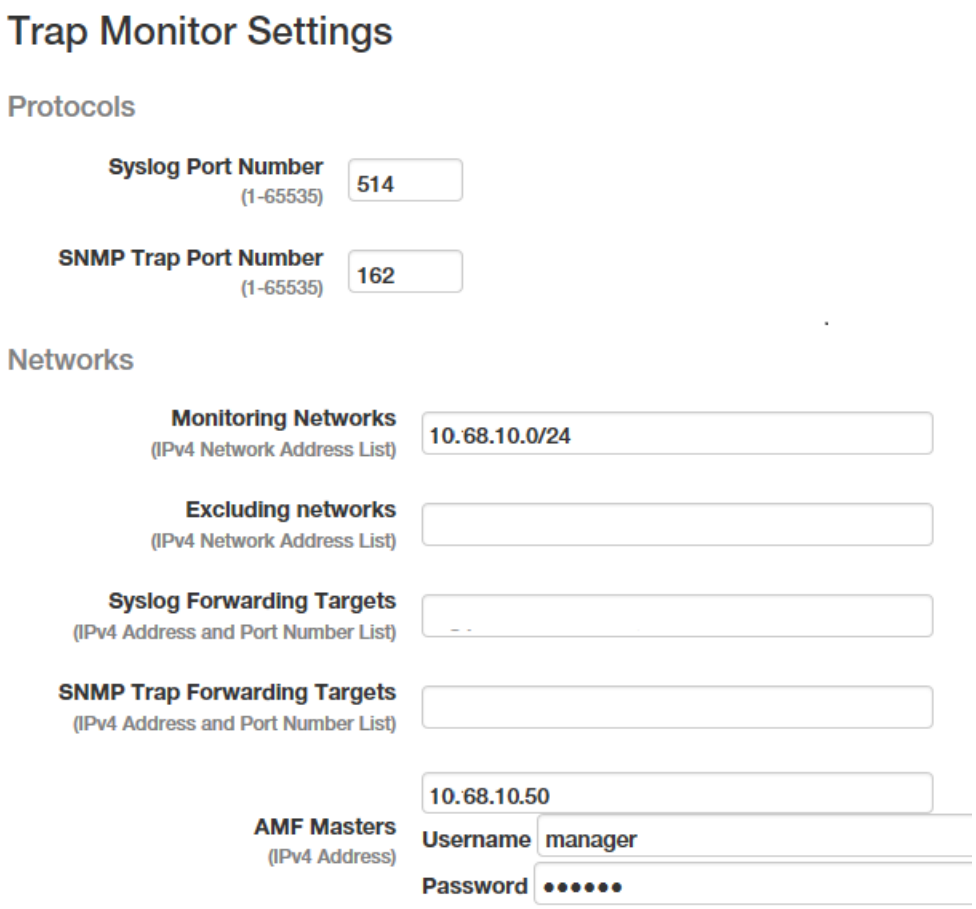
SES Controller and Autonomous Management Framework (AMF) Application Proxy

Secure Enterprise Software Defined Networking (SES)



Installation and User Guide

SES Controller Version 1.3

613-002550 Rev. A

This product includes software licensed under the GNU General Public License available from:

http://www.gnu.org/licenses/gpl2.html

Omnisphere

Copyright (c) 2013-2015 Internet Initiative Japan Inc. All rights reserved.

CentOS

CentOS-7 comes with no guarantees or warranties of any sort, either written or implied.

The Distribution is released as GPLv2. Individual packages in the distribution come with their own licenses.

SQLite

All of the code and documentation in SQLite has been dedicated to the public domain by the authors. All code authors, and representatives of the companies they work for, have signed affidavits dedicating their contributions to the public domain and originals of those signed affidavits are stored in a firesafe at the main offices of Hwaci. Anyone is free to copy, modify, publish, use, compile, sell, or distribute the original SQLite code, either in source code form or as a compiled binary, for any purpose, commercial or non-commercial, and by any means.

The previous paragraph applies to the deliverable code and documentation in SQLite - those parts of the SQLite library that you actually bundle and ship with a larger application. Some scripts used as part of the build process (for example the "configure" scripts generated by autoconf) might fall under other open-source licenses. Nothing from these build scripts ever reaches the final deliverable SQLite library, however, and so the licenses associated with those scripts should not be a factor in assessing your rights to copy and use the SQLite library.

All of the deliverable code in SQLite has been written from scratch. No code has been taken from other projects or from the open internet. Every line of code can be traced back to its original author, and all of those authors have public domain dedications on file. So the SQLite code base is clean and is uncontaminated with licensed code from other projects.

Linux Kernel, rpm, python: GPLv2, GPL-compatible

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

MIT Copyrights

python-vittualenv

Copyright (c) 2007 Ian Bicking and contributors.

Copyright (c) 2009 Ian Bicking, The Open Planning Project

Copyright (c) 20011-2014 The virtualenv developers.

gevent

gevent is written and maintain by Denis Bilenko with help from the contributors and is licensed under the MIT license.

sqla1chemy

SQLA1chemy is a trademark of Michael Bayer. mike(&)zzzcomputing.com. All rights reserved.

bootstrap

Copyright (c) 2011-2015 Twitter, Inc.

MIT License

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BSD Copyrights

python-flask

Copyright (c) 2013 by Armin Ronacher and contributors. See AUTHORS for more details.

python-jinja2

Copyright (c) 2009 by the Jinja team. See AUTHORS for more details.

python-flask-wtf

Copyright (c) 2010 by Dan Jacob. Copyright (c) 2013 - 2015 by Hsiaoming Yang.

BSD License

Some rights reserved.

Redistribution and use in source and binary forms of the software as well as documentation, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The names of the contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE AND DOCUMENTATION ARE PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE AND DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Contents

Figures

Tables

Preface

This guide contains installation and user instructions for the Secure Enterprise Software Defined Networking (SES) controller and the Autonomous Management Framework (AMF) application proxy. The controller and proxy work with selected firewalls to provide additional protection to AMF hosts from malware or virus attacks in AMF networks.

This preface includes the following sections:

Document Conventions

This document uses the following conventions:

Note

Notes provide additional information.

Caution

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning

Warnings inform you that performing or omitting a specific action may result in bodily injury.

Allied Telesis Contact Information

For assistance with this product, contact Allied Telesis technical support in the Support & Services section of the Allied Telesis web site at **www.alliedtelesis.com/support**. The web site has links for the following services:

- 24/7 Online Support - Enter our interactive support center to search for answers to your questions in our knowledge database, check support tickets, learn about Return Merchandise Authorizations (RMAs), and contact Allied Telesis technical experts.
- USA and EMEA phone support - Select the phone number that best fits your location and customer type.
- Hardware warranty information - Learn about Allied Telesis warranties and register your product online.
- Replacement Services - Submit an RMA request via our interactive support center.
- Documentation - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.
- Software Updates - Download the latest software releases for your product.

For sales or corporate contact information, go to **www.alliedtelesis.com/purchase** and select your region.

Chapter 1

Introduction

This guide contains installation and user instructions for the Secure Enterprise Software Defined Networking (SES) controller and Autonomous Management Framework (AMF) application proxy. The controller and proxy work with selected firewalls to provide additional protection to AMF hosts from malware or virus attacks in AMF networks.

Please review the information in this chapter before installing the Secure Enterprise Software Defined Networking (SES) controller or configuring AMF nodes. This chapter includes the following sections:

Secure Enterprise Software Defined Networking Controller

The Secure Enterprise Software Defined Networking (SES) controller is a management program for Allied Telesis switches. It is part of the Software-defined Networking (SDN) solution, which is a network architecture for controlling network traffic from a central controller. It simplifies network management by removing management tasks and decisions from individual switches or device stacks, and centralizing them in the controller.

The SES controller and switches communicate over a network pathway referred to as the control plane. The control plane can be based on either the OpenFlow protocol or AMF and the AMF application proxy. However, the two control planes do not support the same SES controller features. As shown in Table 1, a control plane based on the OpenFlow protocol supports all SES controller features while a control plane of the AMF application proxy supports only the enhanced firewall protection feature.

Table 1. Supported SES Controller Features

Feature	Description	OpenFlow Protocol	AMF Application Proxy
Network Policies	Used to assign hosts (edge devices) to virtual LANs.	Yes	No
Location Policies	Used to restrict network access by hosts to specified switches.	Yes	No
Schedule Policies	Used to define the days and times that hosts can access networks.	Yes	No
Manually isolate hosts	Used to manually block switch ports of hosts who represent a network threat.	Yes	No
Manually quarantine hosts	Used to manually assign hosts to isolated VLANs.	Yes	No

Table 1. Supported SES Controller Features (Continued)

Feature	Description	OpenFlow Protocol	AMF Application Proxy
Enhanced firewall protection	Used with selected firewalls to block switch ports when malware or virus attacks are detected on a firewall's WAN port.	Yes	Yes

This manual explains how to implement the enhanced firewall protection feature in an AMF network with the AMF application proxy. For information on the OpenFlow protocol and the other SES controller features, refer to the Secure Enterprise Software Defined Networking Controller and OpenFlow Protocol User Guide.

Autonomous Management Framework (AMF) Application Proxy

The Autonomous Management Framework (AMF) application proxy is part of AMF. AMF is a suite of features that combine to simplify network management from the core to the edge of a network. Brief descriptions of the AMF features are given here:

- Unified command line interface - With AMF you can configure multiple devices from a single, unified command line interface management session. You can direct the commands in a unified management session to all devices in an AMF network or a subnet, as needed.
- Configuration backup - You can automatically backup AMF device files to a central storage device. The archived files include boot configurations, firmware, licenses, and user scripts. Once the files are archived, you can restore them to devices that need to be reconfigured or to replacement devices.
- Automatic recovery - Should an AMF member node fail, AMF can minimize network disruption by automatically configuring a replacement device with the archived files from the failed unit.
- Automatic upgrades of the AlliedWare Plus operating system - When new releases of the operating system become available, AMF can update the devices for you. All you do is specify the devices to be updated and the location of the new firmware.
- Pre-provision AMF master nodes for new member devices - You can store configurations of new AMF member nodes on controller or master nodes so that AMF automatically configures the new members are as soon as you connect them to your network.

The AMF application proxy makes it possible for your AMF network to function as a control plane for the SES controller and enhanced firewall protection feature. The SES controller uses the control plane to notify AMF master and member nodes of possible malware or virus attacks on firewall WAN ports. For more information, refer to “Enhanced Firewall Protection Feature” on page 20.

The AMF application proxy comes as a standard part of AMF. However, some switches require additional subscription licenses to support the it. For information, refer to “Allied Telesis Switches” on page 25.

In addition to the AMF application proxy, which the master node uses to communicate with the SES controller, there is another component called the proxy service. This is used by the master and member nodes to communicate with each other over the AMF network. The default state of the service is disabled. You must enable it on master and member nodes that are to be part of the enhanced firewall protection feature.

Note

The AMF application proxy requires AlliedWare Plus v5.4.7-2 or later.

Note

The AMF application proxy and OpenFlow protocol should not be used on the same network devices. The results may be unpredictable.

Note

This manual does not contain instructions on how to install or configure AMF networks. For directions, refer to the Autonomous Management Framework Feature Overview and Configuration Guide or Software Reference Guides on the Allied Telesis web site:

Enhanced Firewall Protection Feature

The enhanced firewall protection feature improves the reliability and security of your network by enabling the SES controller to monitor firewalls for malware or virus attacks on their WAN ports. When an attack is detected, the controller communicates with the AMF master and member nodes over the AMF network to disable switch ports of hosts that are the sources or targets of attacks. Figure 1 is a example of the SES controller and AMF application proxy, in an AMF network.

