Cisco RF Gateway 1 Software Version 2.6.x Security Features

Addendum

For Your Safety

Explanation of Warning and Caution Icons

Avoid personal injury and product damage! Do not proceed beyond any symbol until you fully understand the indicated conditions.

The following warning and caution icons alert you to important information about the safe operation of this product:

You may find this symbol in the document that accompanies this product. This symbol indicates important operating or maintenance instructions.

You may find this symbol affixed to the product. This symbol indicates a live terminal where a dangerous voltage may be present; the tip of the flash points to the terminal device.

You may find this symbol affixed to the product. This symbol indicates a protective ground terminal.

You may find this symbol affixed to the product. This symbol indicates a chassis terminal (normally used for equipotential bonding).

You may find this symbol affixed to the product. This symbol warns of a potentially hot surface.

You may find this symbol affixed to the product and in this document. This symbol indicates an infrared laser that transmits intensity-modulated light and emits invisible laser radiation or an LED that transmits intensity-modulated light.

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

Safe Operation for Software Controlling Optical Transmission Equipment

If this manual discusses software, the software described is used to monitor and/or control ours and other vendors' electrical and optical equipment designed to transmit video, voice, or data signals. Certain safety precautions must be observed when operating equipment of this nature.

For equipment specific safety requirements, refer to the appropriate section of the equipment documentation.

For safe operation of this software, refer to the following warnings.

WARNING:

- **Ensure that all optical connections are complete or terminated before using this equipment to remotely control a laser device. An optical or laser device can pose a hazard to remotely located personnel when operated without their knowledge.**
- **Allow only personnel trained in laser safety to operate this software. Otherwise, injuries to personnel may occur.**
- **Restrict access of this software to authorized personnel only.**
- **Install this software in equipment that is located in a restricted access area.**

1

Introduction

Overview

This document describes the Cisco RF Gateway 1 security features in software version 2.6.x, including SFTP support, SNMPv3 support, unified user management, and GUI authenticity.

Who Should Use This Document

This document is intended for authorized service personnel who have experience working with the RF Gateway 1 or similar equipment. The service personnel should have appropriate background and knowledge to complete the procedures described in this document.

Qualified Personnel

Only appropriately qualified and skilled personnel should attempt to install, operate, maintain, and service this product.

WARNING:

Allow only qualified and skilled personnel to install, operate, maintain, and service this product. Otherwise, personal injury or equipment damage may occur.

Document Version

This is the first release of this guide.

2

Software Version 2.6.x Security Features

This chapter describes the Cisco RF Gateway 1 2.6.x security features.

In This Chapter

Security Features Overview

The following enhancements are included in software version 2.6.x.

1. SFTP support (SSHv2 with DSA key supported).
2. SFTP client support to perform release management, backup/restore configuration, license management, and SSL/SSH key download.
3. Expanded firewall settings to include SFTP port enable/disable option, FTP, HTTPS, HTTP, and Telnet ports.
4. DSA key download for SFTP.
5. SNMPv3 support (snmpNotifyFilterProfileTable and snmpNotifyFilterTable are not supported, therefore filtering based on trap OIDs is not allowed). INFORM PDUs are not supported.
6. Unified user management: SNMPv3, SFTP (server mode), and GUI authentication all use the same set of user credentials. All configurations related to trap settings and community strings are done from the SNMP Manager. The SNMP Traps page is not available in 2.6.x.
7. RADIUS user authentication is not supported for SNMPv3 and SFTP.
8. Passwords are now stored as MD5/SHA encoded string.

SFTP Support

For SFTP client and server, SSHv2 with DSA key is used as the security protocol. SFTP client and server will be operational only after the DSA key is downloaded and installed (firewall permitting for SFTP server) and provided the transfer mode is set to SFTP (for SFTP client).

Note: By default, the firewall for FTP and SFTP is enabled and the default file transfer method is set to FTP.

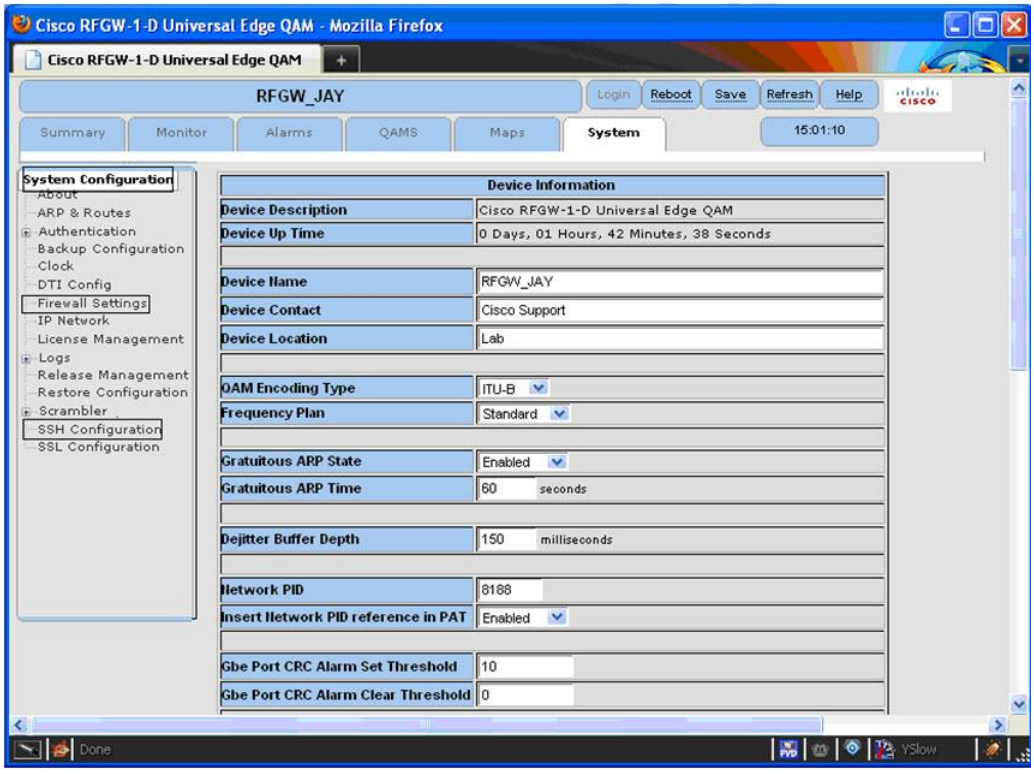
GUI Changes for SFTP

The following GUI changes have been added for SFTP support.

System Tab Changes

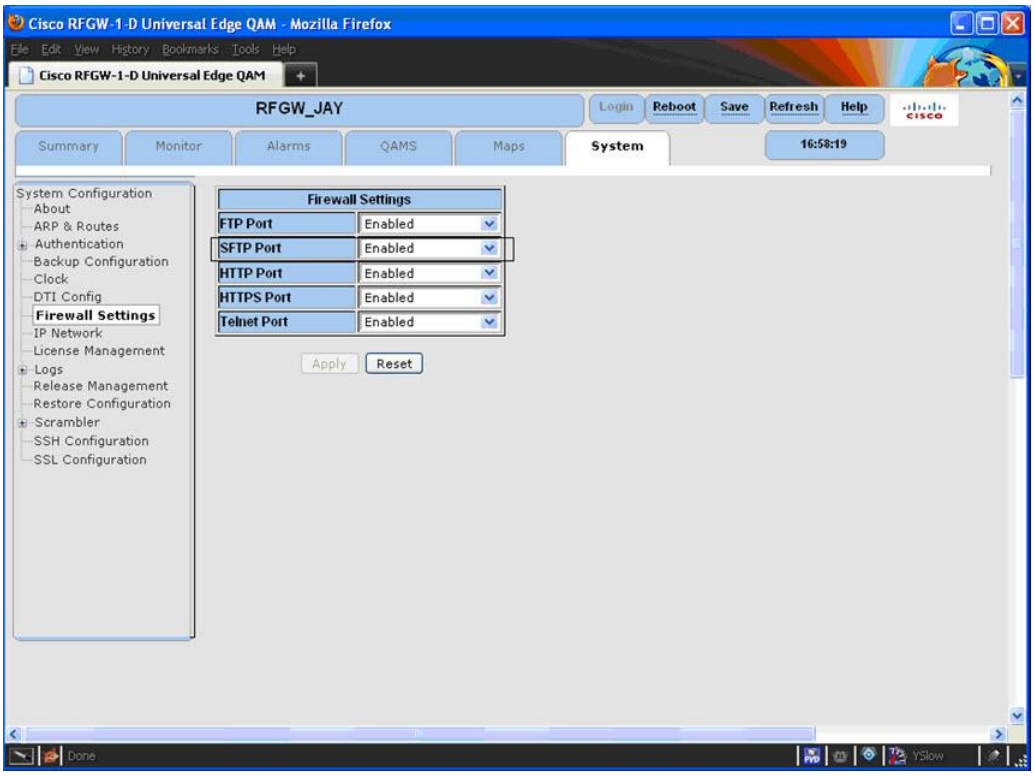
1. *System Configuration* page now includes an option to select FTP or SFTP for file download/upload.
2. *Firewall Settings* now include an option to enable/disable the SFTP port.

