

# Stratix 6000 Ethernet Managed Switch

Catalog Numbers 1783-EMS04T, 1783-EMS08T



# Important User Information

Solid-state equipment has operational characteristics differing from those of electromechanical equipment. Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls (publication [SGI-1.1](#) available from your local Rockwell Automation sales office or online at <http://www.rockwellautomation.com/literature/>) describes some important differences between solid-state equipment and hard-wired electromechanical devices. Because of this difference, and also because of the wide variety of uses for solid-state equipment, all persons responsible for applying this equipment must satisfy themselves that each intended application of this equipment is acceptable.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.



**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.



**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.



**SHOCK HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.



**BURN HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

---

**IMPORTANT**

Identifies information that is critical for successful application and understanding of the product.

---

Allen-Bradley, Rockwell Software, Rockwell Automation, RSLinx, RSLogix, Logix5000, FLEX I/O, RSLogix 5000, Stratix 6000, and TechConnect are trademarks of Rockwell Automation, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

This manual contains new and updated information. Changes throughout this revision are marked by change bars, as shown to the right of this paragraph.

Topic	Page
Studio 5000™ Logix Designer application is the rebranding of RSLogix™ 5000 software	9

## Notes:

<b>Preface</b>	Studio 5000 Environment . . . . .	9
	Terminology . . . . .	10
	Additional Resources . . . . .	11
	<b>Chapter 1</b>	
<b>Basic Configuration</b>	Access the Home Page . . . . .	13
	Access Basic Configuration Options . . . . .	15
	Set the IP Address . . . . .	15
	Set the IP Address with BOOTP . . . . .	17
	Set Security . . . . .	17
	Work with Miscellaneous Settings . . . . .	18
	Status Indicators . . . . .	20
	<b>Chapter 2</b>	
<b>Network Services Setup</b>	SNMP . . . . .	21
	Supported MIBs . . . . .	22
	SNMP Configuration . . . . .	23
	IGMP . . . . .	25
	IGMP Product Support . . . . .	25
	IGMP Querier . . . . .	26
	IGMP Configuration . . . . .	27
	DHCP . . . . .	30
	Dynamic IP Address Assignment by IP Address Pool . . . . .	30
	Dynamic IP Address Assignment by Port . . . . .	31
	DHCP Address Table . . . . .	32
	MAC Address Labels . . . . .	33
	Email Configuration . . . . .	33
	SMS Configuration . . . . .	35
	Send Email via a Logix Controller-initiated Message Instruction . . . . .	35
	Enter the Text of the Email Message . . . . .	39
	Send an SMS from the Logix Controller . . . . .	40
	Modify the SMTP Server Setup in a Logix Controller Program . . . . .	40
	Email and SMS Error Codes . . . . .	41
	<b>Chapter 3</b>	
<b>Diagnostics</b>	Device Utilization . . . . .	44
	RSTP Report . . . . .	45
	IGMP Report . . . . .	45
	MAC Address Report . . . . .	46
	Alarm Setup . . . . .	46
	PLC Configuration . . . . .	48
	Automatic Email Alerts . . . . .	48
	Email Queue Status . . . . .	50
	Switch Restart . . . . .	50
	Display Switch Counters . . . . .	50

	<b>Chapter 4</b>	
<b>Switch Management</b>	STP/RSTP .....	53
	Spanning Tree Protocol .....	53
	Rapid Spanning Tree Protocol .....	54
	STP/RSTP Configuration .....	55
	VLAN Configuration .....	57
	Port Configuration .....	59
	Mirror Configuration .....	61
	MAC ID Management .....	63
	Port Segmenting .....	64
	QoS Setup .....	65
	<b>Appendix A</b>	
<b>Upgrade Firmware</b>	Upgrade with the Web Management Interface .....	67
	<b>Appendix B</b>	
<b>User Name and Password Rules</b>	User Name and Password Characters .....	69
	Other Rules .....	69
	<b>Appendix C</b>	
<b>Factory Reset</b>	Access the Reset Button .....	71
	Reset IP Address .....	72
	Change Settings to Default .....	72
	<b>Appendix D</b>	
<b>Data Layout</b>	DINT Input .....	73
	DINT Output .....	74
	<b>Appendix E</b>	
<b>Add the Switch to Software</b>	Generic Profile .....	75
	Add-on Profile .....	77
	Enter General Information .....	78
	Enter Connection Information .....	79
	View Identification and Status Information .....	80
	Configure Network and Port Settings .....	80
	View Port Diagnostic Information .....	82
	Configure IGMP .....	83
	Configure DHCP .....	84
	Configure Bandwidth and MAC ID Management Alarming .....	85
	Configure Port Behavior for Fault and Idle States .....	85

	<b>Appendix F</b>	
<b>Download or Upload a Configuration</b>	Upload Configuration.....	87
	Download Configuration.....	87
	<b>Appendix G</b>	
<b>Available SFP Modules and Cables</b>	Available SFP Modules .....	89
	SFP Module Cable Specifications.....	89
<b>Index</b>		

## Notes:



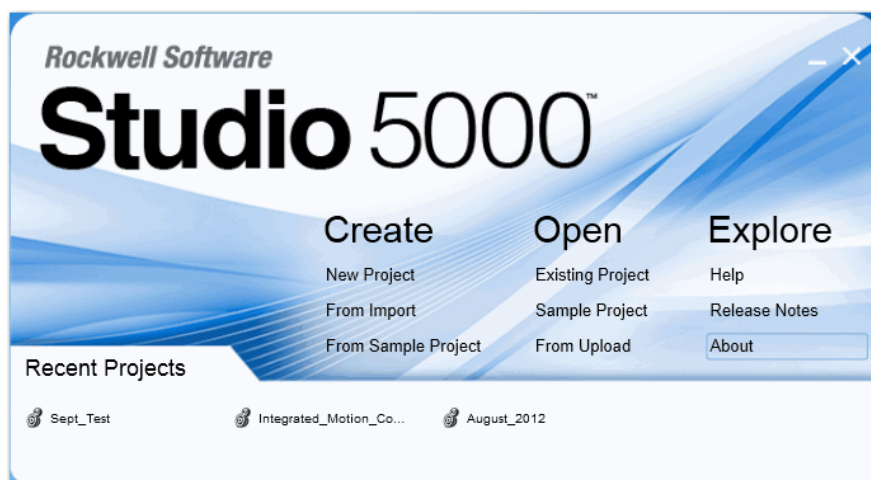
This manual is intended for users of the switch. We assume you are familiar with the procedures in the Stratix 6000™ Ethernet Managed Switch Installation Instructions, publication [1783-IN004](#).

Read and understand this manual before using the products. Consult your Rockwell Automation representative if you have any questions or comments.

For information about the features supported in your firmware revision, refer to the firmware release notes, publication [1783-RN003](#).

## Studio 5000 Environment

The Studio 5000™ Engineering and Design Environment combines engineering and design elements into a common environment. The first element in the Studio 5000 environment is the Logix Designer application. The Logix Designer application is the rebranding of RSLogix™ 5000 software and will continue to be the product to program Logix5000™ controllers for discrete, process, batch, motion, safety, and drive-based solutions.



The Studio 5000 environment is the foundation for the future of Rockwell Automation® engineering design tools and capabilities. It is the one place for design engineers to develop all of the elements of their control system.

## Terminology

Refer to this table for terms used in this publication.

**Table 1 - Managed Switch Terminology**

Term	Description
1783-EMS	All references to 1783-EMS in this manual refer to catalog numbers 1783-EMS04T and 1783-EMS08T.
Auto-MDIX	Automatic Medium-dependent Interface Crossover. Allows the switch to detect the required cable type (straight-through or crossover) for copper Ethernet connections and configures the interfaces accordingly.
BOOTP	Commonly used with Allen-Bradley Ethernet products, the BOOTP protocol is used by a client machine to locate its IP address and network mask.
DHCP	Dynamic Host Configuration Protocol. A network protocol that is used to configure devices, so that they can communicate on an IP network. A client machine uses this protocol to acquire configuration information, such as an IP address and default gateway, from a server running the protocol. The client then uses this information to configure itself.
DNS	Domain Name Server. Translates domain names into IP addresses, for example, www.example.com can translate to 192.168.100.100.
Domain	A group of computers and devices on a network that are controlled as a unit with common rules and procedures.
IGMP	Internet Group Management Protocol. A protocol that manages how adapters and other components join and leave multicast groups. IGMP snooping is a feature of IGMP that allows Ethernet switches to look (snoop) inside packets to determine which destinations really need to receive the data.
QoS	Quality of service. A method of managing network resources through the classification of Ethernet traffic into high and low priority queues.
SMS	Short Message Service. A communication service that allows text messaging between mobile phones.
SNMP	Simple Network Management Protocol. A protocol that exchanges messages with devices on a network for the purpose of monitoring the devices. SNMP enables a switch to be remotely managed through other network management software.
Spanning Tree	Refers to Rapid Spanning Tree Protocol (RSTP) or Spanning Tree Protocol (STP). Used with network topologies that provide more than one physical path between two devices, spanning tree protocol manages path redundancies while preventing undesirable loops in the network. If a fault should occur on an active port, the switch will begin transmitting out one of the blocked ports.
TCP	Transmission Control Protocol. TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets are delivered in the same order in which they were sent.
UDP	User Datagram Protocol. This protocol offers a minimal transport service. UDP is used by applications that do not require the level of service of TCP or use communication services (for example, multicast or broadcast delivery) not available from TCP. An application program running over UDP must deal directly with end-to-end communication anomalies that a connection-oriented protocol would have handled - for example, retransmission for reliable delivery, packetization and reassembly, flow control, and congestion avoidance, when these are required. This is commonly seen with I/O type devices that send out information at an RPI rate.
VLAN	Virtual local-area network. A logical segment of network users and resources grouped by function, team, or application. This segmentation is without regard to the physical location of the users and resources.

## Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

Resource	Description
Stratix Ethernet Switch Specifications, publication <a href="#">1783-TD001</a>	Provides technical specifications for Stratix Ethernet switches.
Stratix 6000 Ethernet Managed Switch Installation Instructions, publication <a href="#">1783-IN004</a>	Provides detailed specifications and information related to installation of the switch.
Industrial Automation Wiring and Grounding Guidelines, publication <a href="#">1770-4.1</a>	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, <a href="http://www.ab.com">http://www.ab.com</a>	Provides declarations of conformity, certificates, and other certification details.
Internet Engineering Task Force website, <a href="http://www.ietf.org">http://www.ietf.org</a>	Provides access to documents such as the RFC (request for comment), public documents on networking topics and protocols, Internet standards documents, best current-practices information, and related informational documents.

You can view or download publications at <http://www.rockwellautomation.com/literature/>. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

**Notes:**

## Basic Configuration

This chapter covers how to access the switch's web interface home page. It also includes information about how to set an IP address and security, work with miscellaneous options, and understand status indicators.

### Access the Home Page

Use these steps to access the web interface home page for the switch.

---

<b>IMPORTANT</b>	Before connecting to the network, set the IP address of the switch as described in <a href="#">Set the IP Address</a> .
------------------	---

---

1. Connect the switch to your computer's LAN card.

This connection is required before you can access the home page. For information about how to establish this connection, see the Stratix 6000 Ethernet Managed Switch Installation Instructions, publication [1783-IN004](#).

2. Open your web browser once the connection is established.

3. In the address bar of your web browser, type your switch's IP address.

For example, to use the default IP address, type `http://192.168.1.1`.

4. From the user name and password dialog box, leave the user name empty and type the following case-sensitive password: `PASSWORD`

If the web browser does not open, verify this information:

- The IP address of the switch. The default IP address is 192.168.1.1.
- Your connection setup. Refer to the Stratix 6000 Ethernet Managed Switch Installation Instructions, publication [1783-IN004](#).
- Whether the switch has power. The green power-status indicator should be on.
- Whether the cable is connected. A green or yellow status indicator should be lit on the Ethernet port.
- A proxy server is not preventing you from accessing the switch.

5. When the home page appears, refer to [Table 2](#) for information about the items on the page.

The screenshot shows the 'Home' page of a network switch configuration interface. It contains several sections:

- Switch Status:** A table showing various switch settings and their status.
 

Setting	Status
Spanning Tree	Disabled
VLAN 802.1Q	Disabled
IGMP Snooping	Disabled
Port Mirroring	Disabled
QoS	Disabled
MAC ID Management	Disabled
Product Type	1783-EMS08T
Serial Number	D00E1440
MAC Address	00:00:BC:61:16:10
Firmware Revision	0.53w110216
Web Revision	0.31w110216
Uptime	0 days, 00h:04m:33s
- Port Status:** A table showing the status of each port.
 

#	Link	VLAN	Speed	Duplex	Status
1	ON	---	100	Full	OK
2	OFF	---	---	---	---
3	OFF	---	---	---	---
4	OFF	---	---	---	---
5	OFF	---	---	---	---
6	OFF	---	---	---	---
7	OFF	---	---	---	---
8	OFF	---	---	---	---
9	OFF	---	---	---	---
- Gigabit Port Info:**
  - Fiber Optic Transceiver: Not present
  - Manufacturer Name: N/A
  - Model Number: N/A
- Resources:**
  - [Visit www.ab.com for additional information](#)
  - [Technical Reference Manual](#)
  - [EDS File and ICD File](#)
- Contacts:**
  - Info:
  - E-mail:

On the right side of the page, there is a diagram of the switch's front panel showing 8 ports. Ports 1-4 are on the left, and ports 5-8 are on the right. Arrows indicate the port numbers for each connector.

Table 2 - Items on the Home Page

Value	Description
Device Name	You provide this entry to identify the switch. See <a href="#">page 18</a> for instructions on entering the switch's name.
Spanning Tree	Indicates the current Rapid Spanning Tree Protocol (RSTP) mode of the switch. Possible values are Enabled (RSTP), Enabled (STP Compatibility), or Disabled. For more about setting the RSTP mode, see <a href="#">page 55</a> .
VLAN 802.1Q	Indicates whether the virtual local-area network (VLAN) feature is enabled on the switch, as described on <a href="#">page 57</a> . Note that the VLAN feature used in earlier firmware revisions has been renamed port segmenting. As of firmware revisions 0.11 and 0.53, a new VLAN feature is provided for only the 1783-EMS08T switch.
IGMP Snooping	Filtering mechanism for multicast traffic should be used when I/O is running on the Ethernet network. For more about IGMP snooping, see <a href="#">page 25</a> .
Port Mirroring	Allows traffic on one port to be copied and sent (mirrored) to another port so that an Ethernet protocol analyzer can capture it. For more about port mirroring, see <a href="#">page 61</a> .
QoS	When enabled, the switch can prioritize packet delivery to a certain port or MAC address. For more about QoS, see <a href="#">page 65</a> .
MAC ID Management	Determines if a MAC ID is authorized on the network by checking the allowed MAC IDs and notifies the switch's controller when an unauthorized node appears on the network. For more about MAC ID management, see <a href="#">page 63</a> .
Product Type	Shows the part number of the switch.
Serial Number	Unique to every switch.
MAC Address	Indicates the Ethernet address of the switch.
Firmware Revision	Check our website to make sure you are up to date. This file updates product firmware. The web interface must be updated separately.
Web Revision	Check our website to make sure you are up to date. This file updates your web interface. For related information, see <a href="#">Appendix A</a> .
Uptime	This setting indicates the switch's running time. This timer is reset when the switch is powered up.
Link (Port Status)	Possible values are ON and OFF. ON is if a device is connected to the port and has power. ON corresponds to the Link State Status indicator on the switch port being either solid or flashing green.

**Table 2 - Items on the Home Page (continued)**

Value	Description
VLAN (Port Status)	If virtual local-area network (VLAN) is enabled on the switch, the VLAN column indicates the VLAN ID assigned to each port. If the port is assigned the role of a switch or router, the VLAN column displays the word 'trunk'. For more about VLAN configuration, see <a href="#">page 57</a> .
Speed (Port Status)	Possible values are 10 or 100 signifying a 10 Mbps or 100 Mbps connection. This corresponds to the Data Rate status indicator on the switch port being off (10 Mbps) or solid amber (100 Mbps).
Duplex (Port Status)	Possible values are Full and Half.
Gigabit Port Information	This is offered as an option to the 1783-EMS08T switch and requires a pluggable SFP MSA-compliant transceiver that you must purchase separately. A fiber optic transceiver can be used to connect to a fiber optic network. Information about the transceiver used and the connection speed are found on the home page.
Resources	Provides links to our website and this manual (you have to be connected to the Internet to reach our website). The manual link in this section does not require an Internet connection because it is embedded in the product. For convenience, we have also embedded the EDS file for this device under the EDS file link in this section. Download and install it with the EDS hardware installation tool (one of the RSLinx® tools).
Contacts	Displays contact information entered on the Miscellaneous tab, as described on <a href="#">page 18</a> . This lets you enter a name or phone number and email address of the appropriate contact person.

## Access Basic Configuration Options

From the home page, click the Basic Configuration folder to expand the menu bar in the left pane to show these tabs:

- Network Configuration
- Set Security
- Miscellaneous

## Set the IP Address

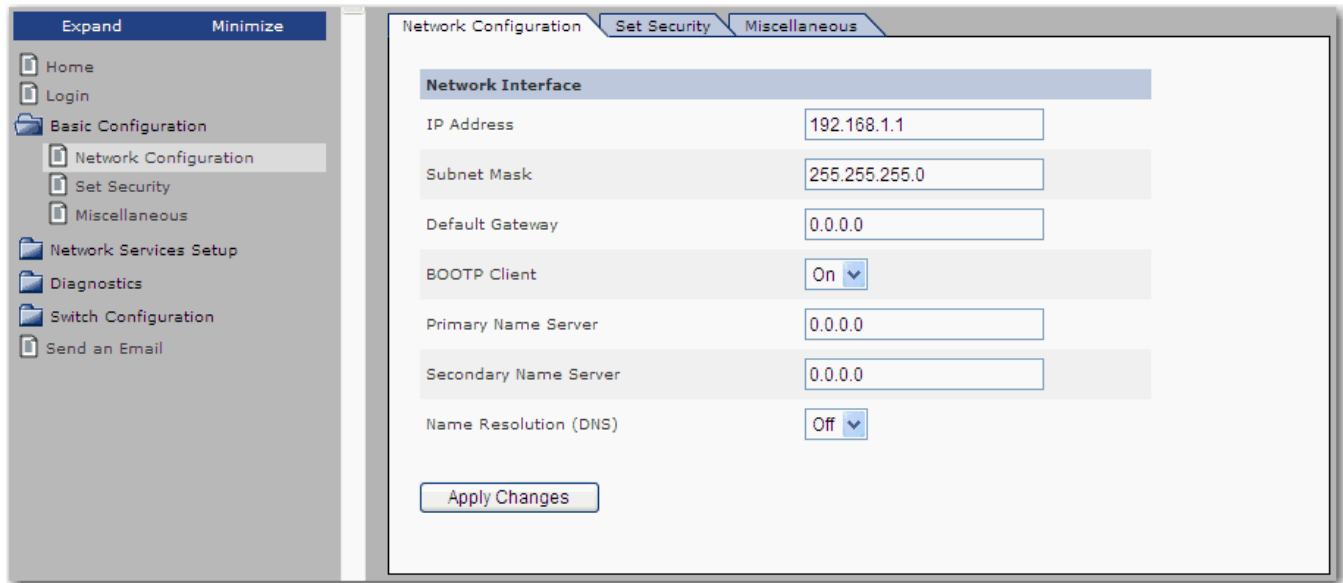
You normally need to change your IP address to install the switch into your Ethernet network.

