

501 SE Columbia Shores Boulevard, Suite 500 Vancouver, Washington 98661 USA +1 360 859 1780 / smartrg.com

/ Gateway User Manual

Model: SR400ac

Release: 5.1

Software Version: 10.8.4.1

March 2020

Table of Contents



Welcome!	. 4
Purpose & Scope	. 4
Intended Audience	. 4
Getting Assistance	. 4
Copyright and Trademarks	. 4
Disclaimer	. 4
Getting Familiar with your Gateway	. 5
LED Indicators	. 5
Connections	. 6
LAN	. 6
WAN	. 6
USB	. 6
POWER	. 6
External Buttons	. 7
WPS Button (5 GHz Band)	. 7
WiFi Button (2.4 GHz Band)	. 7
On/Off Button	. 7
Reset Button	. 7
Installing your SR400ac Gateway	. 8
Logging in to the SR400ac Interface	9
User Preferences	10
Saving Your Changes	.11
Dashboard	12
Network	12
Status	13
Fthernet WAN	13
Internet	14
DHCP for IPv4 WANs	15
Static Address for IPv4 WANs	16
PPPoF for IPv4 WANs	16
DHCPv6 for IPv6 WANs	18
Static Address for IPv6 WANs	19
IPTV	19
Management	21
Cross-Connect	27
I AN Network	23
DHCP Server	24
Defining a Custom DNS Server	26
Defining a Static DHCP IP Address Association	27
DHCP Clients	28
Ethernet Ports	29
Guest Network	30
DHCP Server	31
Defining a Static DHCP IP Address Association	33
DHCP Clients	34
Video Network	35
Static	35
DHCP	36
DHCP Server	. 30
Defining a Static DHCP IP Address Association	30
DHCP Clients	
Multicast	. ⊿1
Video Analyzer	. <u>⊿</u> 2
Routing	.⊣∠ ⊿२
Nouring	

DNS	46
Advanced	47
Downstream QoS	. 48
Firewall	. 48
Firewall Settings	48
Router Access	
Firowall Pulos	51
	JI E4
DML	
Port Forwarding	. 55
W1F1	. 58
Status	. 58
Scan	. 58
Radios	. 59
Networks	61
Mesh	. 63
Clients	. 63
Performance	. 64
Client Performance	65
Advanced	66
Advanced	67
Intellifi Devices	67
According Device Information	. 07
Accessing Device Information	. 07
	. 00
	68
Configure Wireless Settings	. 70
View Interface Statistics	. 73
Reboot the Device	/3
Reset the Device to Factory Default Settings	73
Reset the Device to Factory Default Settings . Update Device Software	73 74
Reset the Device to Factory Default Settings Update Device Software Connected Devices	73 74 . 74
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups	73 74 . 74 76
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule	73 74 74 76 79
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services	73 74 74 76 79 82
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP	73 74 76 76 79 82 82
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA	73 74 74 76 79 82 82 83
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration	73 74 76 76 79 82 82 83 .83
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP	73 74 76 76 79 82 83 83 83
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts	73 74 76 79 82 83 83 83 83
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts	73 74 76 .79 . 82 .82 .83 83 83 83 .86 .87 .88
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS	73 74 76 .79 .82 .83 83 83 83 83 83 83
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage	73 74 .74 .76 .79 .82 .82 .83 .83 .83 .83 .86 .87 .88 .92
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing	73 74 .74 .76 .79 .82 .82 .83 .83 .83 .83 .83 .83 .83 .83 .83 .83
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing Content Filter	73 74 .74 76 .79 .82 .82 .83 83 83 83 86 .87 .88 .92 95
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing Content Filter	73 74 76 79 82 82 83 83 83 83 83 83 83 83 83 83 84 92 92 95 92
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing Content Filter Admin Update	73 74 .74 .76 .79 .82 .82 .83 .83 .83 .83 .83 .83 .83 .83 .83 .83
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing Content Filter Admin Update Configuration	73 74 .74 .76 .79 .82 .82 .83 .83 .83 .83 .83 .83 .83 .83 .83 .83
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing Content Filter Admin Update Configuration Router Management	73 74 .74 .76 .79 .82 .82 .83 .83 .83 .83 .83 .83 .83 .83 .83 .83
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing Content Filter Admin Update Configuration Router Management Passwords	73 74 .74 .76 .79 .82 .83 .88 .83 .88 .88 .92 .92 .95 .96 .98 .99 101
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing Content Filter Admin Update Configuration Router Management Passwords Net Tools	73 74 .74 .76 .79 .82 .83 .88 .83 .88 .88 .92 .92 .95 .96 .98 .99 101 102
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing Content Filter Admin Update Configuration Router Management Passwords Net Tools Event Log	73 74 .74 .76 .79 .82 .83 .88 .83 .88 .88 .92 .92 .95 .96 .98 .99 101 102 104
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing Content Filter Admin Update Configuration Router Management Passwords Net Tools Event Log Configuring Log Settings	73 74 .74 .76 .79 .82 .83 .88 .83 .88 .92 .92 .95 .96 .98 .99 101 102 104 105
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing Content Filter Admin Update Configuration Router Management Passwords Net Tools Event Log Configuring Log Settings	73 74 .74 .76 .79 .82 .83 .88 .83 .88 .92 .92 .95 .96 .98 .99 101 102 104 105 106
Reset the Device to Factory Default Settings Update Device Software Connected Devices Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing Content Filter Admin Update Configuration Router Management Passwords Net Tools Event Log Configuring Log Settings Time Operating Mode	73 74 .74 .76 .79 .82 .83 .88 .88 .88 .92 .95 .96 .98 .99 101 102 104 105 106 107
Reset the Device to Factory Default Settings Update Device Software Device Groups Access Schedule Services UPNP DLNA TR-069 Configuration SNMP Hosts DDNS Cloud Storage File Sharing Content Filter Admin Update Configuration Router Management Passwords Net Tools Event Log Configuring Log Settings Time Operating Mode Reboot	. 73 . 74 . 74 . 76 . 79 . 82 . 83 . 83 . 88 . 83 . 88 . 92 . 95 . 96 . 98 . 99 101 102 104 105 106 107

SmartRG Inc., an Adtran company. Proprietary and Confidential. All Rights Reserved. © 2020

Table of Contents



Logging out	109
Appendix: Compliance Statements	
FCC Interference Statement	
FCC Radiation Exposure Statement	110
5GHz	110
Revision History	111



Welcome!

Thank you for purchasing this SmartRG product.

SmartRG offers solutions that simplify the complex Internet ecosystem. Our solutions include hardware, software, applications, enhanced network insights, and security delivered via a future-proof operating system. Based in the USA, SmartRG provides local, proactive software development and customer support. We proudly offer the best, most innovative broadband gateways available. Learn more at www.SmartRG.com.

Purpose & Scope

This User Manual provides SmartRG customers with installation, configuration and monitoring information for their SR400ac gateway.

Intended Audience

The information in this document is intended for Network Architects, NOC Administrators, Field Service Technicians and other networking professionals responsible for deploying and managing broadband access networks. Readers of this manual are assumed to have a basic understanding of computer operating systems, networking concepts and telecommunications.

Getting Assistance

Frequently asked questions are provided at the bottom of the Support page of the SmartRG Web site.

- Subscribers: If you require further help with this product, please contact your service provider.
- Service providers: if you require further help with this product, please open a support request.

Copyright and Trademarks

SmartRG Inc., an Adtran company. Proprietary and Confidential. All Rights Reserved. © 2020

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of SmartRG, Inc.

Disclaimer

SmartRG does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor patent rights of others. SmartRG further reserves the right to make changes to any products described herein without notice. This publication is subject to change without notice.

Any trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.



Getting Familiar with your Gateway

This section explains the SR400ac gateway's lights, ports, and buttons.

LED Indicators

Your SR400ac gateway has several status indicators (LEDs) on its top which are described below.



There is also a small LED on the front of the gateway that flickers when data is being transferred.

Legend:	🔿 White	{©}	White blinking	🔵 Green	- Č	Green blinking		Red
---------	---------	-----	----------------	---------	-----	----------------	--	-----

LED	Action	Explanation
POWER	୍ଦି ୦	Device in CFE mode Device powered on and ready for use
WAN	0	Device online (at 1000 BASE-T) Device online (at 10/100 BASE-T)
	0 ©	WAN Ethernet connected (at 1000 BASE-T) Data being transferred (at 1000 BASE-T)
	©	WAN Ethernet connected (at 10/100BASE-T) Data being transferred (at 10/100BASE-T)
INTERNET	0 © ●	Gateway on line Data being transferred Internet authentication / connection has failed
USB / USB 3.0	0 ©	USB device connected Data being transferred
2.4 GHZ 5 GHZ	0 ∅	WiFi enabled Data being transferred
((• 🔒 •)) (locked WiFi / WPS)	0 ∅	WPS enabled Data being transferred
LAN 1-4	0 ∅	LAN Ethernet connected (at 1000 BASE-T) Data being transferred (at 1000 BASE-T)
	٥	LAN Ethernet connected (at 10/100BASE-T) Data being transferred (at 10/100BASE-T)



Connections

The SR400ac's exterior ports are shown in the following cabling diagram.



LAN

The four yellow RJ45 Ethernet ports located on the back of the gateway (labeled LAN1, LAN2, LAN3, LAN4) are used to connect client devices such as computers and printers.

WAN

The red RJ45 port labeled WAN is used to connect the SR400ac gateway to another network device using a RJ45/Ethernet cable.

USB

The two USB ports (2.0 port on the back and 3.0 on the left side) are used to connect USB storage devices to the gateway for transferring data. They also provide +5 VDC for charging other devices.

POWER

- Use ONLY the dedicated power supply included with your gateway (3 amp 12 v). Intended for indoor use only.
- Do NOT open the device. Opening or removing covers can expose dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.



External Buttons

The SR400ac gateway provides push-button controls on its exterior for critical features. These buttons provide a convenient means to trigger WPS mode, toggle the WiFi radios on and off, or reset the gateway. The button functions are described below.

WPS Button (5 GHz Band)

WiFi Protected Setup^M (WPS) is a standard means for creating secure connections between the gateway and various wireless client devices. It is designed to simplify the pairing process between devices. This button is located on the left side of the SR400ac gateway.

Press this button for 1-3 seconds, the **5 GHz** LED starts to flash. If no client pairs with the gateway after 2 minutes, the **5 GHz** LED turns off.

When the gateway pairs successfully with a client, the 5 GHz LED glows solid for 5 minutes and then turns off.

WiFi Button (2.4 GHz Band)

The WiFi button toggles the 2.4 GHz WiFi radio on and off. This button is located on the left side of the SR400ac gateway. Look at the 2.4 GHz LED indicator to determine the current state of the WiFi radio.

To activate the radio, press and hold the WiFi button for 3-5 seconds then release. Expect a 1-3 second delay before the 2.4 GHz LED turns on. The WiFi radio is now on.

To deactivate the radio, press and hold the WiFi button for 3-5 seconds then release. Expect a 1-3 second delay before the 2.4 GHz LED turns off. The WiFi radio is now off.

On/Off Button

The On/Off button turns the gateway on and off. This button is located on the left side of the gateway.

Reset Button

The **Reset** button returns the gateway to its default settings.

This button is in a small circular hole in the back of the gateway case with the actual button mounted behind the surface. This style of push button prevents the gateway from being inadvertently reset during handling.

Warning: Do not press the Reset button unless you want to clear the current settings.

To restore the default settings, insert a thin wire (such as a paper clip) into the hole, press the **Reset** button for 1 second, then release the button. The gateway reboots and returns to the current defaults.

To return the gateway to factory default settings, press the **Reset** button until the LEDs flash red and orange. The gateway reboots and returns to the default settings applied in the factory. This process may take a few minutes.



Installing your SR400ac Gateway

- 1. Connect a LAN port on the SmartRG gateway to a PC using an Ethernet cable.
- 2. To connect a broadband device (such as a cable modem):
 - a. Connect one end of an Ethernet cable to the WAN port on the SmartRG gateway and connect the other end of the cable to the broadband modem.
 - b. Connect one end of the supplied silver cable to the broadband modem and connect the other end of the cable to the wall jack installed by your provider.
- 3. Plug the power adapter to the wall outlet and then connect the small end of to the **Power** port on the back of the gateway.
- 4. Turn on the unit by pressing the Power button on the side of the gateway.

The gateway is now automatically being set up to connect to the Internet. This process may take a few minutes to complete before you can begin using your Internet applications (browser, email, etc.).

If connection to the Internet is unsuccessful, verify that all cable connections are in place and the gateway's power is turned on.





Logging in to the SR400ac Interface

To manually configure the SR400ac gateway, you must access the gateway's Web-based UI.

- 1. Configure your computer's IP interface to acquire an IP address automatically using DHCP.
- 2. Open a browser and enter the gateway's default address: http://192.168.1.1 in the address bar. The sign-in page appears.

	SMART/RG°
	Please enter sign in credentials
	admin
	a password
	Sign in
Forgot	password?

- 3. Enter the default username and password.
 - For the administrator user, these are "admin" and "admin".
 - For the support user, these are "support" and the last three octets of the MAC address. The MAC address is located on a label on the back of the gateway. Make sure to enter the letters in all caps and include the separating colons (e.g., AA:BB:CC).

To review the end user license agreement, click the License Agreement link at the bottom right corner of the browser window. The agreement appears in a separate tab.

Note: If you have forgotten the password, click **Forgot password**? and follow the instructions to reset the gateway to the factory defaults. Then, enter the credentials provided with the gateway when it first arrived.

4. Click Sign In. The Dashboard page appears, showing data about your system.



User Preferences

The top of the screen displays various options that are always present:

- Next to the logo in the upper-left is the Menu button (🚐). Click to minimize or reveal the left navigation menu.
- To the right is a **Search** box which returns a list of pages that match the search terms entered. Click the page name that you want to view.
- Next is the Dark Mode icon (
). Click to engage an alternate color scheme for the UI. The icon changes to the Light Mode icon (
). Click to return to the original color scheme.
- Next is the Language icon (). Click to select the preferred interface language from the list.
- The far right corner displays the username currently logged in (typically "Admin"). Click the name to reveal a list of additional preferences.



The preferences under the **User Profile** link to options found under **Admin** in the left menu.

- Settings: Save or load a router configuration file. Go to instructions.
- Passwords: Change passwords for gateway access. <u>Go to</u> instructions.
- **Reboot:** Initiate a reboot of the gateway. <u>Go To instructions</u>.
- Logout: Ends the current session with the gateway.

The page footers display the WAN IP address and firmware version. Mouse over the labels to view the details.



Saving Your Changes

When you change settings, the Pending changes dialogue appears at the top of the page.



Changes made on a page must be applied before you can navigate to a different page.

The circled number shown at left indicates the quantity of changes waiting to be applied. To view a list of your unsaved changes, click the circled number. The Unsaved Changes pop-up window appears.

insaved Changes						
TYPE	CONFIG	SECTION	OPTION	OLD VALUE	NEW VALUE	ACTIONS
SET	iptv	cfg0467f2	fastleave	1	0	Î
						Cancel
						Cancel

To undo a change in the list, click the **trash can** icon in the far right column for the line item to be cancelled. If you remove all of the changes from the change list, the Unsaved Changes window closes and you can proceed to another page.



Dashboard

When you log in to the gateway, the following Dashboard landing page appears. On this page, you can view the IP address, route, number of connected devices, WAN and WiFi traffic, device and system information, system status, and memory statistics. You can also reach this page by clicking **Dashboard** in the left menu.

At the top right of the page, you will find the number of Intellifi devices connected to your gateway plus the View Intellifi topology button that will take you to the Intellifi Devices page.

A list of top talkers appears below the WiFi information.

- To sort this table, click on any of the headings.
- The Minimum rate field appears at the top right of the Top Talkers frame. You can select a different transmission rate. Options are None, 0.01M, 0.1M, 1M, 10M, and 100M. The default is 0.01M.

In the footer of each page are the WAN IP address and the firmware version. Mouse over the labels to view the information.



Network

In this section, you can view and configure information about your gateway connections.



Status

On this page, you can view the status and detailed information for gateway connections.

In the left menu, click Network > Status. The following page appears.

