Cisco RF Gateway 1 Software Release Notes, Release 2.05.06

Overview

Introduction

Software release 2.05.06 contains the following major enhancements not currently available in any other RF Gateway 1 release.

- HTTPS
- GUI support for downloading externally generated keys and certificates to the RF Gateway 1 web server
- Multi-level user access - R/O and R/W
- RADIUS Support of service-type and Cisco-av-pair
- User-configurable firewall settings to block FTP, HTTPS, HTTP, and Telnet ports
- SNMP Trap destination UDP port addresses are now configurable

Purpose

The purpose of this document is to notify RF Gateway 1 users of the enhancements included in the current release, and inform users of any special upgrade procedures needed for using Release 2.05.06.

Audience

This document is intended for system engineers or managers responsible for operating and/or maintaining this product.

Related Publications

Refer to the following documents for additional information regarding hardware and software. Please read the Securities Features Addendum thoroughly before upgrading.

- *Cisco RF Gateway 1 Configuration Guide*, part number 4025112
- *Cisco RF Gateway 1 System Guide*, part number 4024958

- *Cisco RF Gateway 1 Software Version 2.5.x Security Features Addendum*, part number 4037508

Safe Operation for Software Controlling Optical Transmission Equipment

If this document 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 should 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.

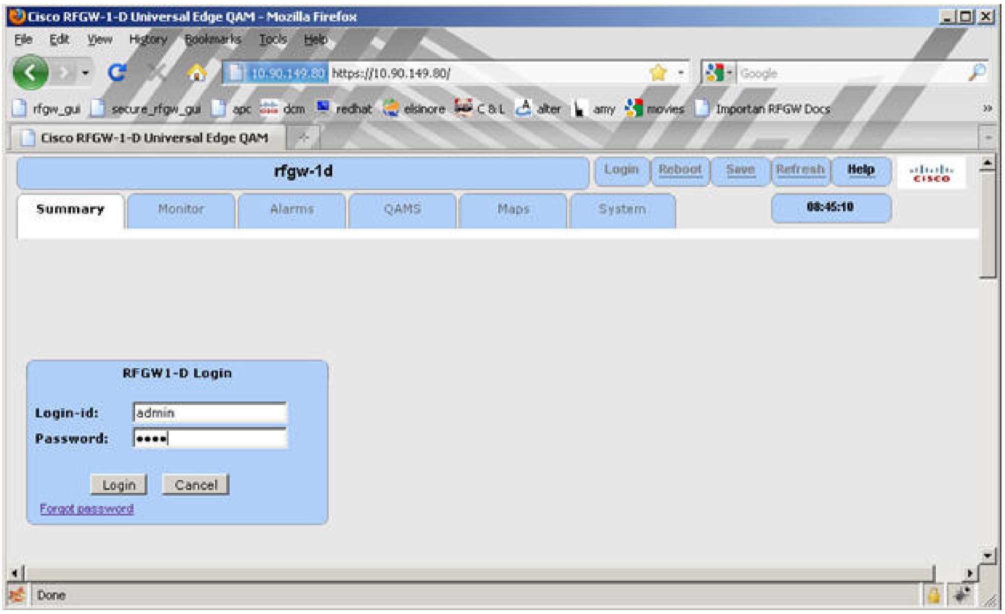
⚠ **WARNINGS:**

- 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.

In This Document

Upgrade Information

- All RFGW1 settings will be the same after upgrading, ensuring that data and video will continue to flow as before.
- All six authentication passwords, admin and, rfgw1-5, will be initialized to 0000 after upgrading.
- If authentication was not disabled before upgrading, you must login as "admin" with 0000 as the password after upgrading. See the following screen.