Use these steps to change the IP address.

1. Find an available IP address on your subnet.
2. Connect the switch to your computer's LAN card.

For additional information, refer to the Stratix 6000 Ethernet Managed Switch Installation Instructions, publication [1783-IN004](#).

3. From the navigation pane, expand the Basic Configuration folder and select Network Configuration to display the Network Configuration tab.



4. Type your new IP address.
5. Change the subnet mask and default gateway, if needed.
6. Turn off BOOTP Client to prevent dynamic IP address assignment.

If using host names on the network, Name Resolution must be turned on and the DNS server addresses must be configured (usually required if using the email function).

7. Click Apply Changes to change the IP and subnet.

---

**IMPORTANT**

The switch does not load the new IP and subnet address until power is cycled.

---

8. Cycle power.

Once the IP and subnet are changed, you must cycle power to load the new address. Power can be cycled remotely through the management interface by expanding the Diagnostics folder and clicking Controller Restart. This restarts the 1783-EMS switch and does not restart the controller. All communication through the switch is interrupted.



## Set the IP Address with BOOTP

The 1783-EMS switch ships with the BOOTP client enabled by default. To assign an address, use this procedure.

1. Put the switch on a network with a BOOTP server.
2. Cycle power to the switch.

The 1783-EMS switch attempts to obtain an IP address several times from the server before timing out and defaulting to the factory preset address of 192.168.1.1.

### IMPORTANT

The MAC address of the switch is on the home page.  
192.168.1.1 could interfere with another device on the network.

## Set Security

We recommend changing the administrator and read-only password before you place the switch in service.

The administrator password is used for the management interface (HTTP session), Telnet, and the FTP interface (used to upgrade the firmware). The user name is verified for the FTP session only. The user name for the HTTP session is not checked (therefore can be anything). The read-only password is used for read-only access to the management interface (HTTP session).

Use these steps to change your administrative or read-only user name and password.

1. From the navigation pane, expand the Basic Configuration folder and select Set Security to display the Set Security tab.

The screenshot shows the 'Set Security' tab in the configuration interface. The left navigation pane has 'Basic Configuration' expanded, and 'Set Security' is selected. The main content area shows the 'Security Settings' section with the following fields:

- Security:** A dropdown menu set to 'On'.
- Administrator Password:** A text field with 8 dots.
- Re-enter Administrator Password:** A text field with 8 dots.
- Read-only Password:** A text field with 4 dots.
- Re-enter Read-only Password:** A text field with 4 dots.
- FTP Administrator Username:** A text field containing 'uploader'.

Below the fields, a message states: 'The password you entered second time does not match with the one entered before. Current password has not been changed.' At the bottom is an 'Apply Changes' button.

2. Change the user name and password.  
See [Appendix B](#) for recommendations.
3. Click Apply Changes.
4. Cycle power to the switch to load the new user name and password.

The administrative password applies to Telnet, FTP, and the web browser interface.

---

**IMPORTANT** The 1783-EMS switch does not load the new settings until power is cycled.

---

## Work with Miscellaneous Settings

Use these steps to configure miscellaneous switch settings.

1. From the navigation pane, expand the Basic Configuration folder and select Miscellaneous to display the Miscellaneous tab.

The screenshot shows a web interface with a navigation pane on the left and a main content area on the right. The navigation pane has a tree view with the following items: Home, Login, Basic Configuration (expanded), Network Configuration, Set Security, Miscellaneous (selected), Network Services Setup, Diagnostics, Switch Configuration, and Send an Email. The main content area has three tabs: Network Configuration, Set Security, and Miscellaneous (active). The Miscellaneous tab displays the 'Device Settings' section with the following fields and values:

Device Settings	
Box Name	<input type="text"/>
Minutes of User Inactivity	<input type="text" value="3"/> Range: 0-99
Seconds Between Refresh, Disable with 0	<input type="text" value="5"/> Range: 0-99
Software Version	0.53w110216
Menu Last Compiled	16-Feb-2011
Contact Info	<input type="text"/>
Contact Email	<input type="text"/>
<input type="button" value="Apply Changes"/>	

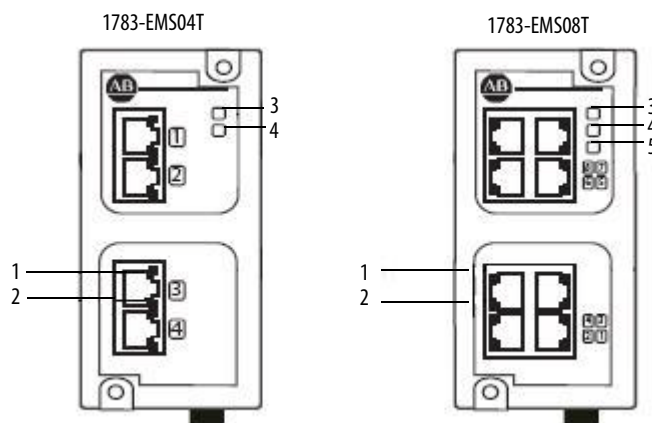
2. Use the information in [Table 3](#) to configure the settings.
3. Click Apply Changes.

**Table 3 - Miscellaneous Switch Settings**

Setting	Description
Box Name	Lets you give your 1783-EMS switch a name that describes its location or connected devices. This feature is useful when multiple 1783-EMS switches are installed. The switch reports this name on the home page. To change this setting, complete this procedure. <ol style="list-style-type: none"><li>1. Click Basic Configuration.</li><li>2. Click Miscellaneous.</li><li>3. Type the new name in the text box and click Apply Changes.</li></ol> The new name does not show in the home page until you click Refresh on the browser.
Minutes of User Inactivity	Lets you change the length of time the management interface (HTTP session) remains open while inactive. Choose from 0...99 min. Select 0 = Feature Disabled for the interface to remain open until it is closed. The default is 3 min.
Seconds Between Refresh	Controls the refresh rate of the management interface. <ul style="list-style-type: none"><li>• Valid values are 0...99 seconds</li><li>• 0 = Feature disabled for no refresh</li><li>• Default value is 5 seconds</li></ul>
Contact Info, Contact Email	Use to identify the responsible service personnel.

## Status Indicators

The figures and table show the status indicators.



Item	Indicator	State	Description
1	Link state <sup>(1)</sup>	Solid green	Ethernet link exists.
		Flashing green	Valid link is present and transmitting data.
2	Data rate <sup>(1)</sup>	Solid amber	100 Mbit link is present.
		Off	10 Mbit link is present.
3	PWR	Solid green	Power to the switch is present.
4	STA	Flashing green	This heartbeat indicator normally flashes at a slow rate. It flashes at a faster rate when the switch is being upgraded or set back to factory default settings by using the button on the back of the switch.
5	UPL	Solid green	Fiber transceiver present.
		Flashing green	Flashing indicates data is being transmitted over the gigabit link on the 1783-EMS08T switch that has a gigabit fiber transceiver on the bottom of the switch.

(1) Appears on all copper Ethernet ports.

## Network Services Setup

This chapter covers information related to network services setup using the switch's web interface, including how to configure these protocols:

- Simple Network Management Protocol (SNMP)
- Internet Group Management Protocol (IGMP)
- Dynamic Host Configuration Protocol (DHCP)

For information about how to access the web interface for the switch, refer to [Chapter 1](#).

### SNMP

Simple Network Management Protocol (SNMP) specifies the diagnostic data that a host computer must maintain for network management software. Hosts typically keep statistics on the status of their network interfaces, incoming and outgoing traffic, dropped datagrams, and error messages generated. Network management protocols let network management software access these statistics.

SNMP is based on three concepts:

- SNMP managers, also known as client software or SNMP browsers
- SNMP agents, also known as network devices or SNMP servers
- Management Information Base (MIB)

The SNMP manager runs SNMP management software. Network devices to be managed, such as bridges, routers, servers, and workstations, have an agent software module. The agent provides access to a local MIB of objects that reflects the resources and activity of the device. The agent also responds to manager commands to retrieve values from the MIB. The agent and the MIB are on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

The Stratix 6000 switch supports SNMP versions 1 and 2.

- SNMP versions 1 and 2 are generally used for network monitoring without network control.
- The supported versions use a community-based form of security. SNMP managers can access the agent MIB through passwords referred to as community names.
- The Stratix 6000 switch automatically recognizes the SNMP version from an incoming request, but you must manually set the version for SNMP trap destinations, as described on [page 24](#).

## Supported MIBs

The Stratix 6000 switch supports the MIBs listed below.

- MIB-II—The published definition of MIB-II has been modified for the Stratix 6000 switch, as described in [MIB-II Modifications](#) below. For a detailed definition of MIB-II, refer to RFC 1213 at <http://www.ietf.org/rfc/rfc1213.txt>.
- ETHERLIKE-MIB—For a detailed definition, refer to RFC 1643 at <http://tools.ietf.org/html/rfc1643>.
- RMON-MIB—The Stratix 6000 supports only the Ethernet Statistics Group in the RMON-MIB. For a detailed definition, refer to RFC 2819 at <http://tools.ietf.org/html/rfc2819>.

### *MIB-II Modifications*

Standard read-write access has been changed to read-only access for the MIB-II variables listed below.

interface.ifTable.ifEntry.ifAdminStatus  
(Fixed value—device is UP)

at.atTable.atEntry.atIfIndex  
at.atTable.atEntry.atPhysAddress  
at.atTable.atEntry.atNetAddress  
(The ARP cache table cannot be modified)

ip.ipForwarding (Fixed value, not-forwarding, **not** acting as a gateway)  
ip.ipDefaultTTL (Fixed value IP\_DTTTL - 60s)

ip.ipRouteTable.ipRouteEntry.ipRouteDest  
ip.ipRouteTable.ipRouteEntry.ipRouteIfIndex  
ip.ipRouteTable.ipRouteEntry.ipRouteMetric1  
ip.ipRouteTable.ipRouteEntry.ipRouteMetric2  
ip.ipRouteTable.ipRouteEntry.ipRouteMetric3  
ip.ipRouteTable.ipRouteEntry.ipRouteMetric4  
ip.ipRouteTable.ipRouteEntry.ipRouteNextHop  
ip.ipRouteTable.ipRouteEntry.ipRouteType  
ip.ipRouteTable.ipRouteEntry.ipRouteAge  
ip.ipRouteTable.ipRouteEntry.ipRouteMask  
ip.ipRouteTable.ipRouteEntry.ipRouteMetric5  
(A routing entry cannot be added via SNMP)

ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaIfIndex  
 ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaPhysAddress  
 ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaIpAddress  
 ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType  
*(A static entry cannot be added into the ARP cache table)*

tcp.tcpConnTable.tcpConnEntry.tcpConnState  
*(An established or pending TCP connection cannot be reset)*

## SNMP Configuration

Enable SNMP if you want to run SNMP on your network. SNMP is disabled by default.

Before configuring SNMP settings, understand these concepts:

- **Community names**—Community names are passwords to the switch Management Information Base (MIB) that allow a remote manager read-only or read-write access to the switch. The Stratix 6000 switch supports one read-only community name and one read-write community name. You can change the default names.
- **SNMP traps**—SNMP traps are unsolicited messages sent to a remote manager from an agent. Traps are an efficient way to inform managers that are connected to a large number of devices with many objects. By providing unsolicited messaging, traps can reduce SNMP polling by a manager. The Stratix 6000 switch supports two destination traps that can be enabled or disabled. By default, both traps are disabled.

Use these steps to configure SNMP.

1. From the navigation pane, expand the Network Services Setup folder and select SNMP Configuration.

2. From the SNMP Enabled pull-down menu, choose Enabled to use SNMP.
3. Change the default case-sensitive community names if desired.
  - The read-only community enables the switch to validate Get (read-only) requests from a network management station. If you set the SNMP read community, users can access MIB objects, but cannot change them.
  - The read-write community enables the switch to validate Set (read-write) requests from a network management station.
4. In the System Info area, provide optional information about the switch for informational purposes only.
  - a. In the Location field, type the physical location of the switch, such as the building where the switch is located.
  - b. In the Contact field, type the switch name or network administrator.
5. Identify up to two trap destinations by completing the fields below.

Trap Destination Field	Description
Enabled	Check to enable trap messages to be sent.
IP Address	Type the IP address of the SNMP trap recipient.
Port	Type the UDP port number to which traps will be sent. The default port number is 162.
Community	Type the read-only or read-write SNMP community name to be used in traps sent to the destination. Community names are case-sensitive.
SNMP Version	Choose the SNMP version to use.



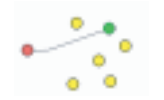
6. Click Apply Changes.

The changes will take effect immediately without requiring you to cycle power to the switch.



## IGMP

Internet Group Management Protocol (IGMP) snooping sorts multicasting devices into groups. This limits the multicast packets received by hosts that do not need the information and makes the network more efficient and deterministic.

Option	Description
Broadcast 	Without IGMP snooping, an I/O module acts like a broadcasting device and all devices on the subnet are flooded with I/O traffic.
Multicast 	IGMP snooping filters the I/O traffic from devices that are not in the intended multicast group.
Unicast 	A message instruction from one Logix controller to another is an example of unicast; it contains one source and one destination address.

By default, IGMP is disabled. Enable IGMP snooping when I/O is running on your network. IGMP helps to isolate this UDP traffic to ports that need to receive it. When it is not used, other devices may be slowed down by the continuous flow of UDP packets.

### IGMP Product Support

Rockwell Automation products support IGMP, version 2.

When using the Logix Designer application to configure your switch, consider the following:

- Settings on the IGMP page in the Add-on Profile overwrite settings made on the web management interface.
- If you are scanning the 1783-EMS switch with the Logix Designer application, use the IGMP page in the Add-on Profile to configure IGMP to avoid confusion. See [Appendix E](#) for more information.

The switch manages a report of IGMP information, including multicast groups, querier information, and IGMP states per virtual local-area network (VLAN). The report is available through the web interface. For more information about this report, refer to [IGMP Report on page 45](#).

## IGMP Querier

The IGMP querier function can be enabled to query your network for group information at a specified time interval. The configuration options available for IGMP querier depend on whether VLANs are enabled on your network.

- If you plan to use VLANs on your network, the IGMP querier function can be enabled for only one VLAN per switch. The IP address of the querier may be different on each VLAN.

You can choose to assign the querier to the management VLAN or a custom VLAN. The querier is assigned to the management VLAN by default.

- If the querier is assigned to the management VLAN, the querier IP address is the IP address defined on the Network Configuration tab, as described in [Set the IP Address on page 15](#).
- If you want to assign the querier to a custom VLAN, you must first set up the custom VLAN on the VLAN Configuration tab, as described in [VLAN Configuration on page 57](#). Assigning the querier to a custom VLAN requires you to know which IP address you want to assign to the querier.
- If you do not plan to use VLANs on your network, you can enable or disable a single querier instance on the network. The querier function is enabled by default. If more than one querier instance is detected on the network, only the querier with the lowest IP address is active. All other queriers are silent.

## IGMP Configuration

Use these steps to configure IGMP.

1. From the navigation pane, expand the Network Services Setup folder and select IGMP Configuration.
2. From the IGMP Snooping pull-down menu, choose Enabled to use IGMP snooping.

When you enable IGMP snooping, additional configuration options appear on the screen.

The screenshot displays the IGMP Configuration interface. The left sidebar contains a navigation tree with 'Network Services Setup' expanded, showing options like SNMP Configuration, IGMP Configuration (selected), DHCP Configuration, DHCP Address Table, MAC Address Labels, Email Configuration, and SMS Configuration. The main content area has tabs for different configuration sections. The 'IGMP Configuration' tab is active, showing the following settings:

- IGMP Configuration:**
  - IGMP Snooping (Multicast Routing): Enabled
  - IGMP Version: V2
- IGMP Querier Configuration:**
  - Querier Mode: Enabled
  - Querier Period (in minutes): 2 (Range: 1-60)
- Router Ports Configuration:**
  - Autodetect (Querier, MRD, CDP): Enabled
  - Manual: Disabled
- Advanced Configuration:**
  - Multicast Packets Forwarding: To Listeners And Uplink Port
  - Uplink port: Autodetect (Querier)

An 'Apply Changes' button is located at the bottom of the configuration panel.

3. From the IGMP Version menu, choose version 1 or 2.

Version 2 is the default when IGMP snooping is enabled and is the recommended setting. Per the IGMP definition, hosts and routers implementing differing IGMP versions will interoperate correctly on the network.

4. If VLAN is **not** enabled on the switch, choose to enable or disable the IGMP querier function from the Querier Mode pull-down menu.

or

If VLAN is enabled on the switch, choose one of these options from the Querier Mode pull-down menu:

- Disabled—The IGMP querier function is disabled on all VLANs.
  - Enabled on Management VLAN—The IGMP querier function is enabled and assigned to the management VLAN only. This is the default setting. For more information about setting up the management VLAN, refer to [VLAN Configuration on page 57](#).
  - Enabled on Custom VLAN—The IGMP querier function is enabled and assigned to a custom VLAN. If you choose this option, you must also specify the querier VLAN and IP address as described in step 6.
5. In the Querier Period field, specify a time interval in minutes, 1...60, to determine how often your network is queried for group information.

The default querier period is 2 minutes.

---

**IMPORTANT** Specify the same number of minutes on all switches in the network. The querier period must be specified even if the querier function is disabled.

---

6. If you chose the Enabled on Custom VLAN querier mode, complete the fields described below.
  - Querier VLAN—Choose the custom VLAN to which to assign the querier.
  - Querier IP Address—Type the IP address of the querier running on the custom VLAN.

Additional fields appear when you choose the Enabled on Custom VLAN querier mode.

The screenshot shows the 'IGMP Querier Configuration' dialog box. It has four fields: 'Querier Mode' (a dropdown menu set to 'Enabled on Custom VLAN'), 'Querier Period (in minutes)' (a text box with '2' and a 'Range: 1-60' note), 'Querier VLAN' (a dropdown menu set to 'Default - 1'), and 'Querier IP Address' (a text box with '0.0.0.0'). Each field has a help icon (a question mark in a circle) to its left.

7. In the Router Ports Configuration area, choose the methods to use for detecting when a multicast router is connected to a switch port.

When a multicast router, including IGMP querier, is connected to a switch port, all multicast packets and IGMP reports are forwarded on that port. This behavior is important for the proper functioning of IGMP snooping.