3 *SSH Configuration* page has been added to provide access to the new security features. See screen below.



Firewall Settings

The SFTP port can be enabled/disabled using the following screen. Disabling the port prevents any external SFTP client from logging in to the RFGW-1.



Generating a DSA Key

Overview

The RFGW-1 is shipped from the factory with SFTP disabled. To enable SFTP, you will need the following:

- FTP server to download the required DSA key
- Open Source toolkit for SSH to generate the DSA key
- Software containing SSH/SFTP kernel support such as 2.6.x.

Important: It is recommended that you consult your IT and security departments before installing on live RFGW-1 systems. The key files you'll be creating contain a private key and must be handled in accordance with your company's security procedures, especially the unprotected key known as dsa_key.pem.

Creating an Unprotected DSA Key:

The dsa_key.pem is not password protected. It contains your private DSA key in the open for all to see. Generating a DSA key requires an openssh shell (Cygwin is used in our example). Follow the instructions below to create a DSA key.

1 Enter the following command at the shell prompt:

ssh-keygen -t dsa (the "-t" flag is used to specify the key type).

Result: You will be prompted for the location to save the file. The default location is ~/.ssh/id_dsa.

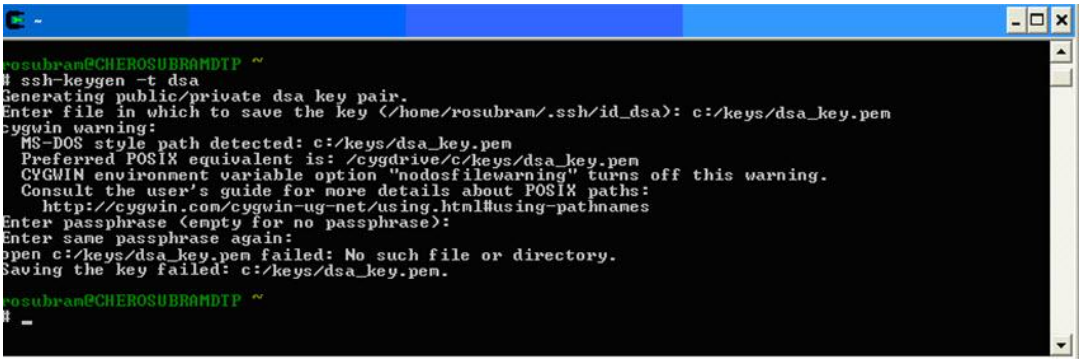
2 Click **Enter** to save the file to the default location, or specify a different location.

Result: You will then be prompted for a passphrase.

3 Click **Enter** twice to generate an unprotected file.

Result: The following 2 files are created:

- dsa_key.pem - the private key (to be downloaded to the RFGW-1)
- dsa_key.pem.pub - the public key (may be downloaded to the server)



Note: You can specify the filename on the command line by inserting an "-f". This flag forces the path for storing the key file. See example below.

ssh-keygen -t dsa -f /path/to/my_dsa

Installing SFTP

By default, SFTP is disabled and FTP is used as the default file transfer method.

Follow the steps below to enable and configure SFTP.

Step 1: Download DSA Key to RFGW-1

a Navigate to the *System/SSH Configuration* page. Set the FTP *Server IP Address*, *User Name*, and *Password*. You can also enter the *DSA Key Path* and *DSA Key Name* for downloading the DSA key file. The key file must not be password protected.

b Once all the parameters have been set, click **Download DSA Key** to download and validate the files.

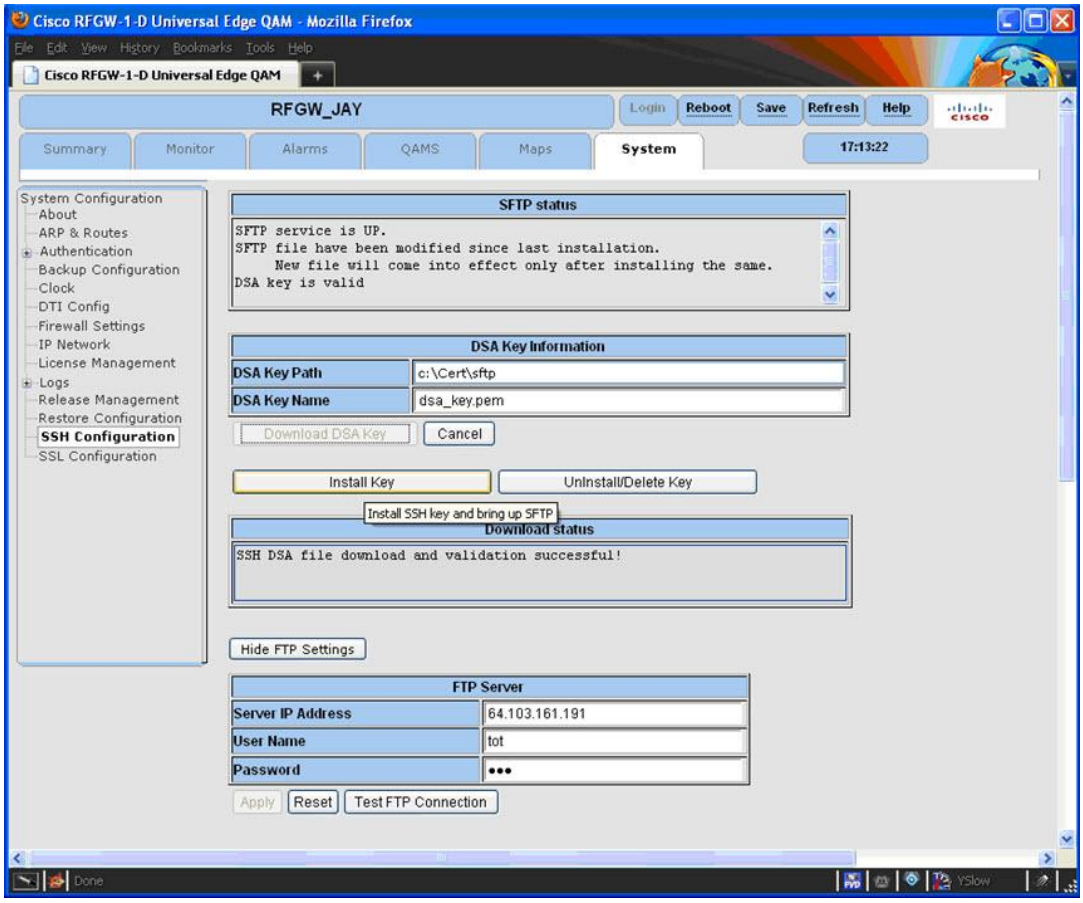
Result: The status window indicates whether the download and validation was successful.

Step 2: Install SFTP in RFGW-1

a Once the files are validated, click **Install Key** to install the files. Invalid key files are automatically deleted.