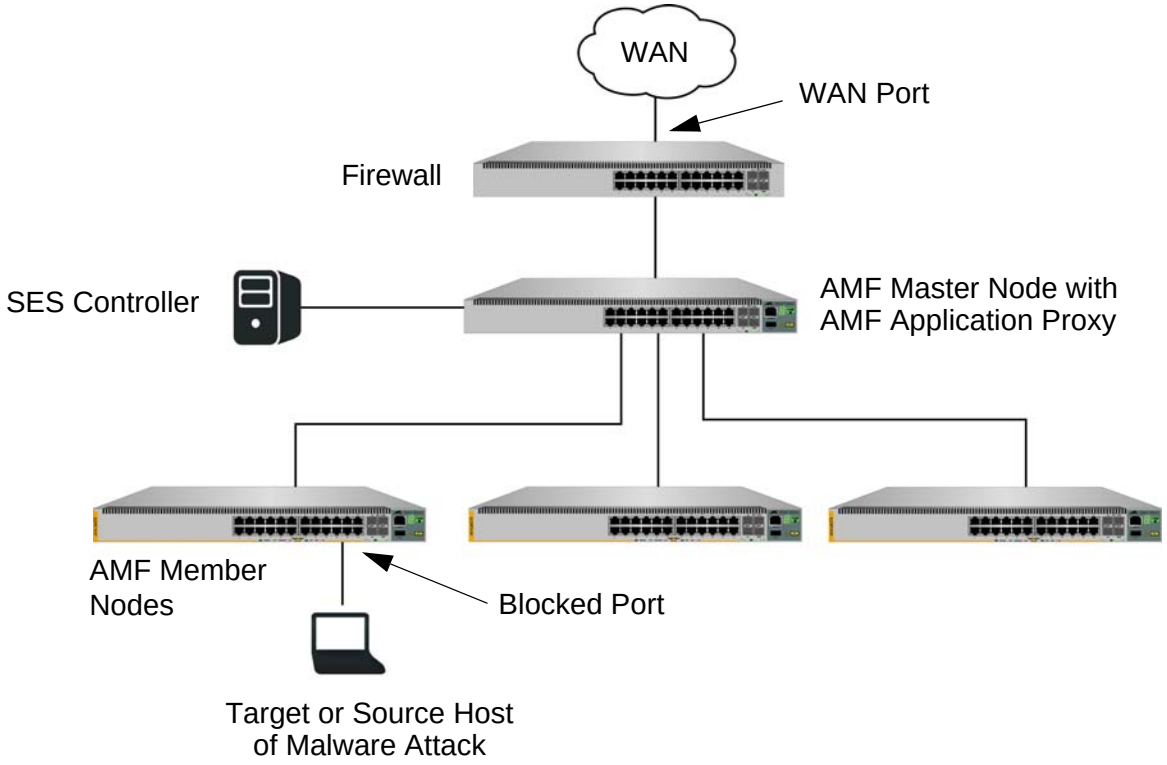


Figure 1. Enhanced Firewall Protection Feature in an AMF Network

Here is an overview of how the enhanced firewall protection feature works in an AMF network:

1. The network sends its traffic through the firewall for threat detection.
2. If the firewall detects a threat on its WAN port, it sends a syslog message to the SES controller.
3. The SES controller monitors the messages from the firewall for threat alerts.

4. If the SES controller receives a syslog message from the firewall of a possible attack, it extracts the IP address of the source or target host of the attack from the message and transmits it to the AMF master node that has the application proxy.

5. The master node forwards the message with the host address to all AMF member nodes using the proxy service.

6. Each AMF node checks its forwarding databases to determine whether the identified host is connected to one of its ports.

7. The AMF node with the identified host blocks the corresponding port to isolate the host from the network.

8. The port remains blocked until you unblock it with the SES controller, as explained in “Viewing or Restoring Isolated Hosts” on page 89.

Note

The controller is designed for managing edge switches. It should not be used to manage devices in a network core.

SES Controller

Please review the following information before installing the SES controller on a network server.

Note
Allied Telesis does not sell server hardware for the SES controller.

SES Controller Licenses

The SES controller has two licenses:

- AT-FL-SESC-Base-5YR license. This license is required. It has to be installed on the controller during the initial installation.
- AT-FL-SESC-ADD50-5YR license. This license is not required when the control plane is based on AMF and the AMF application proxy. This license is intended for the OpenFlow protocol.

Note
Licenses are ordered separately from the controller. For information, contact your Allied Telesis sales representative.

Server Requirements

The following servers have been tested and approved for use with the SES controller.

PC-based Server

The requirements for a PC-based server are listed here:

- 2.5 GHz or faster x86 processor (2 core and 2 thread or more)
- 4 Gigabyte or larger RAM
- 80 Gigabyte or larger hard disk
- DVD ROM
- Gigabit Ethernet network interface card
- Monitor and keyboard

VMware vSphere ESXi 5.5 (Hypervisor)

Here are the specifications for a VMware vSphere ESXi5.5 server (Hypervisor):

- CPU settings - number of virtual sockets: 1
- CPU settings - number of cores per socket: 2
- Memory: 4GB or more
- Hard disk setting: chic provisioning (Lazy Zeroed)

- NIC setting - number of NIC: 1
- Virtual disk size: 80GB or more
- Network adapter settings: VMXNET 3

VMware vSphere ESXi 6.0 (Hypervisor)

Here are the specifications for a VMware vSphere ESXi6.0 server (Hypervisor):

- CPU settings - number of virtual sockets: 1
- CPU settings - number of cores per socket: 2
- Memory: 4GB or more
- Hard disk setting: chic provisioning (Lazy Zeroed)
- NIC setting - number of NIC: 1
- Virtual disk size: 80GB or more
- Network adapter settings: VMXNET 3

Microsoft Windows Server 2012 R2 Hyper-V

Here are the specifications for a Microsoft Windows Server 2012 R2 Hyper-V:

- Processor settings - number of logical processors: 2:
- Start memory: 4096MB or more
- Network adapter settings: network adapter (not a legacy network adapter)
- Hard drive configuration settings: variable volume VHDX 80GB or more
- First generation: virtual machine generation

AMF Application Proxy and Service Requirements

Communications between the SES controller, AMF master nodes, and member nodes are accomplished using two components. The first is the AMF application proxy itself. Master nodes use it to communicate with the SES controller. The second is the proxy service. This is used by the master node to communicate with the member nodes. For example, when a master node is notified by the SES controller of a malware attack on a firewall WAN port, it responds using the AMF application proxy. To forward the alert to the member nodes, the master nodes use the proxy service.

The AMF application proxy and proxy service have different requirements. Here are the requirements for the AMF application proxy:

- The proxy is supported only on AMF master nodes.
- AMF nodes must have AlliedWare Plus v5.4.7-2 or later and current AMF subscription licenses.
- The proxy comes as a standard part of AMF in AlliedWare Plus v5.4.7-2 or later. However, some Allied Telesis switches require an additional subscription license. For information, refer to “Allied Telesis Switches” on page 25.

Here are the requirements for the AMF application proxy service:

- The service is supported on AMF controller, master, and member nodes.
- AMF nodes must have AlliedWare Plus v5.4.7-2 or later and current AMF subscription licenses.
- The service comes as a standard part of AMF. No additional subscription licenses are required.
- As explained later in this guide, you have to activate the service on all AMF nodes.

Allied Telesis Switches

The AMF application proxy is supported on a variety of Allied Telesis switches. For some switches the base subscription license includes the proxy, while in others a separate subscription license is required.

Listed here are switches that support the AMF application proxy and whose base subscription license includes the AMF application proxy:

- x908 Series
- SBx908 Gen2 Series
- SBx8100 Series with either the CFC400 or CFC960 Management Module

These switches do not require a separate license for the proxy.

Listed here are additional switches that support the proxy. However, their base licenses do not include the proxy:

- x230 Series
- x310 Series
- x510 Series
- x930 Series

You must purchase and install separate AMF application proxy licenses on these switches if they are functioning as AMF master nodes and you want them to be part of the enhanced firewall protection service. (As mentioned earlier, the proxy is used only on AMF master nodes.)

Here are switch requirements:

- The switches must have AlliedWare Plus v5.4.7-2 or newer.
- The switches must have current AMF licenses.

Installation Overview

Here are the general steps to implementing the enhanced firewall protection feature with the SES controller in an AMF network with the AMF application proxy:

1. Select and install the server hardware for the SES controller. Refer to “Server Requirements” on page 22.

2. Obtain the SES controller application from Allied Telesis. Refer to “Obtaining the SES Controller Application” on page 28.

3. Install the SES controller on the server. Refer to “Installing the SES Controller on a Server” on page 30.

4. Install AMF application proxy licenses on AMF master switches whose base licenses do not include the proxy. Refer to “Installing AMF Proxy Licenses on AMF Master Nodes” on page 36.

5. Activate the HTTP service on AMF master switches. Refer to “Configuring AMF Master and Member Nodes” on page 43.

6. Activate the AMF application proxy service on master and member switches. Refer to “Configuring AMF Master and Member Nodes” on page 43.

7. Configure the management settings in the SES controller. Refer to “Recommended Procedures for the First Management Session” on page 52. This includes:

   - Installing the AT-FL-SESC-Base-5YR license. Refer to “Managing the SES Controller Licenses and Software” on page 76.
   - Installing the trap monitoring rule file from Allied Telesis. Refer to “Uploading the Trap Monitoring Rule File” on page 82.
   - Defining the networks to be protected by the feature, and the network threats to protect against. Refer to “Configuring the Enhanced Firewall Protection Feature” on page 83.

8. Configure the firewall to send its syslog messages to the SES controller. Refer to the SES Controller and Firewall Installation Guide.

Chapter 2

Installing the SES Controller on a Server

This chapter includes the following sections:

Obtaining the SES Controller Application

This section contains the procedure for downloading the SES controller application from the Software Support web page on the Allied Telesis web site. The procedure requires a computer with a web browser and access to the Internet. To obtain the application, perform the following procedure:

1. Open your web browser.
2. Click on or enter the following web address in the URL field of your web browser:

   http://www.alliedtelesis.com/services-and-support/support/software

   The introductory Software Downloads window is shown in Figure 2.