You can enable one or both of the following options:

- **Autodetect**—Accept the default setting of Enabled if you want the switch to automatically determine whether an end station or multicast router is connected to its ports. To determine which type of device is connected to a port, the switch uses Cisco Discovery Protocol (CDP) or Multicast Router Discovery (MRD).
  - **Manual**—Enable this setting if you need to connect a switch from a different vendor that does not support CDP or MRD protocols. When you enable the Manual setting, a series of checkboxes appears, so you can specify which ports will be connected to a router that does **not** support CDP or MRD protocols.
8. From the Multicast Packets Forwarding pull-down menu, choose where to forward multicast packets.
    - **To Listeners Only**—The switch forwards multicast packets to ports in the Listening state only.
    - **To Listeners and Uplink Port**—The switch forwards multicast packets to ports in the Listening state and the uplink port. This is the default setting.

**TIP** This setting is useful if you need to route multicast packets between two networks.

- **To Listeners and All Snooper Ports (Standard)**—The switch forwards multicast packets to ports in the Listening state and to all multicast routers, or snoopers. Use this setting if you want multicast traffic to be filtered only on ports where end stations are connected and not between switches.
9. From the Uplink Port pull-down menu, choose Autodetect (Querier) if you want the Stratix 6000 switch to automatically determine the uplink port. Otherwise, set the uplink port manually by choosing a specific port.
  10. Click Apply Changes.

The changes will take effect immediately without requiring you to cycle power to the switch.

## DHCP

The 1783-EMS switch can function as a Dynamic Host Configuration Protocol (DHCP) or BOOTP server.

### IMPORTANT

Do not confuse this with the BOOTP/DHCP client, which lets the 1783-EMS switch receive an address from a DHCP/BOOTP server.

## Dynamic IP Address Assignment by IP Address Pool

### IMPORTANT

Keep this feature shut off if this device is on a larger IT-controlled network. Company networks typically have DHCP servers in place to service the computers on the network with IP addresses. This device can conflict with the existing DHCP servers on the network and prevent them from assigning addresses.

The 1783-EMS switch has the ability to assign IP addresses to 32 nodes. Use these steps to configure DHCP settings.

1. Establish a connection with the 1783-EMS switch.
2. From the navigation pane, expand the Network Services Setup folder and select DHCP Configuration.
3. From the DHCP Server pull-down menu, choose On—Assigned from Pool.

This setting enables DHCP server functionality. By default, this setting is off.

The screenshot displays the configuration interface for the 1783-EMS switch. The left-hand navigation pane is expanded, showing the 'Network Services Setup' folder with 'DHCP Configuration' selected. The main configuration area is titled 'DHCP Configuration Settings' and includes the following fields:

- DHCP Server:** Set to 'On - Assigned From Pool' (dropdown menu).
- DHCP Pool From:** 192.168.1.70
- DHCP Pool To:** 192.168.1.101
- Subnet Mask:** 255.255.255.0
- Default Gateway:** 192.168.1.1
- DNS Primary:** 192.168.1.1
- DNS Secondary:** 192.168.1.1
- Domain Name:** ra.rockwell.com
- Dynamic Bootp:** Enabled (dropdown menu)
- Default Lease Time:** 7 days, Range: 0-49710

On the right side of the settings, there is a section for 'Port Based Address Assignment' with 8 ports, each with an associated IP address:

Port	IP Address
Port 1	192.168.1.70
Port 2	192.168.1.71
Port 3	192.168.1.72
Port 4	192.168.1.73
Port 5	192.168.1.74
Port 6	192.168.1.75
Port 7	192.168.1.76
Port 8	192.168.1.77

At the bottom of the configuration area, there is a note: 'Note: If using DHCP Assignment by port, use 0.0.0.0 to disable DHCP on a port' and an 'Apply Changes' button.

4. Type your subnet and gateway addresses for the network.
5. Type the primary and secondary DNS server addresses.
6. Type the domain name, if applicable.
7. Use DHCP Pool From and DHCP Pool To to assign a range of addresses.

The switch assigns an address within the specified range.

8. Enable Dynamic BOOTP to answer BOOTP requests.
9. Type the number of days to specify the default lease time for DHCP requests.

The default value is 7 days.

10. Click Apply Changes and cycle power for the changes to take effect.

## Dynamic IP Address Assignment by Port

The 1783-EMS switch has the ability to assign IP addresses based on the port where the device is connected. When used properly, this feature provides for easy replacement of Ethernet equipment on the factory floor.

---

<b>IMPORTANT</b>	If multiple devices are connected to a port with an uplink to another switch, the IP address is sent to the first device to request it from the port. If a field is set to an address of 0.0.0.0, a DHCP request on the port is ignored.  Most applications with programmable controllers do not require changes to the DNS, domain name, and lease time fields. If these functions do not apply to your network, leave these fields at their default value.
------------------	--

---

Use these steps to set up dynamic IP address assignment by port.

1. Establish a connection with the 1783-EMS switch.
2. Click Network Services Setup and DHCP Configuration.
3. From the DHCP Server pull-down menu, choose On - Assigned by Port.

By default, this setting is off.

**DHCP Configuration Settings**

DHCP Server:  Port Based Address Assignment

DHCP Pool From:  Port 1:

DHCP Pool To:  Port 2:

Subnet Mask:  Port 3:

Default Gateway:  Port 4:

DNS Primary:  Port 5:

DNS Secondary:  Port 6:

Domain Name:  Port 7:

Dynamic Bootp:  Port 8:

Default Lease Time:  days, Range: 0-49710

**Note: If using DHCP Assignment by port, use 0.0.0.0 to disable DHCP on a port**

4. Type your subnet and gateway addresses for the network.
5. Type the primary and secondary DNS server addresses.  
The domain name is automatically populated if the 1783-EMS switch resides on a domain.
6. Type an IP addresses for each port.
7. Click Apply Changes and cycle power for the changes to take effect.

## DHCP Address Table

The DHCP Address table is populated when the server is set to assign an IP address from a pool. This table details which IP address is assigned to a device.



## MAC Address Labels

MAC address labels let you associate a user-friendly label to a MAC ID within the 1783-EMS user interface. When a label is associated with a MAC ID, it is reflected in the MAC ID table and the MAC ID management interface. This feature eases troubleshooting a network. The labels are reflected in the MAC Address Report and the MAC ID Management Configuration page.

To access the MAC Address Label tab, from the navigation pane, expand the Network Services Setup folder and select MAC Address Labels.

MAC Address Labels		MAC Address Labels	
MAC Address	Descriptive Name	MAC Address	Descriptive Name
00:00:00:00:00:00		00:00:00:00:00:00	
00:00:00:00:00:00		00:00:00:00:00:00	
00:00:00:00:00:00		00:00:00:00:00:00	
00:00:00:00:00:00		00:00:00:00:00:00	
00:00:00:00:00:00		00:00:00:00:00:00	
00:00:00:00:00:00		00:00:00:00:00:00	
00:00:00:00:00:00		00:00:00:00:00:00	
00:00:00:00:00:00		00:00:00:00:00:00	
00:00:00:00:00:00		00:00:00:00:00:00	
00:00:00:00:00:00		00:00:00:00:00:00	

Apply Changes

## Email Configuration

The 1783-EMS switch includes an embedded email client that uses an email relay server or gateway message server to send email and text messages to a mail recipient, mobile telephone, or portable wireless device.

The network gateway address and DNS information must be entered on the Network Configuration tab. This setup is required once and is stored in 1783-EMS nonvolatile memory. See [Set the IP Address](#) for help setting up the network addresses. For help locating these IP addresses, see your network administrator.

---

**IMPORTANT** If you do not intend to use symbolic names, for example, smtp@yahoo.com, but rather only IP addresses to access your mail server, you can leave the DNS configuration empty.

---

Use these steps to set up SMTP server parameters.

1. From the navigation pane, expand the Network Services Setup folder and select Email Configuration.

The screenshot shows a web interface for configuring network services. On the left is a navigation pane with a tree view containing: Home, Login, Basic Configuration, Network Services Setup (expanded), SNMP Configuration, IGMP Configuration, DHCP Configuration, DHCP Address Table, MAC Address Labels, Email Configuration (selected), SMS Configuration, Diagnostics, Switch Configuration, and Send an Email. The main content area has tabs for: SNMP Configuration, IGMP Configuration, DHCP Configuration, DHCP Address Table, MAC Address Labels, and Email Configuration. The Email Configuration tab is active, displaying two sections: 'SMTP Server Configuration' and 'Email Message Configuration'. The SMTP section includes fields for 'IP or Hostname', a checkbox for 'SMTP Authentication', 'UserName', and 'Password'. The Email Message section includes a 'Signature' text area. An 'Apply Changes' button is at the bottom.

2. In the IP or Hostname field, type your SMTP server name or IP address.
3. If authentication is used, as required by most ISPs, check SMTP Authentication and type your user name and password.

Basic authentication, compatible with POP servers, is supported, and the name and password entered here are those associated with your outgoing email account.

4. Test sending an email message from the Send an Email web page making sure that the 1783-EMS switch is connected to a network that has access to your email server, which may require access to the Internet.

---

**IMPORTANT** A status message providing the result of this operation is displayed at the bottom of the page. Detailed error descriptions let you identify a potential anomaly.

---

## SMS Configuration

If you intend to use a Short Message Service (SMS) gateway service to send text messages to a mobile telephone or portable wireless device, use this procedure.

1. From the navigation pane, expand the Network Services Setup folder and select SMS Configuration.

The screenshot shows the 'SMS Configuration' page in a web browser. On the left is a navigation pane with a tree view containing 'Home', 'Login', 'Basic Configuration', 'Network Services Setup' (expanded), 'Diagnostics', 'Switch Configuration', and 'Send an Email'. Under 'Network Services Setup', 'SNMP Configuration', 'IGMP Configuration', 'DHCP Configuration', 'DHCP Address Table', 'MAC Address Labels', 'Email Configuration', and 'SMS Configuration' are listed. The 'SMS Configuration' item is highlighted. The main content area has a tabbed interface with tabs for 'SNMP Configuration', 'IGMP Configuration', 'DHCP Configuration', 'DHCP Address Table', 'MAC Address Labels', 'Email Configuration', and 'SMS Configuration'. The 'SMS Configuration' tab is selected. It contains two sections: 'SMS Gateway Configuration' and 'SMS Configuration'. The 'SMS Gateway Configuration' section has fields for 'SMS GW Server', 'Email Address', 'Authentication', 'Account ID', 'User', and 'Password'. The 'SMS Configuration' section has a 'Signature' field. An 'Apply Changes' button is located at the bottom of the page.

2. In the SMS GW Server field, type the email address of your SMS gateway provider.
3. Type your account ID.
4. Type your user name and password.

---

**IMPORTANT** Most newer cell phones accept email directly. If your phone accepts email, you do not need to use an SMS gateway service to get text messages from the 1783-EMS switch. See your cell phone provider website to get the email address of your cell phone.

---

5. Test this setup by using the Send an Email page, making the To: field the phone number of the device to receive the message.

## Send Email via a Logix Controller-initiated Message Instruction

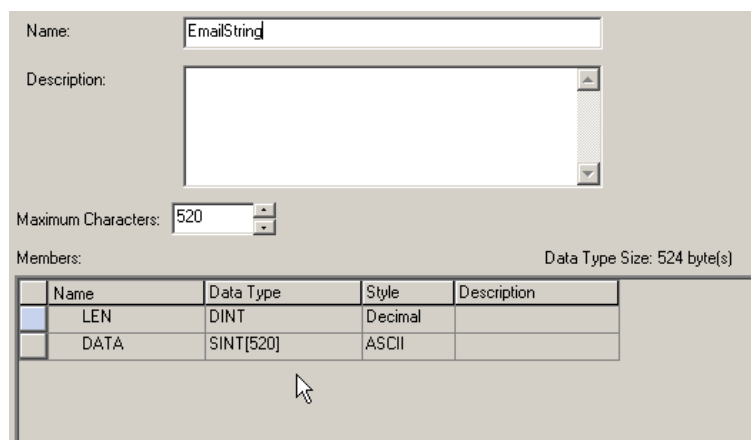
A Logix controller can send a generic CIP message to the 1783-EMS switch instructing it to send an email message to an SMTP email server. This is useful to communicate Logix controller data, network alerts, and application conditions to appropriate personnel. You need two controller-scoped string tags.

One tag contains the email text and the other contains the status of the email transmission (the result code). These tags contain as many as 520 characters. You must first create a user-defined STRING data type. The default STRING data type is not large enough for most email text.

For example, create a STRING data type named EmailString. Next, create one controller-scoped tag of this new data type to contain the email text named

EMS\_EMAIL. Create a second controller-scoped tag of this new data type to contain the transmission status named EmailDstStr.

Both of these tags are of the type EmailString.



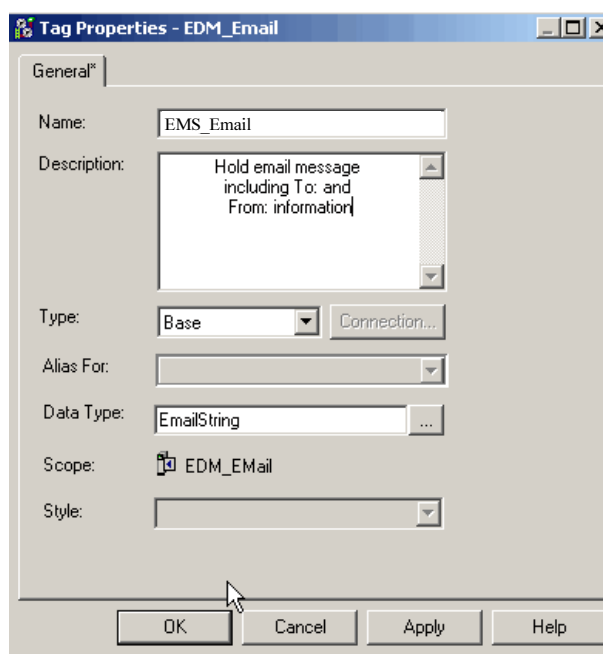
Name	Data Type	Style	Description
LEN	DINT	Decimal	
DATA	SINT[520]	ASCII	

Use these steps to send an email via a Logix controller-initiated message instruction.

1. Open the Logix Designer application.
2. From the Controller Organizer, expand Data Types and Strings.
3. Create an EmailString type and note the initial LEN field.

When you edit this tag, its length is inserted by the RSLogix editor.

When you send email with MSG instructions, the length of the LEN field must be added to the string length, as shown in the program example.



4. Open tags and click the Edit tab.
5. Insert EMS\_EMAIL and EmailDstStr.

Both tags are of the type EmailString. These tags can be created later when the MSG instruction is inserted. The text of the email does not have to be static. You can program a Logix controller project to collect specific data to be sent in an email. For more information on using ladder logic to manipulate string data, see the Logix5000 Controllers Common Procedures Programming Manual, publication [1756-PM001](#).

Scope: EDM\_Email Show... Show All

	Name	Alias For	Base Tag	Data Type	Style	Description
	EDM_Email			EmailString		Holds Email message can include To: and From: or this can be set using attributes
	EmailDstStr			EmailString		Holds result from sending email
	SendEmail			MESSAGE		Structure used to send email
	Stratix6K:C			AB:1783_EMS08...		
	Stratix6K:I			AB:1783_EMS08...		
	Stratix6K:O			AB:1783_EMS08...		
	Set_Attribute			MESSAGE		
	Set_Attribute_...			EmailString		

**6. Create a tag of the type MESSAGE.**

The example uses a tag named SendEmail\_EDM.

**7. Set the message type to generic CIP, service code object class 32f, instance 1, attribute 0.**

Note that the source length is the length of the string in the EMS\_EMAIL tag + 4.

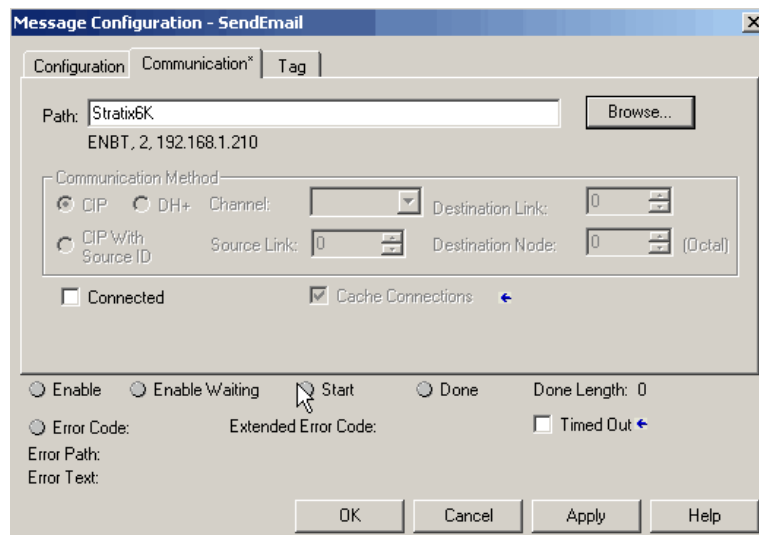
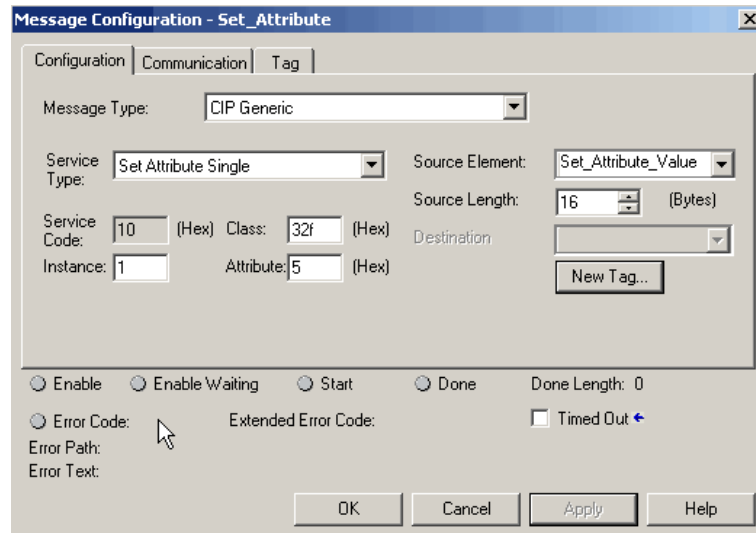
---

**IMPORTANT** Be sure to enter the correct communication path. Click the Communication tab and then Browse. Select the name associated with your 1783-EMS switch from the I/O tree and click Apply.

In this example, the name is Stratix6K. For more information on configuring the path of a MSG instruction, see the Logix Controllers General Instructions Reference Manual, publication [1756-RM003](#).

---

If an error occurs, you see the Error Code (Extended Error Code). The result code from the SMTP server is stored in the EmailDstStr tag. See [page 41](#) for a table of status codes.