Results:

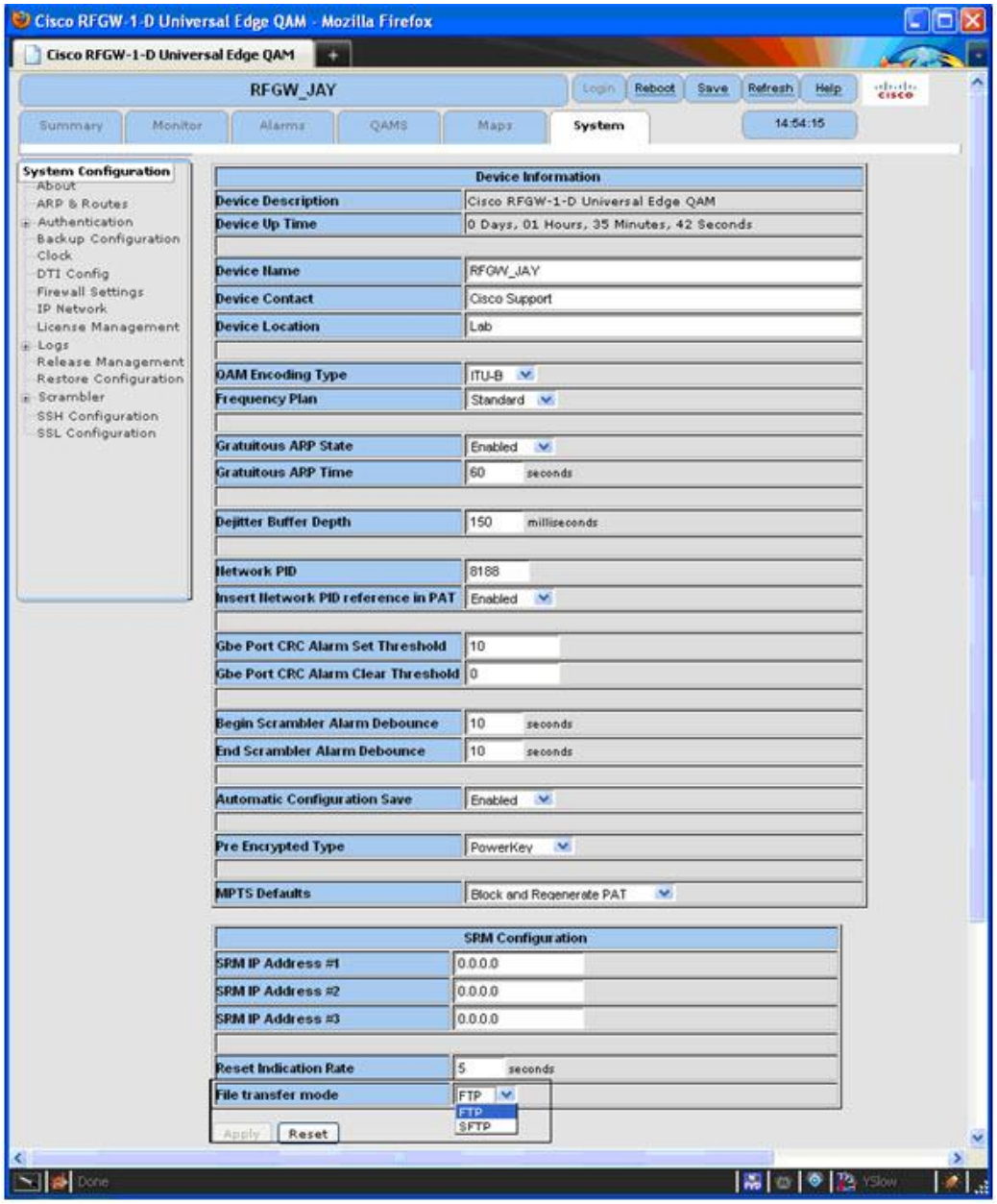
- SFTP Server: Once the key is installed (firewall for SFTP port must be set to enable), the RFGW-1 responds to both SFTP and FTP requests.
- SFTP client: Once the key is installed (file transfer mode must be set to SFTP), all further download/upload operations (such as release, license download, configuration backup, etc.) are done using SFTP.



Step 3: Select SFTP as File Transfer mode

The user can switch between FTP and SFTP client for file transfer.

Note: When the SFTP is selected as the file transfer mode, before downloading and installing the DSA key, a message appears indicating that the configuration will not be allowed.



Uninstalling SFTP

To uninstall SFTP, follow the step below.

On the *SSH Configuration* page, click **Uninstall**.

Results:

- The key is deleted

- All existing SFTP connections are closed
- SFTP server and client are disabled

Note: The File transfer method remains unaltered. If set to SFTP, change to FTP manually.

SNMP V3 Support

Overview

SNMPv3 allows you to define views, select which SNMP users and groups receive full access rights, and select which users should only have access to specified parts of the Management Information Base (MIB).

The following features are available for SNMPv3:

- Authentication
- Privacy
- Encryption

GUI Changes for SNMPv3

Configurations related to trap settings and community strings can be done using the SNMP manager. The SNMP & Traps page has been removed.

Standard MIBs Supported

The following standard MIBs are supported in version 2.6.x.

1 snmpFrameworkMIB (1.3.6.1.6.3.10) – RFC 3411

2 snmpTargetMIB (1.3.6.1.6.3.12) – RFC 3413
snmpTargetAddrTable
snmpTargetParamsTable

3 snmpNotificationMIB (1.3.6.1.6.3.13) – RFC3413
snmpNotifyTable

4 snmpUsmMIB (1.3.6.1.6.3.15) – RFC 3414
usmUserTable

5 snmpVacmMIB (1.3.6.1.6.3.16) – RFC 3415
vacmAccessTable
vacmSecurityToGroupTable
vacmViewTreeFamilyTable

6 snmpCommunityMIB (1.3.6.1.6.3.18) – RFC 3584
snmpCommunityTable

SNMPv3 Configurations

Note: The SNMP browser configurations and snapshots are illustrated using the MG-Soft MIB Browser. If any other MIB browser is used, a similar configuration should be done.

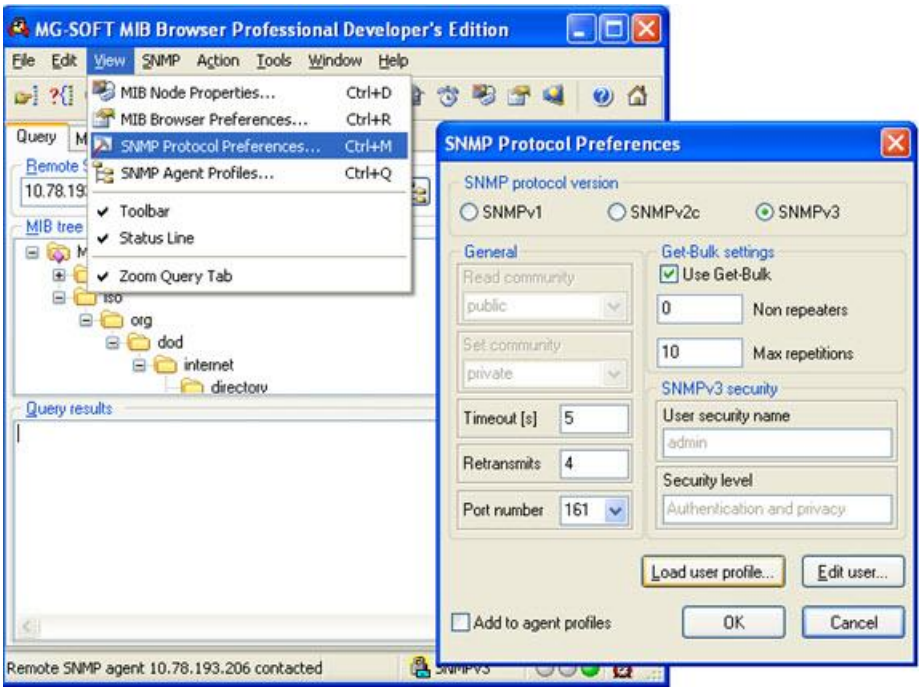
Configuring the User Profile (in the SNMP Manager)

User profile configurations are related to the SNMP manager, which in this case is the MG-Soft MIB Browser. It is not related to the SNMPv3 agent.

Follow the instructions below to configure the user profile.

1 In the MIB browser, click **View/SNMP Protocol Preferences.**

Result: The following screen appears.