SMART/RG	=	Q Search							🔺 🤇 🤀 😂 Adri
2 Dashboard		Network S	itatus						네 View charts 😋 Restart Network
R Network	~	Network							
Status		Network	Interfaces						
Ethernet WAN		NAME	STATUS	PROTOCOL	IPV4 ADDRESS/MASK	IPV6 ADDRESS/MASK		DEFAULT ROUTE	IPV6 PREFIX
LAN Network Guest Network	3	WAN	UP	DHCP	192.168.1.152/24	2603-9000:d804:7055:ea2	0c:6d#f#e29:78d0/64	192.168.1.1, fe80::9691:7fff.fe78:c348	N/A
Video Network	5	LAN	UP	STATIC	192.168.65.1/24	fdbf:9983:ed4a:0:ee42:34	a6:2b27:59ab/64	N/A	fdb//9983:ed4a::/64
Multicast	2	01000		CT.1710	1001000101			A.12	A14
Frewall	5	GOEST		SIAIIC	192,100.2,1724	204		N/A	N/A
WIFI	2	Interface	Statistics						
Devices									
Services		NAME		LINK STAT	re i i i i i i i i i i i i i i i i i i i	SPEED	TX PACKETS	RX F	PACKETS
Admin		WAN		CP.		1000F	22112	410	86
		LANT		DOWN		a)	, ë	0	
		LANZ		(ur)		1000F	47970	318	85
10000000000000000									

To restart your network, click the **Restart Network** button at the upper right. The confirmation message appears. Click **Ok**, **restart** to proceed. The **STATUS** column for WAN may briefly change to **PENDING** and then back to the previous status.

To view detailed transmission data for the individual interfaces, click the **View Charts** button at the upper-right. The netdata window opens in a new tab, showing information about the overall SR400ac system, memory, CPUs, firewall, IPv4 networking, etc. Use the navigation menu at right to select the statistics that you want to view.

Ethernet WAN

On this page, you can configure WAN settings for connecting to the Internet via Ethernet.

To access this page, click Network > Ethernet WAN in the left menu. The following page appears, showing the Internet settings.



SMART/RG*	=	Q Search
Dashboard		Ethernet WAN
Network	÷	
Status		WAN Services
Ethernet WAN		
LAN Network	>	Internet IPTV Management Cross-Connect
Guest Network	2	internet in the management story connects
Video Network	×:	
Multicast		
Routing	>	Internet Service
Firewall	2	
🕈 WIFI	>	Enabled
Devices	×	Tag mode Untagged
Brandissan	Q.	
Routing	Σ.	MAC Address 58-20-60-29-78-00
Firewall	5	E0.24.00.427.70.00
WIFI	5	
Devices		
Riverburgs	- 6	IPv4 Configuration
Routing	5	
Firewall	>	Configuration method DHCP -
WIFI	2	Hostname \$8400ar.7800
Devices	2	
Anoraleanas	12	Create Default Route
Routing	30	
Firewall	2	Allow DNS server list
WIFI	×.	override
Devices	5	
mandauas	8	D. C. C. Constanting
Routing	20	IPv6 Configuration
Firewall	>	
WIEI	2	Configuration method DHCPv6 •
and when the second sec		

By clicking the buttons across the top of the page, you can select and configure the following WAN services.

Internet IPTV		Management	Cross-Connect	
Internet				

- 1. After selecting Network > Ethernet WAN in the left menu, the Ethernet WAN page appears, showing the Internet settings.
- 2. By default, the Internet Service is enabled. To disable the Internet feature, click the slide button next to Enabled.
- 3. Configure the tagging options:
 - a. In the **Tag mode** field, select the type of tagging that should be performed. Options are **Untagged**, **Tagged**, and **DQTagged**. The default is **Untagged**.
 - b. If **Tagged** or **DQTagged** is selected, the **VLAN** and **P-bit** fields appear. Enter the ID of the appropriate VLAN. Valid values are 1 4079. The default is 2. Enter the P-bit type. Options are 0 7. The default is 0.



- c. If **DQTagged** is selected, the **CVID** field also appears. Enter the Customer VLAN ID or the first in a range of CVIDs that will be accepted and mapped to the specified WAN. Valid values are 1 4062. The default is 0.
- 4. (Optional) In the MAC Address field, enter the MAC address that to be used with this configuration. By default, this value is set to the gateway MAC address.
- 5. Complete the fields for IPv4 Configuration and IPv6 Configuration sections as they apply to your environment, using the information provided below.
 - a. In the **Configuration method** field, select the appropriate method for your WAN.

Options for IPv4 WANs are DHCP, Static Address, and PPPoE. The default is DHCP.

Options for IPv6 WANs are DHCPv6, Static Address, and None. The default is DHCPv6.

- b. Complete the remaining fields as instructed below for each option:
 - "DHCP for IPv4 WANs" (IPoE)
 - "Static Address for IPv4 WANs"
 - "PPPoE for IPv4 WANs"
 - "DHCPv6 for IPv6 WANs"
 - "Static Address for IPv6 WANs"
- c. To disable the default route for this WAN, click the slide button to the right of Create default route.
- 6. Click the Apply button in the Pending changes... dialogue to save your settings.

DHCP for IPv4 WANs

The following fields appear when DHCP is selected as the configuration method. This method is the default for IPv4 WANs.

IPv4 Configuration	
Configuration method	DHCP
Hostname	SR400ac-1520
Create Default Route	
Allow DNS server list override	

- 1. To use a different host, enter the desired host name to be included in DHCP requests in the Hostname field.
- 2. To disable the default route for this WAN, click the slide button to the right of Create default route.
- 3. To allow override of the DNS server list, click the slide button next to Allow DNS server list override.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.



Static Address for IPv4 WANs

The following fields appear when **Static Address** is selected as the configuration method.

IPv4 Configuration	
Configuration method	Static Address 👻
Address	IPv4 Address
Subnet mask	Subnet Mask
Default route	Route
Create default route	••

- 1. Complete the fields using the information in the table below.
- 2. To disable the default route for this WAN, click the slide button to the right of Create default route.
- 3. Click the Apply button in the Pending changes... dialogue to save your settings.

The fields for this option are explained in the table below.

Field	Description
Address	Enter the IP address for IPv4 communications (such as 192.168.1.44).
Subnet mask	Enter the IP address for the subnet mask.
Default route	Enter the IP address for the default IPv4 route.

PPPoE for IPv4 WANs

The following fields appear when **PPPoE** is selected as the configuration method.



IPv4 Configuration			
Configuration method	РРРОЕ	•	
Username	Username		
Password	Password	0	
Access concentrator	Auto		?
Service name	Auto		?
Allow DNS server list override			

- 1. To access LCP and PPP settings, click the down arrow next to Advanced.
- 2. Complete the fields using the information in the table below. To configure
- 3. Click the Apply button in the Pending changes... dialogue to save your settings.

The fields for this option are described in the following table.

Field	Description
Username	Enter the user ID for this WAN.
Password	Enter the password for this WAN. To view the password characters, click the Show icon (④).
Access concentrator	Enter the name of the concentrator application. To have the system detect this automatically, accept the default of Auto
Service name	Enter the name of the service for this interface. To have the system detect this automatically, accept the default of Auto
Allow DNS server list override	(<i>Optional</i>) To <i>allow</i> override of the DNS server list, click this slide button . To <i>prevent</i> override, click the slide button again.
Advanced section	
LCP Echo Interval	Enter the interval for sending echos in seconds. Options are None and 1 - 60 seconds. The default is None .
LCP Echo Retry	Enter the number of ping retries before the connection is identified as down. The default is None .
PPP Persist	PPP persistent dialing ensures that a dropped call link is rebuilt. To <i>enable</i> PPP persistence, click the slide button.
PPP Holdoff	Enter the number of seconds before attempting to reconnect a dropped call. The default is zero (0).



Field	Description
Allow DNS server list override	(<i>Optional</i>) To <i>allow</i> override of the DNS server list, click this slide button. To <i>prevent</i> override, click the slide button again.

DHCPv6 for IPv6 WANs

The following fields appear when **DHCPv6** is selected as the configuration method. This method is the default for IPv6 WANs.

IPv6 Configuration		
Configuration method	DHCPv6	
DHCPv6 Client Mode	Autoconfig -	
Request Prefix Length	Auto	
Prefix Hint	e.g. 1234	
Allow DNS server list override		

- 1. Complete the fields using the information in the table below.
- 2. Click the Apply button in the Pending changes... dialogue to save your settings.

The fields for this option are described in the following table.

Field	Description
DHCPv6 Client Mode	Select the mode for the DHCPv6 client. Options are:
	• Autoconfig: Attempt to use the DHCP server for configuration. If no IP address is provided, then use SLACC for configuration. This is the default.
	• Stateful: Use only the IP address provided by the DHCP server.
	Stateless: Use only SLACC for configuration.
Request Prefix Length	Select the length of the prefix sent with the request. Options are Auto, 48, 52, 56, 59 - 64 , and None . The default is Auto .
Prefix Hint	Enter the 4-digit hint for the subprefix ID.
Allow DNS server list override	(Optional) To allow override of the DNS server list, click this slide button. To prevent override, click the slide button again.



Static Address for IPv6 WANs

The following fields appear when **Static Address** is selected as the configuration method.

IPv6 Configuration	
Configuration method	Static Address 🔹
Address	IPv6 Address
Gateway	Default Route

- 1. Complete the fields using the information in the table below.
- 2. Click the Apply button in the Pending changes... dialogue to save your settings.

Complete the fields using the information in the table below.

Field	Description
Address	Enter the static address for IPv6 communications (such as 2001:db8:a0b:12f0::1).
Gateway	Enter the IP address for the default IPv6 route.

IPTV

On this page, you can configure the IPTV settings for your Ethernet WAN.



- 1. In the left menu, click Network > Ethernet WAN. The Ethernet WAN page appears showing the Internet settings.
- 2. Click the **IPTV** button. The following page appears.

2 Dashboard		Ethernet WAN				
So Network	*		WAN Services			
Status			That Services			
Ethernet WAN						
LAN Network	3 6		Internet	IPTV	Management	Cross-Connect
Guest Network	2					
Multicast	S.					
Routing	30		IPTV Service			
Firewall	5					
🗢 WiFi	5		Enabled	0		
Devices						
			Tag mode	Tagged		-
Services	2					
🖸 Admin	>		VLAN	3		
						1.12
			P-Dit	0		0
			IPv4 Configuration			
			-			
			Configuration method	DHCP		-
			Hostname	Hostname		
			Create Default Route			

- 3. To *enable* the IPTV feature, click the slide button to the right of Enabled.
- 4. Configure the tagging options:
 - a. In the **Tag mode** field, select the type of tagging that should be performed. Options are **Untagged** and **Tagged**. The default is **Tagged**.
 - b. If **Tagged** is selected, the **VLAN** and **P-bit** fields appear. Enter the ID of the appropriate VLAN. Valid values are 1 4079. The default is 3. Enter the P-bit type. Options are 0 7. The default is 0.
- 5. In the IPV4 Configuration section, configure the settings using the information in "DHCP for IPv4 WANs" and "Static Address for IPv4 WANs".
- 6. Click the Apply button in the Pending changes... dialogue to save your settings.



Management

On this page, you can configure the settings for managing your network and the devices connected to it.

- 1. In the left menu, click Network > Ethernet WAN. The Ethernet WAN page appears showing the Internet settings.
- 2. Click the Management button. The following page appears.

Ð	Dashboard		Ethernet WAN			
**	Network	~				
	Status			WAN Services		
	Ethernet WAN					
	LAN Network	>		Internet	IPTV Management	Cross-Connect
	Guest Network	2				
	Video Network	>				
	Multicast	2				
	Routing	>		Management Service		
	Firewall	>				
•	WIFI	>		Enabled		
	Devices	>		Tag mode	Tagged	
D	Services	>				
D	Admin	Σ		VLAN	6	
				P-bit	0	۲
				IPv4 Configuration		
				Configuration method	DHCP	×
				Hostname	Hostname	
				Create Default Route		

- 3. Configure the tagging options:
 - a. In the Tag mode field, select the type of tagging that should be performed. Options are Untagged, Tagged, and DQTagged. The default is Tagged.
 - b. If Tagged or DQTagged are selected, the VLAN and P-bit fields appear. Enter the ID of the appropriate VLAN. Valid values are 1 4079. The default is 6. Enter the P-bit type. Options are 0 7. The default is 0.
 - c. If **DQTagged** is selected, the **CVID** field also appears. Enter the Customer VLAN ID or the first in a range of CVIDs that will be accepted and mapped to the specified WAN. Valid values are **1 4062**. The default is **0**.
- 4. In the IPV4 Configuration section, configure the settings using the information in "DHCP for IPv4 WANs", "Static Address for IPv4 WANs", or "PPPoE for IPv4 WANs".
- 5. In the IPV6 Configuration section, configure the settings using the information in "DHCPv6 for IPv6 WANs" and "Static Address for IPv6 WANs".
- 6. Click the Apply button in the Pending changes... dialogue to save your settings.



Cross-Connect

On this page, you can configure bridge settings for traffic moving from a WAN-side VLAN to a LAN port. This can be used for bridged IPTV or other services.

- 1. In the left menu, click Network > Ethernet WAN. The Ethernet WAN page appears showing the Internet settings.
- 2. Click the Cross-Connect button. The following page appears.

Dashboard		Ethernet WAN				
	101	Luiemet WAN				
network	Č.		WAN Services			
Status			1500-70704005			
Ethernet WAN						01
LAN Network	>		Internet	IPTV	Management	Cross-Connect
Guest Network	>					
Video Network	2					
Multicast	>					
Routing	2		Cross-Connect Ser	vice		
Firewall	×					
😧 WIFI	×.		Enabled			
Devices	>		Tag mode	Transd		
Services	>		ing mode	192260		
O Admin	3		VLAN	5		
			P-bit	0		0

- 3. Configure the tagging options:
 - a. In the Tag mode field, select the type of tagging that should be performed. Options are Untagged, Tagged, and DQTagged. The default is Tagged.
 - b. If **Tagged** or **DQTagged** is selected, the **VLAN** and **P-bit** fields appear. Enter the ID of the appropriate VLAN. Valid values are 1 4079. The default is 5. Enter the P-bit type. Options are 0 7. The default is 0.
 - c. If **DQTagged** is selected, the **CVID** field also appears. Enter the Customer VLAN ID or the first in a range of CVIDs that will be accepted and mapped to the specified WAN. Valid values are 1 4062. The default is 0.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.



LAN Network

In this section, you can view and configure information about the DHCP server, DHCP clients and Ethernet ports.

1. In the left menu, click Network > LAN Network. The following page appears.

SI	MART/RG°	II	Q Search			
æ	Dashboard		LAN Network			
器	Network	~				
	Status			IPv4 Configuration		
	Ethernet WAN					
	LAN Network	*		IP Address	192.168.65.1	
	DHCP Server					
	DHCP Clients			Subnet mask	255.255.255.0	
	Ethernet Ports					
	Guest Network	>		Create default route		
	Video Network	>				
	Multicast	×				_
	Routing	>				
	Firewall	•		IPv6 Configuration		
(;	WiFi	>				
۵	Devices			Enabled	•	
D	Services	>		Prefix length	64	3
0	Admin	>				
				Suffix	Random	

- 2. Fill in the fields using the information in the table below.
- 3. Click the Apply button in the Pending changes... dialogue to save your settings.

Field	Description
IPv4 Configuration section	
IP Address	Enter the IP address for IPv4 communications (such as 192.168.1.44). The default is the address assigned to the gateway.
Subnet mask	Enter the IP subnet mask for this gateway. The default is 255.255.255.0 .
Create default route	(Optional) To create the default route for this LAN, click the slide button.
IPv6 Configuration section	
Enabled	This option is <i>enabled</i> by default. To <i>disable</i> IPv6 address configuration, click the slide button to the right of Enabled. The Prefix length and Suffix fields are hidden.
Prefix length	Enter the prefix length for this IPv6 address. Options are 0 - 64 . The default is 64 .



Field	Description
Suffix	Select the interface identifier for this IPv6 address. Options are Random , MAC Based , and Suffix Address. The default is Random .
	If you select Suffix Address , the Suffix Address field appears. Enter the address in format: "::a:b:c:d".

DHCP Server

On this page, configure the DHCP settings for the gateway. The Dynamic Host Control Protocol Server (DHCP) feature of this gateway will automatically assign LAN IP addresses to host devices as they connect.