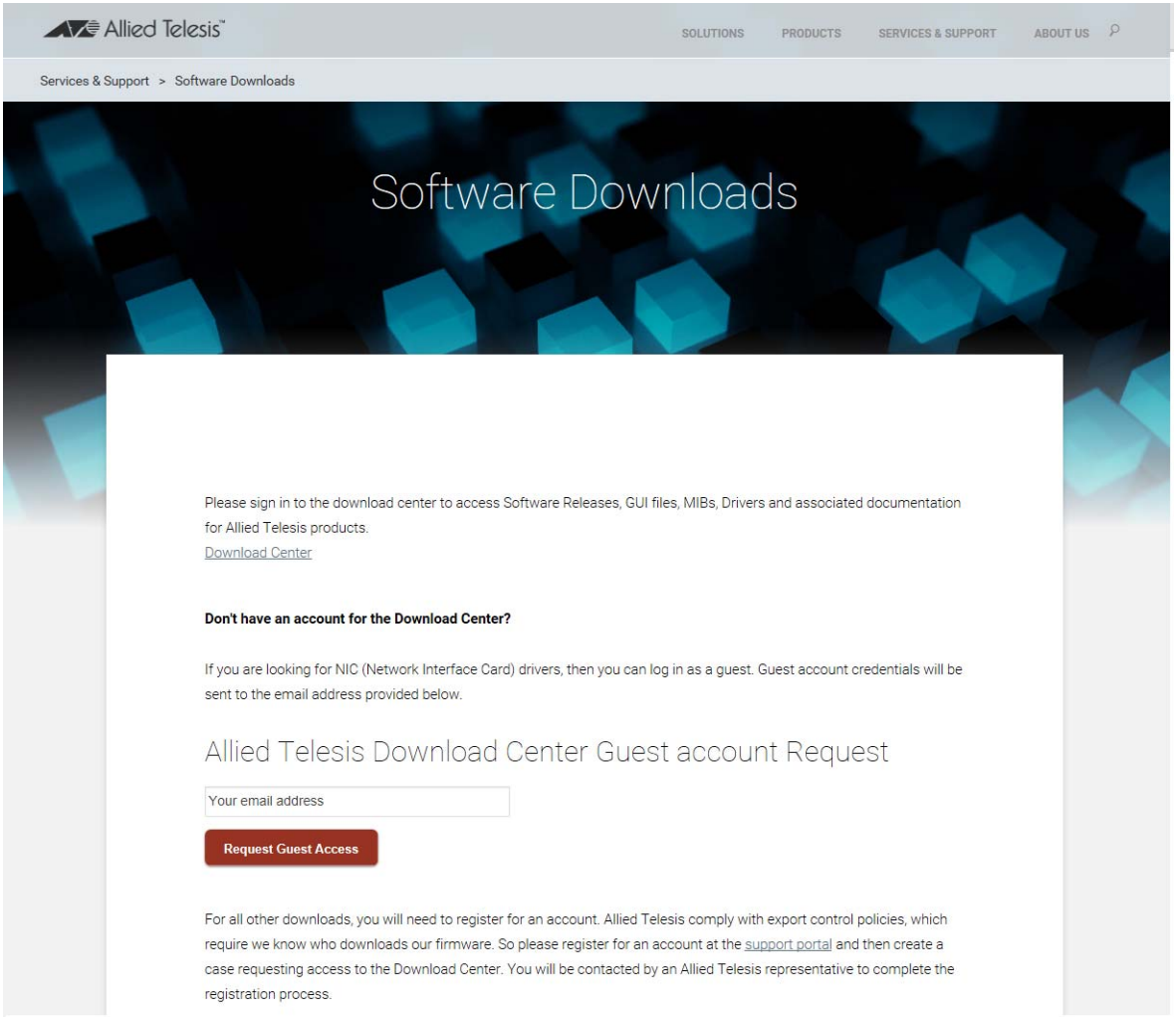


Figure 2. Introductory Software Downloads Window

Note

If you do not have an account on the Download Center, do not continue with this procedure. Instead, click the **support portal** link in the window and follow the prompts to open an account.

3. If you have an account, click the **Download Center** link in the upper left corner.

   The web site displays the Software Download Login Window. Refer to Figure 3.

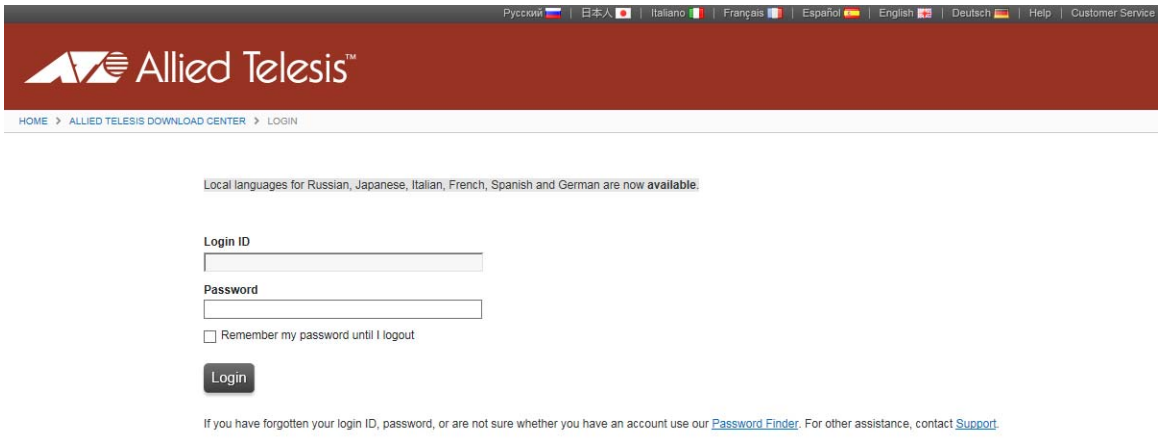


Figure 3. Software Downloads Login Window

4. Enter your login name and password. They are case-sensitive.
5. Select **Allied Telesis** from the My Products heading.
6. Select **AT-SESC Controller** from the Product Lines List.
7. Click the ISO application file for the controller and save the file on your computer or a network server.
8. Generate a DVD using the ISO file.

Note

The steps for generating a DVD from the ISO file will differ depending on your DVD program. Refer to the program's documentation for instructions.

Installing the SES Controller on a Server

This section contains the procedure for installing the SES controller application on a server. The server requirements are listed in “Server Requirements” on page 22.

Caution

Installing the SES controller deletes all files on the server’s hard disk.

You have to provide the following information during the installation:

- IPv4 address and subnet mask for the network interface in the server hardware.
- IPv4 address of a default gateway.
- IPv4 addresses of primary and secondary domain name servers (DNS).

Please review the following information before installing the SES controller:

- The server must have a video monitor and keyboard.
- You must boot the server from the DVD.
- The SES controller installation program must be booted in traditional BIOS mode. It does not support UEFI.PC boot loaders.

To install the SES controller, perform the following procedure:

1. Power on the server.
2. Insert the SES controller DVD in the DVD drive.

   The installation program displays the prompt in Figure 4.

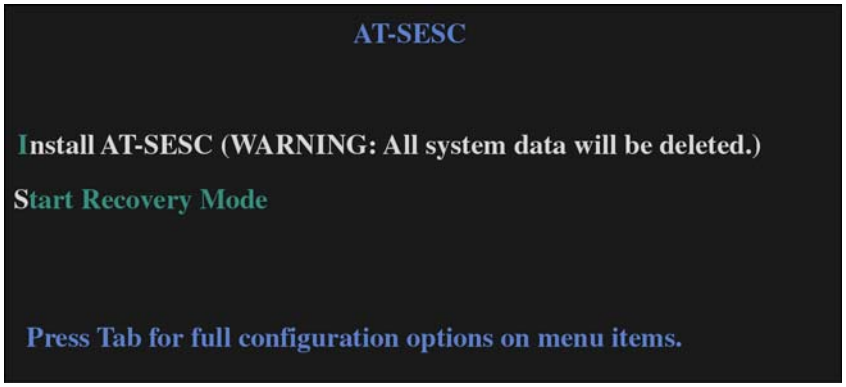


Figure 4. Starting the Installation Prompt

3. Press the **Enter** key to begin the installation.

   The program deletes all the existing files on the hard disk and afterwards copies over the SES controller files from the DVD. At the completion of the file transfer, which may take several minutes, the installation program displays the message in Figure 5.

Figure 5. Choosing Your Management Interface

   This window lists the network interfaces in the server. The server must have at least one interface.

4. Use the up and down arrow keys to select an interface, press the Tab key to select **Ok**, and press the **Enter** key.

   If the server has more than one interface, you can configure only one during the installation. You can configure additional interfaces after installing the SES controller by performing the instructions in “Changing the IPv4 Address of the SES Controller” on page 55.

   The installation program displays the prompt in Figure 6.

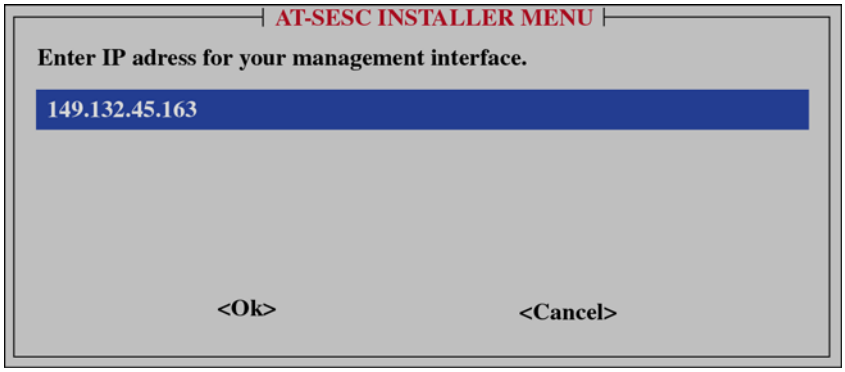


Figure 6. Entering an IP Address

5. Enter an IPv4 address for the server. Press the Tab key to select **Ok**, and then press the **Enter** key.

   The program displays the prompt in Figure 7 on page 32.

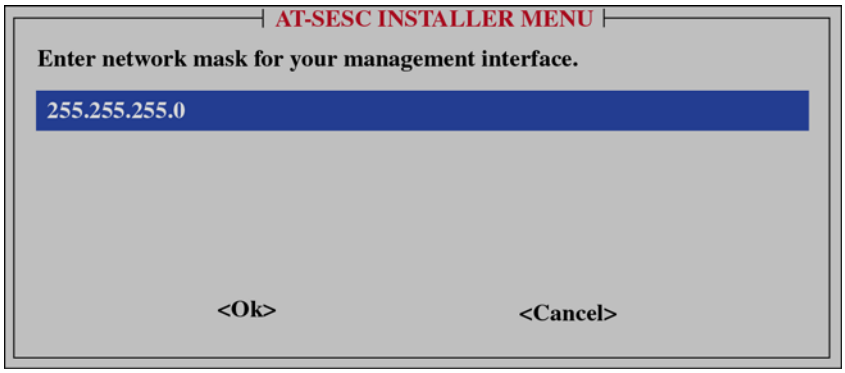


Figure 7. Entering a Subnet Mask

6. Enter a subnet mask for the server's IP address and select **OK**.

   The program displays the prompt in Figure 8.

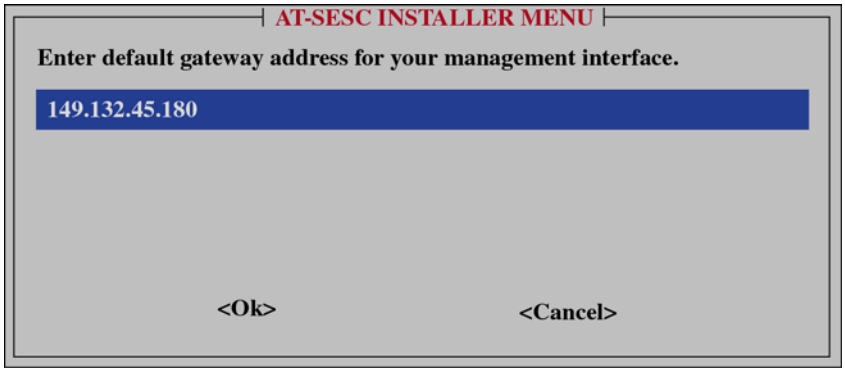


Figure 8. Entering a Default Gateway

7. Enter the IPv4 address of a default gateway and select **OK**.

   The program displays the prompt in Figure 9.

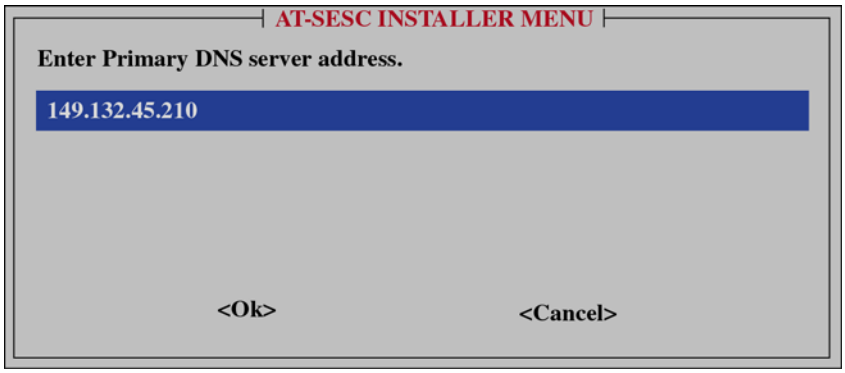


Figure 9. Entering the IPv4 Address of a Primary Domain Name Server

8. Enter the IPv4 address of a primary domain name server for the server and select **OK**.

The program displays the prompt in Figure 10.