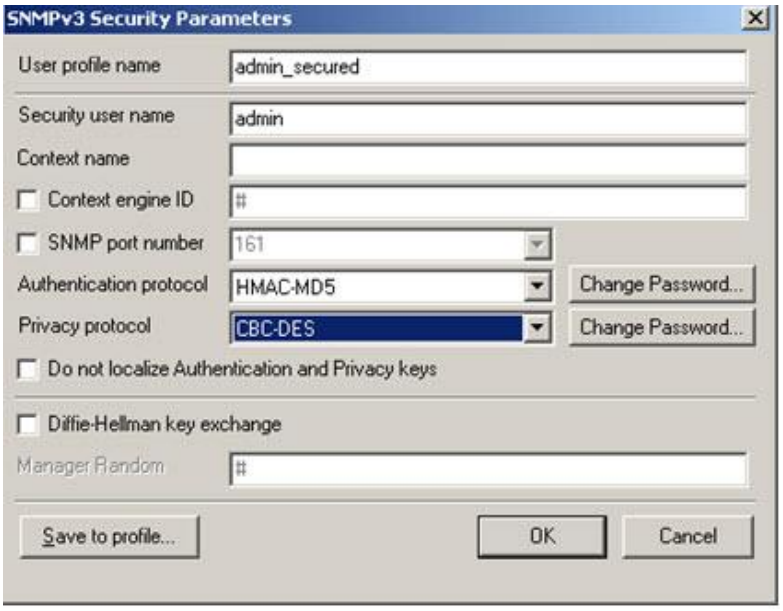
2 Select **SNMPv3**.

3 Click **Load user profile.**

Result: The following screen is displayed.

4 Click the new user icon at the top left corner.

Result: The following screen is displayed.



5 Enter the *User profile name, Security user name, Authentication protocol* (None, HMAC-MD5, HMAC-SHA), and *Privacy protocol* parameters (None, CBC-DES). Also, set the correct password for authentication and privacy protocol.

The valid combination for authentication and privacy protocol choices are:

- None, None
- HMAC-MD5, None
- HMAC-SHA, None
- HMAC-MD5, CBC-DES
- HMAC-SHA, CBC-DES

6 Click **OK**.

Result: The user profile is created in the *SNMPv3 USM User Profiles* dialog box as shown below.

Note: The user profile can be modified, or deleted.

Selecting a User Profie (Login)

Follow the instructions below to select a user profile.

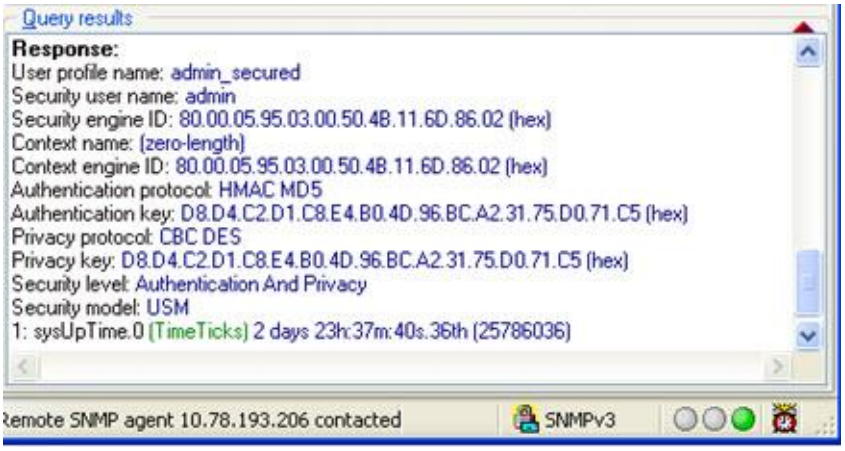
1 In the MIB browser, select **View/SNMP Protocol Preferences**.

2 Click **Load user profile**.

Result: The dialog box opens with the list of user profiles created.

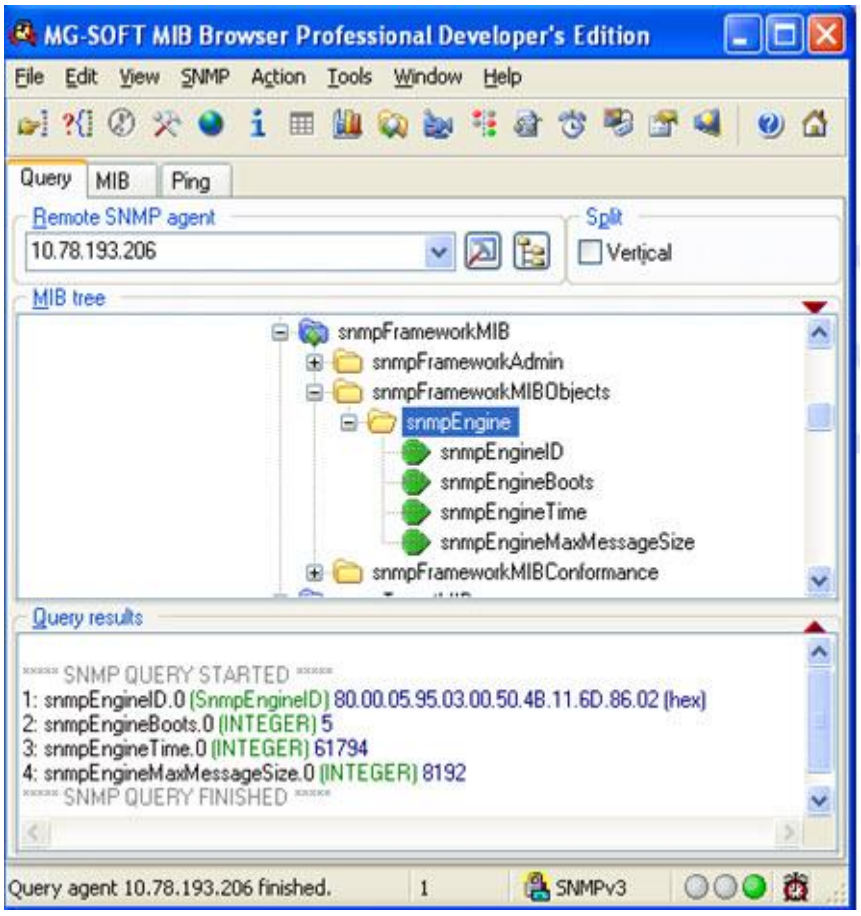
3 Select the required user profile, and click **OK** in the *SNMP Protocol Preferences* dialog box.

Result: If the configured values are correct, login is successful and the following query response is displayed.



SNMP framework (snmpFrameworkMIB)

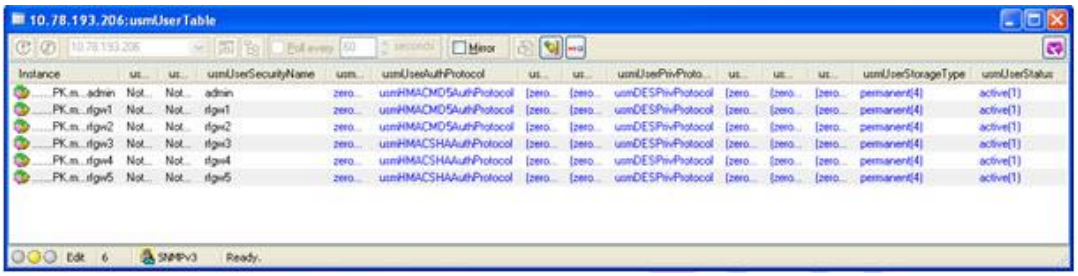
The following screen displays the SNMP framework MIB objects.



- The engine ID uniquely identifies the SNMP engine/agent. To maintain this identity, the RFGW-1 SNMPv3 agent implementation derives the engine ID from the Management interface's MAC address.
- The snmpEngineBoots is the total number of times the SNMP engine has been started or re-initialized. Re-initialization occurs whenever the snmpEngineID is modified or if the snmpEngineBoots reaches 2147483647.
- snmpEngineTime is the number of seconds since the value of snmpEngineBoots has changed. When this value reaches its maximum value (2147483647), it wraps back to 0 and snmpEngineBoots increments by 1.
- snmpEngineMaxMessageSize, is the maximum size in octets of an SNMP message that the SNMP engine can send or receive.

User Table Configuration (usmUserTable)

The User Table maintains authentication and privacy information for each user. The number of rows in this table is fixed at 6. Entries can only be modified, not added or deleted. To view the table, right-click the *usmUserTable* in the MIB tree. Select *Table View* to get to the following screen. The values in this table remain persistent across reboots.