SI	MART/RG°	=	Q Search						
Ð	Dashboard		LAN DHCP Server						
묾	Network	~		Loose Configuration					
	Status			Lease Configuration					
	Ethernet WAN								
	LAN Network	~		Lease duration:	1 Hour			•	
	DHCP Server								
	DHCP Clients								
	Ethernet Ports								
	Guest Network	>		DHCPv4 Configuration	n				
	Video Network	>							
	Multicast			Enabled					
	Routing	2							
	Firewall	ĺ.		Pool start	100				
÷	WiFi	>							
	Devices	>		Pool size	150				
	Services								
	Services								
0	Admin	>							
				DHCPv6 Configuration	n				
				Tradid					
				Enabled					
				Pouter advertisement	Managed				
				Router auvertisement	Manageu				
				DHCP Custom DNS Se	ervers				+ Add DNS
				- IP)	NUNE22				ACTIONS
				DHCP Static Association	ons				+ Add host
				# DEVICE NAME	MAC ADDRESS	IP ADDRESS	IPV6 DUID	IPV6 HOST ID	ACTIONS

1. In the left menu, click Network > LAN Network > DHCP Server. The following page appears.

- 2. Fill in the fields using the information in the table below.
- 3. Click the Apply button in the Pending changes... dialogue to save your settings.

Field	Description			
Lease duration	Select the amount of time for which an IP address will be leased. Options range from 5 minutes to 24 hours . The default is 1 hour .			
DHCPv4 Configuration section				
Enabled	This feature is <i>enabled</i> by default. To <i>disable</i> this feature, click this slide button .			



Field	Description				
Pool start	Enter the beginning of the class-C IP address range to be assigned by the DHCP server. The default is 100 .				
Pool size	Enter the size of the DHCP pool. The maximum size allowed is 252 . The default is 150 .				
DHCPv6 Configuration se	ection				
Enabled	This feature is <i>enabled</i> by default. To <i>disable</i> this feature, click this slide button.				
Router advertisement	Select how this gateway will be advertised through this DHCPv6 server. Options are:				
	• Assisted: Advertises this gateway with all configuration, with stateless auto-configuration, or both.				
	• Managed: Advertises this gateway with all configuration. This is the default.				
	Unmanaged: Advertises this gateway with only stateless auto-configuration.				
Custom DNS Servers	(Optional) To define a custom DNS server, follow the steps in "Defining a Custom DNS Server".				
DHCP Static Associations	(<i>Optional</i>) To define a static DHCP server, follow the steps in "Defining a Static DHCP IP Address Association".				

Defining a Custom DNS Server

If desired, you can define custom DNS servers.

1. To define a custom DNS server, click + Add DNS to the right of the DHCP Custom DNS Servers section heading. The Add Custom DNS Server dialog box appears.

Add Custom DNS Server		×
IP Address Enter IP Address		
	Close	Save changes

- 2. Enter the IP address of the host device (such as 192.168.1.44).
- 3. Click Save changes to commit your changes.

To add another DNS server, repeat Steps 1-3.

To edit a static DHCP IP address, click the Edit () icon next to it. The Add/Edit dialog box appears. Change the entries as needed and click Save Changes to commit your changes.

To remove a custom server IP address, click the Delete icon ()next to it.



Defining a Static DHCP IP Address

Association

If desired, a static IP address may be associated with the MAC address of a specific LAN host device.

1. To select a LAN client device, click + Add host to the right of the DHCP Custom DNS Servers section heading. The Add Custom DNS Server dialog box appears.

Add/Edit DHCP Static Associa	tion	×
Connected hosts		
No host selected		Ψ.
Device Name		
Hostname		
MAC Address		
MAC		
IP Address		
IPv4 Address		
IPv6 DUID		
IPv6 Duid		
IPv6 Host ID		
IPv6 Host ID		
	Close	Save changes

- 2. Enter the IP address of the host device (such as 192.168.1.44).
- 3. Click Save changes to commit your changes.

To add another static DHCP configuration, repeat Steps 1-3.

To edit a static DHCP IP address, click the Edit () icon next to it. The Add/Edit dialog box appears. Change the entries as needed and click Save Changes to commit your changes.

To remove a static DHCP IP address, click the **Delete** icon ()next to it.

Click the Apply button in the Pending changes... dialogue to save your settings.



DHCP Clients

On this page, you can view the IPv4 and IPv6 DHCP clients connected to your LAN.

In the left menu, click Network > LAN Network > DHCP Clients. The following page appears.

SMART/RG*	=	Q Se	arch				•	C 🖶 🕘 Admin
Dashboard		LAN C	OHCP Clients					
Retwork	~							
Status		DHO	CPv4 Clients					
Ethernet WAN			IP ADDRESS	MAC ADDRESS	HOSTNAME		EXPIRES	
LAN Network DHCP Server	~	1	192.168.65.187	c8:f7:50:b4:61:c1	kdadamo7390w1	D	4/17/2020, 9:58:13	AM America/Vancouver
DHCP Clients								
Ethernet Ports		DHO	CPv6 Clients					
Guest Network	>							
Video Network	>	1.1	IP ADDRESS	DUID	HW ADDRESS	HOSTNAME	EXPIRES	
Multicast	×	1	fdbf:9983:ed4a:0:ee42:34a6:0:a75/128	0001000123fbbe039cebe8b05c6a		kdadamo7390w10	4/17/2020, 8:32:	50 AM America/Vancouver
Routing	X							



Ethernet Ports

On this page, you can select which service to run for each interface defined on your gateway.

1. In the left menu, click Network > LAN Network > Ethernet Ports. The following page appears.

SI	MART/RG°	=	Q Search			
Ð	Dashboard		Ethernet Ports			
8	Network	~				
	Status			Port Isolation		
	Ethernet WAN					
	LAN Network	*		Enabled	-	
	DHCP Server					
	DHCP Clients					
	Ethernet Ports			Dant Canfirmation		
	Guest Network	>		Port Configuration		
	Video Network	>				
	Multicast	>		LAN1	LAN	
	Routing	>				
	Firewall	>		LAN2	LAN	*
Ŷ	WiFi	>				
	Devices	>		LAN3	LAN	•
D	Services	>		LAN4	LAN	•
0	Admin	>			[

- 2. To disable Port Isolation, click the slide button next to Enabled.
- 3. Select an option for each port where a particular service is to be defined. Options are LAN, Guest, Video, Cross-Connect, and None. The default is LAN.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.



Guest Network

On this page, you can configure settings for a guest network.

1. In the left menu, click Network > Guest Network. The following page appears. This feature is enabled by default.

S	MART/RG°	III	Q Search			
Ð	Dashboard		Guest Network			
묾	Network	~				
	Status			Guest Configuration		
	Ethernet WAN					
	LAN Network	>		Enabled		
	Guest Network	~				
	DHCP Server					
	DHCP Clients					
	Video Network	>		IPv4 Configuration		
	Multicast	>				
	Routing	>		Configuration method	Static 👻	
	Firewall	>				
(î-	WiFi	>		IP Address	192.168.2.1	
	Devices	>		Subnet mask	255 255 255 0	
D	Services	>				
0	Admin	>		Create default route		
				IPv6 Configuration		
				Enabled	•	
				Prefix length	64	0
				Suffix	Random	

- 2. To *disable* the guest network feature, click the **slide button** next to **Enabled**.
- 3. Fill in the fields using the information from the table below.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.

Field	Description
IPv4 Configuration secti	on



Field	Description				
Configuration method	Select the appropriate method for your WAN. The page refreshes to show the fields that apply for the selected method. Options are Static , DHCP , and None . The default is Static .				
Fields available for Stat	ic Configuration Method				
IP Address	Enter the IP address for IPv4 communications (such as 192.168.1.44). The default is the address assigned to the gateway.				
Subnet mask	Enter the IP subnet mask for this gateway. The default is 255.255.255.0.				
Create default route	To create a default route for this LAN, click this slide button.				
Fields available for DHC	P Configuration Method				
Hostname	Enter the host name to be included in DHCP requests.				
IPv6 Configuration sect	ion				
Enabled	This feature is <i>enabled</i> by default. To <i>disable</i> IPv6 address configuration, click the slide button to the right of Enabled.				
Prefix length	Enter the prefix length for this IPv6 address. Options are 0 - 64 . The default is 64 .				
Suffix	Select the interface identifier for this IPv6 address. Options are Random , MAC Based , and Suffix Address . The default is Random .				
	When you select Suffix Address , the Suffix Address field appears. Enter the address in format: "::a:b:c:d".				

DHCP Server

On this page, you can configure DHCP server settings for the guest network.



SM	ART/RG [®]	=	Guest DHCP Server			
🙆 Da	ashboard			Lease Configuration		
St.	etwork atus	•		Lease duration:	5 Minutes	
Et	hernet WAN					
LA	AN Network	>				
Gu	uest Network	*		DUCDu4 Configuration		
1	DHCP Server			DHCPV4 Configuration		
	DHCP Clients					
Vi	deo Network	>		Enabled		
M	ulticast	2		Declaration		
Eir	rewall	5		POOLStart	100	
? ₩	/iFi	>		Pool size	150	
D D	evices	>				
0						
C Ad	dmin	>		DHCPv6 Configuration		
				Enabled	•	
				Router advertisement	Managed 👻	
				DHCP Static Associations	+ Add H	lost
				# DEVICE NAME MAC ADDR	ESS IP ADDRESS IPV6 DUID IPV6 HOST ID ACT	IONS

1. In the left menu, click Network > Guest Network > DHCP Server. The following page appears.

- 2. Fill in the fields using the information in the table below.
- 3. Click the Apply button in the Pending changes... dialogue to save your settings.

Field	Description			
Lease duration	Select the amount of time for which an IP address will be leased. Options range from 5 minutes to 24 hours. The default is 5 minutes .			
DHCPv4 Configuration see	ction			
Enabled	This feature is <i>enabled</i> by default. To <i>disable</i> this feature, click the slide button .			
Pool start	Enter the beginning of the class-C IP address range to be assigned by the DHCP server. The default is 100 .			
Pool size	Enter the size of the DHCP pool. The maximum size allowed is 252 . The default is 150 .			
DHCPv6 Configuration see	ction			
Enabled	This feature is <i>enabled</i> by default. To <i>disable</i> this feature, click the slide button.			



Field	Description			
Router advertisement	Select how this gateway will be advertised through this DHCPv6 server. Options are:			
	 Assisted: Advertises this gateway with all configuration, with stateless auto-configuration, or both. Managed: Advertises this gateway with all configuration. This is the default. Unmanaged: Advertises this gateway with only stateless auto-configuration. 			
DHCP Static Associations	(<i>Optional</i>) To define a static DHCP server, follow the steps in "Defining a Static DHCP IP Address Association".			

Defining a Static DHCP IP Address Association

If desired, a static IP address may be associated with the MAC address of a specific LAN host device.

1. To select a LAN client device, click + Add host to the right of the DHCP Static Associations section heading. The Add/Edit DHCP Static Association dialog box appears.

Add/Edit DHCP Static Associatio	on	3	×
Connected hosts			
No host selected		•	
Device Name			
Hostname			
MAC Address			
MAC			
IP Address			
IPv4 Address			
IPv6 DUID			
IPv6 Duid			
IPv6 Host ID			
IPv6 Host ID			
	Close	Save changes	



- 2. When you select a connected host, the fields in the dialog box are populated with the necessary information. If the host is currently offline or you select **None** in this field, you must enter the information manually.
- 3. Complete the fields, using the
- information in the table below.
- 4. Click Save changes to commit your changes.

The fields in this section are described in the following table.

Field	Description
Device Name	Enter a name for the host device.
MAC Address	Accept the displayed address or enter the MAC address of the host device (such as 00:23:6A:A3:7C:C3). The MAC address of the device selected in Step 1 appears in this field.
IP Address	Accept the displayed address or enter the IP address of the host device (such as 192.168.1.44). The IP address of the device selected in Step 1 appears in this field.
IPv6 DUID	Enter the DHCP Unique Identifier (DUID) for the IPv6 server.
IPv6 Host ID	Enter the ID for the IPv6 server.

To add another static DHCP configuration, repeat Steps 1-4.

To edit a static DHCP IP address, click the Edit () icon next to it. The Add/Edit dialog box appears. Change the entries as needed and click Save Changes to commit your changes.

To remove a static DHCP IP address, click the **Delete** icon ()next to it.

Click the Apply button in the Pending changes... dialogue to save your settings.

DHCP Clients

On this page, you can view the IPv4 and IPv6 DHCP clients connected to your gateway.

In the left menu, click Network > Guest Network > DHCP Clients. The following page appears.

SMART/RG°	ll.	Q Search	1				▲ C ⊕ (🕘 Admin
🙆 Dashboard		Guest DI	HCP Clients					
So Network	~							
Status		DHCPv4	4 Clients					
Ethernet WAN			IP ADDRESS	MAC A	DDRESS	HOSTNAME	EXPIRES	
LAN Network	>							
Guest Network DHCP Server	ř	DHCPv	6 Clients					
DHCP Clients		1.0	IP ADDRESS	DUID	HW ADDRESS	HOSTNAME	EXPIRES	
Video Network	>							
Multicast	>	man						



Video Network

In this section, you can configure WAN settings for video data.

1. In the left menu, click Network > Video Network. The following page appears. This feature is disabled by default.

SM	1art/rg°	=	Q Search		
Ð	Dashboard		Video Network		
器	Network	~			
	Status			Video Configuration	
	Ethernet WAN				
	LAN Network	>		Enabled	
	Guest Network	>			
	Video Network	*			
	DHCP Server				
	DHCP Clients			IPv4 Configuration	
	Multicast	>			
	Routing	>		Configuration	Static 👻
	Firewall	>		method	
(î	WiFi	>			
	Devices	,		IP Address	192.168.3.1
	Denet S				
þ	Services	>		Subnet mask	255.255.255.0
•	Admin	>		Create default route	()

- 2. To enable this feature, click the slide button to the right of Enabled.
- 3. In the **Configuration method** field, select the appropriate method for your WAN. Options are **Static**, **DHCP**, and **None**. The default is **Static**. The page refreshes to show the fields that apply for the selected method. If you select **None**, the other fields are hidden.
- 4. Fill in the other fields as explained below for each option:
 - "Static"
 - "DHCP"
- 5. Click the Apply button in the Pending changes... dialogue to save your settings.

Static

When you select Static in the Configuration method field, the following fields appear.



SMAR	T/RG°	=	Q Search		
🔁 Dashb	oard		Video Network		
😤 Netwo	rk	~			
Status				Video Configuration	
Etherne	et WAN				
LAN Ne	twork	>		Enabled	
Guest N	Vetwork	>			
Video N	letwork	*			
DHC	Server				
DHCF	Clients			IPv4 Configuration	
Multica	st	>			
Routing	5	>		Configuration	Static -
Firewal	1	>		method	
穼 WiFi		>		ID Address	
Device	s	>		IP Address	192.168.3.1
				Subnot mack	
🖵 Service	25	>		Subher mdSK	255.255.255.0
🚺 Admin		>		Create default route	

- 1. Modify the fields using the information in the table below.
- 2. Click the Apply button in the Pending changes... dialogue to save your settings.

Field	Description
Address	Enter the IP address for IPv4 communications (such as 192.168.1.44).
Subnet mask	Enter the IP address for the subnet mask.
Create default route	To create a default route for this WAN, click the slide button next to Create default route.

DHCP

When you select **DHCP** in the **Configuration method** field, the following fields appear.


IPv4 Configuration	
Configuration method	DHCP -
Hostname	Hostname
Create default route	

- 1. (Optional) In the Hostname field, enter the host name to be included in DHCP requests.
- 2. To create a default route for this WAN, click the slide button for Create default route.
- 3. Click the Apply button in the Pending changes... dialogue to save your settings.

DHCP Server

On this page, you can configure DHCP settings for the video network.



S	MART/RG°	=	Q Search			
æ	Dashboard		Video DHCP Server			
묾	Network	~		Lease Conferentian		
	Status			Lease Configuration		
	Ethernet WAN					
	LAN Network	>		Lease duration:	5 Minutes	•
	Guest Network	>				
	Video Network	~				
	DHCP Server					
	DHCP Clients			DHCPv4 Configuration		
	Multicast	>				
	Routing	>		Enabled		
	Firewall	>				
ĉ	WiFi	>		Pool start	100	
۵	Devices	>				
	Sanvicas	5		Pool size	150	
	Services					
0	Admin	>				
				DHCBy6 Configuration		
				DHCFV6 Configuration		
				Enabled		
				DHCP Static Associations		+ Add host
				# DEVICE NAME MAC ADDE	RESS IP ADDRESS IPV6 DUID II	PV6 HOST ID ACTIONS

1. In the left menu, click Network > Video Network > DHCP Server. The following page appears.

- 2. Fill in the fields using the information in the table below.
- 3. Click the Apply button in the Pending changes... dialogue to save your settings.