Cisco RFGW-1-D Universal Edge QAM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
10.90.149.80 https://10.90.149.80/
Google
rfgw_gui secure_rfgw_gui apc dcm redhat elsinore C & L alter amy movies Importan RFGW Docs
Cisco RFGW-1-D Universal Edge QAM
rfgw-1d
Login Reboot Save Refresh Help
CISCO
Summary Monitor Alarms QAMS Maps System
08:45:10
Login Cancel
Forgot password
Done

RFGW1-D Login

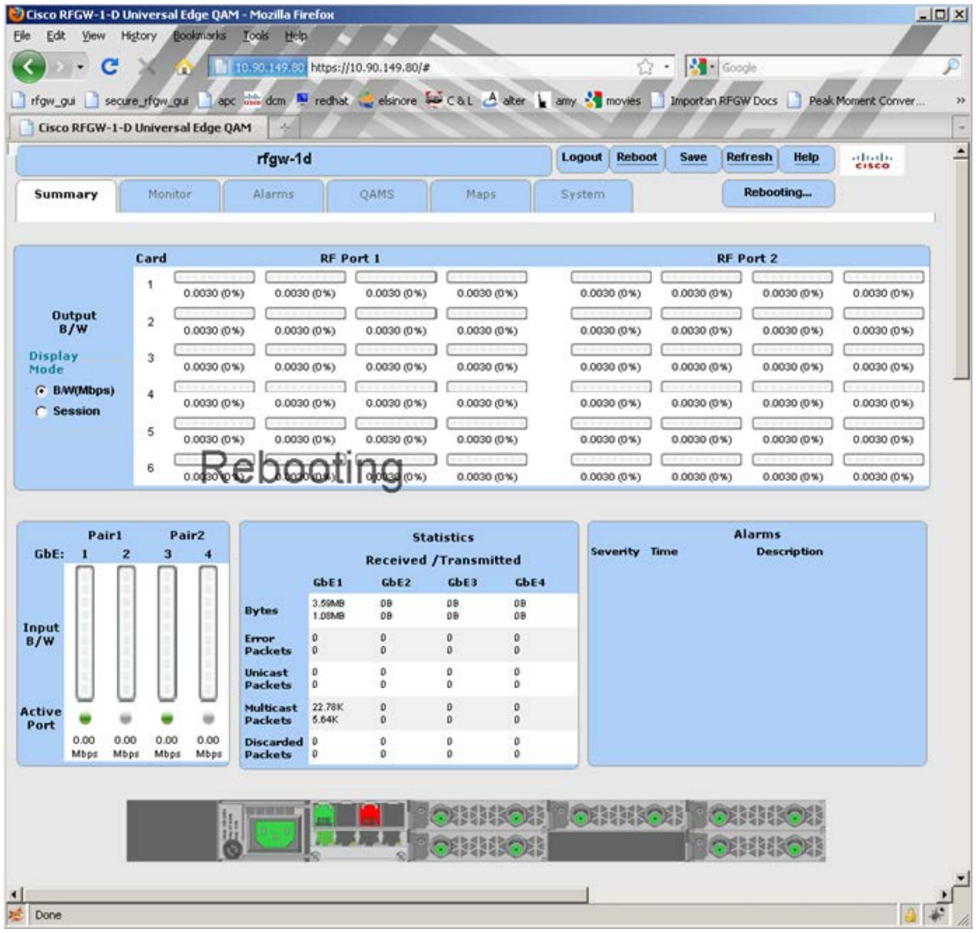
Login-id: admin

Password: ••••

Known Issues

The following list identifies known limitations planned to be resolved as part of an upcoming GA release.

- The GUI times out after about 17 seconds of inactivity and no longer automatically reconnects to the RF Gateway 1. For example, if the RF Gateway 1 is rebooted from the GUI, the following page is displayed.


Cisco RFGW-1-D Universal Edge QAM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
10.90.149.80 https://10.90.149.80/#
Google
rfgw_gui secure_rfgw_gui apc dcm redhat elsinore C & L alter amy movies Importan RFGW Docs Peak Moment Conver...
Cisco RFGW-1-D Universal Edge QAM
rfgw-1d
Logout
Reboot
Save
Refresh
Help
CISCO
Summary
Monitor
Alarms
QAMS
Maps
System
Rebooting...
Output B/W
Display Mode
◉ B/W(Mbps)
○ Session
Rebooting
Input B/W
Active Port
Done

Card	RF Port 1				RF Port 2			
1	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)
2	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)
3	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)
4	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)
5	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)
6	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)	0.0030 (0%)