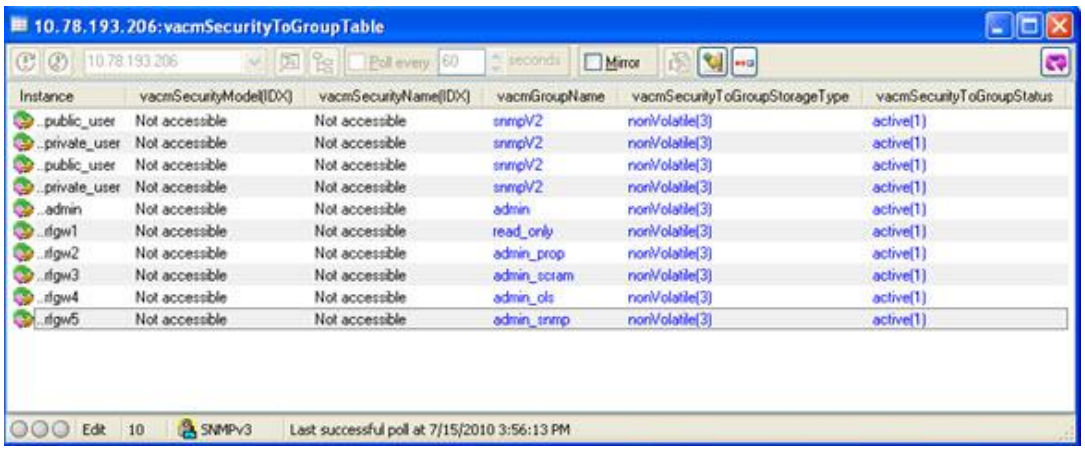


- The above screen displays the default user profiles with default user names. The first three user profiles have MD5 as Authentication protocol, and the last three have SHA. The privacy protocol is DES for all users. For all practical purposes, the authentication and privacy protocol cannot be changed to anything other than "None."
- The usmUserStorageType is permanent for all users, which indicates the user profiles cannot be deleted.
- Changes made to the user profile (user name and password) using the GUI is reflected in this table.
- Resetting the admin's password using the front panel is reflected in this table.

Group Table Configuration (vacmSecurityToGroupTable)

The Group Table maps a security model and security name to a group name. Entries in this table can be added, modified, or deleted. Configurations remain persistent across reboots. The Group Table can have a maximum of 32 rows. If the user name is changed from the GUI, it is reflected in this table as well.

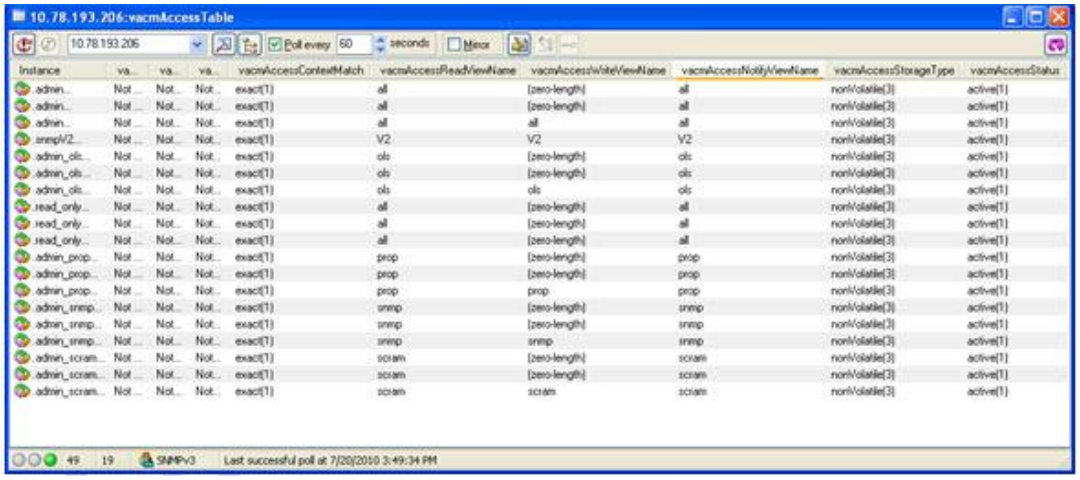
The default entries for this table are shown below.



Access Table Configuration (vacmAccessTable)

The Access Table is used to map a group name, security information, context, and message type into a MIB view. In MIB view, you can determine whether a managed object is allowed to be accessed. Views can be defined for read, write, and notify access. Entries in this table can be added, modified, or deleted. Configurations remain persistent across reboots. The maximum limit for entries is 32.

The default entries for this table are shown below.

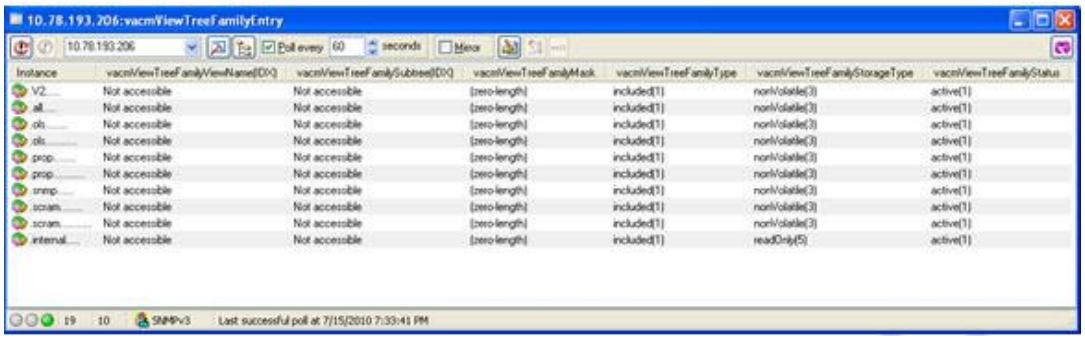


View Table Configuration (vacmViewTreeFamilyTable)

The View Table identifies objects allowed to be accessed for a given MIB view. Each row within this table specifies a MIB view, a MIB sub-tree, and whether an object in a MIB sub-tree should be included or excluded. If an object is included, it can be accessed and if excluded, it cannot. Entries in this table can be added, modified, or deleted. Configurations remain persistent across reboots. A maximum of 32 entries can be added. Each view name maps to a particular OID, and any access defined for this view will have access to the mapped OID and all its sub-nodes.

Note: The internal view is used internally and is not required by the external user. Any change to this entry is not allowed and is therefore marked as "read-only".

The default entries for this table are shown below.



Community Table Configuration (snmpCommunityTable)

The Community Table provides a mapping of a community string to a security name, contextEngineID, and context name to resolve SNMP co-existence issues. By mapping SNMPv1 or SNMPv2c community strings to version independent SNMP message parameters, SNMPv1 and v2c messages can be processed within the SNMP framework in the same manner as the SNMPv3 message. The maximum length of the community string is fixed at 255 characters. The set/get community strings are in column 3, rows 1 and 2, and may be changed per the application. See screen below.

Traps and Notifications

In regards to the trap packet, there is no difference between SNMPv2c and SNMPv3 traps. However, in SNMPv2c, a trap notification is sent to all targets registered for notification, whereas in SNMPv3, selected trap notifications (TRAP/INFORM PDU) can be sent to selected targets.

Note: RFGW-1 does not support INFORM PDU.

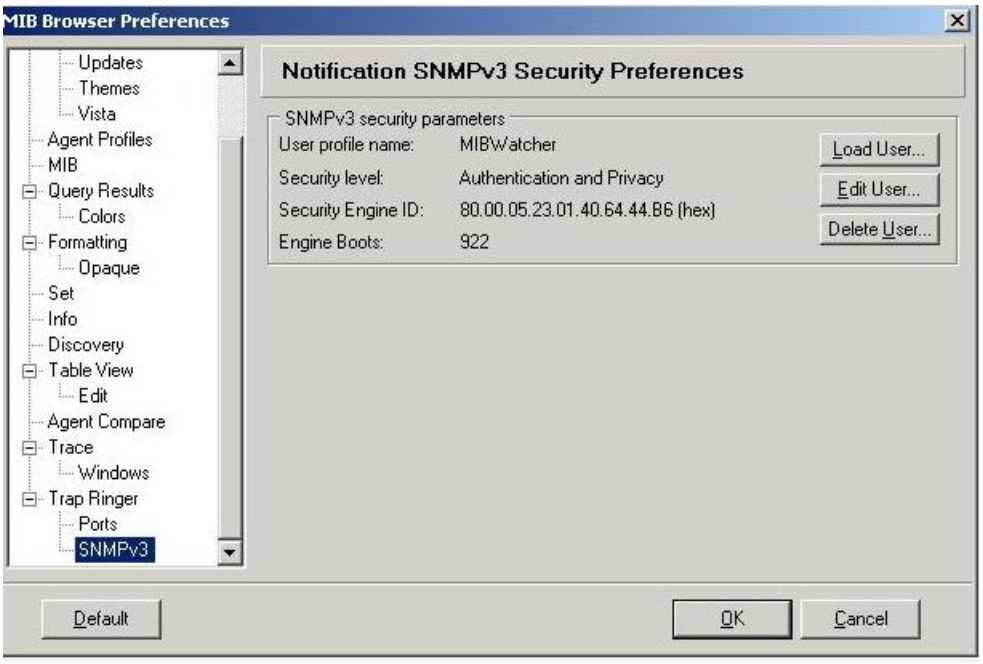
Configuring the SNMP Manager (for Trap Ringer)

The configurations explained in this section are related to the MIB manager, which in this case is the MG-Soft MIB Browser and is not related to the SNMPv3 agent. This user profile configuration is required to receive and decrypt SNMPv3 traps on the SNMP Manager. If any other SNMP manager is used, a similar configuration should be done.