Field	Description					
Lease duration	Enter the amount of time for which an IP address will be leased. Options range from 5 minutes to 24 hours . The default is 5 minutes .					
DHCPv4 Configuration se	ction					
Enabled	This feature is <i>enabled</i> by default. To <i>disable</i> this feature, click the slide button.					
Pool start	Enter the beginning of the class-C IP address range to be assigned by the DHCP server. The default is 100.					
Pool size	Enter the size of the DHCP pool. The maximum size allowed is 252 . The default is 150 .					
DHCPv6 Configuration se	ction					
Enabled	This feature is <i>disabled</i> by default. To <i>enable</i> this feature, click the slide button.					
Router advertisement	(Appears when Enabled is set to On) Select how this gateway will be advertised through this DHCPv6 server. Options are Assisted, Managed, and Unmanaged. The default is Managed.					
	The Assisted option advertises this router with all configuration through a DHCPv6 server <i>and/or</i> stateless auto configuration.					
DHCP Static Associations	(<i>Optional</i>) To define a static DHCP server, follow the steps in "Defining a Static DHCP IP Address Association".					

Defining a Static DHCP IP Address Association

If desired, a static IP address may be associated with the MAC address of a specific LAN host device.

1. To select a LAN client device, click + Add host to the right of the DHCP Static Associations section heading. The Add/Edit DHCP Static Association dialog box appears.



Add/Edit DHCP Static Associa	tion	×
Connected hosts		
No host selected		•
Device Name		
Hostname		
MAC Address		
MAC		
IP Address		
IPv4 Address		
IPv6 DUID		
IPv6 Duid		
IPv6 Host ID		
IPv6 Host ID		
	Close	Save changes

- 2. When you select a connected host, the fields in the dialog box are populated with the necessary information. If the host is currently offline or you select **None** in this field, you must enter the information manually.
- 3. Complete the fields, using the information in the table below.
- 4. Click Save changes to commit your changes.

The fields in this section are described in the following table.

Field	Description
Device Name	Enter a name for the host device.
MAC Address	Accept the displayed address or enter the MAC address of the host device (such as 00:23:6A:A3:7C:C3). The MAC address of the device selected in Step 1 appears in this field.
IP Address	Accept the displayed address or enter the IP address of the host device (such as 192.168.1.44). The IP address of the device selected in Step 1 appears in this field.
IPv6 DUID	Enter the DHCP Unique Identifier (DUID) for the IPv6 server.
IPv6 Host ID	Enter the ID for the IPv6 server.



To add another static DHCP configuration, repeat Steps 1-4.

To edit a static DHCP IP address, click the Edit () icon next to it. The Add/Edit dialog box appears. Change the entries as needed and click Save Changes to commit your changes.

To remove a static DHCP IP address, click the **Delete** icon ()next to it.

Click the Apply button in the Pending changes... dialogue to save your settings.

DHCP Clients

On this page, you can view the IPv4 and IPv6 DHCP clients connected to the video network.

In the left menu, click Network > Video Network > DHCP Clients. The following page appears, showing any active video clients.

SMART/RG*	=	Q Search	h				▲ C ⊕ 🙁	Admin
Dashboard		Video DI	HCP Clients					
Network Status	*	DHCPv	4 Clients					
Ethernet WAN LAN Network	>	*	IP ADDRESS	MAC A	DDRESS	HOSTNAME	EXPIRES	
Guest Network Video Network	>	DHCPv	6 Clients					
DHCP Server DHCP Clients			IP ADDRESS	DUID	HW ADDRESS	HOSTNAME	EXPIRES	

Multicast

On this page, you can configure IGMP settings such as the Fast-Leave option and view details of the joined groups including IP address, device name, and bridge ID.



- **SMART/RG°** = **Q** Search Dashboard Multicast 者 Network **IGMP** Configuration Status Ethernet WAN LAN Network Force IGMPv2 Guest Network Enable Fast-Leave Video Network Multicast Video Analyzer Routing **IGMP** Joined Groups Firewall ᅙ WiFi GROUP DEVICE BRIDGE Devices 239.255.255.250 LAN2 br-lan 🖸 Services 239.255.255.250 WIFI2G br-lan 🚺 Admin 239.255.255.250 WIFI5G br-lan
- 1. In the left menu, click Network > Multicast. The following page appears.

(Optional) To disable the IGMPv2 feature, click the slide button next to Force IGMPv2.

(Optional) To disable the Fast-Leave feature, click the slide button next to Enable Fast-Leave.

Click the Apply button in the Pending changes... dialogue to save your settings.

Video Analyzer

On this page, you can configure the IP multicast video streams.

1. In the left menu, click Network > Multicast > Video Analyzer. The following page appears. If video is configured for your gateway, data about the video stream appears in the bottom section of the page.



S	MART/RG°	=	Q Search		
Ð	Dashboard		Video Stream Ar	nalyzer	
묾	Network	~			
	Status			Video Stream Configu	ration
	Ethernet WAN				
	LAN Network	>		Enabled	
	Guest Network	>			
	Video Network	>		Mode	Snoop 👻
	Multicast	~			
	Video Analyzer			IPv4 multicast address	224.0.0.0
	Routing	>			
	Firewall	>			
î	WiFi	>			
	Devices	>		Video Stream Data	
D	Services	>			
0	Admin	>		N	O VIDEO STREAM DETECTED

- 2. To enable this feature, click the slide button to the right of Enabled.
- 3. In the Mode field, select the analyzer mode. Options are Snoop and Join. The default is Snoop.
- 4. (*Optional*) In the IPv4 multicast address field, enter the IP address. Options range from 224.0.0.0 through 239.255.255.255. The default is 224.0.0.0.
- 5. Click the Apply button in the Pending changes... dialogue to save your settings.

In the Video Stream Data section, when a video stream is active, the stream summary is shown along with information about the stream rate, media delivery index, packet header, and PID counters display.

Routing

On this page, you can view the static routes configured for the network (including tables for ARP, IPv4, IPv6, and IPv6 Neighbors). In the left menu, click **Network** > **Routing**. The following page appears.



SMART/RG°	=	Q Search			🜲 🕻 🤀 🖳 Admin
Dashboard		Routing Status			
* Network	~				
Status		ARP Table			
Ethernet WAN		IP ADDRESS		MAC ADDRESS	DEVICE
LAN Network	>	192.168.65.187		c8:f7:50:b4:61:c1	BR-LAN
Video Network	>	192.168.1.1		94:91:7f:78:c3:48	WAN
Multicast Routing	> •	192.168.0.2		00:00:00:00:00:00	BR-LAN
Static Routes DNS Advanced		IPv4 Routing Table			
Downstream QoS		IPV4 ADDRESS	GATEWAY	GENMASK	DEVICE
Firewall	>	0.0.0.0	192.168.1.1	0.0.0.0	WAN
🗢 WIFI	>	25.1.5.0	0.0.0	255,255,255.0	WIFI5G-MESH
Devices	>	192.168.1.0	0.0.0.0	255.255.255.0	WAN
Services	>	192.168.1.1	0.0.0.0	255.255.255.255	WAN
V Admin	>	192.168.2.0	0.0.0.0	255.255.255.0	BR-GUEST
		192.168.65.0	0.0.0.0	255.255.255.0	BR-LAN
		IPv6 Routing Table			
		IPV6 ADDRESS		NEXT HOP	DEVICE
		::/0		fe80::9691:7fff:fe78:c348	WAN

Static Routes

On this page, you can specify the routes over which interface and gateway for a certain host or network can be reached. When several networks are accessible from the gateway, Static Routes become useful to ensure packets get correctly routed between them.

1. In the left menu, click Network > Routing > Static Routes. The following page appears, showing sections for IPv4 Static Routes and IPv6 Static Routes.



SMART/RG	=	Q Search				٠	C 🕀 🙆 Admir
🙆 Dashboard		Static Routes					
Network	~						
Status		IPv4 Static Rout	es				+ Add route
Ethernet WAN		INTERFACE	TARGET	NETMASK	GATEWAY	METRIC	ACTIONS
LAN Network	>						
Guest Network	5						
Video Network	×:	IPv6 Static Rout	es				+ Add route
Multicast	8	WTENTACT		CATEWAY		IT YOUR	ACTIONS
Routing	~	INTERFACE	TARGET	GATEWAT		TETRIC	ACTIONS
Static Routes							

- 2. Click the + Add Route button to the right of the heading for the desired IP version.
 - a. The appropriate Add Static Route dialog box appears.

Add Static IPv4 Route		×
Interfaces		
WAN		•
Target		
Target IPv4 Address		
Netmask		
Netmask		
Gateway		
Gateway		
Metric		
0		
	Cancel	Accept

- b. Complete the fields, using the information provided in the table below.
- c. Click Accept to save your changes. You are returned to the Static Routes page.



- 3. To edit an existing route:
 - a. Click the Edit icon () to the right of the entry to be edited. The Add Static Route dialog box appears.
 - b. Modify the fields as needed and then click Accept.
- 4. To delete a route, click the **Delete** icon () to the right of the entry to be deleted.
- 5. Click the Apply button in the Pending changes... dialogue to save your settings.

The following table describes the fields on this page.

Field Name	Description
Interfaces	Select the interface for the static route.
Target	Enter the host IP or network address. Enter specific IP addresses for a single device or identify an entire subnet. e.g., enter 192.168.1.0 to identify that subnet as the target.
Netmask	(Appears for IPv4 routes only) Enter the net mask for the target IP address.
Gateway	Enter the gateway address for the route.
Metric	Enter the number of hops needed to reach the default gateway. The default is 0 .

DNS

On this page, you can configure network DNS servers.

1. In the left menu, click Network > Routing > DNS. The following page appears.

SMART/R	G° =	Q Search		
🙆 Dashboard		DNS		
Retwork	~			
Status		Custom DN	IS Servers	
Ethernet WAN			IPV4/IPV6 ADDRESS	
LAN Network	>			
Guest Network	8			





- 2. To add a custom DNS server, in the Custom DNS Servers section:
 - a. Click the + Add server button. The Add/Edit DNS Server dialog box appears.

	×
Close	Save changes
	Close

- b. Enter the IP address of the custom DNS server and click Save changes.
- c. To add another IP address, repeat steps a and b.
- 3. To edit a DNS server address, click the Edit ()) icon next to it. The Add/Edit dialog box appears. Enter the new server

address and click Save Changes to commit your changes.

- 4. To remove a server, click the **Delete** icon (**C**) next to it.
- 5. Click the Apply button in the Pending changes... dialogue to save your settings.

Advanced

On this page, you can configure the WAN MTU setting.

1. In the left menu, click Network > Routing > Advanced. The following page appears.

SI	MART/RG°	=	Q Sear	rch		٠	¢	۲	
Ð	Dashboard		Advand	ed Network Co	nfiguration				
*	Network	•							
	Status			Advanced Con	figuration				
	Ethernet WAN								1
	LAN Network	>		WAN MTU	1500				- 1
	Guest Network	>							- 1
	Video Network	5	mann		-	 ~~	~~~		_

- 2. Enter or select the MTU (Maximum Transmission Unit) size for the network. Options are 0 2048. The default is 1500.
- 3. Click the Apply button in the Pending changes... dialogue to save your settings.



Downstream QoS

On this page, configure how traffic is prioritized over wireless networks to improve quality of service.

1. In the left menu, click Network > Routing > Downstream QoS. The following page appears.

12	MART/RG°	=	Q Search		* (
Ð	Dashboard		Quality of Service		
-	Network	•			
	Status		QoS Configuration	1	
	Ethernet WAN				
	LAN Network	>	Enabled		
	Guest Network	>			
	Video Network	>	IP multicast video	COS4	-
	Multicast	5	05		
	Routing	~	LIDP games COS	C056	, î
	Static Routes		obr games cos	030	•
	DNS		TCD games COS		
	Advanced		TCP games COS	COS5	•
	Downstream QoS				

- 2. To enable the quality of service feature, click the slide button to the right of Enabled.
- 3. In the three remaining fields, select the appropriate COS (priority) level. Options are COS7 COS0. The default settings work for most systems.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.

Firewall

In this section, you can configure router access, rules, DMZ settings, and port forwarding settings.

Firewall Settings

On this page, you can enable the firewall for your system.





1. In the left menu, click Network > Firewall. The following page appears. The firewall is enabled by default.

S	MART/RG°	=	Q Search	
Ð	Dashboard		Firewall	
器	Network	~		Eirowall Configuration
	Status			Filewall configuration
	Ethernet WAN			
	LAN Network	>		Enabled 🛛
	Guest Network	>		
	Video Network	>		Stealth mode
	Multicast	>		
	Routing	>		
	Firewall	~		
	Router Access			Conntrack Helper
	Rules			
	DMZ			Enabled
	Port Forwarding			

- 2. To disable the firewall, click the slide button next to Enabled.
- 3. To prevent malicious users from discovering information about your network and its devices and service, click the slide button next to Stealth mode.
- 4. The Conntrack Helper feature is *enabled* by default. To *prevent* these modules from assisting the firewall in tracking the various protocols used to establish traffic flow. click the **slide button**.
- 5. Click the Apply button in the Pending changes... dialogue to save your settings.

Router Access

On this page, you can configure a destination port and source IP address for router access.

1. In the left menu, click Network > Firewall > Router Access. The following page appears.

SI	MART/RG°	=	Q Searc	h		٠	C	•	2 Admin
Ð	Dashboard		Router	Access					
器	Network	•							
	Status		Access	s Rules					+ Add
	Ethernet WAN			NAME	DEST PORT	SRC IP			ACTIONS
	LAN Network	>							
	Guest Network	>		allow-cwmp-solicit	7547				2 😢
	Video Network	>							



2. To add a mapping, click the + Add button at the right side of the page. The Add / Edit Item dialog box appears.

Add / Edit Item		×
Name		
new_rule		
Destination Port		
Port		
Source IP		
IP Address		
Enabled		
-		
	Close	Save changes

- 3. Fill in the fields using the information provided in the table below. All fields are optional.
- 4. Click Save changes. The dialog box closes and the new mapping appears in the Router Access list.
- 5. To edit a mapping:
 - a. Click the Edit icon () next to the line item to be changed. The Add / Edit Item dialog box appears.
 - b. Modify the fields as needed.
 - c. Click Save changes. The updated values appear on the page.
- 6. To *disable* a mapping, clear the checkbox in the far left column for the mapping you wish to suspend. The mapping definition remains on the page but is not active.
- 7. To *remove* a mapping, click the **Delete** icon (👧) at the end of the row to be deleted. The mapping definition is removed.
- 8. Click the Apply button in the Pending changes... dialogue to save your settings.

The fields on this page are explained in the following table.

Field Name	Description
Name	Enter a descriptive name for this rule. No spaces are allowed.



Field Name	Description
Destination Port	Enter the destination port for this rule.
Source IP	Enter the IP address for the source device (such as 192.168.1.44).
Enabled	New rules are <i>enabled</i> by default. To <i>disable</i> this rule but save the settings, click the slide button.

Firewall Rules

On this page, you can define firewall rules to filter traffic.

1. In the left menu, click Network > Firewall > Rules. The following page appears.

SI	MART/RG°	=	Q Sea	arch			٠	C 🕀 🌘	Admin
æ	Dashboard		Firewa	all Rules					
*	Network	~							
	Status		Rule	5				+ A	dd rule
	Ethernet WAN			NAME	SRC ZONE	SRC PORT	DEST IP	DEST PORT	PROTO
	LAN Network	>							
	Guest Network	>		Allow-Voice-ICMPv6	voice				icmp
	Video Network	>							
	Multicast	>	2	Allow-Video-Video	wan		224.0.0.0/4		udp
	Routing	>							
	Firewall	~	2	Allow-Video-DNS	video			53	tcpudp
	Router Access								
	Rules			Block-SSDP	wan		239.255.255.250	1900	udp
	DMZ								
	Port Forwarding		2	Allow-MLD	wan				icmp
î	WiFi	>							
۵	Devices	>	2	Allow-ICMPv6-Forward	wan				icmp
O	Services	2	×	Allow-Video-DHCPv6	video	546-547		546-547	udp
0	Admin	>		Allow-Voice-Ping	woice				

2. To create a new rule:

a. Click the + Add rule button to the right of the Rules section heading. The Add / Edit Firewall Rule dialog box appears.



new_rule			
Family			
ny			
otocol			
CP + UDP			
ewall Actior	1		
ACCEPT			
	SOURCE		DESTINATION
one	LAN	, Zone	WAN -
	IP Address	IP	IP Address
p			MAC Address
IAC	MAC Address	MAC	MAC ADDIESS
nAC ort	MAC Address Port	MAC Port	Port

- b. In the Rule Name field, enter a descriptive name for the rule.
- c. Fill in the other fields using the information in the table below.
- d. Click Save changes.
- 3. To edit a mapping:
 - a. Click the Edit icon () next to the line item to be changed. The Add / Edit Item dialog box appears.
 - b. Modify the fields as needed.
 - c. Click Save changes. The updated values appear on the page.
- 4. To remove a rule, click the **Delete** icon () at the end of the row to be deleted. The rule is removed.
- 5. To *disable* a rule, clear the checkbox in the far left column. The rule remains on the page but is not active.
- 6. Click the Apply button in the Pending changes... dialogue to save your settings.