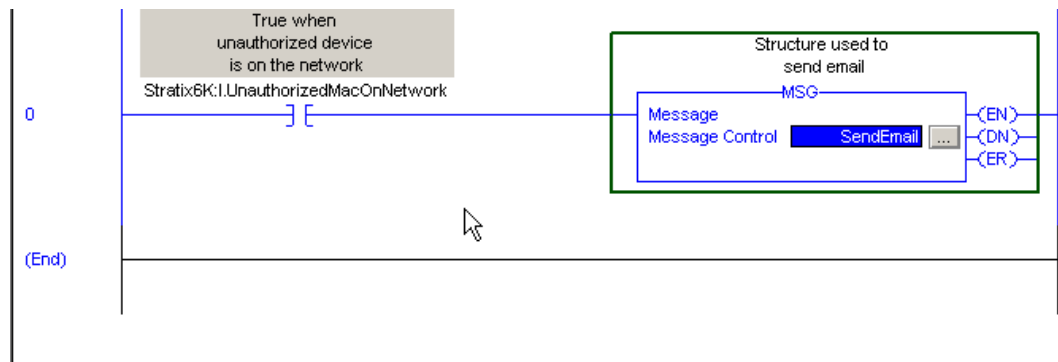


8. Open your routine window (for example, MainRoutine) and insert an MSG instruction.
9. Select the SendEmail MESSAGE tag.
10. Double-click the MSG block and choose source (EMS\_EMAIL) and destination (EmailDstStr) tags.

In our example, we have GetAttributeValue and SetAttributeValue tags and GetAttribute/SetAttribute MESSAGE tags for individual attribute handling.

Message sending is triggered by the trigger\_send BOOL tag. The message is sent when you press Ctrl+T in the rung or set the tag value to 1.

The figure shows an example of a program that sends an email when any unauthorized MAC is detected by the 1783-EMS switch.

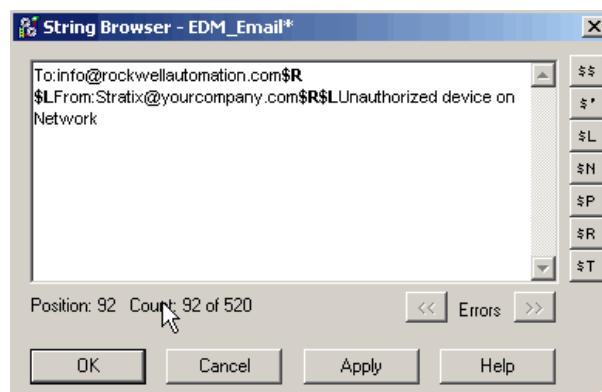


## Enter the Text of the Email Message

Use the string browser to enter the text of the email. In the example, you enter the email text into the EWEB\_EMAIL tag. To include To, From, and Subject fields in the email, use <CR><LF> symbols to separate each of these fields. The To and From fields are required. The Subject field is optional. Use a second set of <CR><LF> symbols after the last one of these fields you enter.

**EXAMPLE** To: email address of recipient \$r\$l  
 From: email address of sender \$r\$l  
 Subject: subject of message \$r\$l \$r\$l  
 body of email message

The maximum length of an email message is 520 characters. An additional 4-byte string-length value is added to the tag. As a result, the maximum source length is 524 characters.



**TIP** <CR><LF> characters are coded as \$r\$l.

## Send an SMS from the Logix Controller

Text messages are sent in the same way as a normal email message. The only difference is the recipient in the To: field is a telephone number instead of an email address.

The email format for sending text messages by using a SMS gateway service is as follows:

- api\_id:nnnnnnn\$r\$l
- user:xxxxx\$r\$l
- password:ppppp\$r\$l
- to:cell\_phone#\$r\$l
- text:Simple text\$r\$l
- text:on all\$r\$l
- text:3 lines. \$r\$l
- text:Sms signature - 1234567890123456\$r\$l

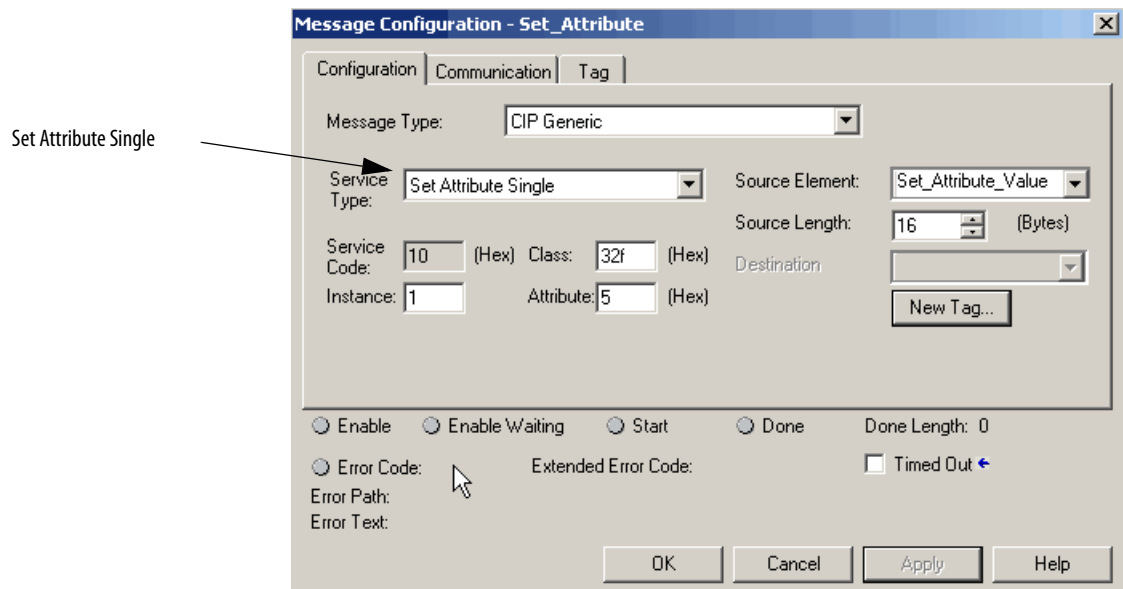
## Modify the SMTP Server Setup in a Logix Controller Program

You can modify the SMTP server you use to send email by setting class 32f, attribute #5.

---

**IMPORTANT** Set Attribute Single uses service code 10.

---





## Email and SMS Error Codes

Examine the destination element of the email MSG to see if the email was successfully delivered to the mail relay server.

This indicates that the mail relay server placed the email message in a queue for delivery. It does not mean the intended recipient successfully received the email message.

This table shows possible codes that could be in this destination element.

**Table 4 - Error Codes**

Error Code (hex)	Extended-error Code (hex)	Description
0x00	None	Delivery successful to the mail relay server.
0x02		Resource unavailable. The email object was unable to obtain memory resources to initiate the SMTP session.
0x08		Unsupported Service Request. Make sure the service code is 0x4B and the class is 0x32F.
0x11		Reply data too large. The Destination string must reserve space for the SMTP server reply message. The reply can be 470 bytes max.
0x13		Configuration data size too short. The Source Length is less than the Source Element string size plus the 4-byte length. The Source Length must equal the Source Element string size + 4.
0x15		Configuration data size too large. The Source Length is greater than the Source Element string size plus the 4-byte length. The Source Length must equal the Source Element string size + 4.
0x19		Data write failure. An error occurred when attempting to write the SMTP server address (attribute 4) to nonvolatile memory.
0xFF	0x0100	Error returned by email server; check the Destination string for reason. The email message was not queued for delivery.
	0x0101	SMTP mail server not configured. Attribute 5 was not set with a SMTP server address.
	0x0102	To: address not specified. Attribute 1 was not set with a To: address with no To: field header in the email body.
	0x0103	0x0103 From: address not specified. Attribute 2 was not set with a From: address <b>and</b> no From: field header in the email body.

Table 4 - Error Codes

Error Code (hex)	Extended-error Code (hex)	Description
0xFF	0x0104	<p>Unable to connect to SMTP mail server set in Attribute 5. If the mail server address is a hostname, make sure that the device supports DNS and a Name Server is configured.</p> <p>If the hostname is not fully qualified, for example, mailhost and not mailhost.xx.yy.com, then the domain must be configured as xx.yy.com.</p> <p>Try ping &lt;mail server address&gt; to be sure the mail server is reachable from your network.</p> <p>Also try telnet &lt;mail server address&gt; 25 to attempt to initiate a SMTP session with the mail server via telnet over port 25. If you connect, enter 'QUIT'.</p>
	0x0105	<p>Communication error with SMTP mail server. An error occurred after the initial connection with the SMTP mail server.</p> <p>See the ASCII text following the error code for more details on the type of error.</p>
	0x0106	<p>SMTP mail server hostname DNS query did not complete. A previous send service request with a hostname as the SMTP mail server address did not yet complete.</p> <p>Note that a timeout for a DNS lookup with an invalid hostname can take up to 3 min.</p> <p>Long timeouts can also occur if a domain name or name server is not configured correctly.</p>
	0x0107	No DNS entry.
	0x0108	DNS not configured.
	0x0109	GW not configured.
	0x0110	System fail (socket error).

## Diagnostics

This chapter provides information about these switch diagnostic features available through the web interface:

- Device utilization
- Rapid Spanning Tree Protocol (RSTP) report
- Internet Group Management Protocol (IGMP) report
- MAC address report
- Alarm setup
- PLC configuration
- Automatic email alerts
- Email queue status
- Switch controller restart
- Display switch counters

For information about how to access the web interface for the switch, refer to [Chapter 1](#).

To upgrade firmware for the 1783-EMS switch, refer to [Appendix A](#).

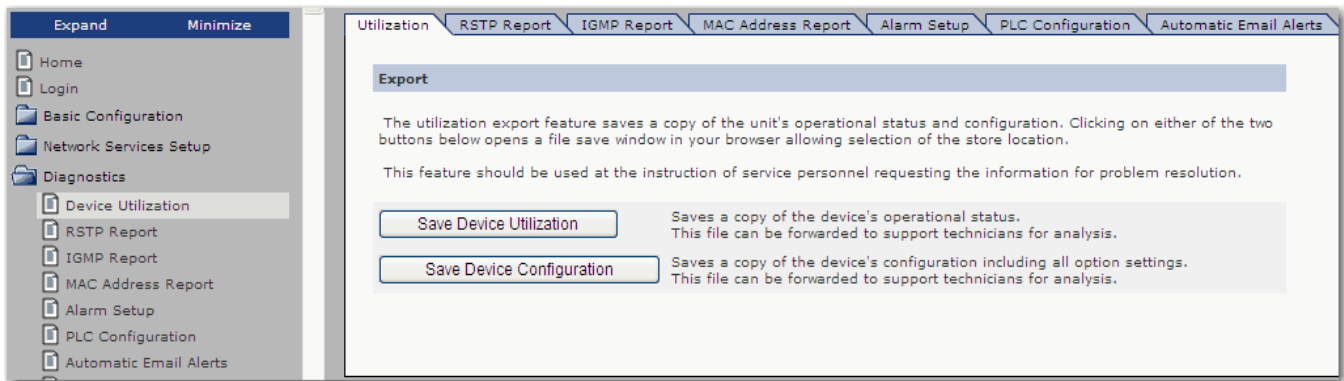
## Device Utilization

The Device Utilization tab provides a way to download these files that may be useful to send to Technical Support for diagnostic purposes:

- Device utilization file—Includes various performance metrics about how the memory and processor is affected by your network.
- Device configuration file—Includes all of the switch's configuration settings.

To download device files to your computer, use these steps.

1. From the navigation pane, expand the Diagnostics folder and click Device Utilization to display the Utilization tab.



2. To download the device utilization file, click Save Device Utilization and then browse to the location on your computer where you want to download the file.
3. To download the switch's configuration file, click Save Device Configuration and then browse to the location on your computer where you want to download the file.

## RSTP Report

If Rapid Spanning Tree Protocol (RSTP) mode is set to Enabled or STP Compatible on the RSTP Configuration tab, the STP/RSTP status for all switch ports appears on the RSTP Report tab.

To access the RSTP Report tab, from the navigation pane, expand the Diagnostics folder and click RSTP Report. The Clear Statistics button lets you reset the data on the page without having to cycle power after testing.

For more information about configuring STP/RSTP, refer to [STP/RSTP on page 53](#).

The screenshot shows the RSTP Report tab selected in the navigation pane. The main content area displays the following information:

Spanning Tree Information	
Name	Value (Priority-MAC)
Switch ID	8000-0000BC611610
Root ID	8000-0000BC611610
Mode	RSTP

Performance Information				
Name	Current	Peak	Limit	Overruns
RSTP Processing Delay [ms]	0 (0)	0 (0)	1000	0 (0)
BPDU Transmission Delay [ms]	2 (2)	3 (3)	200	0 (0)

Clear Statistics

Port Status							
Port #	Priority(hex)	Path Cost	Status	Role	Root Path Cost	Type	Uptime
1	80	200000	Forwarding	Designated	200000	p2p edge	00:00:15

## IGMP Report

Internet Group Management Protocol (IGMP) manages membership in IP multicast groups. Only hosts in that group receive the packet. IGMP prevents a multicast packet from behaving like a broadcast (transmitted to all network hosts).

The switch manages a report of IGMP groups and hosts belonging to those groups, along with querier information, IGMP states per VLAN, and neighboring routers.

To access the report, from the navigation pane, expand the Diagnostics folder and click IGMP Report.

The screenshot shows the IGMP Report tab selected in the navigation pane. The main content area displays the following information:

Multicast Groups (Listeners)		
Ports	MAC Address	IP Address
No IGMP listeners detected.		

Querier Info	
State	OK
IP Address	192.168.1.1
Version	V2
VLAN ID	400

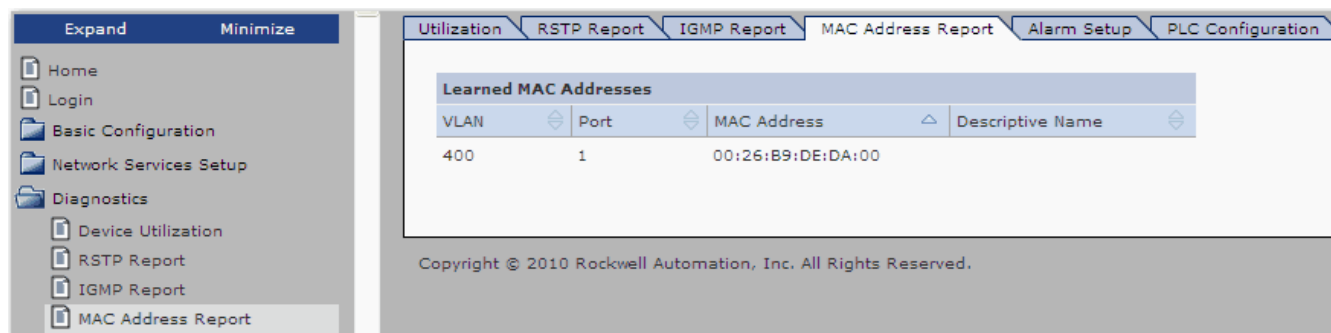
IGMP State (per VLAN)					
VLAN	Querier (IP, Port, Version)	Listeners	Router Ports	Forward Ports	
400	192.168.1.1 M V2	0	-	-	

Neighboring Switches/Routers				
VLAN	Port	IP Address	Snooping	Protocol
400	M	192.168.1.1	Enabled	querier

## MAC Address Report

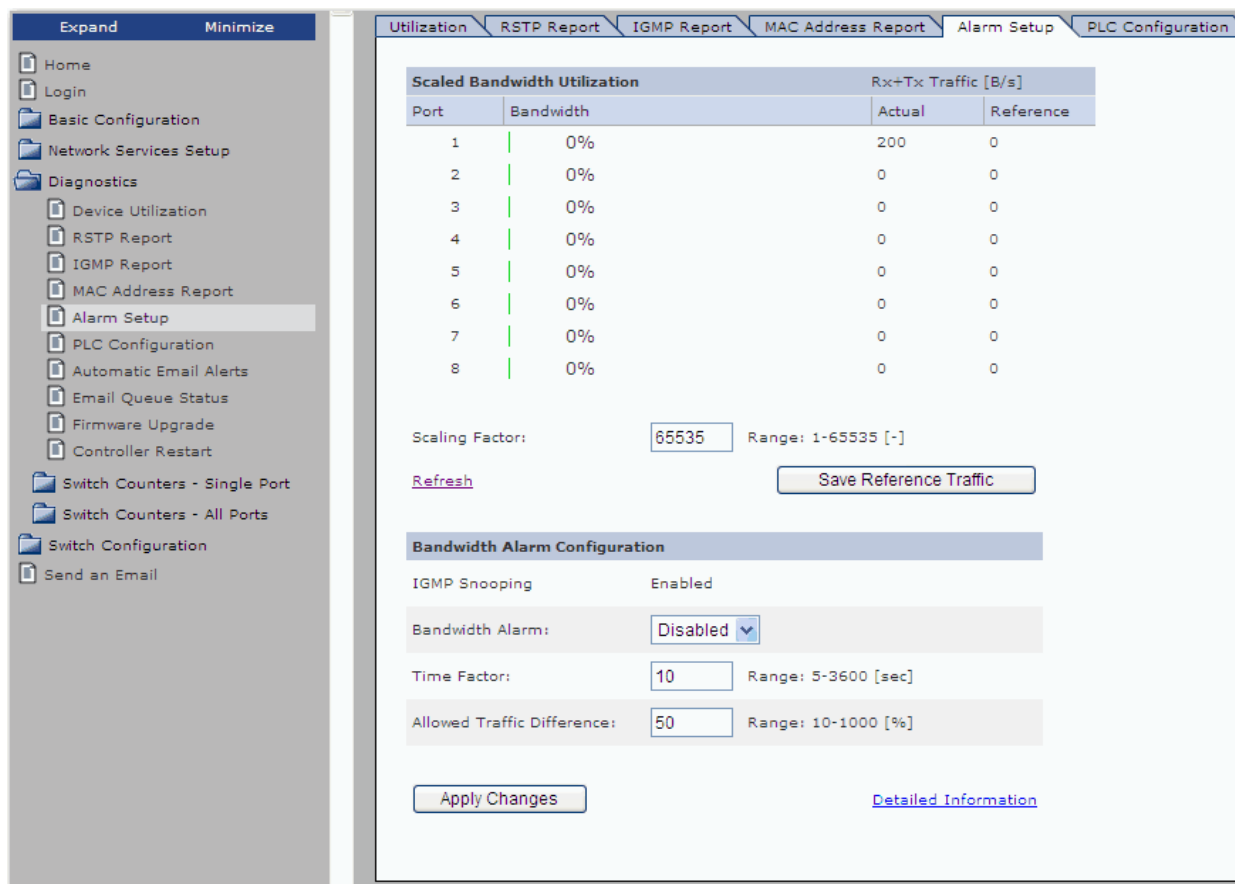
All Ethernet equipment has a MAC address (hardware address). To access a list of these addresses, from the navigation pane, expand the Diagnostics folder and click MAC Address Report.