Follow the instructions below to configure the SNMP Manager.

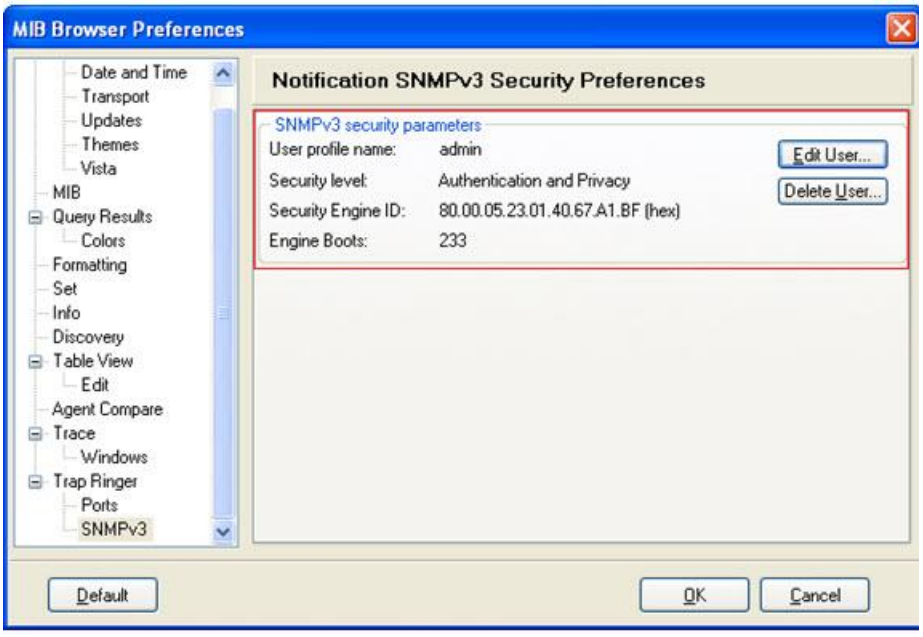
1 In the MIB browser, click **View/MIB Browser Preferences.**

Result: The following screen is displayed.



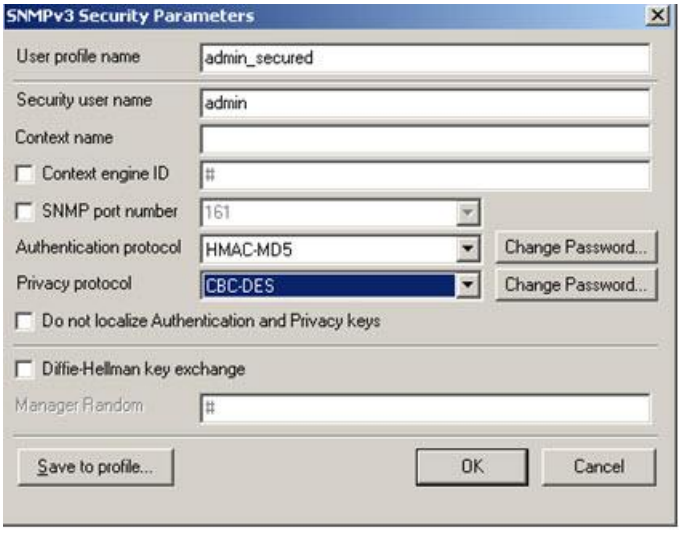
2 Select **SNMPv3.**

Result: The following screen is displayed.



3 Click **Edit User**.

Result: The following screen is displayed.



4 Configure the *User profile name*, *Security user name*, *Authentication protocol* (None, HMAC-MD5, HMAC-SHA), and *Privacy protocol* (None, CBC-DES) parameters. Also, set the correct password for the authentication and privacy protocols.

The valid combination for Authentication and Privacy protocol choices allowed are:

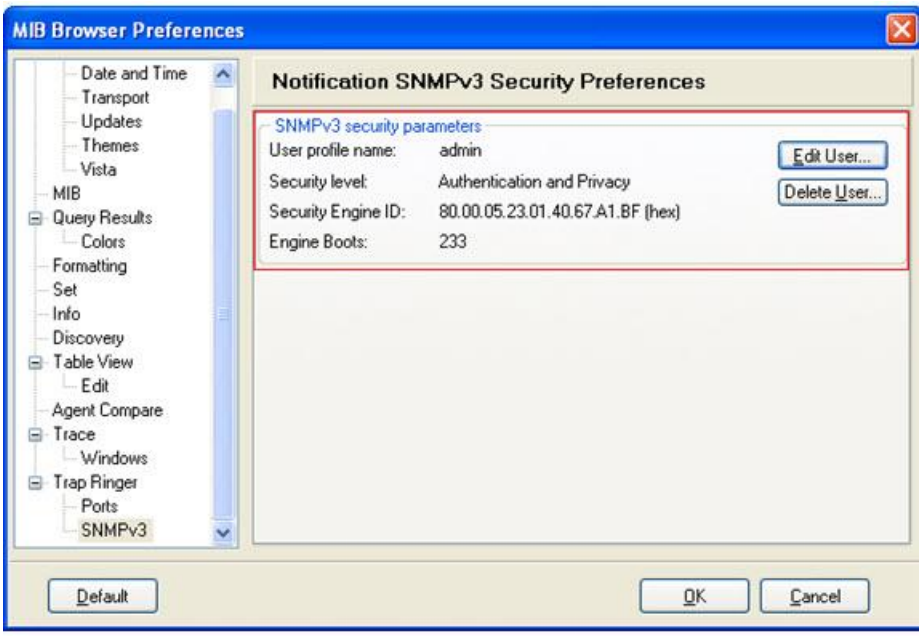
- None, None
- HMAC-MD5, None
- HMAC-SHA, None
- HMAC-MD5, CBC-DES
- HMAC-SHA, CBC-DES

5 Click **Save to profile** to save your settings.

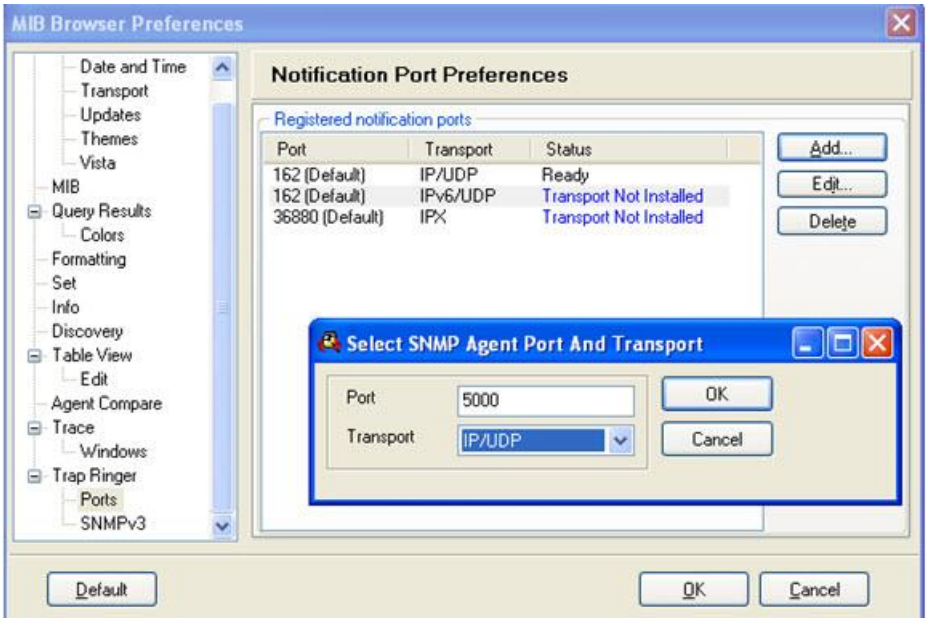
6 Click **OK.**

Result: The user details are displayed in the MIB browser preferences dialog box.