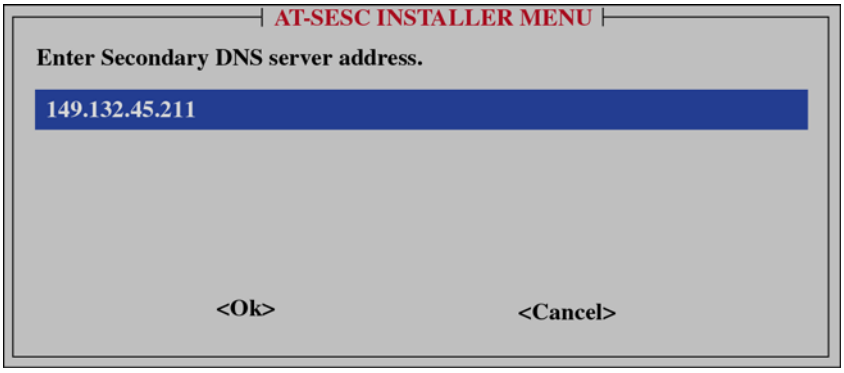


Figure 10. Entering the IP Address of a Secondary Domain Name Server

9. Enter the IPv4 address of a secondary domain name server for the server and select **OK**.

   The program displays the prompt in Figure 11.

Figure 11. Server Settings Installation Window

10. Review the settings. If they are correct, select **Correct**. If any of the settings are incorrect, select **Modify** and return to step 4.

    The program displays the following message at the completion of the installation:

```
AT-SESC Install Successfully Finished.
Remove Installation DVD and Press [Enter] key to
Reboot.
```

11. Remove the DVD and press the **Enter** key.

    The server reboots. The SES controller installation procedure is complete.

12. Go to Chapter 3, “Configuring AMF Master and Member Nodes” on page 35:

Chapter 3

Configuring AMF Master and Member Nodes

This chapter contains instructions on how to configure AMF master and member nodes for the enhanced firewall protection feature. Please review the information in “Allied Telesis Switches” on page 25 before performing the following procedures. This chapter includes the following sections:

Installing AMF Proxy Licenses on AMF Master Nodes

To be able to communicate with the SES controller, AMF master nodes must have subscription licenses for the AMF application proxy. In some cases the license comes with the base license for the switch while in others the license has to be purchased and installed separately. For a list of switches, refer to “Allied Telesis Switches” on page 25.

This section contains the procedures for installing a subscription license for the AMF application proxy on switches whose base license does not include the proxy. Remember, the proxy is only required on switches that are to function as AMF master nodes. Subscription licenses are available from the Download Center on the Allied Telesis web site. A subscription license is a Capability Response File (CRF) in a BIN format that has to be downloaded from the Download Center to the flash memory in a switch.

Subscription licenses are based on the serial numbers of switches and are valid only on devices with matching serial numbers. Consequently, purchasing a subscription license requires knowing the switch’s serial number and providing it to Allied Telesis. This is explained in “Displaying a Switch’s Serial Number” on page 36.

After purchasing a proxy subscription license proxy, you download it from the Download Center web site and install it on a switch. There are two ways to do this. One way is automatically with the LICENSE UPDATE ONLINE command in the AlliedWare Plus operating system. The command downloads the license from the Download Center and stores it on a switch. For instructions, refer to “Automatically Downloading a License to a Switch” on page 37.

The other way to download a license to a switch is to do it manually. This involves going to the Download Center web site, obtaining the license, and then downloading it to the switch. For instructions, refer to “Manually Downloading a License to a Switch” on page 38.

For further information on subscription licenses, refer to the Licensing: Feature Overview and Configuration Guide on the Allied Telesis web site.

Displaying a Switch’s Serial Number

The first step to ordering a subscription license for the AMF application proxy is obtaining a switch’s serial number. You can find it on a label on the bottom panel of the device or view it with the SHOW SYSTEM SERIALNUMBER command, as explained here:

1. Start a local or remote management session with the switch. For instructions, refer to the appropriate Installation Guide.

2. In the User Exec mode, enter the SHOW SYSTEM SERIALNUMBER command. Here is an example of the command:

```
awplus> show system serialnumber
A05050G149801293
```

3. Contact your authorized Allied Telesis representative and provide the device's serial number to purchase the license.

4. After the license becomes available on the Download Center, perform "Automatically Downloading a License to a Switch" on page 37 or "Manually Downloading a License to a Switch" on page 38.

Automatically Downloading a License to a Switch

The following procedure explains how to use the LICENSE UPDATE ONLINE command to automatically download a license from the Download Center to a switch. The procedure assumes the following:

- You have a Download Center account.
- The license for a switch exists in your Download Center account.
- A switch has an Internet connection to the www.alliedtelesis.com web site. You can verify this by using the PING command in the User Exec or Privileged Exec mode to have a switch send an Echo Request query to the web site.

To automatically download a license to a switch from the Download Center, perform the following procedure:

1. Start a local or remote management session with a switch. For instructions, refer to the appropriate Installation Guide.

2. Enter the ENABLE command to move from the User Exec mode to the Privileged Exec mode.

```
awplus> enable
awplus#
```

3. Enter the LICENSE UPDATE ONLINE command.

```
awplus# license update online
```

   The switch performs the following steps:

   - Connects to the Download Center.
   - Checks if new or changed licenses are available for the device, based on the device's serial number.
   - Downloads and installs the licenses.

   The update process normally takes approximately five seconds. If the console does not respond for ten or more seconds after typing the command, a network error is probably preventing the connection from establishing. If this happens, abort the command by pressing Ctrl-C, or wait for the command to time out after 30 seconds, and then resolve

the network error or use the manual procedure for downloading licenses.

If the update is successful, the device produces log messages indicating which feature licenses have been updated (activated, deactivated, or expiration/count changed). If the command completes successfully but there are no available licenses or there is no change in the licenses already on the device, no log messages are produced.

4. Activate the license. For instructions, go to “Activating a Subscription License” on page 41.

Manually Downloading a License to a Switch

This procedure explains how to manually obtain a license from the Download Center and download it to the flash memory of a switch. The procedure assumes the following:

- ❒ You have a Download Center account.
- ❒ You purchased the license using the switch’s serial number.

To manually download a license to a switch, perform the following procedure:

1. Start your web browser.
2. Enter the following path in the URL field:

www.alliedtelesis.com/support/software

3. Click the **Download Center** link. Refer to Figure 12.

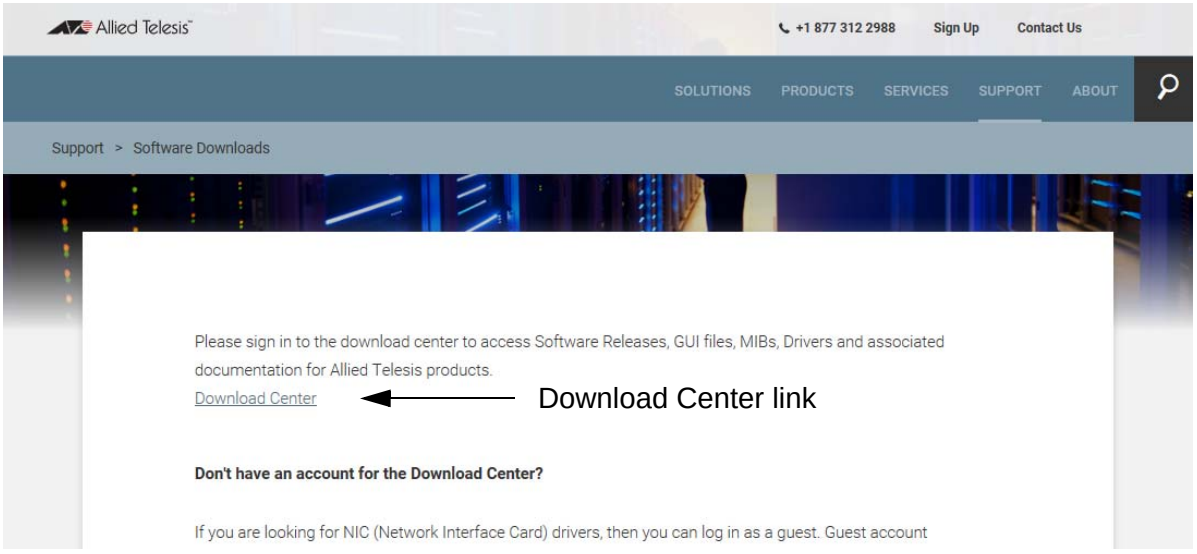


Figure 12. Download Center Web Site

The web site displays the login window. Refer to Figure 13 on page 39.

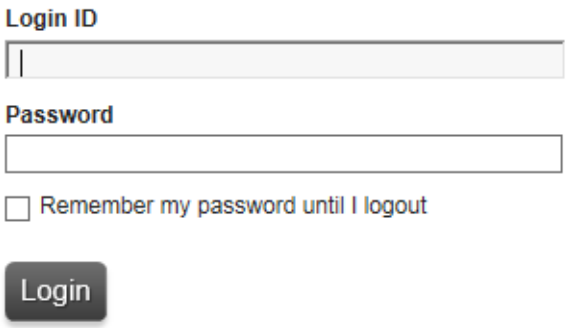


Figure 13. Download Center Login Prompts

4. Enter you login ID and password. They are case-sensitive.

5. To locate your device type, click **Search Devices** from the Devices menu in the left column of the window. Refer to Figure 14.

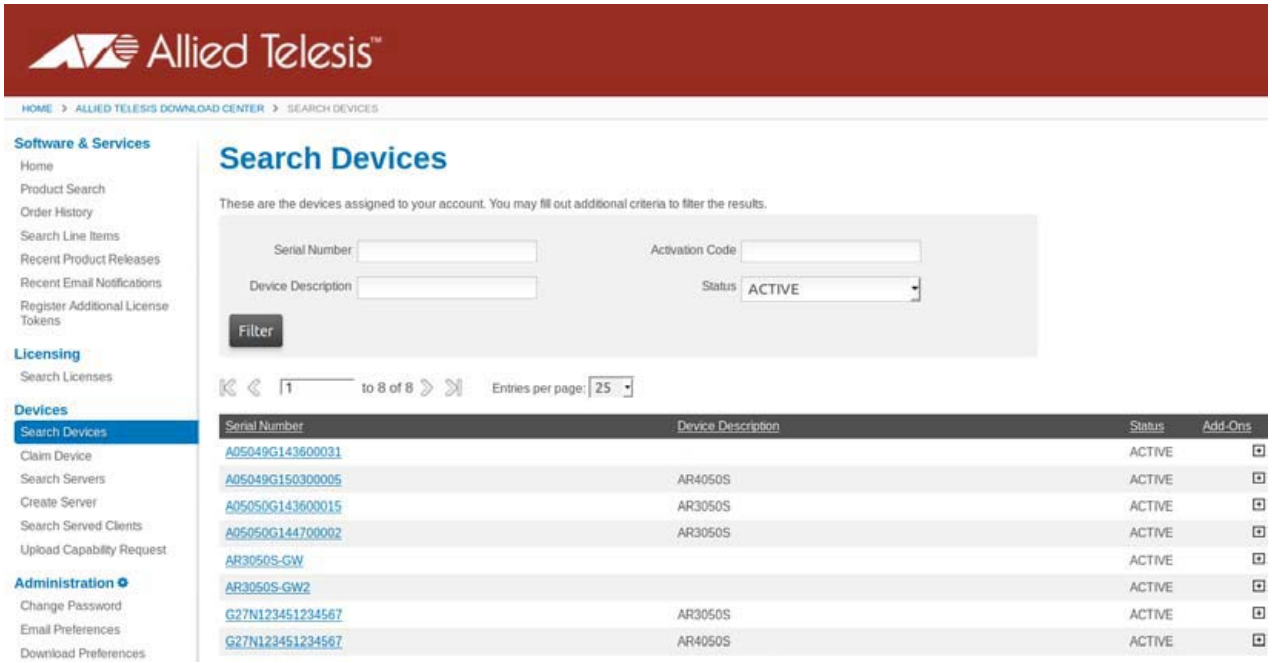


Figure 14. Search Devices Window

6. To select a specific license, click its serial number from the Serial Number list.

   The Download Center displays the View Device window for the license. An example is shown in Figure 15 on page 40.