A pool of MAC addresses is assigned to each Ethernet product manufacturer. For example, Allen-Bradley Ethernet equipment MAC addresses usually begin with 00:00:BC.



## Alarm Setup

The Alarm Setup tab displays the bandwidth on each port. To access the Alarm Setup tab, from the navigation pane, expand the Diagnostics folder and click Alarm Setup.



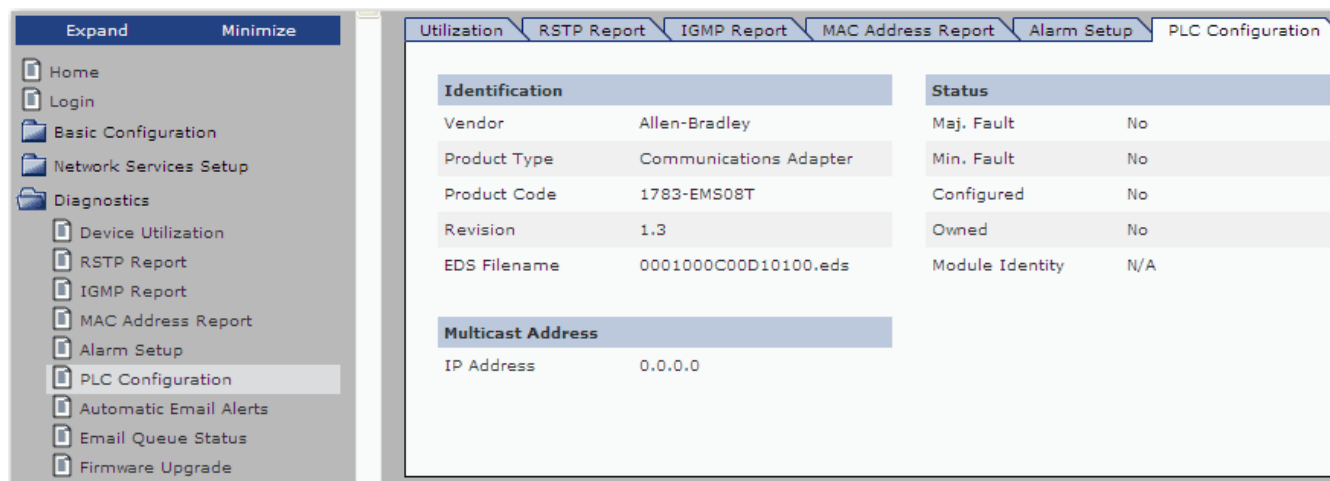
The bar turns red when the bandwidth is out of range. The Alarm Setup tab also displays these items:

- **Refresh**—Used to refresh your screen with the latest information, the screen automatically refreshes at the rate configured under Basic Configuration and Refresh Rate.
- **Save Traffic Reference**—Used as a benchmark for the system network. Click this button when the network is running as it should in production. The switch calculates the difference between the reference point and the current levels of traffic for each port. If it varies to an alarm state, it sends an input to the switch's controller indicating the port number. See [Appendix D](#) for the complete I/O table for the 1783-EMS switch.
- **Bandwidth Alarm**—Disabled by default, when enabled calculates the difference between the reference point of the network and the current rate of traffic. If a variation exceeding the allowed traffic difference occurs, it sends an input to the switch's controller indicating the port number where the bandwidth shortage is occurring.
- **Scaling Factor**—Most applications have such a small amount of traffic that the bandwidth is only a fraction of a percent. The scaling factor provides a more visual representation of the traffic on each port. See the detailed information link on the Alarm Setup page for more information on how the bandwidth is calculated.
- **Time Factor**—The length of time packets are counted to determine the bandwidth percentage for each port. See the detailed information link on the Alarm Setup page for more information on how the bandwidth is calculated.
- **Allowed Traffic Difference**—The percentage that the current traffic level can vary in either direction, from the stored reference value, before an input is sent to the switch's controller.

## PLC Configuration

The PLC Configuration tab display read-only information about the 1783-EMS switch relating to the PLC connection. Information includes the EDS file name, multicast address used by the 1783-EMS switch, and status information on the 1783-EMS switch.

To access the PLC Configuration tab, from the navigation pane, expand the Diagnostics folder and click PLC Configuration.



## Automatic Email Alerts

The 1783-EMS switch can be configured to automatically send system alert messages via the email client to a recipient's email address, mobile telephone, or portable wireless device.

This can be useful in a critical control network to alert network personnel of an anomaly in the network as it occurs.

Events in the network like unauthorized MAC ID's, bandwidth utilization alarms, or port down can be communicated automatically to the responsible supervisor.



**Automatic Email Alerts**

Automatic Alerts: Disabled

From Identifier:

**Recipients**

**Automatic Email Alert Messages**

Select	Automatic Alert	Select	Automatic Alert
<input type="checkbox"/>	CIP Communication Established	<input type="checkbox"/>	Unauthorized MAC ID on Port y
<input type="checkbox"/>	CIP Communication Lost	<input type="checkbox"/>	Port z Active
<input type="checkbox"/>	CIP Multicast Connections Active	<input type="checkbox"/>	Port z Down
<input type="checkbox"/>	CIP TCP Connections Active	<input type="checkbox"/>	Bandwidth Alarm on Port w
<input type="checkbox"/>	Configuration Changed		

To enable this capability, use this procedure.

1. From the navigation pane, expand the Diagnostics folder and select Automatic Alerts.
2. From the Automatic Alerts pull-down menu, choose Enabled.
3. Specify the recipients for the alerts by typing up to six email addresses or mobile telephone numbers.
4. Specify which alerts you want to automatically trigger a message by checking the checkbox next to each alert.

You can select any number of automatic alerts from the list.

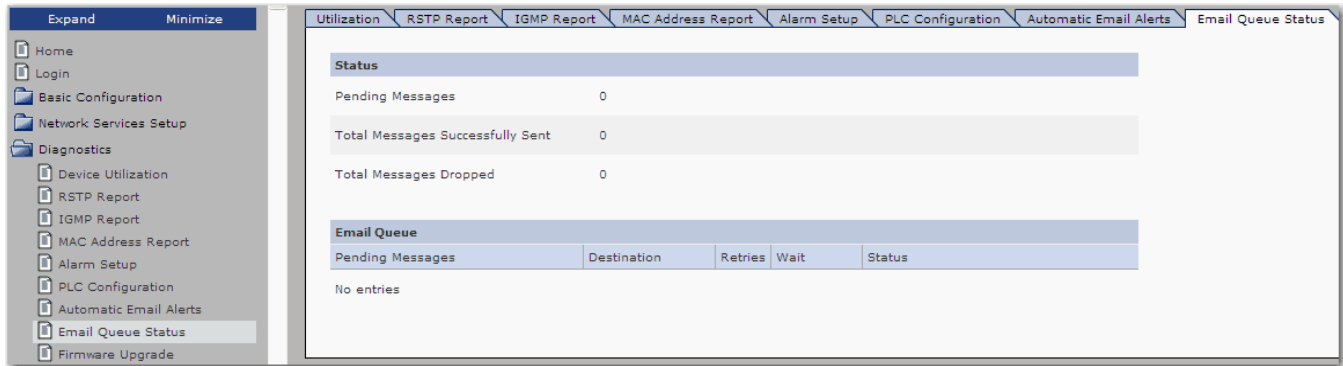
5. Click Apply Changes.

## Email Queue Status

Use the Email Queue Status tab to view these email statuses:

- Number of emails sent successfully
- Any dropped messages
- Pending messages

To access the Email Queue Status tab, from the navigation pane, expand the Diagnostics folder and click Email Queue Status.



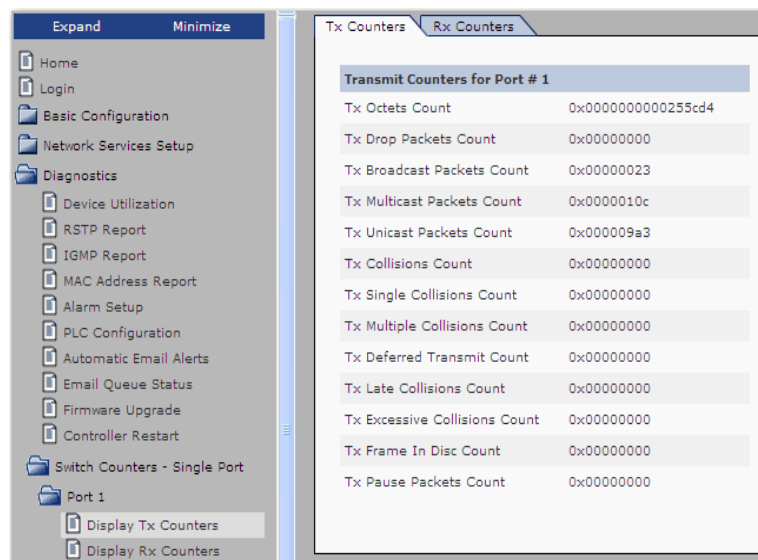
## Switch Restart

You can restart 1783-EMS switch on the Controller Restart tab. Restarting the switch is useful when making configuration changes. The switch must be restarted for some changes to take effect.

To restart the switch, from the navigation pane, expand the Diagnostics folder and click Restart Controller. When a message prompts you to confirm, click OK.

## Display Switch Counters

To access various counts, from the navigation pane, expand the Diagnostics folder, and then expand the Switch Counters - Single Port or Switch Counters - All Ports folder. Navigate to the menu item for the counters you want to view.



Counters are displayed in hex where an octet equals 8 bits. [Table 5](#) lists Transmit (Tx) counters.

**Table 5 - Tx Counters**

Counter	Description
Tx Octet Count	Total of transmitted good octets from the selected port.
Tx Drop Pkts Count	Packet is not acknowledged by the receiving host.
Tx BroadcastPkts Count	Number of good packets sent with destination of everyone. Receivers are unspecified.
Tx MulticastPkts Count	Packets sent to members of multicast group. One terminal to many hosts.
Tx UnicastPkts Count	In contrast with multicast, consists of one terminal transmitting to one host.
Tx Collisions Count	Two terminals transmit packets at the same time causing them to collide. Collision Count should be very low. Collisions could indicate a faulty device on the network.
Tx SingleCollision Count	Packet collides with one other terminal's transmitted packet.
Tx MultipleCollision Count	Packet collides with more than one terminal's transmitted packets.
Tx DeferredTransmit Count	Number of packets delayed because the network is busy. The higher the number, the less deterministic your network.
Tx LateCollision Count	Collision is detected later than the 512 bits into the packet transmission.
Tx ExcessiveCollision Count	Network device is not acting in compliance with a flow control request.
Tx PausePkts Count	Pause frames sent by this port.

[Table 6](#) lists Receive (Rx) counters.

**Table 6 - Rx Counters**

Counter	Description
Rx Octets	Total good octets received on selected port.
Rx Undersize Pkts	Good packets that are under 64 octets long.
Rx Pause Pkts	Pause packets received by this port.
Pkts64 Octets	Data packets = 512 bits.
Pkts65to127 Octets	Data packets = 520 ... 1016 bits.
Pkts128to255 Octet	Data packets = 1024 ... 2040 bits.
Pkts256to511 Octet	Data packets = 2048 ... 4088 bits.
Pkts512to1023 Octet	Data packets = 4096 ... 8184 bits.
Pkts1024to1522 Octet	Data packets = 8192 ... 12,176 bits.
RxOversize Pkts	Packets over 12,176 bits or 1523 ... 1536 octets.
RxJabbers Pkts	Packets longer than 1522 octets and have an error, usually caused by a faulty device.
RxAlignment Errors	Packets between 64 and 1522 octets and have an error.
RxFCS Errors	Packets received (between 645 and 1522 octets) with FCS (frame check sequence) not matching.
RXGoodPkts	Octets received with no errors.
RXDrop Pkts	Packets dropped due to lack of resources, such as bandwidth or input buffer.
RxUnicast Pkts	Unicast packet received (only one receiving host).
RxMulticast Pkts	Multicast packets received (many receiving hosts).
RxBroadcast Pkts	Received by all hosts on the network.
RxSAChanges	Number of times the Source address of a good packet has changed value. A count greater than 1 indicates a repeater based network.
RxFragments	Packets received less than 64 octets.
RxExcessSizeDisc	Packets received greater than 1536 octets and discarded due to excessive length.
RxSymbolError	Invalid data symbol detected.

## Switch Management

This chapter provides information about switch management options provided through the switch's web interface. The web interface provides these management options:

- STP/RSTP configuration
- VLAN configuration
- Port configuration
- Mirror configuration
- MAC ID management
- Port segmenting
- QoS setup

For information about how to access the web interface for the switch, refer to [Chapter 1](#).

### STP/RSTP

The switch supports these network protocols to prevent loops in redundant network topologies:

- Spanning Tree Protocol (STP), as defined in IEEE 802.1D
- Rapid Spanning Tree Protocol (RSTP), as defined in IEEE 802.1w

By default, STP and RSTP are disabled.

To view the STP/RSTP status for all switch ports, use the RSTP report as described on page [45](#).

### Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree
- Backup—A blocked port in a loopback configuration

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch.

Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to select the root switch and root port for the switched network and the root port and designated port for each switched segment.

## Rapid Spanning Tree Protocol

Rapid Spanning Tree Protocol (RSTP) is an enhanced version of STP that uses point-to-point wiring and provides rapid convergence of the spanning tree. When a point-to-point connection fails, the alternate connection transitions to the forwarding state.

RSTP is implemented on the switch in these ways:

- You can enable RSTP or STP mode on the RSTP Configuration tab. By default, both RSTP and STP are disabled.
- A single instance of RSTP exists for the entire network, regardless of the number of VLANs. This implementation is known as Common Spanning Tree (CST).
- RSTP parameters are port-dependent, or used for determining a specific port's behavior.
- If port mirroring is configured on a port, or a port becomes disabled via the switch's web interface, RSTP becomes disabled on the port.

## STP/RSTP Configuration

To configure the switch for STP or RSTP, use the following procedure.

1. From the navigation pane, expand the Switch Configuration folder and select RSTP Configuration to display the RSTP Configuration tab.

The screenshot shows the RSTP Configuration interface. The left navigation pane has 'Switch Configuration' expanded, with 'RSTP Configuration' selected. The main window has two tabs: 'Bridge Parameters' and 'Port Parameters'. The 'Bridge Parameters' tab is active, displaying the following configuration:

Name	Value	Range
RSTP Mode	Disabled	
Bridge Priority [hex]	8000	0000 - F000
Max Age [sec]	20	6 - 40
Forward Delay [sec]	15	4 - 30
Transmit Hold Count [-]	6	1 - 10
Hello Time [sec]	2	

Note: Switch may be unreachable for a while after you change some Bridge Parameters. Maximum response time is 'Max Age + Forward Delay'.

The 'Port Parameters' tab shows a table of 8 ports:

Port #	Priority [00h - F0h]	Auto Cost	Manual Cost [1 - 200,000,000]	Edge Port OFF   Auto   ON
1	80	<input checked="" type="checkbox"/>	200000	<input type="radio"/> OFF <input checked="" type="radio"/> Auto <input type="radio"/> ON
2	80	<input checked="" type="checkbox"/>	2000000	<input type="radio"/> OFF <input checked="" type="radio"/> Auto <input type="radio"/> ON
3	80	<input checked="" type="checkbox"/>	2000000	<input type="radio"/> OFF <input checked="" type="radio"/> Auto <input type="radio"/> ON
4	80	<input checked="" type="checkbox"/>	2000000	<input type="radio"/> OFF <input checked="" type="radio"/> Auto <input type="radio"/> ON
5	80	<input checked="" type="checkbox"/>	2000000	<input type="radio"/> OFF <input checked="" type="radio"/> Auto <input type="radio"/> ON
6	80	<input checked="" type="checkbox"/>	2000000	<input type="radio"/> OFF <input checked="" type="radio"/> Auto <input type="radio"/> ON
7	80	<input checked="" type="checkbox"/>	2000000	<input type="radio"/> OFF <input checked="" type="radio"/> Auto <input type="radio"/> ON
8	80	<input checked="" type="checkbox"/>	2000000	<input type="radio"/> OFF <input checked="" type="radio"/> Auto <input type="radio"/> ON
9	80	<input checked="" type="checkbox"/>	200000	<input type="radio"/> OFF <input checked="" type="radio"/> Auto <input type="radio"/> ON

An 'Apply Changes' button is located at the bottom left of the main window.

2. Configure bridge parameters as described in the table below.

Bridge Parameter	Description
RSTP Mode	Choose one of the following network modes: <ul style="list-style-type: none"> <li>Disabled—The switch does <b>not</b> run RSTP or STP. This is the default mode.</li> <li>Enabled (RSTP)—The switch runs RSTP.</li> <li>Enabled (STP Compatibility)—Enables the switch to be manually configured to run STP.</li> </ul>
Bridge Priority (hex)	Type a hex value from 0000 . . . F000 to determine which switch on the network is assigned the role of root bridge. The default value is 8000. The spanning tree algorithm uses the following rules to determine the root bridge: <ul style="list-style-type: none"> <li>The switch with the lowest priority becomes the root bridge.</li> <li>If two switches have the same priority, then the switch with the lowest MAC address becomes the root bridge.</li> </ul>
Max Age (sec)	Type a value in seconds from 6 . . . 40 to specify the maximum time that a BPDU is saved before expiring. The default value is 40.
Forward Delay (sec)	Type a value in seconds from 4 . . . 30 to specify the time spent in the Listening and Learning states. The default value is 15.
Transmit Hold Count (-)	Type a value from 1 . . . 10 to configure the number of BPDUs that can be transmitted within the Hello Time interval. The default value is 6.
Hello Time (sec)	Displays the hello time interval in seconds. A switch running RSTP generates configuration messages once every hello time interval. If the switch does not receive a configuration message after an interval of three hello times, it determines that communication is lost.