Note: The user profile, if required can be modified, or deleted.



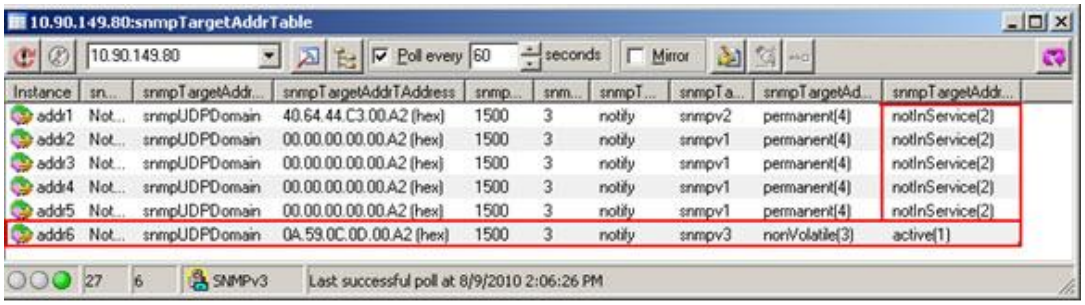
If the trap destination port is changed from default value (162), the same should be configured in the MIB Browser preferences dialog box. See example screen below. Once the user profile and trap destination port is configured, the SNMP Manager's Trap ringer is ready to receive and decrypt SNMPv3 traps.



Additional SNMP agent configurations are needed to successfully send traps. Refer to the sections below.

Target Address Table Configuration (snmpTargetAddrTable)

This table is used to specify the target IP address and port to which the SNMP traps and notifications should be sent. There are 5 default entries in the target address table that are permanent. The default configuration of this table is shown below.



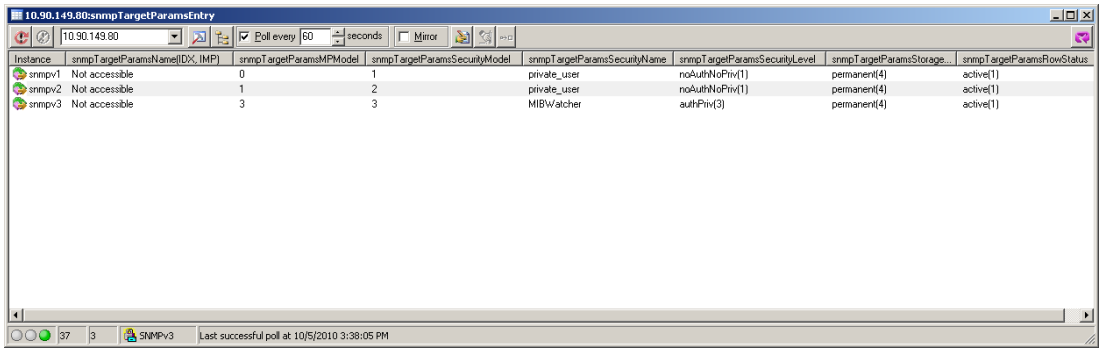
A maximum of 32 rows can be added in this table and the configurations remain persistent across reboots.

The default/permanent entries in this table can be modified, but not deleted.

Instance addr6 has been added to enable v3 traps to be sent to 10.89.12.13 port 162, and v1 and v2 traps have been suppressed in instances addr1-addr5.

Target Params Table Configuration (snmpTargetParamsTable)

This table provides the security parameters for creating a TRAP PDU. The default configuration of this table is shown below.



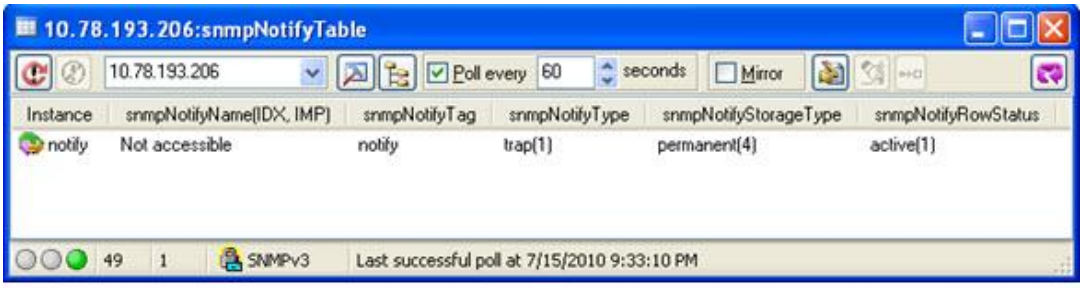
The entries in this table should be mapped to the corresponding target name in the target address table for successful reception of the traps and notifications.

There will be 3 permanent entries in this table which cannot be deleted. A maximum of 32 rows can be configured in this table.

The default/permanent entries in this table can be modified but not deleted. All configurations remain persistent across reboots.

Notification Table Configurations (snmpNotifyTable)

This table is used to select management targets that should receive notifications, as well as the type of notification that should be sent. The default configuration of this table is shown below.



This table contains a permanent entry that cannot be deleted. There are 2 values for snmpNotifyType (trap, inform), and only traps are supported.

Entries could be added, modified, or deleted (except the default permanent entry). This table can have a maximum of 32 rows, and configurations remain persistent across reboots.

Note: snmpNotifyFilterProfileTable & snmpNotifyFilterTable are not supported. Therefore filtering based on trap OIDs cannot be done. Creating a new entry to these tables will result in error.

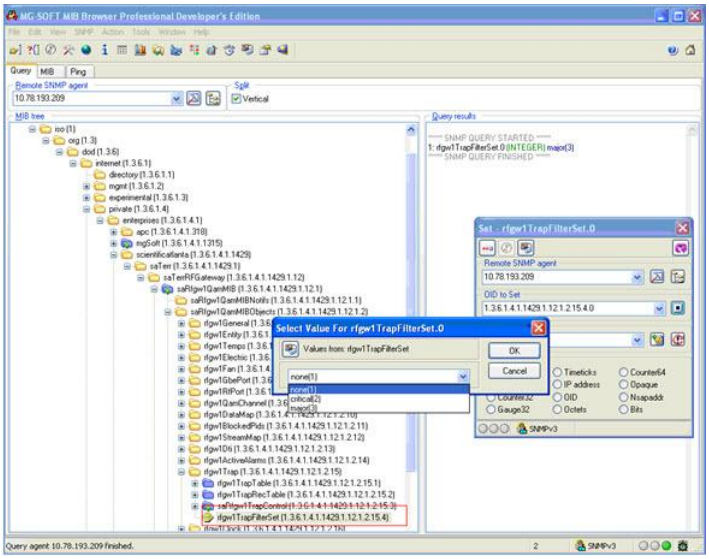
Notification Filter (rfgw1TrapFilterSet)

A new object rfgw1TrapFilterSet (OID - 1.3.6.1.4.1.1429.1.12.1.2.15.4) is added in the proprietary MIB (CISCO-RFGW-1-MIB.my), to filter traps and notifications based on their severity.

The following 3 values are available:

- None - no traps/notifications will be sent.
- Critical - traps/notifications whose severity is critical will be sent.
- Major - all traps/notifications will be sent.

The following screen shows the trap filter.



Unified User Support

- Common user credentials are maintained across the SNMPv3 agent, GUI, and SFTP server.
- The user name and password can be modified using the GUI and the password can be modified using SNMPv3. However both cannot be modified through SFTP. Changes done via one interface are reflected in all three user interfaces.
- The admin's password can be reset from the front panel to default value and the same is reflected in all 3 interfaces.
- For SNMPv3, a view-based access control mechanism specific to each user is available. For SFTP, all users are the same, and for GUI, admin is read-write and others are read-only.
- RADIUS users do not classify as unified user.
- Passwords are not stored as plain text.
- The default authentication hash algorithm is MD5 for admin, rfgw1, and rfgw2 login ids, and SHA for rfgw3 to 5. These default values cannot be changed.
- User credentials and SNMPv3 configurations are RFGW-1 box-specific and are not portable to other RFGW-1 boxes.