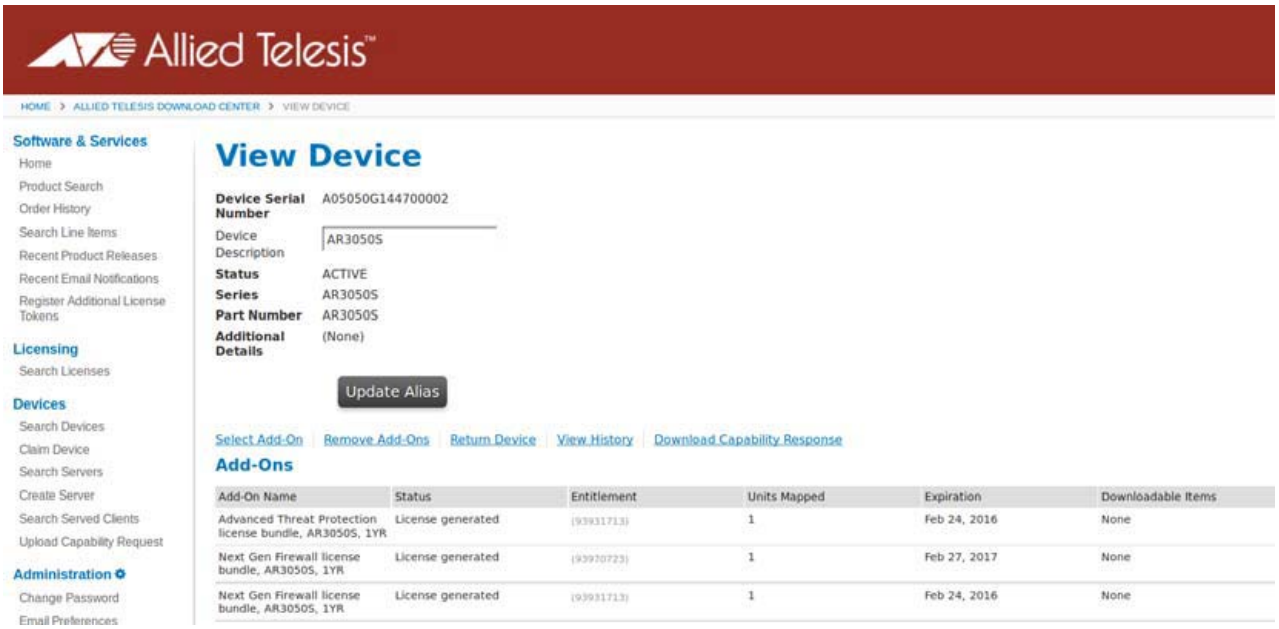


Figure 15. View Device Window

7. Click the **Download Capability Response** link.

   The Download Center displays the prompt in Figure 16.

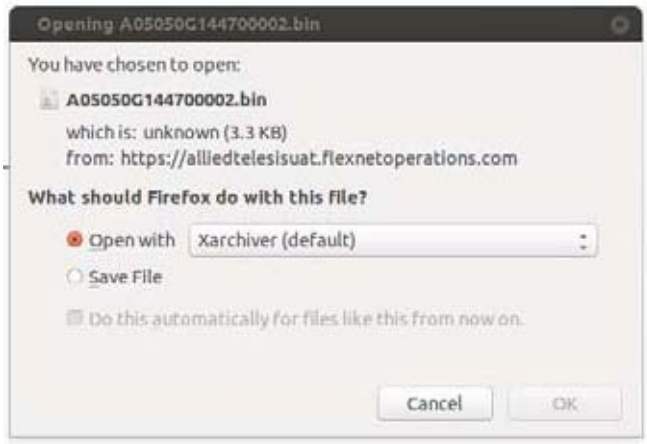


Figure 16. Prompt for Saving the License

8. Click the **Save File** option.

9. Enter a filename for the license and a location on your network or computer to store the file. The default filename is the switch's serial number. Do not change the BIN extension.

10. Start a local or remote management session on the switch. For instructions, refer to the appropriate Installation Guide.

11. Copy the license from your network or computer to the flash memory in the switch.

    You can copy the license to the switch several ways. For example, you can store the file on a USB device, insert the device into the USB port in the switch, and then copy the file with the COPY command. For example:

```
awplus# copy usb flash
Enter source path with file name[}:A050373903.bin
Copying...
Successful operation
```

    Alternatively, you can copy the license to the switch from a TFTP server. In the following example, the TFTP server has the IP address 10.201.43.128

```
awplus# copy tftp flash
Enter source host name []: 10.210.43.128
Enter source path with file name []:A050373903.bin
Enter destination file name [A050373903.bin]:
Copying...
Successful operation
```

12. After copying the license to the switch, activate it with the instructions in “Activating a Subscription License” on page 41.

Activating a Subscription License

Once a subscription license is stored in the switch’s flash memory, you have to activate it with the LICENSE UPDATE command. To activate a license, perform the following procedure:

1. In the Privileged Exec mode, enter the DIR command to view the BIN files in the flash memory of the switch: Here is an example:

```
awplus# dir *.bin
   2386 -rwx Sep 24 2017 10:20:54 flash:/A050373903.bin
```

2. Activate the license with the LICENSE UPDATE command. The command has the following format:

```
license update <url.bin>
```

    Here is an example:

```
awplus# license update A050373903.bin
```

    The command copies license entitlements in the CRF file to the device’s internal encrypted license library. The command does not display a confirmation message.

3. To confirm the activation, enter the SHOW LICENSE EXTERNAL command.

4. After confirming the activation, you can delete the CRF file from the switch. This step is optional.

   The AMF application proxy license is now installed and activated on the switch.

5. Repeat this procedure to install AMF application proxy licenses on other AMF master nodes.

6. Afterwards, go to “Configuring AMF Master and Member Nodes” on page 43.

Configuring AMF Master and Member Nodes

Here are the steps to configuring AMF master and member nodes to communicate with the SES controller. For more information, refer to the appropriate software reference manual from Allied Telesis. The procedure assumes you have already configured the nodes for AMF. The procedure does the following:

- Activates the HyperText Transfer Protocol (HTTP) service on master nodes.
- Activates the AMF application proxy service on master and member nodes.

1. Start a management session of a master or member node. For instructions, refer to the appropriate Installation Guide or AlliedWare Plus Software Reference Guide.

2. In the User Exec or Privileged Exec mode, enter the SHOW VERSION command to display the software version number of the AlliedWare Plus operating system on the switch. The version must be 5.4.7-2 or later. Earlier versions of the operating system do not support the AMF application proxy service.

```
awplus> show version
```

3. Enter the ENABLE and CONFIGURE TERMINAL commands to move from the User Exec mode to the Global Configuration mode:

```
awplus> enable
awplus# configure terminal
awplus(config)
```

4. If you are configuring an AMF master node, enter the SERVICE HTTP command to enable the HyperText Transfer Protocol service. The SES controller communicates with the master node using HTTP.

```
awplus(config) service http
```

5. In the Global Configuration mode of a master or member node, enter the SERVICE ATMF-APPLICATION-PROXY command to activate the proxy service.

```
awplus(config) service atmf-application-proxy
```

6. Return to the Privileged Exec mode and save the new configuration.

```
awplus(config) exit
awplus# copy running-config startup-config
```

7. Repeat this procedure on any remaining AMF master or member nodes.

8. If you have not configured the firewalls for the enhanced firewall protection feature, refer to SES Controller and Firewall Installation Guide for instructions. Otherwise, go to Chapter 4, “Introduction to Managing the SES Controller” on page 45.

Chapter 4

Introduction to Managing the SES Controller

This chapter includes the following sections:

Web Browser Windows

The SES controller has a web browser interface. Figure 17 is an example of a window. It is the Active Device List window. It is the first window that the SES controller displays at the start of management sessions.

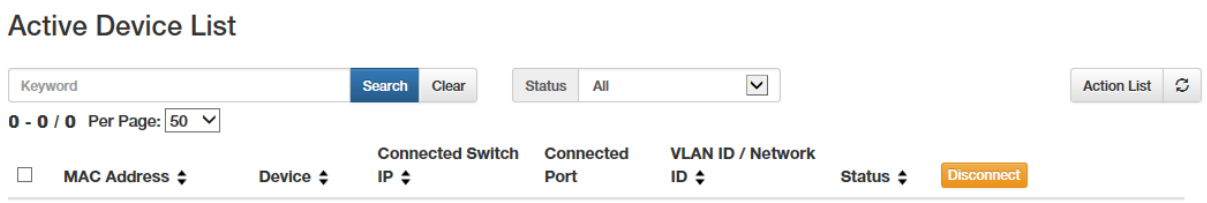


Figure 17. Active Device List Window

The SES controller interface is compatible with the following web browsers:

- Internet Explorer 11
- Google Chrome
- Mozilla Firefox

Your web browser must support JavaScript. For instructions on how to activate JavaScript, refer to “Enabling JavaScript on Your Web Browser” on page 92.

The web server interface has the five pull-down menus listed here and shown in Figure 18:

- Device
- Group
- OpenFlow Switch
- Policy Settings
- System Settings

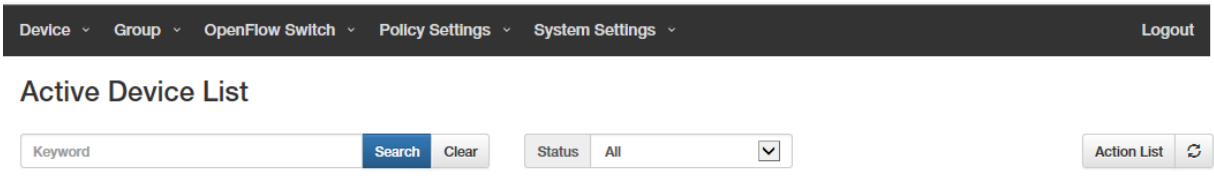


Figure 18. Pull-down Menus

Most of the menus and windows in the web interface are not applicable to the AMF application proxy. Table 2 on page 47 lists the menus and menu options that are applicable.

Table 2. SES Controller Menu Selections that are Applicable to the AMF Application Proxy

Menu	Menu Selection	Description
Policy Settings	Action List	View or restore hosts that the controller has disconnected, blocked, or quarantined. Refer to “Viewing or Restoring Isolated Hosts” on page 89.
System Settings	Administrator Settings	Change the login password. Refer to “Changing the Password” on page 54.
	Network Settings	The Network Settings window has the following settings: - Interfaces: Adjust the IPv4 address configurations of the network interfaces in the SES controller’s server. Refer to “Changing the IPv4 Address of the SES Controller” on page 55. - Services: Select the HTTP or HTTPS mode of the web server. Refer to “Configuring the Web Server” on page 62.
	Email Notification Settings	Configure email alerts that the controller sends to a designated email address. Refer to “Configuring Email Notifications” on page 58.
	Maintenance	The Maintenance window has the following sections: - System: Archive or restore basic controller information, such as IPv4 addresses. Refer to “Backing Up or Restoring System Information” on page 69. - Authentication Data: Not applicable to the AMF application proxy.
	Log Settings	Specify the severity levels of log messages to transmit to a syslog server and specify the IP address of a syslog server. Refer to “Configuring the Syslog Client” on page 73.
	AT-SESC Log	Display log messages. Refer to “Viewing Log Messages” on page 73.

Table 2. SES Controller Menu Selections that are Applicable to the AMF Application Proxy

Menu	Menu Selection	Description
System Settings (Continued)	System Information	The System Information window has the following sections: - Software Information: Display the controller's firmware version number. Refer to "Displaying the SES Controller Software Version Number" on page 77. - License: Add or delete controller licenses. Refer to "Installing or Deleting SES Controller Licenses" on page 76.
	Maintenance	The Maintenance window has the following sections: - System: Archive or restore the controller's configuration or restore the default configuration. Refer to "Backing Up System Information" on page 70, "Restoring System Information" on page 71, or "Restoring Default System Information" on page 71 - Technical Support Information: Download a technical support file from the controller to your computer to troubleshoot controller problems. Refer to "Downloading the Technical Support Information File" on page 79.