Field Name	Description
IP Family	Select the address family. Options are Any, IPv4, and IPv6.
Protocol	Select the protocol for this rule. Options are UDP, TCP, ICMP, TCP + UDP, and ESP.
Firewall Action	Select the action to be performed when this rule is triggered. Options are ACCEPT, REJECT, FORWARD, and DROP. The default is ACCEPT.
SOURCE	
Zone	Select the source zone. Options are Unspecified , Any , GUEST , VIDEO , WAN , MGMT , LAN and VOICE . The default is LAN .
IP	Enter the source IP address for this rule.
MAC	(<i>Optional</i>) To associate a source MAC address (such as 00236AA37CC3) with this rule, enter the MAC address for your gateway. If an IP address has been entered, the related MAC address appears in this field. To change the source MAC address, enter a new address.
Port	(<i>Optional</i>) To associate a source port with this rule, click the checkbox next to the entry field and then enter the port number for the source address.
DESTINATION	
Zone	Select the destination zone. Options are Unspecified , Any , GUEST , VIDEO , WAN , MGMT , LAN , and VOICE . The default is WAN .
IP	Enter the destination IP address for this rule.
MAC	<i>Optional</i>) To associate a source MAC address (such as 00236AA37CC3) with this rule, enter the MAC address for your gateway. If an IP address has been entered, the related MAC address appears in this field. To change the source MAC address, enter a new address.
Port	(Optional) To associate a destination port with this rule, enter the port number for the destination address.



DMZ

On this page, you can configure DMZ settings for your gateway. For security reasons, it is recommended that you create a static IP address for the host server that you enter on this page.

1. In the left menu, click Network > Firewall > DMZ. The following page appears. The WAN IP Address is read-only.

smart/rg° =		Q Sea	rch		•	٢
Dashboard		DMZ				
Network	~					
Status			DMZ Configuratio	on		
Ethernet WAN						
LAN Network	5		Enabled			
Guest Network	2					
Video Network	2		WAN IP address	192.168.1.152,2603:9000:d804:	:7055:ea2c:6dff:fe29:7	
Multicast				800,2005.9000.0804.7055926		
Routing	>		Host IPv4 address	Choose option	-	
Firewall	~					

- 2. To enable this feature, click the slide button to the right of Enabled.
- In the Host IPv4 Address field, select or enter the IP address for which unrestricted Internet access is to be allowed.
 Note: It is recommended to create a static DHCP association to this host address.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.



Port Forwarding

On this page, you can configure a local network device to have unrestricted access to the Internet. This is useful when local network devices cannot run an Internet application properly behind the firewall. This is also known as *exposed host* or *virtual server*.

1. In the left menu, click Network > Firewall > Port Forwarding. The following page appears.

SMART/RG° =	Q Search A C D C	Admin
🔁 Dashboard	Port Forwarding	
😤 Network 🗸		
Status	Port Forwarding + Add	d rule
Ethernet WAN	NAME DIRECTION SOURCE IP DESTINATION IP PROTOCOL LOCAL PORT PUBLIC PORT AC	CTIONS
LAN Network >		_
Guest Network >		

2. To add a mapping, click the + Add Rule button to the right of the Port Forwarding section heading. The Add/Edit Port Forwarding dialog box appears.



Add / Edit Port Forwarding		×
Source Zone		
WAN		•
Destination Zone		
LAN		*
Source IP		
Source IP Address		
Destination Device		
Select connected device		•
Destination IP		
*Required		
Mode		
Select Service from List		•
Service Type		
Select service type		•
Enable Hairpin		
	Cancel	Accept

3. Fill in the fields using the information provided in the table below. All fields are optional.

Field Name	Description
Source Zone	Select the source zone from the drop-down list of zones defined on this network. Options are GUEST, VIDEO, WAN, MGMT, LAN and VOICE. The default is WAN.
Destination Zone	Select the destination zone from the drop-down list of zones. Options are GUEST, VIDEO, WAN, MGMT, LAN and VOICE. The default is LAN.
Source IP	Enter the IP address for the source device (such as 192.168.1.44).
Destination Device	Select a connected device from the devices available in the selected zone.



Field Name	Description
Destination IP	This field is populated when a destination device is selected. To change this address, type a different address in the field.
Mode	Select whether to use the settings defined for a service or to define the port settings manually. Options are Select Service From List and Configure Manually . The default is Select Service From List .
Fields defined for usin	ig a service
Service Type	Select the type of service. The Service field appears. Options are Server, Consoles, Remote Access, VPN, Messaging Telephone, and Audio and Video.
Service	Select the service for the service type selected. The options vary by the type of service.
Fields defined for conj	figuring the rule manually
Public port/ Public port range	(<i>Appears when Configure Manually is selected in the Mode field</i>) Enter the applicable port number or range of numbers. Options are 1 - 65535 .
Protocol	(Appears when Configure Manually is selected in the Mode field) Select the correct protocol. Options are UDP , TCP , and TCP + UDP .
Local port/ Local port range	(Appears when Configure Manually is selected in the Mode field) Enter the local port number or range of numbers. Options are 1 - 65535.
Port Type	(Appears when Configure Manually is selected in the Mode field) Select whether to enter a single port or a range of ports. If Port range is clicked, the Public port field changes to the Public port range fields and the Local port field changes to the Local port range fields.
Enable Hairpin	To <i>enable</i> hairpin protocol, click the slide button .

4. Click Accept. The dialog box closes and the new mapping appears in the Port Forwarding list.

- 5. To edit a mapping:
 - a. Click the 🜈 icon to the right of the mapping entry. The Add/Edit Port Forwarding dialog box appears.

b. Modify the fields as needed, and then click Save. The updated values appear on the page.

- 6. To *disable* a mapping, clear the checkbox that appears before the Name column. The mapping definition remains on the page but is not active.
- 7. To *remove* a mapping, click the **Delete** icon () at the end of the row to be deleted. The rule is removed.
- 8. Click the Apply button in the Pending changes... dialogue to save your settings.



WiFi

In this section, you can adjust settings and view performance associated with the Wi-Fi networks configured on this gateway.

Status

On this page, you can view information about the wireless networks connected to your system.

In the left menu, click WiFi > Status. The following page appears, showing information for the 2.4 GHz and 5 GHz wireless networks.

SMART/RG° =	Q Search				٠	C 🛛 😫	Admin
🙆 Dashboard	Wi-Fi Status					년 Vie	w charts
Network	Wireless Ra	dios					
Status	NAME	STATUS	CHANNEL	HW M	ODE	TX POWER	
Scan	2.4GHz	ENABLED	11	11b, 1	11g, 11n	24 dBm	
Radios Networks	5GHz	ENABLED	36	11ac,	11n	22 dBm	
Mesh							
Clients Performance	2.4GHz Net	works		5GHz Netw	orks		
Client Performance	NETWORK	SSID	BSSID	NETWORK	SSID	BSSID	
Advanced	Internet	SmartRG-78d0	E8:2C:6D:29:78:D4	Internet	SmartRG-78d0	E8:2C:6D:29:78:D	A
Devices >							

To view detailed transmission data for the individual interfaces, click the View charts button (Marts) at the top right. The netdata window opens in a new tab, showing information about the overall SR400ac system, memory, CPUs, firewall, IPv4 networking, etc. Use the navigation menu at right to select the desired statistics to be displayed.

Scan

On this page, you can scan for nearby wireless access points. The available data includes the channel number, SSID, BSSID, OUI, STA, usage, signal, and encryption.

 In the left menu, click WiFi > Scan. The following page appears, showing the wireless access points found during the most recent scan. You can find the latest scan date and time in the upper section next to Last scan time. The channels currently in use are displayed below that field.



SI	MART/RG°	=	Q Search					٠	¢	•	Q Admin
Ð	Dashboard		Wi-Fi Scan							C Sta	rt Wi-Fi Scan
**	Network	>		Seen Configure	ation				1		
÷	WiFi	~		Scan Configura	ation						
	Status Scan			Re-scan interval	0			0			
	Radios Networks			Re-scan time	0:0			0			
	Mesh Clients			Last scan time	Fri Apr 17 07:	33:57 2020					
	Performance Client Performance			Auto 2.4GHz char	nnel 11						
	Advanced Devices	,		Auto 5GHz chann	nel 36						
Ø	Services	>									
0	Admin	>	Scan Results								
			CHANNEL SSID		BSSID	oui	STA U	ISAGE SI	GNAL	EN	CRYPTION
			1 (20MHz) MySp	ectrumWiFi20-2G	00:CB:51:47:3B:26	Sagemcom Broadband SAS	14	1396	- 24	4 dB	•
	-					~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~					~~~

- 2. Do any of the following:
 - To re-scan for wireless access points near your location, click the Start Wi-Fi Scan button at the top right. The list refreshes in a few moments.
 - To define how often the scan should occur, in the **Re-scan interval** field, enter the number of hours between scans. To disable scanning, enter **zero** (0) in this field. This is the default.
 - To define the time of day when the scan should occur, in the **Re-scan time** field, enter the time in hh:mm format. Options are **00:01 23:59**. The default is **0:0** (disabled).
- 3. Click the Apply button in the Pending changes... dialogue to save your settings.

Radios

On this page, you can configure 2.4 or 5 GHz wireless networks for the primary SSID.

 In the left menu, click WiFi > Radios. The following page appears, showing the fields for the 2.4 GHz radio. To view and adjust 5 GHz settings, click the 5GHz button.



St	MART/RG°	=	Q Search			
Ð	Dashboard		Wireless Radios			
묾	Network	>		Dadia Configuration		
Ŷ	WiFi	•		Radio Configuration		
	Status Scan Radios			2.4GHz	5GHz	
	Clients Performance			2.4GHz Configuration		
	Client Performance Advanced			Enabled	•	
	Devices	>		Tx Power	24 dBm (251 mW) 👻	
•	Admin	>		Bandwidth Mode	HT20 -	
				Enable Legacy Rates		
				Auto Channel	-	
				Legacy Client Auto Channel Mode		0

- 2. Fill in the fields, using the information in the following table. The same fields are used for both 2.4 GHz and 5 GHz configurations.
- 3. Click the Apply button in the Pending changes... dialogue to save your settings.

Field Name	Description
Enabled	Each radio is enabled by default. To <i>disable</i> a radio, click the slide button.
TX Power	Select the maximum rate at which transmission is allowed. Options range from 6 dBm (4 mw) to 26 dBm (398 mw).
	The default is 24 dBm (250 mw) for the 2.4 GHz radio and 22 dBm (160 mw) for the 5 GHz radio.
Bandwidth Mode	2.4 GHz radio: Select the "high throughput" (HT) bandwidth mode for this device. Options are HT20 and HT40 (MHz). The default is HT20 .
	5 GHz radio: Select the " very high throughput" (VHT) bandwidth mode for this device. Options are VHT20 , VHT40 , and VHT80 . The default is VHT80 .



Field Name	Description					
Enable Legacy Rates	To set the gateway to cut transmission briefly when changing channels, click the slide button. This is useful for legacy WiFi clients, enabling them to connect more effectively to a new channel. This feature is <i>disabled</i> by default.					
Auto Channel	This feature is <i>enabled</i> by default. To <i>disable</i> automatic channel selection , click the slide button. The Channel field appears.					
Channel	(Available only when Auto Channel is disabled) Select the channel for this device.					
	2.4 GHz radio: Options include Channel 1 (2.412 GHz) - Channel 11 (2.462 GHz).					
	5 GHz radio: Options include Channel 36 (5.18 GHz) - Channel 64 (5.32 GHz) and Channel 100 (5.5 GHz) - Channel 165 (5.825 GHz).					
Legacy Client Auto Channel Mode	(<i>Appears for 2.4GHz only</i>) This feature is <i>disabled</i> by default. To allow the gateway to select the best channel for legacy clients, click the slide button .					

Networks

On this page, you can configure the Primary, Guest and Video wireless networks.

1. In the left menu, click WiFi > Networks. The following page appears, showing the information for the primary wireless network.





SN	1art/rg°	-	Q Search					• •
Ð	Dashboard		Networks					
**	Network	>		Wi Ei Notworks				
÷	WiFi	~		WI-FI Networks				
	Status Scan Radios			Primary		Guest		rideo
	Networks Mesh Clients			Dual-band Prima	ıry			
	Performance Client Performance Advanced			Enabled	•			
۵	Devices	>						
Ø	Services			Wi-Fi Configurati	ion			
•	Admin	>						
				SSID	SmartRG-78d0)		3
				Password			۲	0
				Encryption	WPA2 Persona	al (PSK + CCMP)	•	
				Broadcast SSID	-			
				Client Isolation				

- 2. Fill in the fields for the primary network, using the information provided in the table below.
- 3. To configure the guest network, click the **Guest** button and modify the fields as needed, using the information provided in the table below.
- 4. To configure the video network, click the Video button and modify the fields as needed, using the information provided in the table below.
- 5. Click the Apply button in the Pending changes... dialogue to save your settings.

Field Name	Description
Dual-band Primary Dual-band Guest Dual-band Video	This feature is <i>enabled</i> by default. To <i>disable</i> the dual-band feature for these networks, click the slide button.
Wi-Fi Configuration	n section
Enabled	(Appears on the Guest and Video pages only) To enable the Wi-Fi configuration, click the slide button.



Field Name	Description
SSID	(<i>Optional</i>) Customize the wireless network ID. This field cannot contain quotes (") or back slashes (\) but can contain most other special characters. It is recommended that this ID be no more than 32 characters.
Password	Enter the passphrase for this connection. To show the key characters, click the ④ icon. This field cannot contain the following characters: " \ () ; & < > but spaces are allowed.
Encryption	Select the encryption protocol (mode and cypher) for this connection. Options are None and WPA2 Personal (PSK + CCMP). The default is WPA2 Personal (PSK + CCMP).
Broadcast SSID	This option is <i>enabled</i> by default. To <i>hide</i> the SSID from end users, click the slide button .
Client Isolation	This option is <i>disabled</i> by default for the Primary and Video networks and enabled for the Guest network. To <i>enable</i> client isolation, click the slide button .

Mesh

On this page, you can configure WiFi options for your mesh network.

1. In the left menu, click WiFi > Mesh. The following page appears.

SI	MART/RG°	=	Q Search		•
Ð	Dashboard		Mesh WiFi		
80	Network	>		Mark Carl Security	
÷	WiFi	~		Mesh Configuration	
	Status Scan Radios			Enable 2.4Ghz Mesh Backhaul	
	Networks Mesh			Maximum Mesh Hops	*

- 2. To enable the 2.4 GHz mesh backhaul feature, click the slide button next to Enable 2.4Ghz Mesh Backhaul.
- (Optional) In the Maximum Mesh Hops field, select the maximum number of hops allowed for the mesh network. Options are 0 3. The default is 0.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.

Clients

On this page, you can view information about the clients connected to the network via wireless interfaces.

In the left menu, click WiFi > Clients. The following page appears, listing the clients currently connected to your network.



SMART/RG°	=	Q Searc	h						٠	C 🕀	Admin
Dashboard		Wi-Fi Cli	ents								
Retwork	>	Cliente									
🗢 WiFi	~	Clients	5								
Status		- A.	HOSTNAME	BAND	SSID	SNR	RX RATE	RX PACKETS	TX RATE	TX PACKETS	OUI
Scan											
Radios					-						

Performance

On this page, you can view performance information about the wireless networks connected to your system.

In the left menu, click **WiFi** > **Performance**. The following page appears, showing the information for the 2.4 GHz wireless network. To view information about the 5 GHz network, click the **5 GHz** button.





SMART/RG°	=	Q Search						٠	C 🖶 🙁 Admin
🙆 Dashboard		Wi-Fi Perfo	rmance						
😽 Network	2			Wireless Bands					
🗢 WIFI	*								
Status Scan Radios					2.4GHz		5G	Hz	
Networks Mesh Clients		Status							
Performance		BAND	BANDWIDTH	PRIMARY CHANNEL	RX NOISE	RX SNR R	X SIGNAL SSID	SECONDARY CHANNEL	STATION COUNT
Client Performance Advanced		2.4GHz	20MHz	11	-92	19 -	73 SmartRG-78d0	11	0
Devices	>								
C Services	>	Current							
Admin	>	PERIOD	TX AIRTIME	TX (MBPS)	TX EFFICIENCY	TX PACKET	TX PACKET RETRY	TX PACKET RETRY FAIL	TX RETRY RATE
		9 s	0%	0	0%	0	0	0	0%
		Last 15 M	inutes						
		PERIOD	TX AIRTIME	TX (MBPS)	TX EFFICIENCY	TX PACKET	TX PACKET RETRY	TX PACKET RETRY FAIL	TX RETRY RATE
		63 s	096	o	096	0	0	0	0%
		63 s	096	0	096	0	0	0	096
		63 s	0%	0	096	0	0	0	0%

To view detailed information about each network, scroll through the Current, Last 15 minutes, Last Hour, Last Day, and Last Week sections.