## 3. Configure port parameters as described in the table below.

Port Parameter	Description
Priority	Type a hex value from 00h . . . F0h to specify the port priority. The port priority is used in conjunction with the path cost to determine which redundant port on the network will be blocked. The default value for each port is 80.
Auto Cost	Check this box to automatically configure the path cost according to the port speed. The port speed can be 10 MB/s, 100 MB/s, or 1 GB/s depending on the connected device. Auto Cost is the default configuration setting.
Manual Cost	If you cleared the Auto Cost checkbox, type a value from 1 . . . 200,000,000 to manually configure the path cost. The default value is 200,000,000.
Edge Port	Click the method for determining whether the port identifies itself as an edge port. Because edge ports cannot create bridging loops in the network, they transition directly to the forwarding state and function much faster than a normal spanning tree port. <ul style="list-style-type: none"> <li>• OFF—The port functions as a normal spanning tree port. When an end station is connected to the port, the port begins forwarding after the Max Age + Forward Delay = 20 + 15 = 35 seconds.</li> <li>• Auto—The switch automatically identifies whether the port is connected to an end station or switch. This is the default setting. <ul style="list-style-type: none"> <li>– If an end station is connected to the port, the port is identified as an edge port after 3 seconds and begins forwarding BPDUs.</li> <li>– If a switch is connected to the port and a BPTU is received, the port immediately loses edge port status and becomes a normal spanning tree port. When BPTUs are no longer received after 3 seconds, the port regains edge port status.</li> </ul> </li> <li>• ON—The switch automatically identifies whether the port is connected to an end station or switch. If an end station is connected to the port, the port is immediately identified as an edge port.</li> </ul> <p><b>IMPORTANT:</b> Only use the ON mode for ports connected to a single host. Connecting hubs, concentrators, switches, or bridges to a port in ON mode can cause temporary bridging loops. Use this setting with caution.</p>

## 4. Click Apply Changes.

The changes will take effect immediately without requiring you to cycle power to the switch.



## VLAN Configuration

---

**IMPORTANT** The virtual local-area network (VLAN) feature used in earlier firmware revisions has been renamed port segmenting. As of firmware revisions 0.11 and 0.53, a new VLAN feature is provided for only the 1783-EMS08T switch. For more information about port segmenting, refer to [Port Segmenting on page 64](#).

---

A VLAN is a logical segment of network users and resources grouped by function, team, or application. This segmentation is without regard to the physical location of the users and resources. For example, VLANs can be based on the departments in your company or by sets of users who communicate mostly with each other.

VLAN can be configured to span multiple switches, so devices on separate switches can communicate as though they are on the same subnet. A port that is configured as a trunk port provides traffic for all VLANs across the port. VLAN trunking is defined in IEEE 802.1Q.

VLAN is implemented on the 1783-EMS08T switch in these ways:

- VLAN is disabled by default. If VLAN is disabled, the following is true:
  - Packets are filtered faster by the switch control processor.
  - There is no need to internally configure VLAN after powerup.
  - There is no need to reconfigure VLAN after a configuration change.
  - You cannot set up a querier on a custom VLAN.
  - No VLAN information is provided in the IGMP report.
- Each of the switch's nine ports can be assigned the role of an access port (end station) or a trunk port (switch/router).
- One VLAN can be specified as the management VLAN to provide administrative access to the switch.
- The management VLAN is the only VLAN that can run IP services. IP services include the following:
  - Address Conflict Detection (ACD)
  - BOOTP
  - DHCP server
  - SNMP
  - CIP interface
- IGMP is supported on all VLANs. However, the IGMP querier function is limited to only one VLAN. The querier function is assigned to the management VLAN by default, but you can assign the querier to a custom VLAN instead of the management VLAN, as described on [page 26](#).
- The number of VLANs you can have is determined by the number of devices, as defined by this formula:

$$\text{devices per VLAN} = 4000 / \text{number of VLANs}$$

For instance, if you have 4,000 devices, you can have 500 VLANs with eight devices on each VLAN ( $4000 / 500 = 8$ ).

To configure a VLAN, use this procedure.

1. From the navigation pane, expand the Switch Configuration folder and select VLAN Configuration.
2. From the VLAN Enabled pull-down menu, choose Enabled.

The screenshot displays the 'VLAN Configuration' page. On the left, a navigation pane shows the hierarchy: Home, Login, Basic Configuration, Network Services Setup, Diagnostics, Switch Configuration (expanded), and then RSTP Configuration, VLAN Configuration (selected), Port Configuration, Mirror Configuration, MAC ID Management, Port Segmenting, QoS Setup, and Send an Email. The main content area has tabs for various configurations. The 'VLAN Setup' section includes a 'VLAN Enabled' dropdown (currently 'Disabled') and a 'Management VLAN' dropdown (currently 'Default - 1'). Below this is the 'VLAN ID Definitions' table with columns 'VLAN', 'Name', and 'Del'. It contains two entries: VLAN 1 named 'Default' and VLAN 400 named 'Cleveland'. A link 'Add New VLAN ...' is present. An 'Apply Changes' button is at the bottom. To the right is the 'VLAN Port Assignment' table with columns 'Port #', 'Role', 'Access VLAN', and 'Native VLAN'. It lists 9 ports, all with the role 'End Station' and 'Access VLAN' set to 'Default - 1'.

3. To create a custom VLAN, perform these steps:
  - a. Click Add New VLAN.
  - b. From the Add New VLAN dialog box, type a VLAN ID from 1...4094, type a descriptive name to identify the VLAN, and then click Add VLAN.

The new VLAN appears in the VLAN ID Definitions area below the default VLAN.

4. From the Management VLAN pull-down menu, choose a custom VLAN or accept the default VLAN as the management VLAN.

The management VLAN ensures administrative access to the switch. You cannot access the switch and its services through any other VLAN.

5. In the VLAN Port Assignment area, assign one of these roles to each port:
  - End Station—The port receives network traffic from the Access VLAN only. Network traffic from other VLANs is not forwarded to the port. By default, all ports are end stations.
  - Switch/Router—The port is a trunk port that provides traffic for all VLANs across the port.

6. If you assigned the End Station role to a port, choose the VLAN to which the port belongs from the Access VLAN pull-down menu.

By default, end stations are assigned to an access VLAN of Default - 1.

or

If you assigned the Switch/Router role to a port, choose the VLAN to use as the native VLAN from the Native VLAN pull-down menu.

The trunk port uses the specified Native VLAN if a received packet is missing the tag used to identify its VLAN.

---

**IMPORTANT** The same Native VLAN must be configured on both ends of a trunk link. The Native VLAN must always be manually configured. The switch does not provide a default Native VLAN.

---

7. Click Apply Changes.

The Stratix 6000 switch verifies the requested VLAN configuration and issues a warning if the configuration eliminates your access to the switch. For example, you cannot change the management VLAN without assigning it to a port through which you are also accessing the switch.

If accepted, the changes will take effect immediately without requiring you to cycle power to the switch.

## Port Configuration

The switch autonegotiates most of its settings to ease the configuration process. Settings for ports 1...8 can be manually configured on the Port Configuration tab. Refer to [Table 7 on page 60](#) for information about configuring ports 1...8.

---

**IMPORTANT** Port G is reserved for 1G fiber, small form-factor pluggable (SFP) modules only, and its settings are preconfigured at the values shown on the screen. The preconfigured settings cannot be modified.

For more information about using SFP modules with the EMS08T switch, refer to [Available SFP Modules and Cables on page 89](#).

---

To access the Port Configuration tab, from the navigation pane, expand the Switch Configuration folder and click Port Configuration.

The screenshot shows a web-based configuration interface for a switch. On the left is a navigation menu with options like Home, Login, Basic Configuration, Network Services Setup, Diagnostics, and Switch Configuration. Under Switch Configuration, 'Port Configuration' is selected. The main area has tabs for RSTP Configuration, VLAN Configuration, Port Configuration, Mirror Configuration, MAC ID Management, and Port Segmenting. The 'Port Configuration' tab is active, displaying a table of settings for Ports 1 through 8 and Port G. The settings include Transmit & Receive (Both), Negotiation (Auto), Rate (100), Duplex Mode (Half), and Flow Control (ON). An 'Apply Changes' button is at the bottom.

	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port G
Transmit & Receive	Both	Both	Both	Both	Both	Both	Both	Both	Both
Negotiation	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto
Rate	100	100	100	100	100	100	100	100	1000
Duplex Mode	Half	Half	Half	Half	Half	Half	Half	Half	Full
Flow Control	ON	ON	ON	ON	ON	ON	ON	ON	ON

Table 7 - Configuration Options for Ports 1...8

Configuration Option	Description
Transmit & Receive	Controls port communication. Values: <ul style="list-style-type: none"> <li>Both (default)</li> <li>Tx</li> <li>Rx</li> <li>None</li> </ul>
Negotiation	Indicates whether the port configuration settings are autonegotiated. Select None to manually configure the port. Values: <ul style="list-style-type: none"> <li>None</li> <li>Auto (default)</li> </ul>
Rate	Autonegotiates 10 or 100 mbit/s depending on the connected device. The speed must be manually selected if the negotiation parameter is None. Values: <ul style="list-style-type: none"> <li>10</li> <li>100</li> </ul>
Duplex Mode	Autonegotiates half-duplex or full-duplex mode based on the connected device. The duplex mode must be manually selected if the negotiation parameter is changed to None. Values: <ul style="list-style-type: none"> <li>Half—The switch can either send or receive data, but cannot do both simultaneously.</li> <li>Full—The switch can simultaneously send and receive data.</li> </ul>
Flow Control	Prevents buffers from over filling. Values: <ul style="list-style-type: none"> <li>OFF</li> <li>ON (default)</li> </ul>

**TIP**

Ports set for autonegotiation default to half-duplex mode if the connected devices are not configured to autonegotiate.

Turning off autonegotiation disables the auto-MDIX feature. In this case, crossover cables may be needed to establish communication to the connected device.

## Mirror Configuration

Use the Mirror Configuration tab to configure the rules or filters for port mirroring. Optional filters can be configured to capture packets from certain devices (MAC addresses). You can also configure filters to capture packets with a specified destination address. Port mirroring is disabled by default.

**IMPORTANT** Port mirroring is a diagnostic tool. Disable this feature while running in a production environment.

**IMPORTANT** For the 4-port switch, port mirroring and IGMP snooping are mutually exclusive. When port mirroring is enabled, IGMP snooping is disabled.  
For the 8-port switch, port mirroring and IGMP can be used simultaneously in the 8-port switch. However, filtering is not available.

Once the mirror configuration is complete, you can look at the packets with Ethernet protocol analyzer software.

To configure port mirroring, use this procedure.

1. From the navigation pane, expand the Switch Configuration folder and select Mirror Configuration to display the Mirror Configuration tab.

**Mirroring Configuration**

Mirroring Configuration: Disabled

	Mirror From			Capture To		
	Port	In	Out	Port		
	1	<input type="checkbox"/>	<input type="checkbox"/>	1	<input type="radio"/>	
	2	<input type="checkbox"/>	<input type="checkbox"/>	2	<input type="radio"/>	
	3	<input type="checkbox"/>	<input type="checkbox"/>	3	<input type="radio"/>	
	4	<input type="checkbox"/>	<input type="checkbox"/>	4	<input type="radio"/>	
	5	<input type="checkbox"/>	<input type="checkbox"/>	5	<input type="radio"/>	
	6	<input type="checkbox"/>	<input type="checkbox"/>	6	<input type="radio"/>	
	7	<input type="checkbox"/>	<input type="checkbox"/>	7	<input type="radio"/>	
	8	<input type="checkbox"/>	<input type="checkbox"/>	8	<input type="radio"/>	
	G	<input type="checkbox"/>	<input type="checkbox"/>	G	<input type="radio"/>	

**Mirroring Rules**

	Input	Output
Filter	<span>All received</span>	<span>All transmitted</span>
MAC	<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="00:00:00:00:00:00"/>
Divider	<input type="text" value="0"/> Range: 0-999	<input type="text" value="0"/> Range: 0-999

**Note:** To use MAC based filter, disable **IGMP Snooping**.

Apply Changes

2. From the Mirroring Configuration pull-down menu, choose Enabled.
3. In the Mirror From column, specify the traffic to capture and send to a destination port for analysis.
  - To monitor incoming traffic for a port, check the In checkbox next to the port number.
  - To monitor outgoing traffic for a port, check the Out checkbox next to the port number.
  - To monitor both incoming and outgoing for a port, check the In and Out checkboxes next to the port number.
  - If you do not want to monitor traffic for a port, leave both checkboxes cleared. This is the default configuration.
4. In the Capture To column, click the option button next to the port number to which to send captured traffic.
5. Configure optional input and output mirror filters.
 

Options include the following:

  - All transmitted
  - All transmitted frames with the destination address specified in the MAC field
  - All received frames with the source address specified in the MAC field
6. Specify input and output dividers for further filtering.

**EXAMPLE** Port 4 is set up to capture incoming frames from port 3. The input filter is set up to capture traffic with source address 00:00:BC:03:4E:08. The input divider is set to 2 to capture every other frame coming to port 3 with a source address of 00:00:BC:03:4E:08. This MAC address belongs to IP address 100.100.101.2.

Mirroring Configuration		
Mirroring Configuration	Enabled	
Mirroring Rules	Input	Output
Filter	All rcvd SA=MAC	All transmitted
MAC	00:00:BC:03:4E:08	00:00:00:00:00:00
Divider	2 Range: 0-999	0 Range: 0-999
<input type="button" value="Apply Changes"/>		

7. Click Apply Changes.

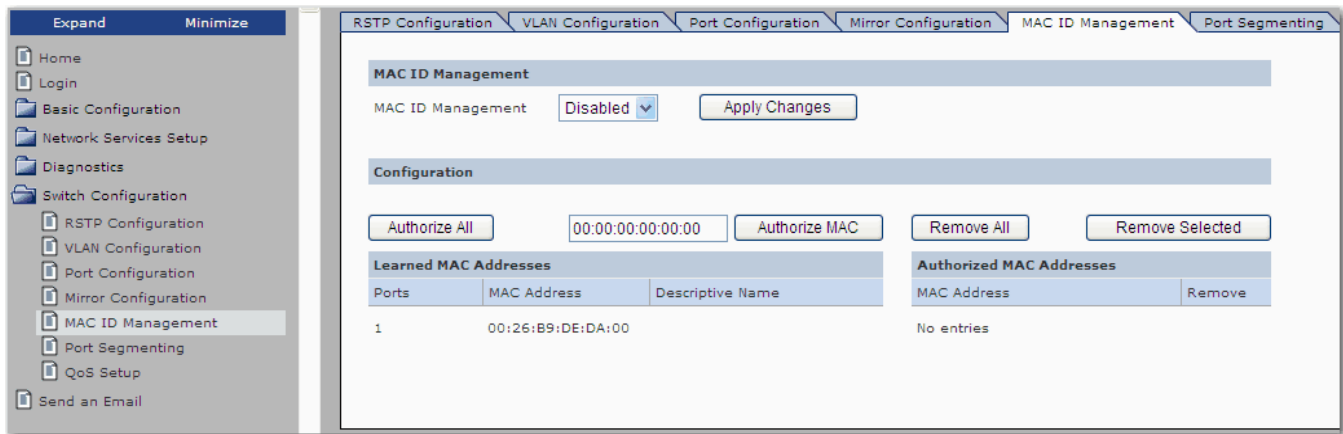
## MAC ID Management

Use the MAC ID Management feature to authorize or deauthorize MAC addresses. The MAC ID Management tab displays the following:

- **Learned MAC Addresses area**—Lists MAC addresses detected on the network by the 1783-EMS switch. The port number and MAC ID are shown for each device detected on the network. This list is built automatically by the 1783-EMS switch.
- **Authorized MAC Addresses area**—This list indicates which MAC addresses are allowed on the network. You must create this list. Whenever a new device comes online, this list is checked to determine if the device is authorized. If the device is not authorized, an input is sent to the switch's controller. See [Appendix D](#) for the I/O table of the switch.

To authorize or deauthorize MAC addresses, use this procedure.

1. From the navigation pane, expand the Switch Configuration folder and click MAC ID Management.



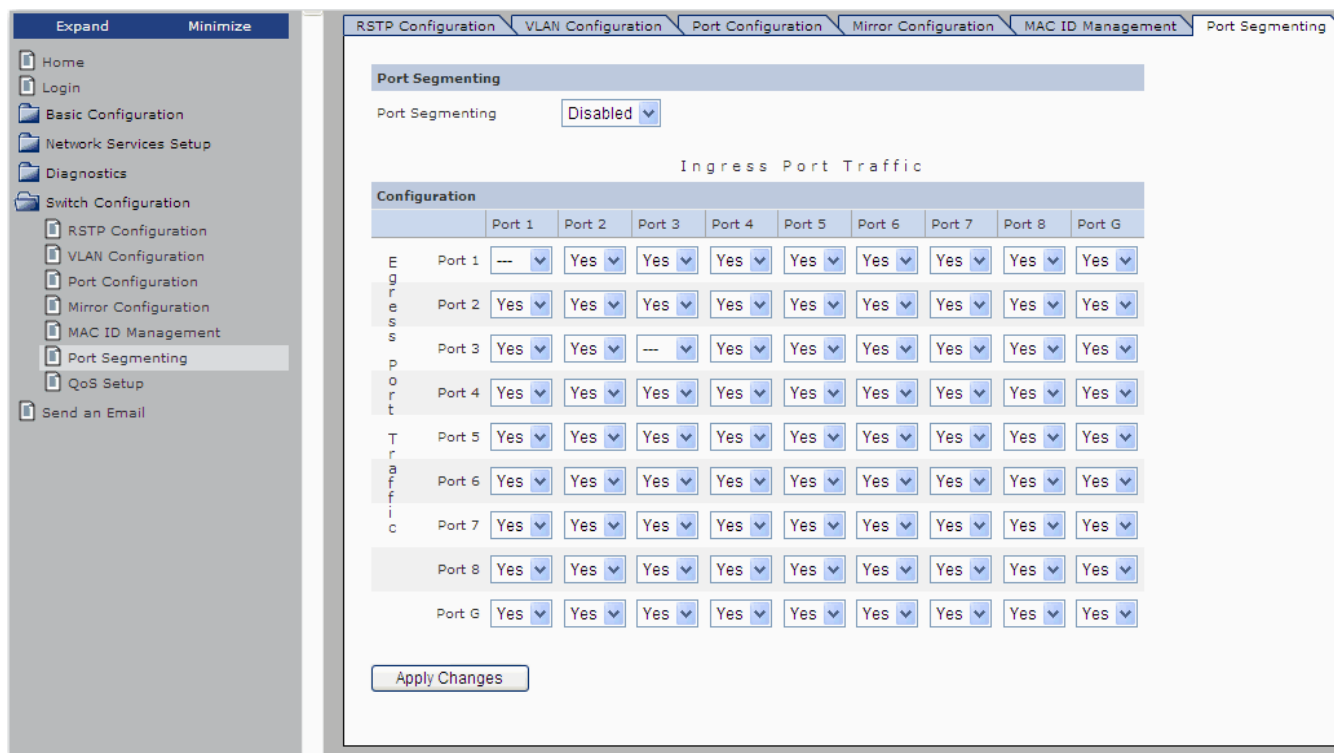
2. From the MAC ID Management pull-down menu, choose Enabled.
3. Click Apply Changes.
4. To authorize MAC addresses, use one of these methods:
  - To authorize the entire list of learned MAC addresses on the left, click Authorize All. Once authorized, the MAC addresses appear in the list of authorized MAC addresses on the right.
  - To manually enter and authorize a MAC address, type the address in the field next to the Authorize MAC button, and then click Authorize MAC. Once authorized, the MAC address appears in the list of authorized MAC addresses on the right.
5. To deauthorize MAC addresses, use one of these methods:
  - To deauthorize all MAC addresses in the list of authorized addresses on the left, click Remove All.
  - To deauthorize individual MAC addresses, check the Remove checkbox next to each address to remove and click Remove Selected.