	Pair1		Pair2	
GbE:	1	2	3	4
	0.00 Mbps	0.00 Mbps	0.00 Mbps	0.00 Mbps

Statistics

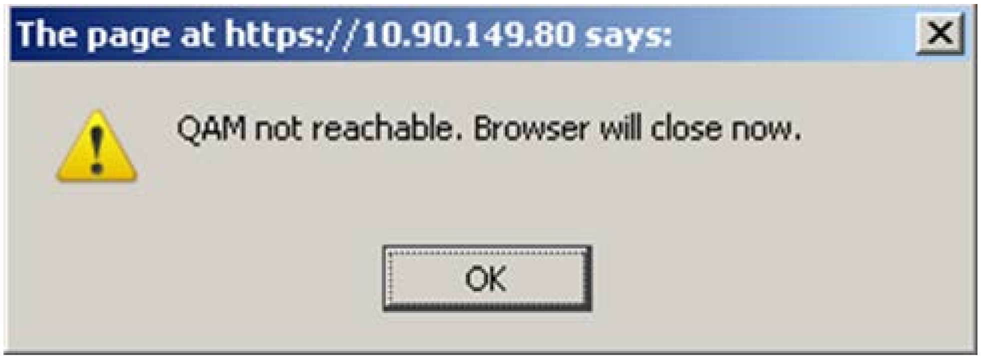
Received /Transmitted

	GbE1	GbE2	GbE3	GbE4
Bytes	3.59MB 1.08MB	0B 0B	0B 0B	0B 0B
Error Packets	0 0	0 0	0 0	0 0
Unicast Packets	0 0	0 0	0 0	0 0
Multicast Packets	22.78K 5.64K	0 0	0 0	0 0
Discarded Packets	0 0	0 0	0 0	0 0

Alarms

Severity	Time	Description

After 17 seconds, the screen below is displayed. Click **OK**. The browser closes. You will need to reopen the browser upon an RFGW reboot.



The page at https://10.90.149.80 says:

QAM not reachable. Browser will close now.

- If port 443 is attacked with approximately twenty, simultaneous telnet sessions, the RF Gateway 1 will run out of sockets, possibly resulting in interruption of services such as SNMP, HTTP, HTTPS, and so forth.
- Use of any of the following six characters: ! $ ^ * ( ) in password strings may cause the GUI to display erratically.
- The RF Gateway 1 web interface is not fully tested with IE-8 and FireFox-3.5 or newer. The RF Gateway 1 web management interface is tested with IE-6 or FireFox-2.00.14 and above. Use of Java 1.6.x is also recommended.
- The Summary page displays the unit rear panel with the Conditional Access (CA) port enabled/disabled as green/gray. The CA port indication represents the on/off setting and not actual link status.
- The database restore feature requires disabling trap settings (in the restore from database file prior to release 2.1.9) before starting the restore procedure. This can be done before starting a restore configuration. The procedure is needed to allow compatibility with the enhanced SNMP version 1 and 2 trap support in this release.
- SNMP community strings are provided to support SNMP v1 and v2 traps. Prior to release 2.1.9, there was a single community string applicable to all five trap receivers configurable for the operator. In release 2.2.11 and beyond, in addition to supporting SNMP v1 and v2 traps, each of the five trap receivers has a separate configurable trap community string. This may cause a possible loss of SNMP trap community strings during an upgrade or downgrade procedure. An operator should carefully verify their trap community strings when upgrading to 2.2.11 or later releases, or downgrading from 2.2.11 or later releases, if they are being used.
- An upgrade to this release from pre-2.1.9 automatically enables insertion of the Network PID into the PAT. If this is an issue in the user's system, it may be disabled using the *System/System Configuration* page.

- The system uptime counter rolls over to zero after about 49 days of continuous use. This behavior manifests on the web management GUI and via SNMP. The rollover does not cause any operational problems or side-effects on active services.

Note: A power cycle or reboot of the RF Gateway 1 resets the system uptime counter as part of normal operation.

For Information

Support Telephone Numbers

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

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

678 277-1120
800 722-2009
www.cisco.com

Product and service availability are subject to change without notice.

September 2012 Printed in USA Part Number 62-7020536-01 Rev B