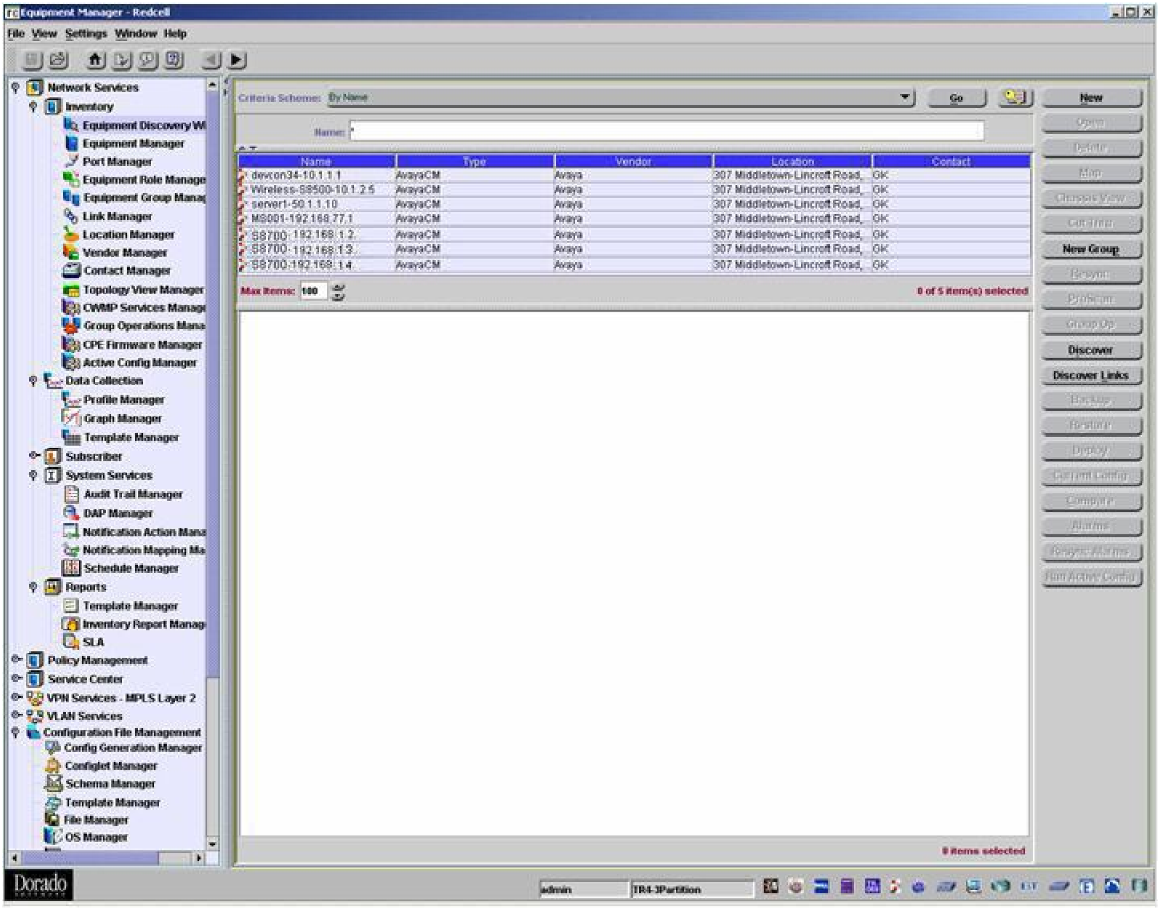
```
Successful : Starting Network Discovery...
  Creating managed object for device found at 10.1.1.1
    Synchronizing devcon34-10.1.1.1
    devcon34-10.1.1.1 has changed
    Saving new components for Region 1 - Media Gateway: G250-DCP
    Saving new components for Region 2 - Media Gateway: MGP-1
    Saving new components for Stations
    Saving new components for Regions
    Saving new components for Trunk Groups
    Discovery of Device at devcon34-10.1.1.1 Complete.
  Creating managed object for device found at 10.1.2.5
    Synchronizing Wireless-S8500-10.1.2.5
    Wireless-S8500-10.1.2.5 has changed
    Saving new components for s8500
    Saving new components for Stations
    Saving new components for Regions
    Saving new components for Trunk Groups
    Discovery of Device at Wireless-S8500-10.1.2.5 Complete.
    Discovery of Device at 10.1.2.5 Complete.
  Creating managed object for device found at 50.1.1.10
    Synchronizing server1-50.1.1.10
    server1-50.1.1.10 has changed
    Saving new components for Region 1 - Media Gateway: G350
    Saving new components for Stations
    Saving new components for Regions
    Saving new components for Trunk Groups
    Discovery of Device at server1-50.1.1.10 Complete.
  Creating managed object for device found at 192.168.77.1
    Synchronizing MS001-192.168.77.1
    MS001-192.168.77.1 has changed
    Saving new components for Region 1 - Media Gateway: MS001
    Saving new components for Stations
    Saving new components for Regions
    Saving new components for Trunk Groups
    Discovery of Device at MS001-192.168.77.1 Complete.
  Creating managed object for device found at 192.168.1.2
    Saving new components for Stations
    Saving new components for Regions
    Saving new components for Trunk Groups
    Discovery of Device at S8700-192.168.1.2 Complete.
    Discovery of Device at 192.168.1.2 Complete.
```

☑ Info ☑ Warning ☑ Error

Wed Dec 06 14:56:51 EST 2006 | Wed Dec 06 14:56:57 EST 2006 | admin

5.19. Configure Equipment Discovery Wizard - Device Discovery Complete

The discovered objects now show in the list.