Starting a Management Session

This section contains the procedure for starting a management session on the SES controller. The procedure requires knowing its IP address or host name. To start a management session, perform the following procedure:

1. Open your web browser.

2. Enter the IP address of the SES controller in the URL field of the web browser. Precede the address with HTTPS://. An example is shown in Figure 19. If the controller has a host name from a Domain Name Server (DNS), enter the name in the URL field.

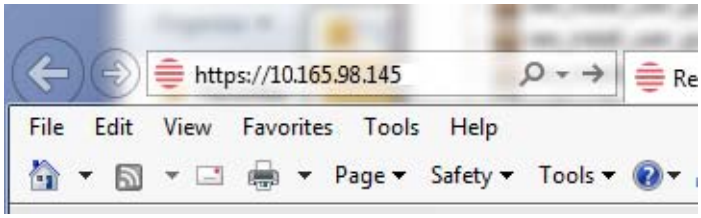


Figure 19. Entering the IP Address of the SES Controller in the URL Field of a Web Browser

Note

The SES controller supports the non-secure HTTP mode, but Allied Telesis does not recommend using it. The web browser and controller send packets in clear text, leaving them vulnerable to snooping.

Note

If this is the initial management session or if you have not replaced the default HTTPS security certificate on the SES controller, your web browser might display a warning message stating that the site certificate is invalid. If this occurs, select an appropriate option to continue to the web site. To avoid the message in future management sessions, add your own SSL certificate to the controller or make the web site a trusted site. For instructions, refer to “Adding an SSL Certificate” on page 63 or “Making the SES Controller a Trusted Website” on page 94.

The SES controller’s login window is shown in Figure 20 on page 50.

Figure 20. Login Window

Note

If the login window is not displayed, it might be because JavaScript is not enabled on your computer. Refer to “Enabling JavaScript on Your Web Browser” on page 92 for assistance in activating JavaScript on your web browser.

3. Enter the login name and password in the fields in the window. The default name is “manager” and default password is “friend”. The login name and password are case-sensitive.

   Your management session begins when the controller displays the Active Device List window, shown in Figure 17 on page 46

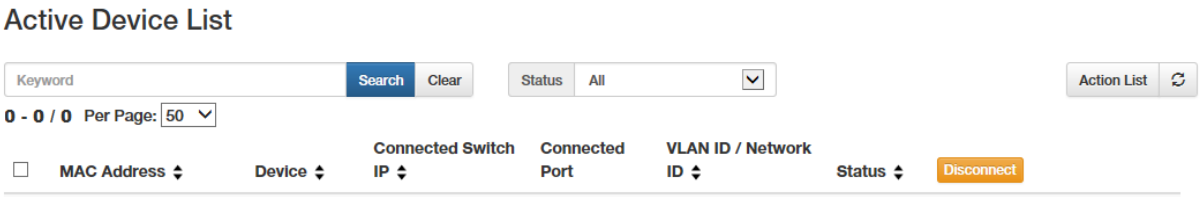


Figure 21. Active Device List Window

This window, as with most of the controller’s windows, is not used with AMF.

4. If this is the first management session, go to “Recommended Procedures for the First Management Session” on page 52.

Ending a Management Session

To end a management session, click the **Logout** link in the upper right corner of a window. Refer to Figure 22. The Logout link is available in most controller windows.

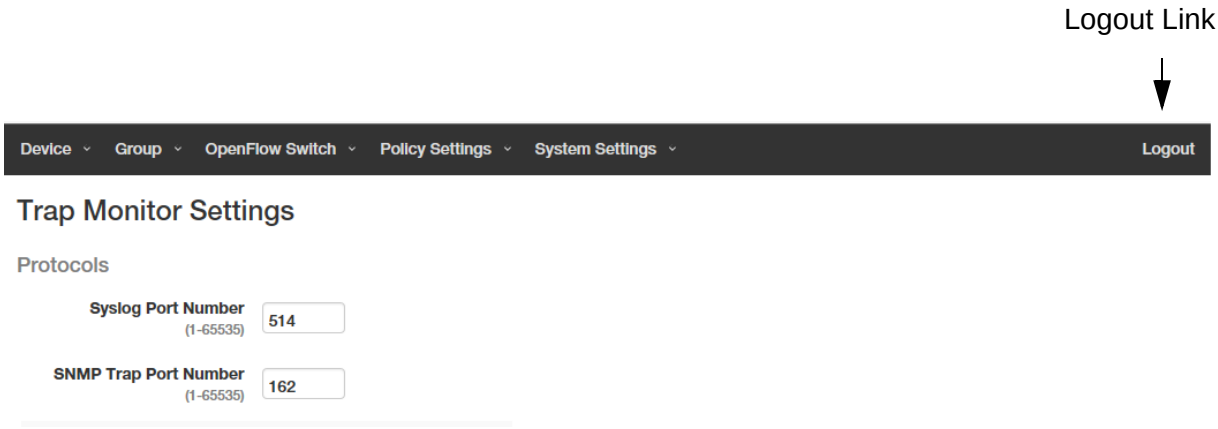


Figure 22. Logout Link

Recommended Procedures for the First Management Session

Here is a list of the recommended procedures for the first management session of the SES controller:

1. Change the login password. Refer to “Changing the Password” on page 54. (You cannot change the login username.)

2. Install the AT-FL-SESC-Base-5YR base license. Refer to “Managing the SES Controller Licenses and Software” on page 76.

3. The SES controller’s installation program lets you configure only one network interface on the server. If the server has multiple network interfaces, perform the procedure in “Changing the IPv4 Address of the SES Controller” on page 55 to configure the other interfaces.

4. To set the date and time on the controller, do one of the following:

   - “Manually Setting the Date and Time” on page 66.
   - “Setting the Date and Time from an NTP Server” on page 67.

5. Upload the trap monitoring rule file to the controller. Refer to “Uploading the Trap Monitoring Rule File” on page 82.

6. Configure the settings for the enhanced firewall protection settings. Refer to “Configuring the Enhanced Firewall Protection Feature” on page 83.

For information about all the options in the System Settings menu, refer to Chapter 5, “Managing the SES Controller” on page 53.

Chapter 5

Managing the SES Controller

The chapter includes the following sections:

Note

This chapter explains those menu selections in the controller’s web interface that apply to the enhanced firewall protection feature, when used with the AMF application proxy. All other menu selections require the OpenFlow protocol and should not be used with the AMF application proxy. For further information, refer to the Secure Enterprise Software Defined Networking Controller and OpenFlow Protocol User Guide.

Changing the Password

The section contains the procedure for changing the login password on the SES controller.

Note
You cannot change the “manager” username.

To change the login password, perform the following procedure:

1. Select **System Settings** - > **Administrator Settings**.

   The Administrator Settings window is shown in Figure 23.

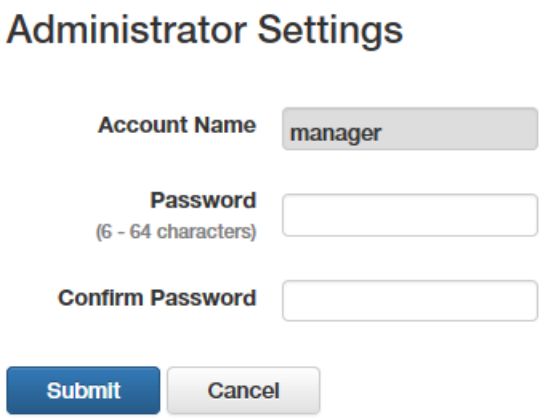


Figure 23. Administrator Settings Window

2. Fill in the fields. Refer to Table 3.

Table 3. Administrator Settings Window

Field	Description
Password	Enter a new login password of 6 to 64 alphanumeric characters. It is case-sensitive. Spaces are not allowed. The default is “friend”.
Confirm Password	Re-enter the password.

3. Click the **Submit** button to implement the new password or the **Cancel** button to cancel the procedure.

   You have to use the new password the next time you start a management session on the SES controller.

Changing the IPv4 Address of the SES Controller

The section contains the procedure for changing the IPv4 addresses of the network interfaces in the SES controller's server.

Note

Your management session is interrupted if you change the IPv4 address of the network interface that the SES controller's server is using to communicate with your management workstation. To resume managing the controller, start another management session on the controller using the new IPv4 address.

To change the IPv4 address of a network interface, perform the following procedure:

1. Select **System Settings** -> **Network Settings**.

   The Network Settings window is shown in Figure 24.

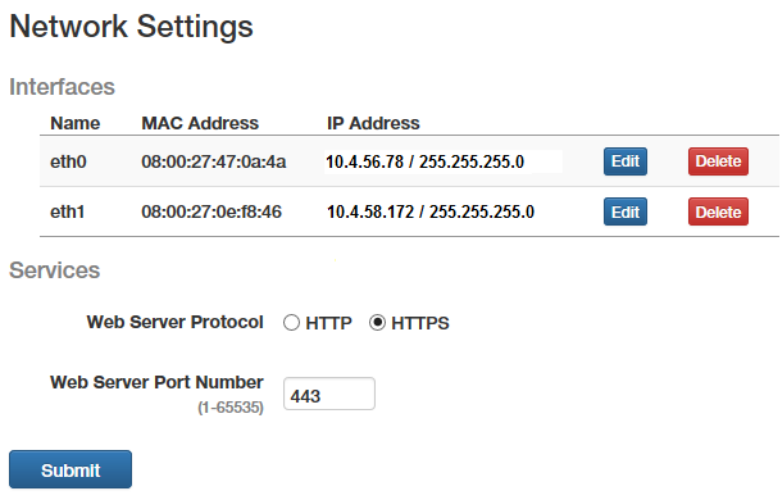


Figure 24. Network Settings Window

2. To change the IPv4 address of a network interface, click the corresponding **Edit** button in the right column. You can edit only one network interface at a time.

   The Edit Interface window is shown in Figure 25 on page 56.

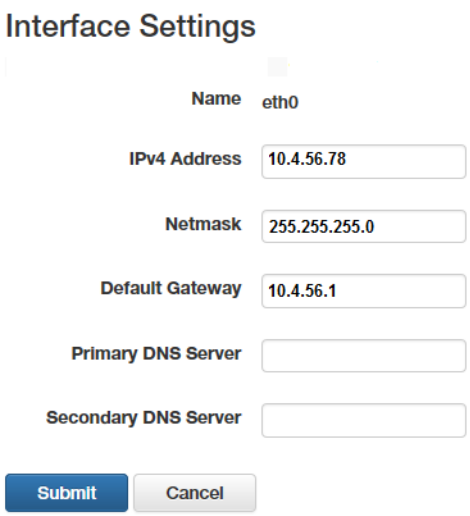


Figure 25. Interface Settings Window

3. Fill in the fields. Refer to Table 4.

Table 4. Interface Settings Window

Field	Description
Name	Displays the name of the server interface. You cannot change this parameter.
IPv4 Address	Enter the IPv4 address for the interface.
Netmask	Enter a subnet mask for the IPv4 address.
Default Gateway	Enter the IPv4 address of a default gateway for the server. Leave this parameter blank if the network interface is not used as a default gateway.
Primary DNS Server	Enter the IPv4 address of a primary domain name server for the SES controller. This parameter is optional
Secondary DNS Server	Enter the IPv4 address of a secondary domain name server. This parameter is optional

4. Click the **Submit** button to implement your changes or the **Cancel** button to cancel the procedure.

Note

The SES controller stops responding to your web browser if you change the IPv4 address of the network interface the server is using to communicate with your workstation. To resume managing the controller, start a new management session with the new IP address.