## Port Segmenting

**IMPORTANT** The virtual local-area network (VLAN) feature used in earlier firmware revisions has been renamed port segmenting. As of firmware revisions 0.11 and 0.53, a new VLAN feature is provided for only the 1783-EMS08T switch. For more information about VLAN, refer to [VLAN Configuration on page 57](#).

When network bandwidth becomes critical, port segmenting is used to eliminate traffic caused by multicast and broadcast Ethernet traffic. With this feature, you can partition the switch ports into different private virtual networks.

To access the Port Segmenting tab, from the navigation pane, expand the Switch Configuration folder and click Port Segmenting.



For each received packet, the switch resolves the destination address and determines the appropriate port. The port segmenting configuration is then checked to see if the destination address is configured to receive traffic from the source port.

**EXAMPLE** A FLEX™ I/O module is connected to port 2 on the 1783-EMS08T switch, and the I/O module is communicating with a ControlLogix module on port 3. You want the ControlLogix module on port 3 to receive traffic from the FLEX I/O module on port 2. You can use port segmenting to prevent other devices on the network from receiving packets from the FLEX I/O module.



## QoS Setup

QoS (quality of service) provides for the classification of Ethernet traffic into high and low priority queues. High priority packets are forwarded to their destination address before a low priority packet.



**WARNING:** I/O devices do not support the QoS protocol.

Packets can be classified as high or low by MAC address, 802.1p priority tag, and/or port ID.

To access QoS setup, from the navigation pane, expand the Switch Configuration folder and click QoS Setup.

**Quality of Service**

Quality of Service: Disabled

Quality Weight: High=15 Low=1 Range: 0-15

**802.1p priority based QoS**

Priority Threshold: 4 Range: 0-7

**Port based QoS**

	Port 1	Port 2	Port 3	Port 4
Port Priority	<span>Low</span>	<span>Low</span>	<span>Low</span>	<span>Low</span>
	Port 5	Port 6	Port 7	Port 8
Port Priority	<span>Low</span>	<span>Low</span>	<span>Low</span>	<span>Low</span>
	Port G			
Port Priority	<span>Low</span>			

**MAC based QoS**

	Status	Port	MAC Address
	<span>Unused</span>	<span>1</span>	<span>00:00:00:00:00:00</span>
	<span>Unused</span>	<span>1</span>	<span>00:00:00:00:00:00</span>
	<span>Unused</span>	<span>1</span>	<span>00:00:00:00:00:00</span>

Note these options:

- **Port-based Priority**—When changed to High, the incoming traffic for that port is considered high priority.
- **High/Low Quality Weight**—Establishes the algorithm for switching between high and low priority queues. The default value of 15/1 sends 15 packets of high priority traffic, then sends 1 packet of low priority traffic.
- **MAC-based Priority**—Incoming packets are cross referenced with the MAC based QoS list and put into the high priority queue if the destination address is on the list.
- **802.1p Priority**—Each incoming packet is examined for a valid 802.1p priority tag. If present, the packet is put in the high priority queue if the priority tag exceeds the QoS Priority Threshold.

## **Notes:**

## Upgrade Firmware

This appendix provides information about how to upgrade 1783-EMS firmware.

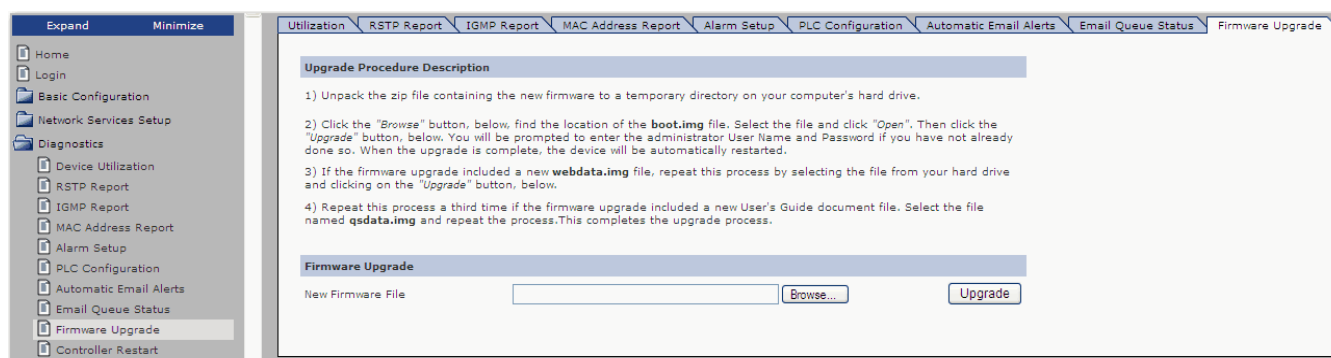


**WARNING:** The 1783-EMS switch cycles power automatically at the end of the upgrade procedure. Any switching activity is temporarily interrupted.

### Upgrade with the Web Management Interface

Use this procedure to upgrade the 1783-EMS switch by using the web interface. For information about how to access the web interface for the switch, refer to [Chapter 1](#).

1. From the navigation pane, expand the Diagnostics folder and click Firmware Upgrade.



2. Click Browse and select the firmware (boot.img) file.
3. Click Upgrade.
4. Enter the user name and password.

By default, the user name is 'uploader' (lowercase) and the password is 'PASSWORD' (all caps). Change the user name and password by selecting Basic Configuration and Set Security from the web interface of the 1783-EMS switch.
5. Check the firmware revision when the upgrade is complete to make sure the upgrade was successful.
6. Repeat this procedure to upgrade the web browser (webdata.img) and the embedded manual (qsdata.img) files.

## Notes:

## **User Name and Password Rules**

This appendix provides information about user name and password characters and rules.

### **User Name and Password Characters**

Use these characters for user name and password:

- Uppercase letters A...Z
- Lowercase letters a...z
- Numbers 0...9
- Spaces, hyphens (-), periods (.), or single quotes (')

### **Other Rules**

Follow these rules concerning the user name and password:

- User name: from 0...20 characters long, spaces count as a character
- Password: from 0...20 characters long, spaces count as a character

## **Notes:**

## Factory Reset

This appendix provides information about how to accomplish a factory reset, setting the 1783-EMS switch to the factory default settings. You have two levels of reset as described in this appendix. To complete the reset, you need the following:

- Small screwdriver
- Means to turn off the power to the switch

### Access the Reset Button

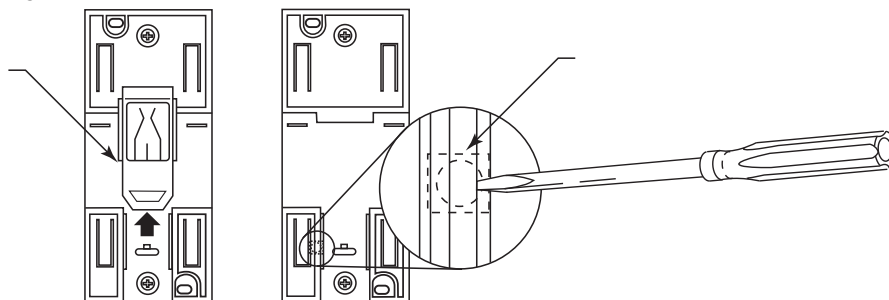
Complete the reset by using a small button on the back of the switch.

To access the button, carefully remove the plastic DIN-rail clip by gently lifting the tab in the center with a screwdriver and sliding the clip upward.

The button is inside the left slot, opened by the removal of the plastic DIN-rail clip.

The figure on the left shows the DIN-rail clip that you remove to access the reset button. The figure on the right shows placement of the screwdriver on the reset button inside the slot.

**Figure 1 - Reset Button**



## Reset IP Address

To reset only the IP address, use this procedure.

1. With power applied, push the reset button with a small screwdriver.
2. Hold the button in for 30 seconds.
3. Cycle power to complete the IP reset.

Your IP address defaults to 192.168.1.1.

## Change Settings to Default

To change all settings back to default, use this procedure.

1. Remove power.
2. Push the reset button with a small screwdriver.
3. Apply power while continuing to hold the reset button.
4. Hold the button in for 30 seconds.
5. Cycle power to complete the reset.



## Data Layout

This appendix provides information about the data layout for DINT input and output bits.

### DINT Input

These tables show the data layout.

Bit	Bit
0	Unauthorized MAC ID on Network
1	Unauthorized MAC ID on Port 1
2	Unauthorized MAC ID on Port 2
3	Unauthorized MAC ID on Port 3
4	Unauthorized MAC ID on Port 4
5	Unauthorized MAC ID on Port 5
6	Unauthorized MAC ID on Port 6
7	Unauthorized MAC ID on Port 7
8	Unauthorized MAC ID on Port 8
9	Device Connected to Port 1(Link Active)
10	Device Connected to Port 2
11	Device Connected to Port 3
12	Device Connected to Port 4
13	Device Connected to Port 5
14	Device Connected to Port 6
15	device Connected to Port 7
16	Device Connected to Port 8
17	Bandwidth Alarm on Port 1
18	Bandwidth Alarm on Port 2
19	Bandwidth Alarm on Port 3
20	Bandwidth Alarm on Port 4
21	Bandwidth Alarm on Port 5
22	Bandwidth Alarm on Port 6
23	Bandwidth Alarm on Port 7
24	Bandwidth Alarm on Port 8
25	Port Shut Off by PLC
26	IGMP Status
27...31	Reserved

Word	Description
Word 1	Multicast Connections Active
Word 2	TCP Connections Active
Word 3	Bandwidth Used Port 1 (%)
Word 4	Bandwidth Used Port 2 (%)
Word 5	Bandwidth Used Port 3 (%)
Word 6	Bandwidth Used Port 4 (%)
Word 7	Bandwidth Used Port 5 (%)
Word 8	Bandwidth Used Port 6 (%)
Word 9	Bandwidth Used Port 7 (%)
Word 10	Bandwidth Used Port 8 (%)
Word 11	Bandwidth Scaling Factor

## DINT Output

This table shows the data layout.

Bit	Bit
0	Shut down All Ports (disables all comms)
1	Shut down Port 1
2	Shut down Port 2
3	Shut down Port 3
4	Shut down Port 4
5	Shut down Port 5
6	Shut down Port 6
7	Shut down Port 7
8	Shut down Port 8
9...31	Reserved

## Add the Switch to Software

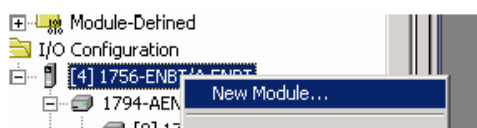
The method for adding the switch to software depends on your version of the software.

Software	Method
RSLogix 5000, version 13.04.00 or earlier	Generic Profile, as described on page 75
RSLogix 5000, version 15.02.00 or later or Logix Designer, version 21.00.00 or later	Add-on Profile, as described on page 77

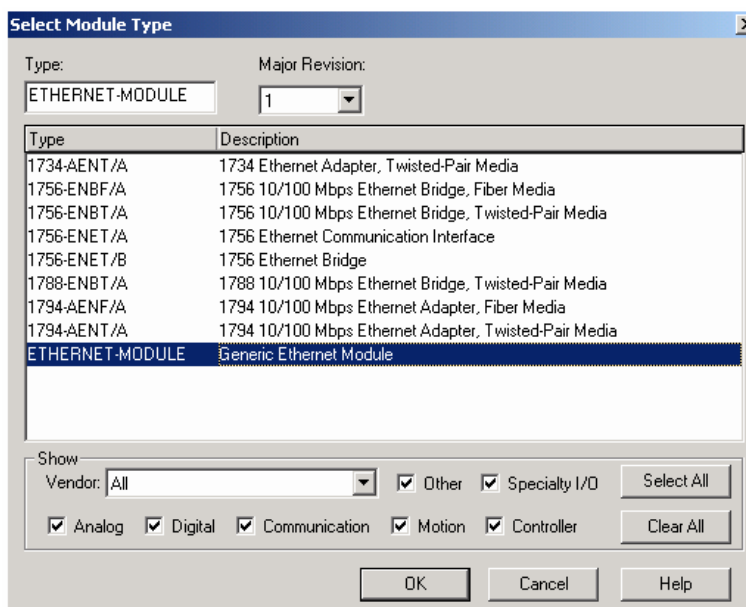
### Generic Profile

Use the switch with the Logix platform only. To add the switch to RSLogix 5000 software, version 13.04.00 or earlier, by using the generic profile, follow this procedure.

1. Right-click your Logix Ethernet card under the I/O configuration section of your program and choose New Module.



2. From the list, choose Generic Ethernet Module.



3. From the General tab of the Module Properties dialog box, complete this procedure.
  - a. Type a name for the 1783-EMS switch.
  - b. Type the IP address of the 1783-EMS switch.
  - c. Enter the Assembly instance and size for Input, Output, and Configuration.
  - d. Click OK.

4. From the Connection tab of the Module Properties dialog box, enter an RPI of 100...700 ms, (we recommend 700 ms), and click OK.

The 1783-EMS switch appears under your I/O configuration.

You can now use the 1783-EMS switch in your program. See [Appendix D](#) for the data layout.

5. Set up the 1783-EMS switch to ignore configuration tags in Logix software by using this procedure.
  - a. Telnet into your 1783-EMS switch by clicking Start and Run and typing telnet followed by the IP address.
  - b. Type the password, which is 'PASSWORD' by default.
  - c. Use keyboard arrows to scroll to Network Services Setup and press Enter.
  - d. Scroll to CIP configuration and press Enter.
  - e. Select NoCfg and press Enter.
  - f. Press ESC twice to get back to the main menu.
  - g. Scroll to Diagnostics and press Enter.
  - h. Highlight Controller Restart and press Enter.

This power cycles your 1783-EMS switch and all traffic going through the switch is interrupted.

## Add-on Profile

To add the switch to RSLogix 5000 software, version 15.02.00 or later, or the Logix Designer application, version 21.00.00 or later, by using the Add-on Profile (AOP), follow this procedure.

1. Locate the module AOP at <http://www.rockwellautomation.com/support/controlflash/LogixProfiler>.

---

<b>IMPORTANT</b>	You need a Rockwell Automation MySupport account to download the AOP. If you do not have one, follow the steps on the MySupport website to obtain an account.
------------------	---

---

2. Check the installation documentation included with the Add-on Profile to determine the required firmware revision for the 1783-EMS switch.
  - If you do not have the minimum revision of 1783-EMS firmware, upgrade your switch before proceeding. Refer to [Appendix A](#) for more information about the upgrade procedure for the 1783-EMS switch.
  - To obtain the latest firmware, check the 1783-EMS website or contact Technical Support.
3. Install the Add-on Profile.

---

<b>IMPORTANT</b>	You must install the Add-on Profile for the switch before using the switch in the Logix programming environment.
------------------	--

---

4. Add the 1783-EMS switch to the software using this procedure.
  - a. Right-click your Logix Ethernet card under the I/O configuration tree and choose New Module.
  - b. Click the Communications tab.
  - c. Choose the 1783-EMS switch from the list.
  - d. Give the switch a name in your program and enter its IP address.
  - e. Click OK.

## Enter General Information

From the Module Properties dialog box, click the General tab. The General tab is available offline and includes these fields:

- Name—Required field gives the module a descriptive name in your Logix program.
- Description—Optional field used for descriptive text.
- Module Definition—Do not change the default values.
- IP Address or Host Name—Required field must be populated with the IP address of the 1783-EMS switch. The RSLogix software cannot talk to the switch unless the 1783-EMS switch is set for the IP address in this field.

The screenshot shows the 'Module Properties' dialog box with the 'General' tab selected. The 'Type' is '1783-EMS08T 1783-EMS08T Ethernet Managed Switch'. The 'Vendor' is 'Allen-Bradley'. The 'Parent' is 'Modul'. The 'Name' field contains 'Enet\_Switch'. The 'Description' field is empty. The 'Address / Host Name' section has 'IP Address' selected with the value '10 . 99 . 99 . 99'. The 'Host Name' field is empty. The 'Module Definition' section shows 'Series: A', 'Revision: 1.1', 'Electronic Keying: Compatible Module', and 'Data Format: Integer-SINT'. The 'Status' is 'Offline'. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom.

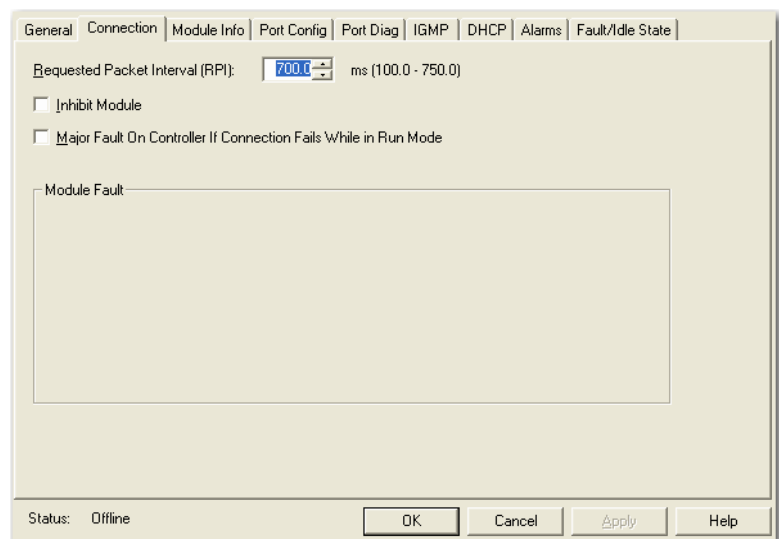
**TIP**

While the fields on the General tab are available offline, many of the fields on the subsequent tabs require an online connection to the switch through the software.

## Enter Connection Information

From the Module Properties dialog box, click the Connection tab to display these fields:

- Requested Packet Interval (RPI)—Default value is 700 ms and supports RPI from 50...750 ms. Because this is a multicasting device and does not need a fast RPI to fulfill its purpose, we recommend a slow RPI to minimize network impact. Available online and offline.
- Inhibit Module—1783-EMS switch is not scanned by the Logix controller when this is checked. Available online and offline.
- Major Fault On Controller If Connection Fails While in Run Mode—When checked, a communication failure with the 1783-EMS switch generates a major fault in the Logix controller. When unchecked, a communication failure generates a minor fault. Available online and offline.



## View Identification and Status Information

From Module Properties dialog box, click the Module Info tab. The Module Info tab displays identification and status information for the 1783-EMS switch. The information appears when the Logix controller is in Run mode only.

- To refresh the identification and status on the tab, click Refresh.
- To reset the 1783-EMS switch (communication to the module will be interrupted), click Reset Module.