Configuring the RFGW-1 for Secure SNMP Access

This example describes how to change a default user name to MIBWatcher (which uses MD5 hash and DES encryption), create a group named secure_snmp (which has read/write access to all the MIB elements), add MIBWatcher to the secure_snmp group, shut off all but MIBWatcher access, and permit only SNMPv3 encrypted traps to MIBWatcher. It's assumed that the RFGW-1 has the default SNMPv3 settings. While written around MG-SOFT and Unbrowse SNMP, any SNMP management tool can be used.

Note: Eight character authentication and privacy passwords were chosen because Unbrowse requires eight characters for authentication and appears to be more stable when using eight characters for the privacy password.

Follow the instructions below to change the default username.

1. Launch the GUI.
   - **a** Change the admin authentication password from the default value of 0000 to one with eight characters.
   - **b** Change the local user name from rfgw2 to MIBWatcher and change the authentication password from the default value of 0000 to 12345678.
   - **c** Close the GUI.
2. Launch MG-SOFT.
   - **a** Create a profile for admin. Authentication and privacy password = 12345678.
   - **b** Contact the RFGW-1 as admin.
   - **c** Change the privacy password of admin and MIBWatcher from 0000 to 12345678. Go to Tools>Manage Agent SNMPv3 USM Users and then right-click the admin row and follow the instructions. Repeat for the MIBWatcher row.
   - **d** Close MG-SOFT.
3. Launch Unbrowse.
   - **a** Create an agent manager for admin. Authentication and privacy password = 12345678. Go to Agents>Manage and then follow the instructions.
   - **b** Create a group called secure_snmp. Go to Security>Manage SNMPv3 Access Control.
   - **c** Move user MIBWatcher from admin_prop group to secure_snmp group. Go to Security>Manage SNMPv3 Access Control and follow the instructions.
   - **d** Close Unbrowse.
4. Launch MG-SOFT.
   - **a** Change the TargetParamsTable snmpv3 row, and TargetParamsSecurityName to MIBWatcher so that the SNMPv3 traps will be sent.
   - **b** Create a profile for MIBWatcher.

c Configure the trap ringer preferences for SNMPv3 and MIBWatcher.

d Contact the RFGW-1 as MIBWatcher.

e Disable all groups except secure_snmp.

f Close MG-SOFT.

Upgrading from 2.5.x to 2.6.x

Follow the instructions below to upgrade from 2.5.x to 2.6.x.

1 When upgrading from 2.5.x to 2.6.x, all configuration changes to user credentials (such as user name, password) will be retained. The user will not notice a difference in access permissions after the upgrade. When downgrading to 2.5.x, the new configurations will not be available. The previous 2.5.x user credentials will be restored.

2 When upgrading from 2.5.x to 2.6.x, all six private passwords are set to 0000. To change them with MG-Soft, select Tools>Manage Agent SNMPv3 USM Users, and then right-click the row and follow the instructions.

3 During an upgrade to 2.6.x, the configurations in the SNMP & Traps page will be copied over to the corresponding SNMPv3 tables. The SNMP & Traps page is not available in 2.6.x, and all configurations using this page can be done from the SNMP manager using the target, target params, and notification tables. When downgrading to 2.5.x, the new configurations will not be available. The previous 2.5.x user credentials will be restored.

4 Any SNMPv1 or SNMPv2c trap configurations in the agent before upgrading will be retained after upgrade, without additional configurations.

5 When upgrading from 2.5.x to 2.6.x, community strings (from previous release) will be copied to the snmpCommunityTable, and the same will be used for v1/v2/trap response.

6 Unified user support is provided, thus user details are shared across the GUI, SNMP, and SFTP server. Any changes made to username and password using the GUI, or changes to the password made from the SNMP manager will be reflected for all types of users (GUI, SNMP, and SFTP). This provides single point of control for user details.

7 RADIUS user authentication is not a part of Unified user management in RFGW-1, SFTP server, and SNMPv3.

8 By default, SFTP will be disabled and FTP will be the default file transfer option. This can be enabled by downloading and installing the DSA key file. Refer to ***Generating a DSA Key.*** (see "***Generating a DSA Key***" on page 6) After an upgrade, the FTP is still available and the user can continue using it.

9 By default, SNMPv2c user is provided read-write access to all objects. This can be restricted by an admin user.

3

Customer Support Information

Introduction

This chapter contains information on obtaining product support.

Obtaining Product Support

IF…	THEN…
you have general questions about this product	contact your distributor or sales agent for product information or refer to product data sheets on www.cisco.com.
you have technical questions about this product	call the nearest Technical Support center.
you have customer service questions about this product	call the nearest Customer Service center.

In This Chapter

Support Telephone Numbers

This table lists the Technical Support and Customer Service numbers for your area.

Region	Centers	Telephone and Fax Numbers
North America	Cisco Services Atlanta, Georgia United States	For *Technical Support*, call: ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 (Press **2** at the prompt) For *Customer Service*, call: ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 (Press **3** at the prompt) ■ Fax: 770-236-5477 ■ Email: customer-service@cisco.com
Europe, Middle East, Africa	Belgium	For *Technical Support*, call: ■ Telephone: 32-56-445-197 or 32-56-445-155 ■ Fax: 32-56-445-061 For *Customer Service*, call: ■ Telephone: 32-56-445-444 ■ Fax: 32-56-445-051 ■ Email: service-elc@cisco.com
Japan	Japan	■ Telephone: 81-3-5908-2153 or +81-3-5908-2154 ■ Fax: 81-3-5908-2155
Korea	Korea	■ Telephone: 82-2-3429-8800 ■ Fax: 82-2-3452-9748 ■ Email: songk@cisco.com
China (mainland)	China	■ Telephone: 86-21-2401-4433 ■ Fax: 86-21-2401-4455 ■ Email: xishan@cisco.com
All other Asia Pacific countries & Australia	Hong Kong	■ Telephone: 852-2588-4746 ■ Fax: 852-2588-3139 ■ Email: saapac-support@cisco.com
Brazil	Brazil	■ Telephone: 11-55-08-9999 ■ Fax: 11-55-08-9998 ■ Email: fattinl@cisco.com or ecavalhe@cisco.com
Mexico, Central America, Caribbean	Mexico	For *Technical Support*, call: ■ Telephone: 52-3515152599 ■ Fax: 52-3515152599 For *Customer Service*, call: ■ Telephone: 52-55-50-81-8425 ■ Fax: 52-55-52-61-0893 ■ Email: sa-latam-cs@cisco.com
All other Latin America countries	Argentina	For *Technical Support*, call: ■ Telephone: 54-23-20-403340 ext 109 ■ Fax: 54-23-20-403340 ext 103 For *Customer Service*, call: ■ Telephone: 770-236-5662 ■ Fax: 770-236-5888 ■ Email: keillov@cisco.com

Glossary

FTP

file transfer protocol. Allows users to transfer text and binary files to and from a personal computer, list directories on the foreign host, delete and rename files on the foreign host, and perform wildcard transfers between hosts.

GUI

graphical user interface. A program interface that takes advantage of a computer graphics capabilities to make the program visually easier to use.

HTTP

hypertext transfer protocol.

HTTPS

hypertext transfer protocol secure.

IP

Internet protocol. A standard that was originally developed by the United States Department of Defense to support the internetworking of dissimilar computers across a network. IP is perhaps the most important of the protocols on which the Internet is based. It is the standard that describes software that keeps track of the internetwork addresses for different nodes, routes, and outgoing/incoming messages on a network. Some examples of IP applications include email, chat, and Web browsers.

IP address

Internet protocol address. A 32-bit sequence of numbers used for routing IP data. Each IP address identifies a specific component on a specific network. The address contains a network address identifier and a host identifier.

ISO

International Organization for Standardization. An international body that defines global standards for electronic and other industries.

PC

personal computer.

RADIUS

Remote authentication dial in service. A networking protocol that provides centralized Authentication, Authorization and Accounting (AAA) management for computers to connect and use a network service.

RMA

return material authorization. A form used to return products.

SFTP

Secure File Transfer Protocol.

SNMP

Simple Network Management Protocol.

SSH

Secure SHell

SSL

Secure Sockets Layer.

UDP

Index

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678.277.1000
www.cisco.com

October 2010 Printed in United States of America Part Number 4039214 Rev A