Configuring Email Notifications

The SES controller can send email alerts after certain events, such as after transmitting alerts of possible malware attacks on the firewall, to AMF master nodes. This feature requires the following:

- You have to add an email account for the SES controller on an email server. This can be a company or Internet server.
- You need to know the IP address or hostname of the email server.
- You also need to know the email addresses of the notification recipients.

To send email notifications, the SES controller logs on its email account using the information in the Email Notifications Settings window, and inserts the notifications into emails it sends to the defined recipients.

Note

If you plan to designate the email server with a hostname rather than an IPv4 address, be sure to configure the DNS settings of the IP interfaces. For instructions, refer to “Changing the IPv4 Address of the SES Controller” on page 55.

To configure the SES controller to send email notifications, perform the following procedure:

1. Select **System Settings** -> **Email Notification Settings**.

   The Email Notification Settings window is shown in Figure 26 on page 59.

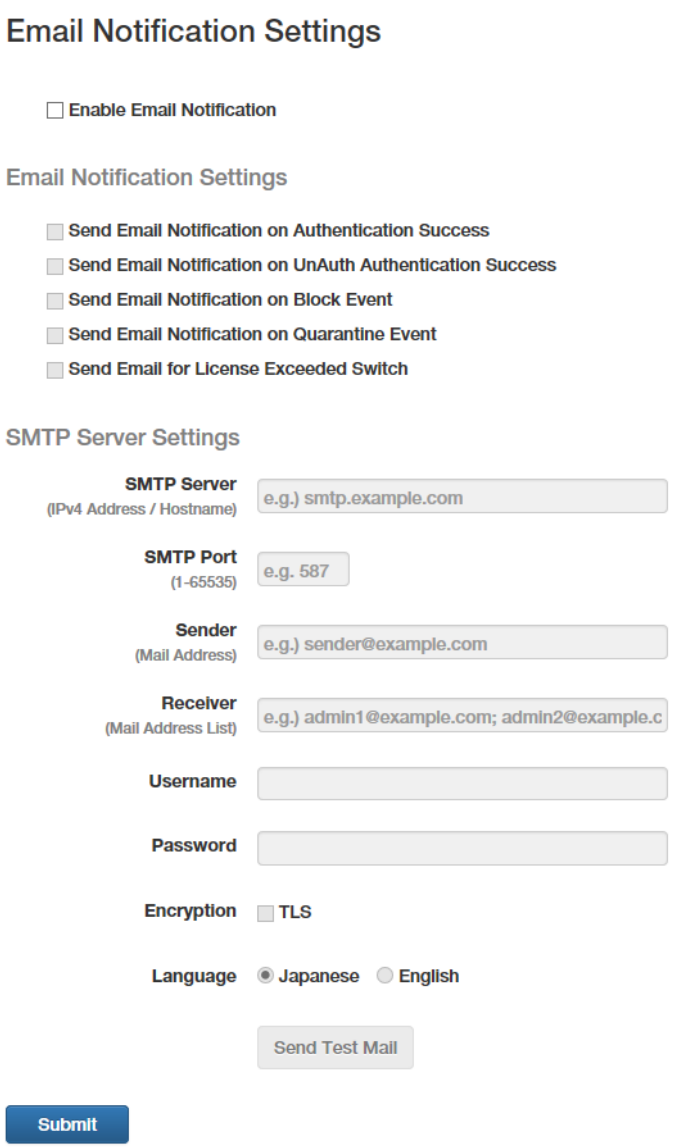


Figure 26. Email Notification Settings Window

2. Configure the options in the window. Refer to Table 5.

Table 5. Email Notification Settings Window

Option	Description
Enable Email Notification	Use this option to enable or disable email notifications. The feature is enabled when the check box has a check mark and disabled when the box is empty. The default is disabled.

Table 5. Email Notification Settings Window (Continued)

Option	Description
Email Notifications Settings	
Send Email Notification on Authentication Success	Not applicable to the AMF application proxy.
Send Email Notification on UnAuth Authentication Success	Not applicable to the AMF application proxy.
Send Email Notification on Block Event	Enable this option to have the SES controller send emails when hosts are blocked.
Send Email Notification on Quarantine Event	Enable this option to have the SES controller send emails when hosts are assigned to the quarantine VID.
Send Email Notification on License Exceeded Switch	Not applicable to the AMF application proxy.
SMTP Server Settings	
SMTP Server	Enter the IPv4 address or hostname of the email server. You can enter only one address.
SMTP Port	Enter the protocol port number of the server. The range is 0 to 65535.
Sender	Enter the email address of the SES controller’s account on the SMTP server. You can enter only one sender address.
Receiver	Enter the email address of the person to receive notifications. You can enter more than one receiver. Separate multiple addresses with semicolons (;).
Username	Enter the username of the SES controller’s account on the SMTP server.
Password	Enter the password of the SES controller’s account on the SMTP server.
Encryption	Add a check mark to the check box if the SMTP server uses TLS encryption. Otherwise, leave the box empty.
Language	Click either Japanese or English to indicate the language for the emails.

3. Click the **Submit** button to implement your changes.
4. To send a test email, click the **Send Test Email** button.

Configuring the Web Server

This sections contains the following procedures:

Changing the HTTP or HTTPS Web Mode

You can use HTTP or HTTPS to manage the SES controller with a web browser. The HTTP mode is non-secure. Management sessions conducted in this mode are vulnerable to eavesdropping because your management workstation and the controller transmit packets in clear text. In contrast, the secure HTTPS mode protects management sessions by encrypting packets. Only the controller and your management workstation can decrypt the packets.

Caution

Management sessions conducted in the HTTP mode are non-secure. The packets exchanged by your web browser application and the SES controller are sent in clear text, leaving them vulnerable to snooping.

Here are the guidelines to configuring the web server:

- ❒ The default is the HTTPS mode.
- ❒ The web server cannot operate in both HTTP and HTTPS modes at the same time.
- ❒ The switch supports HTTP v1.0 and v1.1 protocols.
- ❒ Your management workstations must have Layer 3 connectivity to the IPv4 address of the SES controller.

HTTPS mode requires that the web server have a certificate with an encryption key to encrypt and decrypt packets. Also included in the certificate is a distinguished name identifying the owner of the certificate. The SES controller comes with a default certificate. For instructions on how to change the certificate, refer to “Adding an SSL Certificate” on page 63.

Note

Changing the HTTP or HTTPS mode of the SES controller will interrupt your management session. To resume managing the controller, start a new session using the new web server mode.

To change the HTTP or HTTPS mode on the web server, perform the following procedure:

1. Select **System Settings** -> **Network Settings**.

   The SES controller displays the Network Settings window. Refer to Figure 24 on page 55. The Interfaces section of the window is explained in “Changing the IPv4 Address of the SES Controller” on page 55.

2. In the Services section, click either **HTTP** or **HTTPS**. The default is HTTPS. You cannot activate both modes.

3. For Web Server Port Number, enter the protocol port number for the web server mode. The default values are 80 for HTTP and 443 for HTTPS.

4. Click the **Submit** button to add your change to the SES controller.

Note
The SES controller stops responding to your web browser. To resume managing the controller, start a new management session using the new web server mode.

Adding an SSL Certificate

The SES controller comes with an SSL certificate for HTTPS web management. This section explains how to replace the certificate with one of your own. The SSL certificate specifications are listed in Table 6.

Table 6. SSL Certificate Specification

Requirement	Specification
Format	X.509, RFC 6818
Encryption	PEM (Privacy Enhanced Mail) format
Extension	.crt

Note
If the HTTPS server certificate has an intermediate CA or crossroot certificate, you must concatenate the files into one server file. For instructions, contact the issue of the certificate.

Note
Replacing the server certificate will interrupt your management session. You will have to start a new management session at the completion of the procedure.

To add your own SSL certificate to the SES controller, perform the following procedure:

1. Select **System Settings** -> **System Information**.
2. In the SSL Certificate section of the window, click the **Upload SSL Certificate** button.

   The SES controller displays the SSL Certificate Settings window. Refer to Figure 27.

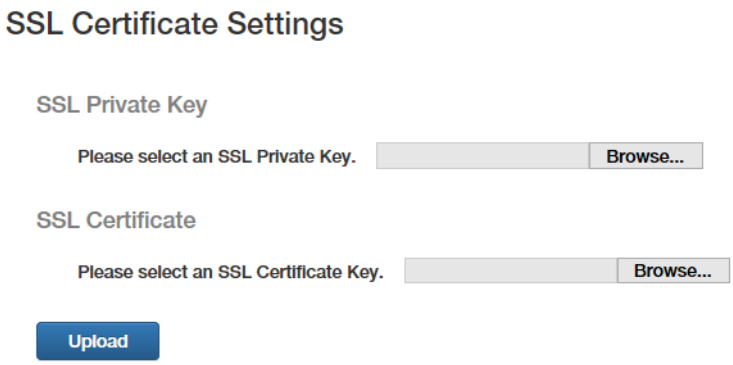


Figure 27. SSL Certificate Settings

3. Click the Please select an SSL Private Key **Browse** button and locate the private key file on your computer or network server.
4. Click the Please select an SSL Certificate Key **Browse** button and locate the SSL certificate file on your computer or network server.
5. Click the **Upload** button to upload the files to the SES controller.

   The controller replaces its current certificate files with the uploaded files.

Note
The SES controller stops responding to your web browser. To resume managing the controller, start a new management session.

Restoring the Allied Telesis SSL Certificate

To restore the original Allied Telesis SSL certificate on the web server for HTTPS web management, perform the following procedure:

1. Select **System Settings** -> **System Information**.
2. Scroll down to the SSL Certificate section in the window
3. In the SSL Certificate section, click the Reset SSL Files **Reset** button.

   The SES controller restores its default SSL certificate files.

Note

Your management session is interrupted if you are using HTTPS. To resume the session, start a new management session.

Setting the Date and Time

The procedures in this section are listed here:

Manually Setting the Date and Time

To manually set the date and time on the SES controller, perform the following procedure:

1. Select **System Settings** -> **Date Times Settings**.

   The SES controller displays the System Time Settings Window. Refer to Figure 28.

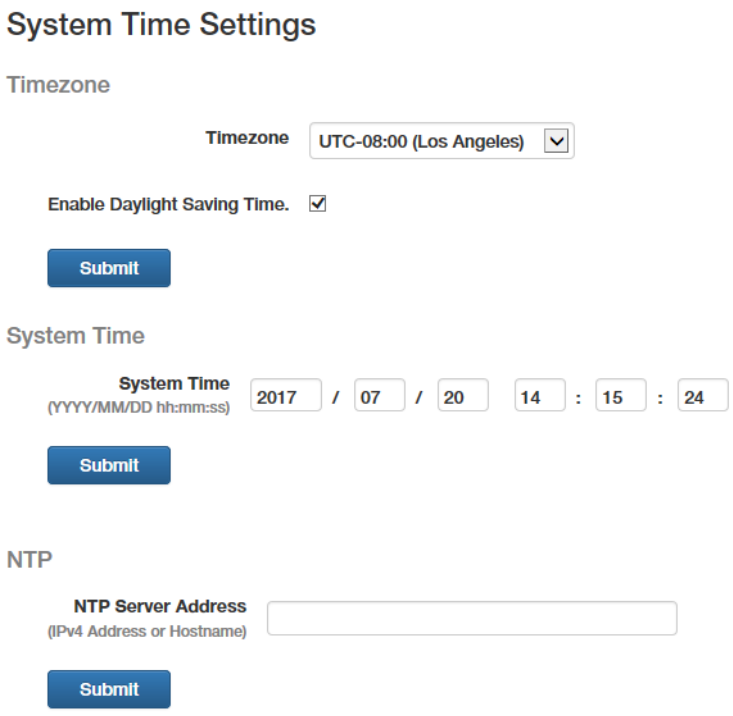


Figure 28. System Time Settings Window

2. From the **Timezone** pull-down menu, select the timezone of the SES controller’s location.

3. For the Daylight Savings Time setting, do one of the following:

   - ❒ The **Enable Daylight Savings Time** check box needs to have a check mark if the location of the SES controller observes Daylight Savings Time. If the box does not have a check mark, click the box to add it. When the option is enabled, the controller automatically

adjusts its time at the start and end of Daylight Savings Time.