Criteria Scheme: By Name

Name: *

Name	Type	Vendor	Location	Contact
devcon34-10.1.1.1	AvayaCM	Avaya	307 Middletown-Lincroft Road,_	GK
Wireless-S8500-10.1.2.5	AvayaCM	Avaya	307 Middletown-Lincroft Road,_	GK
server1-50.1.1.10	AvayaCM	Avaya	307 Middletown-Lincroft Road,_	GK
MS001-192.168.77.1	AvayaCM	Avaya	307 Middletown-Lincroft Road,_	GK
S8700-192.168.1.2	AvayaCM	Avaya	307 Middletown-Lincroft Road,_	GK
S8700-192.168.1.3	AvayaCM	Avaya	307 Middletown-Lincroft Road,_	GK
S8700-192.168.1.4	AvayaCM	Avaya	307 Middletown-Lincroft Road,_	GK

Max Items: 100

0 of 5 item(s) selected

0 items selected

6. Interoperability Compliance Testing

Interoperability compliance testing covered the capability to use SNMP version 2c between Avaya Communication Manager and Dorado Software Redcell Enterprise Bundle.

6.1. General Test Approach

The general test approach entailed verifying the following:

- LAN/IP connectivity between the Avaya and Dorado Software products.
- SNMP Authentication between the Avaya and Dorado Software products.
- SNMP Polling and Trap reception between the Avaya and Dorado software products.

6.2. Test Results

All interoperability tests passed with one exception that was later corrected. The release of the Avaya Device Driver that is bundled with the 5.3 release of Dorado Software's Redcell application (Avaya Device Driver 5.3.1.4) does not properly obtain the software release string. The correct SNMP OID was provided to Dorado Software for obtaining the software release string and a new version of the Avaya Device Driver (version 5.3.1.7) was created which correctly obtains the software release string. Users of Dorado Software Redcell Enterprise Bundle who wish to obtain the software release string need to make sure that the version of the Avaya Device Driver is 5.3.1.7. Dorado Software has instructions for upgrading the device driver.

Redcell Enterprise Bundle was tested and verified to provide the following information to the user. The information obtained from Avaya Communication Manager is the existing administered configuration present on the system.

1. **Media Servers**
   - Correct Model Number
   - Correct Software Version

2. **Media Gateways**
   - Correct Model Number
   - Correct Identification of Gateway Modules (i.e. MM710 MM711 MM712).
   - Correct Serial Number

3. **Stations**
   - Station Name
   - Station Type
   - Station Extension
   - Station Port

4. **Trunk Groups**
    - Trunk Group Name
    - Trunk Group Type (SIP, ISDN)
    - Trunk Group Number
    - Trunk Type
    - Communication Type
    - Service Type
    - Size

5. **Regions**
    - Region Name
    - Region Number
    - Audio 802.1p
    - Audio PHB
    - CC 802.1p
    - CC PHB

7. Verification Steps

This section provides the steps for verifying end-to-end network connectivity between Dorado Software Redcell Enterprise Bundle and Avaya Communication Manager systems running on the various hardware platforms.

1. Verify that the computer running Dorado Software Redcell Enterprise Bundle has IP connectivity with all of the platforms running Avaya Communication Manager. This was done by opening a Command Prompt on the Redcell Enterprise Bundle server and issuing the "ping" command. ICMP connectivity only proves network connectivity but SNMP authentication information, such as community string, need to match as well.

2. System up/down traps were generated from the systems running Avaya Communication Manager and verified to be received by Redcell Enterprise Bundle. An additional SNMP server was also used to verify that Dorado Software Redcell Enterprise bundle could forward a received SNMP trap to an external SNMP system.

8. Troubleshooting

8.1. Software Release String Troubleshooting

In cases of SNMP authentication failure, ensure that the steps outlined in Sections 4.2 and 5.9 have been followed correctly. Ensure the IP address information is correct and that both devices are using the same SNMP version and community values.

For Avaya Media Server 87XX series, make sure that all of the IP addresses belonging to the system have been added. This includes the physical and virtual IP addresses. The Avaya

87XX Media Server series operate as a redundant pair and each unit has a unique physical IP address but share the same virtual IP address. In cases where the Standby system is probed, the SNMP response may contain a "null" value.

When using Dorado Software Redcell to obtain the software release information for Avaya Communication Manager, make sure the Redcell system is using the Avaya Device Driver version 5.3.1.7. Previous versions of this device driver do not report the software release string running on Avaya Communication Manager properly.

9. Support

Technical support for Dorado Software Redcell Enterprise Bundle can be obtained from the information below:

Email	:	tsc@doradosoftware.com
Phone	:	1-916-673-1725

10. Conclusion

These Application Notes describe the configuration steps required for integrating Dorado Software Redcell Enterprise Bundle version 5.3 with Avaya Communication Manager version 3.1.2 as a SNMP network management solution. Dorado Software Redcell Enterprise Bundle was responsible for obtaining inventory and management data from Avaya Communication Manager. SNMP traps were sent by Avaya Communication Manager and received and processed by Dorado Software Redcell Enterprise Bundle.

11. Additional References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at http://support.avaya.com/.

[1] *Administrator Guide for Avaya Communication Manager*, May 2006, Issue 2.1 Document Number 03-300509.

The Dorado Software Redcell Enterprise Bundle documentation can be found at: http://www.doradosoftware.com/products/.