The screenshot shows the 'Module Info' tab of the 'Module Properties' dialog box. The 'General' tab is selected. The 'Identification' section on the left lists fields for Vendor, Product Type, Product Code, Revision, Serial Number, and Product Name. The 'Status' section on the right lists fields for Major Fault, Minor Fault, Internal State, Configured, Owned, and Module Identity. Below these sections are 'Refresh' and 'Reset Module' buttons. At the bottom, the status is 'Offline', and there are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

## Configure Network and Port Settings

From the Module Properties dialog box, click the Port Configuration tab.

The screenshot shows the 'Port Configuration' tab of the 'Module Properties' dialog box. The 'Network Configuration' section on the left includes fields for Box Name, IP Address, Subnet Mask, Gateway Address, Primary DNS Server Address, and Secondary DNS Server Address. There are checkboxes for 'Enable Bootp Client' and 'Enable DNS'. The 'Port Configuration' section on the right includes a 'Select Port Number' dropdown menu (set to 'Port 1'), a checkbox for 'Auto-Negotiate Port Speed and Duplex', and fields for 'Current Link', 'Current Port Speed', and 'Current Duplex'. There are 'Set' and 'Refresh' buttons. At the bottom, the status is 'Offline', and there are 'OK', 'Cancel', 'Apply', and 'Help' buttons.



Use these fields in the Network Configuration area to configure the network:

- **Box Name**—Descriptive name for the switch.
- **IP Address**—IP address of the 1783-EMS switch must match the IP address on the General tab.
- **Subnet Mask**—The subnet mask is used to determine where the network number in an IP address ends and the node number in an IP address begins.
- **Gateway Address**—Address of router on the network (if one exists, if not leave this at 0.0.0.0).
- **Enable BOOTP Client**—Enables the 1783-EMS IP address be assigned by a BOOTP server.
- **Enable DNS**—If using hostnames on the network, DNS must be enabled in the 1783-EMS switch.

Use these fields in the Port Configuration area to configure port settings:

- **Select Port Number**—Choose the port to configure. Only ports 1...8 are configurable.

---

<b>IMPORTANT</b>	Port G is reserved for 1G fiber SPF modules only, and its settings are preconfigured. The preconfigured settings cannot be modified. For more information about using SPF modules with the EMS08T switch, refer to <a href="#">Available SFP Modules and Cables on page 89</a> .
------------------	--

---

- **Auto-negotiate Port Speed and Duplex**—Clear the checkbox to manually configure the port speed and duplex mode for the selected port.
- **Current Link, Port Speed, Duplex**—Displays the current settings for the selected port.
- **Select Port Speed**—Available only when the Auto-negotiate Port Speed and Duplex checkbox is cleared. Choose 10 or 100 mbp/s.
- **Select Duplex**—Available only when the Auto-negotiate Port Speed and Duplex checkbox is cleared. Choose Full or Half.
- **Set**—Click to load settings from this tab.
- **Refresh**—Click to reload settings from the 1783-EMS switch.

## View Port Diagnostic Information

From Module Properties dialog box, click the Port Diagnostic tab to display data for a specified port.

- To display data for a port, choose the port number from the Select Port Number pull-down menu.
- To clear the counters, click Clear Counters.

The screenshot shows the 'Port Diagnostic' tab of a software interface. At the top, there is a tab bar with the following tabs: General, Connection, Module Info, Port Config, Port Diag (selected), IGMP, DHCP, Alarms, and Fault/Idle State. Below the tab bar, there is a 'Select Port Number:' label followed by a pull-down menu showing 'Port 1'. The main area is divided into three sections: 'Ethernet Counters', 'Collisions', and 'Errors'. The 'Ethernet Counters' section contains: Octets In:, Octets Out:, UCast Packets In:, UCast Packets Out:, NUCast Packets In:, and NUCast Packets Out:. The 'Collisions' section contains: Single:, Multiple:, Late:, and Excessive:. The 'Errors' section contains: Alignment:, FCS:, SQE Test:, Deferred Transmissions:, Carrier Sense: (with the value 'Cannot Occur'), Frame Too Long:, MAC Transmit:, and MAC Receive:. At the bottom right of the main area is a 'Clear Counters' button. At the bottom of the dialog box, there is a 'Status: Offline' label and four buttons: OK, Cancel, Apply, and Help.

## Configure IGMP

From the Module Properties dialog box, click the IGMP tab to configure Internet Group Management Protocol (IGMP) using these fields:

- **Enable IGMP**—Enables the IGMP feature in the 1783-EMS switch. See [Chapter 2](#) of this manual for additional information.
- **Version**—Select from version 1 or version 2. See [Chapter 2](#) of this manual for additional information.
- **Query Period**—Select the interval rate that the network is queried for IGMP information.

---

**IMPORTANT**

Settings made on the IGMP tab overwrite settings made on the web interface. If you are scanning the 1783-EMS switch with Logix software, use the IGMP tab to configure IGMP to avoid confusion.

---

The screenshot shows the 'IGMP' tab of the 'Module Properties' dialog box. The 'General' tab is selected, and the 'IGMP' sub-tab is active. The 'Enable IGMP' checkbox is checked. The 'Version' dropdown menu is set to 'V2'. The 'Query Period' is set to '2' minutes, with a range of '0 - 60 [min]'. The 'Status' is 'Offline'. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom right.

General	Connection	Module Info	Port Config	Port Diag	IGMP	DHCP	Alarms	Fault/Idle State
<div><input checked="" type="checkbox"/> Enable IGMP</div> <div>Version: <span>V2</span></div> <div>Query Period: <span>2</span> Range: 0 - 60 [min]</div>								

Status: Offline

OK Cancel Apply Help

## Configure DHCP

From the Module Properties dialog box, click the DHCP tab to configure Dynamic Host Configuration Protocol (DHCP) using these fields:

- Mode—Select from Assigned by Port, Assigned by Pool, Off.
- Subnet Mask—Subnet Mask given to all devices assigned IP addresses with the 1783-EMS switch.
- Default Gateway—Leave blank if no gateway exists on the network.
- DNS Primary—Leave blank if no DNS server is present on the network.
- DNS Secondary—Leave blank if no DNS server is present on the network.
- Default Lease Time—7 days by default.
- DHCP Pool Configuration—Used when Assigned by Pool mode is selected. Assigns the next available IP address from this range of addresses.
- Port Based IP assignment—Associates an IP address with a given port. Any request coming over that port for an IP address is given the address associated with the port. Leaving the port blank instructs the 1783-EMS switch to ignore DHCP requests coming from that port.

### IMPORTANT

Settings made on the DHCP tab overwrite settings made on the HTML management interface. If you are scanning the 1783-EMS switch with Logix software, use the DHCP tab to configure IGMP to avoid confusion.

The screenshot shows the DHCP Configuration dialog box. The 'Mode' is set to 'Off'. The 'Subnet Mask', 'Default Gateway', 'DNS Primary', and 'DNS Secondary' fields are empty. The 'Default Lease Time' is set to 7 days. The 'DHCP Pool Configuration' section has empty fields for 'Pool From' and 'Pool To', and the 'Dynamic Bootp' checkbox is unchecked. The 'Port Based Address Assignment' section shows eight ports (Port 1 to Port 8) with corresponding IP address fields. A note at the bottom right states: 'Note: If using DHCP Assignment by port, use 0.0.0.0 to disable DHCP on a port.' The 'Status' at the bottom left is 'Offline'. Buttons for 'OK', 'Cancel', 'Apply', and 'Help' are at the bottom right.

## Configure Bandwidth and MAC ID Management Alarming

From the Module Properties dialog box, click the Alarms tab to display this information:

- Bandwidth Alarm area
  - Used to configure bandwidth alarming and displays a graph of current network traffic. The bars are red if the port is in alarm and green if it is not.
  - The bandwidth alarm requires a point of comparison. This must be set in the HTML interface.

---

**IMPORTANT** Unlike IGMP, bandwidth alarming can be enabled from here or from the HTML interface.

---

- MAC ID Management
  - Used to configure MAC ID management alarming and displays the alarm status on each port.

---

**IMPORTANT** Unlike IGMP, MAC ID management alarming can be enabled from here or from the HTML interface.

---

- Click Set to load settings from this tab into the 1783-EMS switch.
- Click Refresh to populates this tab with settings from the 1783-EMS switch.

The screenshot shows the 'Alarms' tab of the 'Module Properties' dialog box. It is divided into two main sections: 'Bandwidth Alarm' and 'MAC ID Management'.

**Bandwidth Alarm Section:**

- Scaling Factor: [Empty text box]
- Time Factor: [Empty text box]
- Allowed Variation: [Empty text box]
- ☐ Enable Bandwidth Alarming
- Save Reference Traffic: [Button]
- Port status table:
 

Port	Status
Port 1	0%
Port 2	
Port 3	
Port 4	
Port 5	
Port 6	
Port 7	
Port 8	

**MAC ID Management Section:**

- ☐ Enable MAC ID Management Alarming
- Authorize All Nodes Currently Connected: [Button]
- Port status table:
 

Port	Status
Port 1	No Alarm
Port 2	No Alarm
Port 3	No Alarm
Port 4	No Alarm
Port 5	No Alarm
Port 6	No Alarm
Port 7	No Alarm
Port 8	No Alarm

**Bottom Controls:**

- Set: [Button]
- Refresh: [Button]
- Status: Offline
- OK: [Button]
- Cancel: [Button]
- Apply: [Button]
- Help: [Button]

## Configure Port Behavior for Fault and Idle States

From the Module Properties dialog box, click the Fault/Idle State tab to configure port behavior when the switch loses communication with the Logix

controller or when the Logix controller goes into Program mode. Use this feature to disable ports while the Logix controller is in Run mode and enable them when the Logix controller is offline. The Fault/Idle State tab includes these fields:

- Communication Fault Behavior
  - The default value is Enable All Ports.
  - Enables all ports when the 1783-EMS switch loses communication with the Logix controller. If the controller is disabling a port, it is enabled if communication with the controller is lost.
  - Holds last state when the 1783-EMS switch loses communication with the Logix controller. If a port is disabled by the controller, it continues to be disabled when communication with the controller is lost. To re-enable all of the ports, the 1783-EMS switch requires a power cycle.
  - Applies safe state values to ports when communication with the Logix controller is lost. Port status can be changed when communication to the controller is lost.
- Program Mode Behavior
  - The default value is Enable All Ports.
  - Enables all ports when the Logix controller is in Program mode. If the Logix controller is disabling a port, it is enabled if the Logix controller is in Program mode.
  - Holds last state when the Logix controller is in Program mode. If a port is disabled by the controller, it continues to be disabled when the controller is put in Program mode. To re-enable all of the ports, the 1783-EMS switch requires a power cycle.
  - Applies safe state values to ports when the Logix controller is in Program mode. Program mode lets you change port statuses.

General | Connection | Module Info | Port Config | Port Diag | IGMP | DHCP | Alarms | Fault/Idle State

Communication Fault Behavior:

Program Mode Behavior:

Safe State

Port 1: <input type="text" value="Hold"/>	Port 5: <input type="text" value="Hold"/>
Port 2: <input type="text" value="Hold"/>	Port 6: <input type="text" value="Hold"/>
Port 3: <input type="text" value="Hold"/>	Port 7: <input type="text" value="Hold"/>
Port 4: <input type="text" value="Hold"/>	Port 8: <input type="text" value="Hold"/>

Status: Offline

OK Cancel Apply Help

## Download or Upload a Configuration

This appendix provides information about downloading and uploading switch configurations. The 1783-EMS switch can accept its configuration from a file stored on a personal computer.

This is useful if the same configuration must be used in multiple switches. This file can be retrieved from a switch and downloaded to another switch.

You can also download the configuration file from the Utilization tab, as described in [Device Utilization on page 44](#).

### Upload Configuration

To upload the configuration from the switch and save it on your computer, follow this procedure.

1. Open the Command Prompt window by choosing Start>All Programs>Accessories>Command Prompt.
2. From the Command Prompt window, type 'FTP xxx.xxx.xxx.xxx' where *x* represents the switch's IP address and defaults are as follows:
  - Username is 'uploader'.
  - Password is 'PASSWORD'.
3. Type the following to store Switch\_Config\_file.img on your hard disk drive:

```
get c:\storage_location_on_my_PC\Switch_Config_file.img
```

### Download Configuration

To download the configuration from your computer to the switch, follow this procedure.

1. Open the Command Prompt window by choosing Start>All Programs>Accessories>Command Prompt.
2. From the Command Prompt window, type 'FTP xxx.xxx.xxx.xxx' where *x* represents the IP address of the unit and defaults are as follows:
  - Username is 'uploader'.
  - Password is 'PASSWORD'.
3. Type the following to download the file into the switch:

```
'put c:\storage_location_on_my_PC\Switch_Config_file.img config.img'
```

## **Notes:**



## Available SFP Modules and Cables

This appendix provides information about the small form-factor pluggable (SFP) module and cabling used with the 1783-EMS08T switch.

For instructions on installing, removing, and connecting an SFP module, refer to the Stratix 6000 Ethernet Managed Switches Installation Instructions, publication [1783-IN004](#).

### Available SFP Modules

Available SFP modules include the following:

- 1783-SFP1GSX - 1000BASE-SX multi-mode fiber transceiver
- 1783-SFP1GLX - 1000BASE-LX single-mode fiber transceiver

---

**IMPORTANT** The 1783-EMS08T switch supports only 1G fiber SFP modules.

---

### SFP Module Cable Specifications

The table lists the cable specifications for the fiber-optic SFP module connections.

Each port must match the wave-length specifications on the other end of the cable. For reliable communication, the cable must not exceed the rated maximum cable length.

SFP Module Type	Cat. No.	Wave-length (nm)	Fiber Type	Core Size/Cladding Size (micron)	Modal Band-width (MHz/km) <sup>(1)</sup>	Cable Distance
1000BASE-SX	1783-SFP1GSX	850	MMF	62.5/125	160	220 m (722 ft)
				62.5/125	200	275 m (902 ft)
				50/125	400	500 m (1640 ft)
				50/125	500	550 m (1804 ft)
1000BASE-LX/LH	1783-SFP1GLX	1310	SMF	G.652	-	10 km (32,810 ft)

(1) Modal bandwidth applies only to multimode fiber.

## **Notes:**

## **A**

**Add-on Profile** 77  
**address**  
     hardware 46  
     MAC report 46  
**administrator password** 17  
**alarm setup** 46

## **B**

**bandwidth** 47  
     alarm 85  
**basic configuration** 13  
**boot.img** 67  
**BOOTP** 10, 17

## **C**

**common terms** 10  
**community names** 23  
**configuration**  
     basic options 15  
     DHCP 30  
     downloading 44, 87  
     IGMP 27  
     interface 13  
     port 59  
     RSTP 55  
     STP 55  
     uploading 87  
     VLAN 57  
**counters, switch** 51

## **D**

**device utilization**, 44  
**DHCP configuration** 30, 84  
**diagnostics** 43  
**dialog**  
     Alarming 85  
     Connection 79  
     DHCP 84  
     Fault/Idle Action 86  
     General 78  
     IGMP 83  
     Module Info 80  
     Port Configuration 80  
     Port Diagnostic 82  
**displaying switch counters** 45  
**downloading**  
     configuration 44, 87  
     device utilization file 44  
**dynamic host configuration protocol** 10  
**Dynamic Host Configuration Protocol. See**  
     **DHCP**

## **E**

**email**  
     configuration 33  
     embedded client 33  
     error codes 41  
**error codes** 41

## **F**

**firmware upgrade** 67

## **H**

**home page** 13

## **I**

**IGMP**  
     configuration 27  
     querier 26  
     report 45  
     snooping 25  
**indicators, status** 20  
**Internet Group Management Protocol. See**  
     **IGMP**  
**IP address** 15

## **L**

**layout**  
     data 73  
     DINT input 73  
**Logix Designer application** 9

## **M**

**MAC ID management** 63, 85  
**Management Information Base. See** **MIB**  
**MIBs, supported** 22  
**mirroring**  
     configuration 61  
     port 61  
**miscellaneous settings** 18

## **N**

**network services setup** 21

## **P**

**password** 13, 17, 18, 34, 35, 67  
     administrator 17  
     rules 69  
**PLC configuration** 43  
**port**  
     configuration 59  
     segmenting 64

## Q

### QoS

- MAC-based list 65
- setup 53, 65

**qsdata.img** 67

**quality of service.** *See* QoS

**querier, IGMP** 26

## R

**Rapid Spanning Tree Protocol.** *See* RSTP

**read-only password** 17

### reset

- factory 71
- IP address 72

### RSTP

- about 54
- configuration 55
- report 45

## S

**security** 17

**segmenting, port** 64

**services setup** 21

**set security** 17

**Short Message Service.** *See* SMS

**Simple Network Management Protocol.** *See*

**SNMP**

**SMS** 35

### SNMP

- about 21
- community names 23
- configuration 23
- MIBs supported 22
- traps 23

**Spanning Tree Protocol.** *See* STP

**specifications** 11

**status indicators** 20

### STP

- about 53
- configuration 55

**Studio 5000 environment** 9

**switch counters** 50

**system alerts, automatic** 48

## T

**TCP** 10

**terminology** 10

**transmission control protocol** 10

**Transmission Control Protocol.** *See* TCP

**traps, SNMP** 23

## U

**UDP** 10

**upgrade firmware** 67

**uploading configuration** 87

**user datagram protocol** 10

**User Datagram Protocol.** *See* UDP

**user name** 13, 17, 18, 34, 35, 67

- rules 69

## V

**virtual local area network.** *See* VLAN

### VLAN

- about 57
- configuration 58
- setup 53

## W

**webdata.img** 67

**who should use this manual** 9



# Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products.

At <http://www.rockwellautomation.com/support>, you can find technical manuals, technical and application notes, sample code and links to software service packs, and a MySupport feature that you can customize to make the best use of these tools. You can also visit our Knowledgebase at <http://www.rockwellautomation.com/knowledgebase> for FAQs, technical information, support chat and forums, software updates, and to sign up for product notification updates.

For an additional level of technical phone support for installation, configuration, and troubleshooting, we offer TechConnect<sup>SM</sup> support programs. For more information, contact your local distributor or Rockwell Automation representative, or visit <http://www.rockwellautomation.com/support/>.

## Installation Assistance

If you experience a problem within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the <a href="#">Worldwide Locator</a> at <a href="http://www.rockwellautomation.com/support/americas/phone_en.html">http://www.rockwellautomation.com/support/americas/phone_en.html</a> , or contact your local Rockwell Automation representative.

## New Product Satisfaction Return

Rockwell Automation tests all of its products to ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

United States	Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

## Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication [RA-DU002](#), available at <http://www.rockwellautomation.com/literature/>.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

**[www.rockwellautomation.com](http://www.rockwellautomation.com)**

### Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1783-UM001D-EN-P - January 2013

Supersedes Publication 1783-UM001C-EN-P - April 2011

Copyright © 2013 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.