Client Performance

On this page, you can view information about the performance of clients connected to the network via wireless interfaces.

In the left menu, click WiFi > Client Performance. The following page appears, showing information for the clients connected to the 2 GHz network. To view details about a different band (5GHz, and Guest [2.4GHz and 5GHz]), click the appropriate button.



SN	MART/RG°	ll.	Q. Search
Ð	Dashboard		Wi-Fi Client Performance
80	Network	>	
¢	WiFi	~	Wi-Fi Networks
	Status		
	Scan		2.4GHz 5GHz Guest (2.4Ghz) Guest (5GHz)
	Radios		
	Networks		
	Mesh		Connected Clients
	Clients		Connected Clients
	Performance		
	Client Performance		
	Advanced		NO CLIENT DATA AVAILABLE
	Devices	>	
-	- American		and a second and a

Advanced

On this page, you can configure advanced WiFi options for the gateway.

1. In the left menu, click WiFi > Advanced. The following page appears.

St	MART/RG°	=	Q Search	*
æ	Dashboard		Advanced Wi-Fi	
80	Network	>		External WDS Putton
÷	WIFI	•		External WPS Button
	Status			Enshed
	Scan			
	Radios			
	Networks			
	Mesh			Auto SGHz DES Channels
	Clients			Auto Soliz Dis chameis
	Performance			
	Client Performance			Enabled
	Advanced			

- 2. To *disable* the physical WPS button on the outside of the gateway, click the **slide button** next to **Enabled** below **External** WPS Button.
- 3. To include 5 GHz DFS channels in automatic channel selection, click the slide button next to Enabled below Auto 5GHz DFS Channels.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.



Devices

In this section, you can configure and manage the devices connected to your gateway. You can group and manage LAN devices as well as Intellifi mesh network devices.

Intellifi Devices

On this page, you can view the Intellifi mesh devices connected to the network.

Note: To extend the network, you can connect a satellite to a satellite.

1. In the left menu, click **Devices** > Intellifi Devices. The following page appears showing a diagram of the connected devices.

If a LAN device is connected via wireless, the WiFi band appears as the name instead of LAN or WAN. The device colors identify the device status. See the legend in the **Device Topology** header for details.

There are two views: the simple view (the default) and the detailed view. (The detail view shows the IP addresses for each device.) Click the **Show** button (at the top right) to switch between these views. This map refreshes every 10 seconds.

SN	MART/RG°	=	Q Search	٠	¢	۲	Q Admin
Ð	Dashboard		Intellifi Devices			💎 Sh	ow detail view
•••	Network WiFi	>	Network Topology Connection Status:	•	GOOD	O FAIR	O WEAK
۵	Devices	*	SR400ac-78D0				
	Connected Devices Device Groups Access Schedule		LAN2 2.4GHZ				
O	Services	>	kdadamo7390w10 android-86f5142151551f3b				
0	Admin	>					

2. To view details of a device, click the device label. The Device Details pane appears.

You can edit the host name, click the IP address to log into the device, or click **Internet Access** to pause access to this device. For detailed information about the available information and functions, see <u>Accessing Device Information</u>

3. When finished, close the pane.

Accessing Device Information

From the SR400ac gateway GUI, you can view the details and configure some of the settings on your satellite devices.



Note: Only the Device Details pane and the Internet Access pane are available for devices communicating via wireless. The other panes (Wi-Fi Overrides, Interface Statistics, and Advanced) are available when a device is connected via Ethernet cable to the Intellifi controller (SR400ac gateway).

- 1. Log into your SR400ac gateway and click the View Intellifi topology button at the top right.
- 2. Click the label for the device you want to work with. The device information pane appears to the right.
- 3. Do any of the following:
 - View details of a device
 - Pause Internet access for a device
 - Configure the wireless network and radio settings
 - <u>View Interface Statistics</u>
 - Reboot the Device
 - <u>Reset the Device to Factory Defaults</u>
 - Update the Device Software

Viewing Device Details

To view the device's host name, MAC address, IP address, and uplink type, click **Device Details**.

Device Details	•	
Hostname		
SE80ac-AF70		
MAC Address		
3C:90:66:F8:AF:71		
IP Address		
192.168.65.200		
Uplink		
lan		

You can edit the host name or click the IP address to log into the device and view status and statistics.

Pause Internet Access

You can halt a device's access to the Internet for a specific amount of time.



- 1. Click Internet Access to expand the pane.
- 2. Click Pause. The Pause internet access dialog box appears.

Pause internet access		×
Timeout (ms)		
Choose option		-
	Cancel	Save changes

- 3. Select a time period in the Timeout(ms) field (15 minutes 1 day).
- 4. Click Save changes.



Configure Wireless Settings

To configure the wireless network and radio settings:

1. Click Wi-Fi Overrides.

중 Wi-Fi Overrides	•
Configure wireless radios and netw	vork overrides.
2.4GHz	
Wi-Fi Networks	
SmartRG-78d0	🖋 Primary
Radio Settings Configure	
5GHz	
Wi-Fi Networks SmartRG-78d0	🖋 Primary
Radio Settings Configure	



- 2. To edit the SSID name or password:
 - a. Click the Edit icon () next to the network you want to change.

🗢 Wi-Fi Overrides	*
Configure wireless radios an	nd network overrides.
2.4GH	z
Wi-Fi Networks	
SmartRG-78d0	Primary
Radio Settings Configure	
5GHz	
Wi-Fi Networks	
SmartRG-78d0	Primary
Radio Settings	
Configure	

b. Enter the new information and click Save changes.



- 3. To modify the transmittal power, bandwidth mode or channel settings:
 - a. Click **Configure** for the network you want to change. The setting details appear.

	•
	•
	•
Cancel	Save changes
	Cancel

b. Modify the fields as needed, using the information in the following table.

Field Name	Description
TX Power	Select the maximum transmit power at which transmission is allowed. Options range from 6 dBm (4 mw) to 26 dBm (400 mw) .
Bandwidth mode	 2.4 GHz radio: Select the "high throughput" (HT) bandwidth mode for this device. Options are HT20 and HT40 (MHz). The default is HT20. 5 GHz radio: Select the "very high throughput" (VHT) bandwidth mode for this device. Options are VHT20, VHT40, and VHT80. The default is VHT80.
Channel	 Select the channel for this device. 2.4 GHz radio: Options include Channel 1 (2.412 GHz) - Channel 11 (2.462 GHz). 5 GHz radio: Options include Channel 36 (5.18 GHz) - Channel 64 (5.32 GHz) and Channel 100 (5.5 GHz) - Channel 165 (5.825 GHz).

c. Click Save changes.


View Interface Statistics

To view statistics, click Interface Statistics. The statistics for the wi-fi networks appear.

🔟 Inter	face Stat	istics	-
NAME	LINK	TX PACKETS	RX PACKETS
WIFI2G	UP	10687	0
WIFI5G	UP	10677	0

Reboot the Device

Note: If you reboot multiple devices (APs) at the same time, they may connect in a different topology than before based on what signals they see first when coming up. For example, 2 APs connected to a hub (Intellifi controller) may connect to each other first, creating a daisy-chained setup instead of a hub and spoke configuration.

To reboot the device:

- 1. Expand the Advanced pane.
- 2. Click Reboot. A confirmation message appears.
- 3. Click OK. The device reboots and is removed from the topology. Once the device is reconnected, it appears on the topology.

Reset the Device to Factory Default Settings

To reset the device to factory defaults:

- 1. Expand the Advanced pane.
- 2. Click Reset. A red warning dialog box appears, stating that resetting the device will unpair it from your Intellifi network.
- 3. If you're sure you want to reset the device, click **Yes**, **I'm sure**. The device reboots and is removed from the topology. Once the device is reconnected, it appears on the topology.



Update Device Software

You can update the firmware installed on your SE80ac by way of the gateway to which it's connected. Firmware updates for SmartRG products are available for download in the SmartRG Customer Portal.

Note: Following a firmware upgrade, the device reboots.

To update the firmware installed on the device:

1. Expand the Advanced pane. The following fields appear. The current firmware version is shown at the top.

Lo Advanced	-
Firmware Version SMARTOS SE80ac 10.8.3.1	
Remote Reboot Reboot	
Factory Reset	
Manual Update	Browse

- 2. Next to the Manual Update field, click Browse.
- 3. Select the firmware image file to be installed and then click Open. A progress bar and a Cancel button appears.
- 4. Click Start Upgrade. The Please wait popup appears, showing the Upgrading progress bar.
- 5. Click OK. When the upgrade has completed, the device reboots. When the SE80ac reboots, its outline on the topology changes to a dashed gray line and the LED on the device changes color as it goes through the reconnection process. When the upgrade process has completed, the SE80ac device shows a solid outline again in the Intellifi topology. It takes about 5-7 minutes for the upgraded SE80ac to return to the topology.

If you wish to verify that the software version has been upgraded, click the device label again and then click Advanced. The software version appears at the top of the pane.

Connected Devices

This page displays a list of devices connected to the LAN.



Note: Before you can assign a device to a group, you must configure an access schedule, then configure a device group, and finally assign the schedule to the group.

Warning: Pausing access for LAN devices not only restricts access to the Internet but LAN access as well. This in turn prevents you from logging in to the SmartRG gateway to make changes from any LAN clients included in the pause. With this in mind, users are strongly advised against pausing all LAN devices at the same time. Instead, exclude at least one browser-equipped LAN device from the Device Group to ensure that a means to modify access schedules, device groups and timeout periods is preserved.

1. In the left menu, click Devices > Connected Devices. The following page appears.

SMART/RG°	=	Q Se	tarch					¢	🖶 🙆 Admin
Dashboard		Conne	ected Devices						
Network	>								
🗢 WIFI	>	Dev	ices						Clear Inactives
Devices	~	1	HOSTNAME -	INTERFACE	IP ADDRESS	MAC	001	LAST SEEN	ACTIONS
Intellifi Devices Connected Devices		1	android-86f5142151551f3b	wifi2g	192.168.65.146	00:EE:BD:A0:C8:A5	HTC Corporation	02s	0
Device Groups Access Schedule		2	kdadamo7390w10	lan2	192.168.65.187	C8:F7:50:B4:61:C1	Dell Inc.	06s	0
Services	,					-			

- 2. To edit a device host name:
 - a. Click the 🌈 icon to the right of the entry that you want to edit. The Edit Device dialog box appears.

Ealt device		
Hostname		
-		
	Close	Save changes

- b. (Optional) In the Hostname field, enter a descriptive name for the device.
- c. Click Save changes.



- 3. To pause access for a device temporarily:
 - a. Click the Pause icon (¹¹) to the right of the device for which you want to halt access. The Pause dialog box appears.
 - b. In the Set timeout field, select how long you want access paused. Options are None, 15 60 minutes, 2-8 hours, and 1 day.
 - c. Click Save changes.
- 4. To restart access, click the Play icon (
) to the right of the line item for which you wish to resume Internet access. The

Pause icon (_____) re-appears.

Device Groups

On this page, you can create device groups, assign devices to groups, pause access for devices, delete groups

Note: Before it is possible to assign a device to a group, configuring an access schedule is required first, then configure a device group, and finally assign the schedule to the group.

Warning: Pausing access for LAN devices not only restricts access to the Internet but LAN access as well. This in turn prevents you from logging in to the SmartRG gateway to make changes from any LAN clients included in the pause. With this in mind, users are strongly advised against pausing all LAN devices at the same time. Instead, exclude at least one browser-equipped LAN device from the Device Group to ensure that a means to modify access schedules, device groups and timeout periods is preserved.

1. In the left menu, click **Devices** > **Device Groups**. The following page appears.

SMART/R	G° ≡	Q Sea	arch			🐥 🤇 🤀 Admin
🔁 Dashboard		Device	Groups			+ Create group
8 Network	1900		and the second			
🗢 WiFi	2	Unas	ssigned			Access schedule
Devices	~	*	HOSTNAME	MAC ADDRESS	IP ADDRESS	ACTIONS
Intellifi Devices	ices	1	kdadamo7390w10	C8:F7:50:B4:61:C1	192.168.65.187	0 🔍 🗢
Device Groups	e	2	android-86f5142151551f3b	00:EE:BD:A0:C8:A5	192.168.65.146	0 🕛 🔿
				man and a second		

Note: You cannot delete or rename the unassigned (default) group. You can assign a schedule and pause/restart it.

- 2. To add a new device group:
 - a. Click the **Create group** button (+ Create group) at the upper right. The Create Group dialog box appears.
 - b. In the Name field, enter a descriptive name for the device group.



c. To assign a schedule to the device group, select the schedule in the Access schedule field.

Note: If you do not see the schedule that you want, go to the Devices > Access Schedule page and create it. Then, return to this page and select it.

- d. Click Create. The new group appears on the page and a Delete group button appears at the top right.
- 3. To add a device to a group:
 - a. Click the Assign button () at the far right, next to the device that you want to add to a device group. The Assign device to group dialogue appears.

	×
	•
Close	Save changes
	Close

b. In the **Group** field, select a group.

Note: If you do not see the group that you want, create it, following the steps provided above.

- c. Click Save changes.
- 4. To define a timeout period for a group:

Before pausing a device, read the Warning above.

a. Click the Pause button (¹⁰⁾) at the far right, next to the device for which you want to withhold Internet access. The Pause Internet Access dialogue appears.



Pause Internet Access		×
Timeout (ms)		
Choose option		-
	Close	Save changes

- b. In the Timeout field, select the duration of the pause. Options are None, 15 60 minutes, 2 8 hours, and 1 day.
- c. Click Save changes.
- 5. To customize the host name for a device:
 - a. Click the 🌈 icon next to the device you want to customize. The Edit Device dialog box appears.

Edit Device		×
Hostname		
Davids Laptop J		
	Close	Save changes

- b. Enter the desired host name.
- c. Click Save changes.
- 6. To delete a device group:
 - a. Click the Delete group button (**The Delete group**) at the top of the device pane. The Delete Group dialogue appears.
 - b. Select the group to be deleted from the drop-down list.
 - c. Click Delete.
- 7. Click the Apply button in the Pending changes... dialogue to save your settings.



Access Schedule

On this page, you can configure the access schedules that are needed to control access for LAN device groups.

Note: Before you can assign a device to a group, you must configure an access schedule, then configure a device group, and finally assign the schedule to the group.

Warning: Pausing access for LAN devices not only restricts access to the Internet but LAN access as well. This in turn prevents you from logging in to the SmartRG gateway to make changes from any LAN clients included in the pause. With this in mind, users are strongly advised against pausing all LAN devices at the same time. Instead, exclude at least one browser-equipped LAN device from the Device Group to ensure that a means to modify access schedules, device groups and timeout periods is preserved.

1. In the left menu, click Devices > Access Schedule. The following page appears.

SMART/RC	° =	Q Search		. c ⊕ (
Dashboard		Access Schedule		
Retwork	>			
穼 WiFi	×.	Schedule Cor	nfiguration	+ Add schedule
Devices	•	Schedules	No schedule selected	-
Intellifi Devices				
Connected Device	s	- Andrew States of the second		~

- 2. To create an access schedule:
 - a. Click the Add schedule button at the top right. The Create access schedule dialog box appears.

Enter name		
	Save changes	Close

b. Enter a descriptive name for the new schedule and click **Save changes**. Additional fields appear on the Access Schedule page for configuring blocked access time for every day or for specific days. The **Delete schedule** button



appears at the top right of the pane.

	Access Sche	dul	e - l	Def	ault	t ED	т																		
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
	Monday			-																10	15	20			20
	Tuesday																								
	Wednesday																								
	Thursday																								
	Friday																								
	Saturday																								
	Sunday																								
	Daily Pause Ti	me	s																						
	09:00 - 10:00)					09	:00	- 10	00:00						09:	00 -	10	:00						
M	onday Pause	Tim	es																						
	09:00 - 10:00						09	:00	- 10):00						09:	00 -	10	:00						
Τι	iesday Pause	Tim	es																						
	09:00 - 10:00						09	:00	- 1():00						09:	00 -	10	:00						
w	ednesday Pau	se 1	Time	es					_					_	~~~		-		-					_	

3. Enter start and end times in the fields below the **Pause Times** labels. Use 24-hour format. The separating colon is added for you as you type the numbers.

The entered time periods are shown in **red** on the grid in whole-hour blocks only. When times are entered in the **Daily Pause Times** fields, that period changes to **red** for *every* day.

For example, to prevent access between 2 am and 3 am, enter "0200" in the first (start) field and "0259" in the second (end) field for either every day (daily) or specific days. The grid refreshes to show that access is blocked for the 2:00 hour.

If you enter "0300" in the second field, a 2-hour block is selected in the grid, from 2:00 - 4:00 am.

The maximum number of blocked periods allowed per day is 3.

To add another blocked period for the same day, enter values in the 2nd and 3rd time fields.

Example of a 1-hour block (entered as 02:00 to 02:59)



3	0	1	2	3	4	5	6	7	8
Monday									
Tuesday									
Wednesday									
Thursday									
Friday									
Saturday									
Sunday									

Example of a 2-hour block (entered as 02:00 to 03:00)

	0	1	2	3	4	5	6	7	8
Monday									
Tuesday									
Wednesday									
Thursday									
Friday									
Saturday									
Sunday									

- 3. To change a schedule, select it in the Access Schedule field and modify the fields.
- 4. To delete a schedule, select it in the Access Schedule field and click the Delete schedule button (Delete schedule at the top right.

Note: If you delete a schedule that is assigned to a device group, it is removed from the device group configuration.

5. Click the Apply button in the Pending changes... dialogue to save your settings.



Services

In this section, you can configure the various services for the network including UPnP, TR-069, SNMP, hosts, DDNS, and others.

UPNP

On this page, you can manage the UPnP (Universal Plug and Play) service so that third-party devices on the LAN that support this standard can connect. Common devices include gaming consoles, IP cameras, printers, and so on.

1. In the left menu, click Services > UPnP. The following page appears.

S	MART/RG°	=	Q Searc	h
Ð	Dashboard		UPNP	
器	Network	>		UDND Configuration
Ŷ	WiFi	>		OPNP Configuration
۵	Devices	>		Enabled
D	Services	~		
	UPNP			Enable NAT-PMP
	DUNA	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		

- 2. To *disable* UPnP, click the slide button to the right of Enabled.
- 3. To disable the automatic configuration of NAT settings, click the slide button to the right of Enable NAT-PMP.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.



DLNA

On this page, you can configure the settings for DLNA (Digital Living Network Alliance) server software.

Note: You must reboot the gateway to implement any changes made on this page.

1. In the left menu, click **Services** > **DLNA**. The following page appears.

SI	MART/RG°	=	Q Search		٠	¢	•	0
Ð	Dashboard		DLNA					
*	Network							
(:	WiFi	5	DLNA Co	nfiguration				_
۵	Devices	>	Enabled					
O	Services	•						
	UPNP		Server nan	e SR400ac DLNA Server			3	
	DLNA							
_	-	-	And a			-	~~~	-

- 2. To *enable* this option, click the **slide button** to the right of **Enabled**.
- 3. (Optional) In the Server name field, enter a descriptive name for this network that DLNA clients will see.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.

TR-069 Configuration

On this page, you can configure the gateway with details about the management server to which this gateway will be linked.

Note: You must reboot the gateway to implement any changes made on this page.



SMA	ART/RG°	=	Q Search			
🙆 Das	shboard		TR-069			
Ref Net	twork	>		Server Configuration		
穼 WiF	Fi	>		-		
Dev	vices	>		Enabled		
🕻 Ser	rvices	*		Management server URL	http://acs.smartrg.com/	
	NP NA			Inform interval (secs)	90	
SNI	MP sts			ACS username	admin	
DDI	NS ud Storage			ACS password	💿	
File	e Sharing ntent Filter			Use base MAC as TR-069 serial number	••	?
Adr	min	>				
				Client Configuration		
				Allow solicit from ACS	•	
				TR-069 local port	7547	
				Connection request username	srg-tr069	
				Connection request		
				Manual inform	🌲 Inform now	
				Stun Server		
				Minimum keep alive	30	
				Maximum keep alive	3600	
				Server address	None	
				Server port	19302	
				Username	tr069_stun	

1. In the left menu, click Services > TR-069. The following page appears.

- 2. Fill in the fields, using the information in the following table. Values appear in the **Stun Server** section if that feature is configured for your system.
- 3. To connect to the ACS, in the Client Configuration section, click the Inform now button.
- 4. Management by ACS is *enabled* by default. To *disable* this option, click the **slide button** to the right of **Enabled** near the top of the page.



5. Click the Apply button in the Pending changes... dialogue to save your settings.

Field Name	Description			
Server Configuration				
Management server URL	Enter the URL of the management server such as http://youracsname.youracsprovider.com.			
Inform interval (in secs)	Enter the number of seconds for how often the gateway contacts the host server. The default setting is whatever interval is defined on your ACS.			
ACS username	Enter the user name for the ACS.			
	Note: If you clear this field and the ACS Password field, the ACS will populate these fields on the next inform.			
ACS password	Enter the password for the ACS.			
Use base MAC as TR-069 serial number	This option is <i>enabled</i> by default. The base MAC address of your device is used as the serial number. To use the device's actual serial number instead, click the slide button to the rigid disable this option.			
Client Configuration				
Allow solicit from ACS	This feature is <i>enabled</i> by default. To <i>prevent</i> solicitation transactions from your ACS, click the slide button.			
TR-069 local port	Enter the port number for the local port as defined for your ACS. The default is 7547 .			
Connection request username	Enter the user name for requesting the connection.			
	Note: If you clear this field and the Connection request password field, the ACS will re-populate these fields on the next inform.			
Connection request password	Enter the password for requesting the connection.			
Stun Server				
Note: Values appear for these fie	elds <i>only</i> when a STUN server is configured.			
Minimum keep alive	The minimum time(in seconds)that the keepalive function should be active. Options are 0 - Unlimited . The default is 30 seconds.			
Maximum keep alive	The maximum time(in seconds)that the keepalive function should be active. Options are 0 - Unlimited . The default is 3600 seconds.			
Server address	The assigned network address of the physical STUN server. An invalid address will produce an immediate on-page error message from the gateway. Maximum length is 256 characters.			
Server port	The port number associated with your STUN server infrastructure. Options are 0 - 64435 . The default is 19302 .			
Username	The user name by which the gateway accesses the STUN infrastructure. Maximum length is 256 characters. Special characters are allowed.			



SNMP

On this page, you can configure an SNMP service for the gateway.

1. In the left menu, click Services > SNMP. The following page appears.

SI	MART/RG°	=	Q Search			٠
Ð	Dashboard		SNMP			
*	Network	>				
÷	WiFi	>		SNMP Configura	tion	
۵	Devices	>		Enabled	0	
Ø	Services	•		Read community	Community	
	UPNP			inclu continuity	community	U
	TR-069			Set community	Community	3
	SNMP Hosts			System name	HeartOfGold	0
	DDNS Cloud Storage			System location	office	0
	Content Filter			System contact	bofh@example.com	
0	Admin	>		Trap manager IP	IPv4/IPv6 Address	3
				Allow SNMP to contact device		

- 2. To enable the SNMP service, click the slide button to the right of Enabled.
- 3. Fill in the fields, using the information in the following table. All fields are optional.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.



Field Name	Description
Read community	Enter the SNMP community string for your network which allows read-only access.
Set community	Enter the SNMP community string for your network which allows read-write access.
System name	Modify the name of the gateway.
System location	Modify the default location of this service.
System contact	Enter the email address for the contact person.
Trap manager IP	Enter the IP address of the server where the SNMP trap manager is located.
Allow SNMP to contact device	This option is <i>disabled</i> by default. To <i>enable</i> this option, click the slide button .

Hosts

On this page, you can configure the hostname of the gateway and add IP addresses for other hosts on the gateway. To begin, configure the host servers in the **Network** section.

1. In the left menu, click **Services** > **Hosts**. The following page appears.

SN	1art/rg°	=	Q Search					* C
83	Dashboard		Hosts					
80	Network	2		r dia				
(:	WiFi	2		Edit	Hostname			
۵	Devices	>		Route	er hostname	SR400ac-78	D0	
Ø	Services	~						
	UPNP							
	DLNA							
	TR-069			Host	s			+ Add host
	SNMP				IPV4/IPV6-A	DDRESS	HOSTNAME(S)	ACTIONS
	Hosts			1.00				
	DDNS			1	192.168.65.	.1	setup, router,	
	Cloud Storage							
	File Sharing							



2. To add a host:

a. Click the + Add Host button to the right of the Hosts section heading. The Add Host dialog box appears.

IPv4/IPv6 address	
IP Address	
Hostnames	
Hostnames Add hostname	
Hostnames Add hostname	

- b. In the IPv4/IPv6 address field, enter the host IP address.
- c. In the Hostnames field, enter the host name and press Enter or Tab. The name is added and the cursor moves to a new Add hostname entry field. To add more hosts, repeat this step as needed.

Note: No spaces are allowed.

You can also delete names from this field by click the X next to the name.

- d. Click Save changes.
- 3. To edit the details of a host:
 - a. Click the Edit icon () next to the host that you want to edit. The Add/Edit Item dialog box appears.
 - b. Modify the fields as needed.
 - c. Click Save changes.
- 4. To delete a host, click the **Delete** icon (**x**) to the right of the host that you want to delete.
- 5. Click the Apply button in the Pending changes... dialogue to save your settings.

DDNS

On this page, you can configure the DDNS settings for the gateway.

Dynamic DNS allows remote access the router from the Internet using a domain name instead of an IP address. An account on a DDNS service provider is required to implement this feature.



1. In the left menu, click **Services** > **DDNS**. The following page appears.

SMART/RG*	=	Q Search					▲ C ⊕	Q Admin
Dashboard		DDNS						
So Network	>							-
🗢 WiFi	>	DDNS (Dynan	nic DNS)					+ Add
Devices	>	NAME	DOMAIN NAME	USERNAME	PASSWORD	SHOW PASSWORD	USE HTTPS	ACTIONS
C Senices	~~~							

- 2. To add a dynamic DNS server:
 - a. Click the + Add button near the upper-right. The Add / Edit Item dialog box appears. New definitions are enabled by default.



Add / Edit Item			×
Enabled			
•			
Name			
Name			
DNS Provider			
Select or enter provider			-
Domain name			
Domain name			
Username			
Username			
Password			
Password			۲
Use HTTPS			
	Close	Save cha	nges

- b. Fill in the fields, using the information in the table below.
- c. Click Save changes.
- 3. To edit the details of a server:
 - a. Click the Edit icon () next to the server that you want to edit. The Add/Edit Item dialog box appears.
 - b. Modify the fields as needed, using the information in the table below.
 - c. Click Save changes.
- 4. To delete a server, click the **Delete** icon () to the right of the server that you want to delete.
- 5. Click the Apply button in the Pending changes... dialogue to save your settings.

Field Name	Description
Enabled	New configurations are enabled by default. To <i>disable</i> a configuration, click the slide button.



Field Name	Description
Name	Enter a descriptive name for this entry.
DNS Provider	(Optional) Select the DNS provider.
	To enter a provider that is not found in the drop-down list, click the checkbox next to Enter DDNS Provider and enter the URL of your DDNS provider.
Domain name	Enter the URL or name of the domain.
Username	Enter the user name required to access the domain.
Password	Enter the password required to access the domain. To display the password, click the Show/hide password icon (
Use HTTPS	(Optional) To enable HTTPS security, click the slide button.



Cloud Storage

On this page, you can configure access to a cloud storage account. Cloud storage is supported by box.com.

To create an account, click the Cloud Storage by box.com button at the top of this page.

Warning: To link a box.com account with this gateway, enable the BOX share on the Services > File Sharing page first. Then return to this page and enter the related credentials. If you don't follow this sequence, recovery may require a factory reset (FRESET) of the gateway.

1. In the left menu, click Services > Cloud Storage. The following page appears. The connection status for existing cloud storage accounts is displayed at the bottom of the page.

SMART/RG°	=	Q Search				٠
🙆 Dashboard		Cloud Storage				
Network	5					
🙃 WIFI			Cloud Storage	Configuration	Cloud Storage by	box.com
Devices	>		Enabled			
Services	~					
UPNP			Username	Username		
DLNA						
TR-069			Password	Password	۲	
SNMP						
Hosts			Connection	STOPPED		
DDNS			status			
Cloud Storage						

- 2. To enable cloud storage, click the slide button to the right of Enabled.
- 3. In the Username field, enter the user name for accessing your cloud storage account.
- In the Password field, enter the password for accessing your cloud storage account. To display the password, click the Show/hide password icon (
- 5. Click the Apply button in the Pending changes... dialogue to save your settings.

File Sharing

On this page, you can configure network settings and shares (on box.com) settings for sharing files.

Warning: To link a box.com account with this gateway, enable the BOX share on this page *first*. *Then* go to the Services Cloud Storage page and enter the related credentials. If you don't follow this sequence, recovery may require a factory reset (FRESET) of the gateway.

To create an account, click the Cloud Storage by box.com button at the bottom of this page.



S	MART/RG°	=	Q Search			
Ð	Dashboard		File Sharing			
쁆	Network	>		Share Configuratio	n	
(î	WiFi	>		Share configuratio		
۵	Devices	>		Enabled		
Ø	Services	•				
	UPNP			Network name	WORKGROUP	
	DLNA TR-069			Device name	SR400ac	
	SNMP Hosts			Description	SmartRG SR400ac Gateway	
	DDNS					
	Cloud Storage			Username	samba-user	
	File Sharing Content Filter			Password		0
0	Admin	>				
				Share Modes		
				USB1	Disabled	•
				USB2	Disabled	•
				BOX	Disabled	•
					Configure Box.com cloud s	torage

1. In the left menu, click Services > File Sharing. The following page appears. This feature is disabled by default.

- 2. To enable file sharing, click the slide button to the right of Enabled.
- 3. Modify the fields as needed, using the information provided in the following table.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.

Field Name	Description							
Share Configuration section								
Network name	Enter the name of the network used for file sharing.							
Device name	Enter the device name.							
Description	Enter a brief description of the device.							
Username	Enter the user name for your cloud storage account.							



Field Name	Description
Password	Enter the password for your cloud storage account. To display the password, click the Show/Hide icon (\odot).
Share Modes sectio	n
Note: Information is	shown here if these options are configured for your gateway.
USB1 USB2 BOX	Select whether this share is disabled, read-only or read & write. The USB port to which you connect first is designated as USB1 and the other port is designated as USB2. The gateway uses either port equally. Options are Disabled , Read only , and Read / Write .
	Note: To use the BOX option, create a box.com cloud storage account first. To do so, click the Configure box.com cloud storage link near the bottom of the page.



Content Filter

On this page, you can configure web content filtering, i.e., parental controls.

1. In the left menu, click Services > Content Filter. The following page appears.

S	MART/RG°	=	Q Search		
Ð	Dashboard		Web Content Filte	r	
쁆	Network	>		Network Protection	
(;	WiFi	>		Network Protection	
۵	Devices	>		Enabled	
þ	Services	~			~
	UPNP			Block ads	
	DLNA			Definitions undeted	Nees
	TR-069			Definitions updated	None
	SNMP			IBv4 drop count	0
	Hosts			1PV4 drop count	0
	DDNS			IPv6 drop count	0
	Cloud Storage			in vo drop counc	0
	File Sharing				
	Content Filter				
•	Admin	>		OpenDNS Family Shield	
				Enabled	

- 2. To enable network protection, click the slide button to the right of Enabled.
- 3. Fill in the fields, using the information in the table below.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.

Field Name	Description						
Block ads To <i>enable</i> the advertisement blocking feature, click the slide button.							
Definitions updated	The date and time when the filter definitions were last updated. If the definitions were never updated, "None" appears in the field.						
IPv4 drop count	The number of dropped packets on the IPv4 network.						
IPv6 drop count	The number of dropped packets on the IPv6 network.						
OpenDNS Family Shi	OpenDNS Family Shield section						
Enabled	To <i>enable</i> the adult content blocking feature, click the slide button.						



Admin

In this section, you can update firmware on your gateway, manage passwords, run diagnostics, view the event log, an set the operating mode.

Update

On this page, you can update the firmware of your SmartRG gateway. Software updates for SmartRG products are available for download in the SmartRG Customer Portal.

Note: Following a firmware upgrade, the gateway reboots; rebooting takes approximately 6 minutes.

1. In the left menu, click Admin > Update. The following page appears, showing the Update History at the bottom of the page. The version number and build date are listed for each update.

SI	MART/RG°	=	Q Search					٠	¢
Đ	Dashboard		Firmware Update						
*	Network	э		Manual Undate					
(•	WiFi	2		Current version: SMAR	F/OS 10.8.4.1				
۵	Devices	>							
Ø	Services	>		Upload Firmware Image	No file selected		Browse		
•	Admin	•							
	Update								
	Configuration Router Management Passwords			Available Update Last check: Fri Apr 170	S 7:32:50 PDT 2020				
	Net Tools Event Log	2.		0 Updates availa	able		Check for t	updates	
	Operating Mode Reboot			Update History					
				VERSION		BUILD DATE			
				10.8.3.1		Thu, Jan 23, 2020), 7:45 PM		

Note: The current firmware version is listed below the Manual Update heading.

- 2. To update firmware manually:
 - a. In the Manual Update section, click Browse. An Open dialog box appears.
 - b. Navigate to and select the firmware image file to be installed and then click **Open**. A progress bar and a Cancel button appear.



c. Click Start Upgrade. The Please wait popup appears, showing the Upgrading progress bar.

Note: If the failed message appears, click the message to clear it. Then try downloading the file again and repeating the above steps.

- 3. To check for available updates:
 - a. In the Available Updates section, click the Check for updates button. The CHECKING FOR UPDATES message appears. The Update status field refreshes to show either a list of available updates or the 0 Updates available message.
 - b. If updates are available, click Install Updates. A confirmation message appears.



c. Click Yes. The installing message appears. When the installation has finished, the gateway reboots.

Installing Updates
 Do not disconnect or power off your device(s).

4. To view the update history, review the version number and build date for each update made to this gateway.



Configuration

On this page, you can save your settings (back up) to a local computer, restore previously saved settings, and reset your device to its factory settings. It is recommended that you save your settings as a first step whenever you plan to change the configuration.

1. In the left menu, click Admin > Configuration. The following page appears.

SI	MART/RG*	=	Q search
Ð	Dashboard		Router Configuration
8	Network		
î	WiFi	3	Configuration Management
	Devices	>	Enur Configuration Datase Configuration Entropy Default
Ø	Services	>	Save componential Restore Componential Pactory Denaut
•	Admin	•	
	Update Configuration		Save Configuration
	Router Management Passwords		Download de configuration
	Net Tools Event Los	5	backup

- 2. To back up your settings:
 - a. Click the Save Configuration button.
 - b. Click the **Download** button. The zipped .tar file is saved (.gz.zip format) to your default download location and is named "backup" followed by the gateway model number and the date in *yyyy-mm-dd* format, e.g., backup-SR400ac-2020-10-15.tar.gz.
- 3. To restore settings saved previously saved:
 - a. Click the Restore Configuration button.
 - b. Click the **Browse** button to select a file to upload, such as backup-SR400ac-2020-10-15.tar.gz and then click **Open**. The Reboot required dialog box appears.

Reboot required!		×
Configuration has been restored apply settings. Would you like to	d. A reboot i o reboot nov	s required to v?
	Later	Yes, reboot



- c. Click Yes, reboot. The selected configuration is applied and the gateway reboots.
- 4. To restore the device to factory default settings:
 - a. Click the Factory Default button.
 - b. Click the Factory reset button. The reset warning dialog box appears.
 - c. Click OK. The device is restored to default configuration.

Router Management

On this page, you can enable or disable WAN HTTP and mobile management.

1. In the left menu, click Admin > Router Management. The following page appears.

SN	1art/rg*	=	Q Search		
Ð	Dashboard		Router Management		
8	Network	>		Management Configura	tion
÷	WiFi	>		0	
۵	Devices	2		Hostname	SR400ac-78D0
ø	Services	•		Stealth LED	-
0	Admin	*			
	Update				
	Router Management			HTTP Configuration	
	Passwords				
	Net Tools Event Log	3		Enable LAN HTTP	•
	Time				
	Operating Mode			Enable WAN HTTP	()#·
	Reboot			WAN HTTP Port	80
				WAN HTTP Restrict Source	0.0.0.0/0
				HTTPS Configuration	
				Enable WAN HTTPS	
				WAN HTTPS Port	443
				WAN HTTPS Restrict Source	0.0.0/0

- 2. Fill in the fields using the information in the table below.
- 3. Click the Apply button in the Pending changes... dialogue to save your settings.



Field	Description
Management Config	guration section
Hostname	(<i>Optional</i>) Enter a new name for the host.
Stealth LED	This option <i>prevents</i> the LEDs on the gateway from shining. To <i>allow</i> the LEDs to shine, click the slide button.
Enable Mobile Management	This option is <i>enabled</i> by default. It allows or denies the gateway to be remotely managed. Click the slide button to turn this feature on or off.
HTTP Configuration	i section
Enable LAN HTTP	This feature is <i>enabled</i> by default. To <i>disable</i> LAN HTTP, click the slide button.
Enable WAN HTTP	This feature is <i>disabled</i> by default. To <i>enable</i> WAN HTTP, click the slide button.
WAN HTTP Port	(<i>Optional</i>) Enter a different port number for the WAN. The default is 80 .
WAN HTTP Restrict Source	(Optional) Enter the IP address for which you want access restricted.
HTTPS Configuratio	n section
Enable WAN HTTPS	This feature is <i>disabled</i> by default. To <i>enable</i> WAN HTTPS, click the slide button.
WAN HTTPS Port	(Optional) Enter a different port number for the secure WAN. The default is 443.
WAN HTTPS Restrict Source	(Optional) Enter the IP address for which you want access restricted.



Passwords

On this page, you can change the passwords used to access your device.

1. In the left menu, click Admin > Passwords. The following page appears.

SI	MART/RG°	=	Q Search			
æ	Dashboard		Account Passwor	ds		
器	Network	>		Change Password		
î	WiFi	>		change rassword		
۵	Devices	>		Username	admin	•
D	Services	>				
0	Admin	~		Current password	Password	0
	Update			New password	Password	•
	Configuration					
	Router Management			Re-enter password	Password	0
	Net Tools					
	Event Log	>			Save changes	
	Time					

- 2. In the Username field, select the user password that you want to modify.
- 3. In the **Current password** field, either enter the current password for the selected user, or click in the field to select a stored password.

Note: If you click the **Manage passwords** link, the Settings window opens for your browser. You can change passwords there as well.

 In the New password and Re-enter password fields, enter the new password. The password strength rating located below each of these fields refreshes automatically as each character is typed.

Weak password example



Change Password		
Username	admin	•
Current password		0
New password		٢
		Weak
Re-enter password	Password	0
	Save changes	

Strong password example

Change Password		
Username	admin	•
Current password		0
New password		٢
		Excellent
Re-enter password	Password	•
	Save changes	

5. Click Save Changes. The new password takes effect immediately.

Net Tools

On this page, you can ping a server and use the traceroute utility to display a packet's path over the IP network and measure route transit delays that may be present.



1. In the left menu, click Admin > Net Tools. The following page appears.

Г

SI	MART/RG°	=	Q Search
Ð	Dashboard		Network Tools
*	Network	>	Ding
÷	WiFi	5	Ping
۵	Devices	>	IP / Hostname Host to ping
Ø	Services	>	Start Clear
•	Admin	•	
	Update		
	Configuration		
	Router Management		Traceroute
	Passwords		
	Net Tools		IP / Hostname Host to trace
	Event Log	>	nos to nace
	Time		Start Clear
	Operating Mode		
	Reboot		

2. To ping a server, enter an IP address or host name in the upper IP/Hostname field (such as 192.168.1.44), then click the upper Start button. The PING RESULTS appear.

PING RESULTS:								
PING 192,168,1.1 (192,168,1.1) 56(84) bytes of data.								
64 bytes from 192.168.1.1: icmp rea=1 ttl=64 time=1.94 ms								
64 bytes from 192.168.1.1: icmp_req=2 ttl=64 time=1.93 ms								
64 bytes from 192.168.1.1: icmp_req=3 ttl=64 time=1.79 ms								
64 bytes from 192.168.1.1: icmp_req=4 ttl=64 time=1.81 ms								
64 bytes from 192.168.1.1: icmp_req=5 ttl=64 time=1.81 ms								
192.168.1.1 ping statistics 5 packets transmitted, 5 received, 0% packet loss, time 4003ms rtt min/avg/max/mdev = 1.798/1.861/1.945/0.064 ms								

 To trace a transmission, enter an IP address or host name in the lower IP/Hostname field (such as 192.168.1.44), then click the lower Start button. The TRACE RESULTS appear.



TRACE RESULTS:								
traceroute to 192.168.1.1	(192.168.1.1), 30 hops max, 38 byte packets							
1	192.168.1.1 4.491 ms							

Event Log

On this page, you can view the event log (system log) and configure how the log entries are displayed.

1. In the left menu, click Admin > Event Log. The following page appears.

SI	MART/RG°	=	Q Search			🗍 🕻 🖨 🕘 Admin
Ð	Dashboard		Event Log			Q Search log messages
80	Network	>	Log Messages			
Ŷ	WiFi	>	Log messages			
	Devices	5	DATE	TYPE	SOURCE	MESSAGE
o	Services	>	Fri Apr 17 11:21:14 2020	daemon.warn	odhcpd[3427]	["A default route is present but there is no public prefix on br-guest thus we don't announce a default route!"]
0	Admin		Fri Apr 17 11:21:14 2020	daemon.warn	odhcpd[3427]	["A default route is present but there is no public prefix on br-lan thus we don't announce a default route!"]
C.L.	Update		Fri Apr 17 11:21:58 2020	user.crit	hotplug.iface.wanstate	["INTERFACE wan6 DEVICE wan action ifupdate carrier 1"]
	Configuration Router Management		Fri Apr 17 11:21:59 2020	user.crit	hotplug.iface.status	["Network wan6 action ifupdate"]
	Passwords		Fri Apr 17 11:22:44 2020	user.crit	hotplug.iface.wanstate	["INTERFACE wan6 DEVICE wan action ifupdate carrier 1"]
	Net Tools Event Log	¥	Fri Apr 17 11:22:45 2020	user.crit	hotplug.lface.status	["Network wan6 action ifupdate"]
	Log Settings		Fri Apr 17 11:23:14 2020	user.crit	hotplug.iface.wanstate	["INTERFACE wan6 DEVICE wan action ifupdate carrier 1"]
	Operating Mode		Fri Apr 17 11:23:14 2020	user.crit	hotplug.iface.status	["Network wan6 action ifupdate"]
	Reboot		Fri Apr 17 11:23:36 2020	user.crit	hotplug.iface.wanstate	["INTERFACE wan6 DEVICE wan action ifupdate carrier 1"]

- 2. To filter the displayed messages:
 - a. Click the Search log messages button at top right. The Search log messages dialog box appears.
 - b. Enter a search string and click Search. The list refreshes to show the matching entries. The Clear search button also appears next to the Search log messages button.
- 3. To clear the current filter, click **Clear search** near the upper right corner of the screen.
- 4. To configure log settings, follow the "Configuring Log Settings" instructions below.

As new entries are added to the event log file, the list refreshes to display them.



Configuring Log Settings

On this page, you can enable remote logging.

1. In the left menu, click Admin > Event Log > Log Settings. The following page appears.

SMART/RG° =		Q Search		
Ð	Dashboard		Log Settings	
쁆	Network	>		Log Configuration
(î:	WiFi	>		Log Configuration
۵	Devices	>		Enable remote logging
	Services			

2. (Optional) To activate remote logging, click the slide button next to Enable remote logging.

SMART/RG*	=	Q Search	Pending changes Please pply or cancel your changes before leaving the paget	•
Dashboard		Log Settings	Apply Cancel	
Network	>		Log Configuration	
WIFI	2		Log comparation	
Devices	34		Enable remote logging	
C Services	2		province for the second	
🔨 Admin	*		Logging server IP IPv4/IPv6 Address	Ø
Update			Log port 514	0
Configuration				
Router Management			Log protocol UDP	
Passwords				
Net Tools				

- 3. In the Logging server IP field, enter the IP address (such as 192.168.1.44) of the syslog server to which the log messages should be sent. Log messages are sent to this server in addition to the default local destination.
- 4. In the Log port field, enter or select the port number for the specified logging server. Options are 1 9999.
- 5. In the Log protocol field, select the protocol. Options are TCP and UDP. The default is UDP.
- 6. Click the Apply button in the Pending changes... dialogue to save your settings.



Time

On this page, you can select a timezone and manage connections to the reliable clocking servers available on the Internet.

1. In the left menu, click Admin > Time. The following page appears. All fields on this page are optional.

SM	1art/rg°	=	Q Search		
æ	Dashboard		System Time		
묾	Network	>			
(î	WiFi	>		Time Configuration	
ū	Devices	>		Current time	Fri Oct 11 09:38:02 PDT 2019
D	Services	>			
0	Admin	•		Timezone	America/Vancouver 👻
	Update			Time Servers (NTP)	0.pool.ntp.org
	Router Management				1.pool.ntp.org
	Net Tools				2.pool.ntp.org
	Time	,			
	Operating Mode				

- 2. To change the time zone, in the **Timezone** field, select the appropriate zone.
- 3. To change or remove time servers, in the Time servers (NTP) section, modify or delete the addresses in the fields.
- 4. Click the Apply button in the Pending changes... dialogue to save your settings.



Operating Mode

On this page, you can select whether the gateway operates as a router or a wireless access point.

Intellifi Mode:

1. In the left menu, click Admin > Operating Mode. The following page appears.

SMART/RG°	=	Q Search			
🙆 Dashboard		Operating Mode			
Hetwork	>		Mode Configuration		
🔶 WiFi	>		inoue comgaration		
Devices	>		Operating Mode	Router -	0
Services	>				1
🚺 Admin	~		Intellifi Mode	Intellifi Controller •	0
Update			Intellifi Mode Auto switch	•	0
Configuration					

2. To configure how this gateway should operate, in the **Operating Mode** field, select the appropriate setting. Options are **Router** and **Wireless Access Point**. The default is **Router**.

In **Router** mode, this device functions as a router between your ISP's WAN and your home network LAN. It provides firewall, NAT server, DHCP server, UPnP, DDNS, Cloud File Sharing and other services. Select this option if you do not currently have a router.

Warning: A notification appears, stating that the gateway will reboot upon applying this setting.

 To configure this gateway as part of a mesh network, in the Intellifi Mode field, select the appropriate setting. Options are Intellifi Controller, Satellite, and None. Satellite is only available when you select Wireless Access Point in the Operating Mode field. The default is Intellifi Controller.

In Intellifi Controller mode, this device also becomes the central control center for your Intellifi network. Select this option if you are deploying Intellifi mesh nodes to support WiFi coverage at this location.

4. The Intellifi Mode Auto switch feature is *enabled* by default. To *prevent* the gateway from automatically switching from Intellifi Controller mode to the managed Satellite mode, click the slide button.

To learn more about Intellifi network configuration, refer to the "Setting up an Intellifi Network" How-To article available in the SmartRG Customer Portal.

5. Click the Apply button in the Pending changes... dialogue to save your settings.

Reboot

On this page, you can reboot your device.

1. In the left menu, click Admin > Reboot. The following screen appears. The amount of time that the gateway has been connected is shown in the Uptime line below the Start Reboot button.





2. Click the Start Reboot button.

The restart confirmation dialog box appears, stating that rebooting takes approximately three minutes.

3. Click the Yes, reboot button. The Rebooting dialog box appears, showing the time remaining until completion. When your gateway is ready, the sign-in page appears.


Logging out

- 1. In the top right corner of the interface, click the profile name. The USER PROFILE pane appears.
- 2. Click Logout. The Sign in dialog box appears.



Appendix: Compliance Statements

FCC Interference Statement

This device complies with Part 15 of the Federal Communications Commission (FCC) Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numrique de la classe B est conforme à la norme NMB-003 du Canada.

FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules.

- This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
- This equipment should be installed an operated with a minimum distance of 20cm between the radiator and your body.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution! Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

5GHz

5150-5250 MHz band is restricted to indoor operations only.



Revision History

Rev	Date	Description
5.1	March 2020	Header features updated; related screen captures updated to match. Other minor updates.
5.0	January 2020	New screen captures and updated navigation paths reflect the GUI facelift for Version 10.8.3.1 Related content was updated as well.
4.0	June 2019	Updated to match Version 10.7.1.1.
3.2	December 2018	Updated to match Version 10.6.3.1.
3.1	August 2018	Updated to match Version 10.5.4.1.
3.0	July 2018	Intellifi Devices screen capture replaced. No other changes to content.
3.0	June 2018	Updated to capture redesigned interface for Version 10.5.0.4.
2.1	April 2018	Screen captures updated to match Version 10.5.0.2.
2.0	April 2018	Initial document release for Versions 10.5 and later.