- ❒ The **Enable Daylight Savings Time** check box needs to be empty if the location of the SES controller does not observe Daylight Savings Time. If the box has a check mark, click the box to remove it.

4. Click the Timezone **Submit** button to add your change to the controller.

5. In the System Time fields, enter the date and time. Here are the guidelines:

   - ❒ The year must be four digits (YYYY).
   - ❒ The month and day must be two digits each (MM / DD).
   - ❒ The hours, minutes, and seconds must be two digits each (HH : MM : SS).
   - ❒ Use the 24-four format to specify the time. For example, 8:30pm is entered as 20:30:00.

6. Click the **Submit** button in the System Time section.

7. Verify that the NTP Server Address field at the bottom of the window is empty. If the field has an IP address or hostname, delete it and then click the **Submit** button in the NTP section.

Setting the Date and Time from an NTP Server

This section contains the procedure for setting the date and time on the SES controller from an Network Time Protocol (NTP) server. The procedure requires the following information:

- ❒ The IP address or hostname of a NTP server on your network or the Internet.
- ❒ The timezone of the SES controller. The controller uses the timezone to determine the number of hours and minutes it is ahead or behind Coordinated Universal Time (UTC). This is referred to as the UTC offset.
- ❒ Whether the timezone of the SES controller is in Daylight Savings Time.

Note

If the NTP server will be designated by a hostname instead of an IPv4 address, be sure to configure the DNS settings of the IP interfaces. For instructions, refer to “Changing the IPv4 Address of the SES Controller” on page 55.

To configure the SES controller to receive the date and time from an NTP server, perform the following procedure:

1. Select **System Settings** -> **Date Times Settings**.

   The SES controller displays the System Time Settings Window. Refer to Figure 28 on page 66.

2. With the **Timezone** pull-down menu, select the timezone of the location of the SES controller server.

3. For the Daylight Savings Time setting, do one of the following:

   - The **Enable Daylight Savings Time** check box needs to have a check mark if the location of the SES controller observes Daylight Savings Time. If the box does not have a check mark, click the box to add it. When the option is enabled, the controller automatically adjusts its time at the start and end of Daylight Savings Time.
   - The **Enable Daylight Savings Time** check box needs to be empty if the location of the SES controller does not observe Daylight Savings Time. If the box has a check mark, click the box to remove it.

4. Click the Timezone **Submit** button to add your change to the SES controller.

5. Click the **NTP Server Address** field and enter the IP address or hostname of an NTP server.

6. Click the NTP **Submit** button.

   The SES controller queries your network or the Internet for the specified NTP server. The controller's server sets its date and time according to the information from the NTP server.

Backing Up or Restoring System Information

This section contains procedures for backing up, restoring, or erasing the SES controller system information in Table 7.

Table 7. Archived SES Controller System Configuration

Setting	Configuration Window
Username and password	Administrator Settings window in Figure 23 on page 54
HTTP or HTTPS setting and web server port number	Network Settings window in Figure 24 on page 55
Logging output and syslog host settings	Log Settings window in Figure 30 on page 74
Date and time settings and SNTP server	System Time Settings window in Figure 28 on page 66
Trap monitoring settings	Trap Monitoring Settings window in Figure 37 on page 84
Email notification settings	Email Notification Settings window in Figure 26 on page 59

You cannot archive the SES controller information in Table 8.

Table 8. Non-archived SES Controller Settings

Setting	Window
IP addresses of the SES controller interfaces	Network Settings window in Figure 24 on page 55
Trap monitor rule file	Maintenance window in Figure 36 on page 82
SSL certificate	System Information window in Figure 27 on page 64
Controller licenses	System Information window in Figure 32 on page 76
Log messages	AT-SESC Log window in Figure 31 on page 75

Note

The controller also has a selection for backing up authentication information, consisting of network, location, and schedule policies. That selection does not apply to the AMF application proxy.

The procedures in this section are listed here:

- “Backing Up System Information” next
- “Restoring System Information” on page 71
- “Restoring Default System Information” on page 71

Backing Up System Information

This section contains the procedure for backing up the system information in Table 7 on page 69. to a file on your computer. Please review the following information before performing the procedure:

- The system information is saved in JavaScript Object Notation (JSON) format. Do not edit the file.
- Do not change the filename extension.
- The procedure does not interrupt SES controller operations.

To backup the above system information, perform the following procedure:

1. Select **System Settings** -> **Maintenance**.

   The SES controller displays the Maintenance window. The System section in the window has the options for backing up, restoring, or erasing system settings. Refer to Figure 29.

Figure 29. System Section in the Maintenance Window

2. Click the Download system configuration for backup **Download** button.

3. Follow the prompts to store the file with the SES controller settings on your computer.

Restoring System Information

This section contains the procedure for restoring system information to the SES controller from a backup file on your computer. For a list of system information, refer to Table 7 on page 69. Please review the following information before performing the procedure:

- ❒ The SES controller immediately implements the system settings in the backup file after uploading the file.
- ❒ You do not have to reset the controller after restoring system information. However, there may be a momentary disruption to controller operations as it implements the system settings from the backup file.
- ❒ Performing this procedure may interrupt your web browser management session. You might need to start a new session at the completion of the procedure.

To restore system information from a JSON backup file, perform the following procedure:

1. Select **System Settings** -> **Maintenance**.

   The SES controller displays the Maintenance window. The System section in the window has the options for backing up, restoring, or erasing system settings. Refer to Figure 29 on page 70.

2. Click the **Browse** button and locate the system information file you want to restore to the SES controller.

3. Click the Upload and restore system configuration **Upload** button.

   The SES controller downloads the file and implements the restored system settings.

Note

If the SES controller stops responding to your web browser, start a new management session. If the system backup file has different settings for HTTP or HTTPS mode, or a different manager password, be sure to use the correct settings when starting the new web management session.

Restoring Default System Information

This section contains the procedure for restoring the default settings to the SES controller's system information, listed in Table 7 on page 69. Please review the following information before performing the procedure:

- ❒ You do not have to restart the SES controller after restoring the default settings to the system information. However, there may be a momentary disruption to SES controller operations as it activates the settings.
- ❒ Performing this procedure may interrupt your web browser

management session. You might need to start a new session at the completion of the procedure.

To restore the default settings to the SES controller's system information, perform the following information:

1. Select **System Settings** -> **Maintenance**.

   The System section in the Maintenance window has selections for backing up, restoring, or erasing the system settings. Refer to Figure 29 on page 70.

2. Click the Reset system configuration to factory default **Reset** button.

   The SES controller displays a confirmation prompt.

3. Click the **Continue** button to reset the system information or the **Cancel** button to cancel the procedure.

   The SES controller restores the default settings to its system information. If it stops responding to your web browser, start a new management session using the HTTPS mode and the username and password "manager" and "friend", respectively. Restoring the default settings does not change the SES controller's IP address.

Viewing Log Messages

The SES controller generates log messages with information about operational events. You might find the messages useful when troubleshooting network problems. You can send the messages to a syslog server on your network or view them from a web browser management session. Here are the procedures in this section:

- ❒ “Configuring the Syslog Client” next
- ❒ “Displaying the SES Controller Log” on page 74

Configuring the Syslog Client

The SES controller has a syslog client for transmitting its log messages to a syslog server on your network. Configuring the client requires specifying the IP address of the syslog server and the categories and severity levels of log messages you want transmitted. The log messages are divided into the following categories:

- ❒ Device authentication result
- ❒ OpenFlow controller
- ❒ OpenFlow protocol packets
- ❒ GUI operation
- ❒ Trap monitor

Log messages have the following severity levels:

- ❒ Disabled
- ❒ Emergency
- ❒ Warning
- ❒ Informational
- ❒ Debug

When configuring the syslog client, you can specify the categories and severity levels of messages you want transmitted to the syslog server. The SES controller transmits messages of the selected severity level and all levels above it. For example, to have the controller transmit all messages associated with device authentication, select the debug severity level.

To configure the syslog client so that the SES controller sends its log messages to a syslog server on your network, perform the following procedure:

1. Select **System Settings** -> **Logging Settings**.

   The SES controller displays the Logging Settings Window. Refer to Figure 30 on page 74.

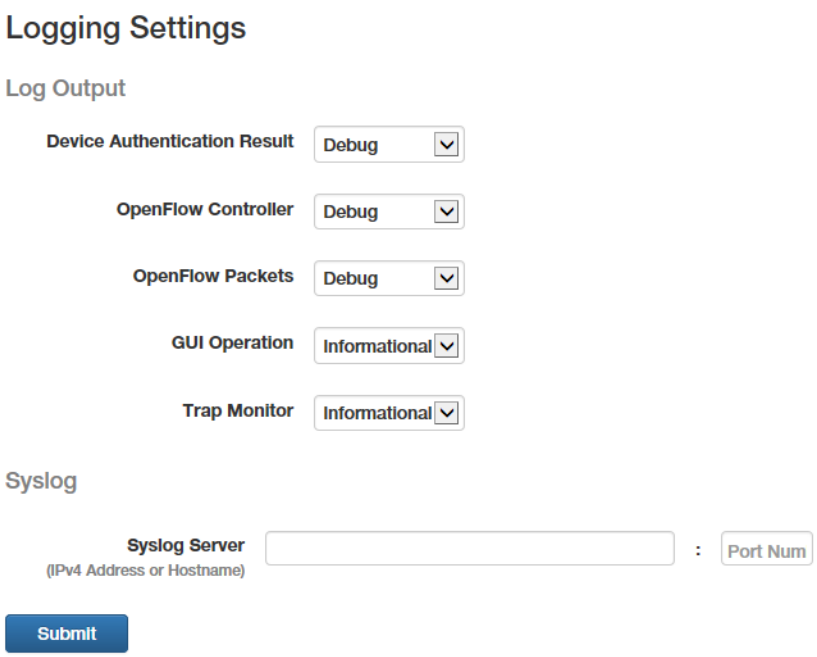


Figure 30. Logging Settings Window

2. In the Log Output section, use the pull-down menus to select the severity levels of the log messages to transmit to the syslog server. The SES controller transmits messages of the selected severity level and all levels above. The Device Authentication Result, OpenFlow Controller, and OpenFlow Packets categories have the default severity level Debug, so all messages are transmitted to the syslog server. The GUI Operation and Trap Monitor have default level Informational, so all levels except the Debug level are transmitted to the server.
3. Click the **Syslog Server** field and enter the IP address or hostname of the syslog server on your network. You can specify only one server.
4. Click the **Port Num** field and enter the UDP port number of the syslog server. The default value is 514.
5. Click the **Submit** button to implement your changes.

   The SES controller transmits log messages as they occur. It does not transmit any messages already in its log.

Displaying the SES Controller Log

To view the messages in the SES controller log, select **System Settings** -> **AT-SESC Log**. An example of the log is shown in Figure 31 on page 75.

Figure 31. SESC Log Window

The options in the window are described in Table 9.

Table 9. Options in the SESC Window

Option	Description
Clear All Logs	Use this button to clear all messages from the logs.
Download	Use this button to download the log as a file to your computer. The maximum is 300,000 messages. The default filename extension is LOG and default file format is text. To download the messages, click the button and follow the prompts.
Update	Use this button to refresh the window.

Managing the SES Controller Licenses and Software

This section contains the following procedures:

- ❒ “Installing or Deleting SES Controller Licenses” next
- ❒ “Displaying the SES Controller Software Version Number” on page 77
- ❒ “Installing New SES Controller Software” on page 77

Installing or Deleting SES Controller Licenses

The SES controller uses the following licenses:

- ❒ AT-FL-SESC-Base-5YR - This is the base license. It supports up to ten switches for five years. The controller must have a base license. You have to install it during the initial installation. The controller can have only one base license.
- ❒ AT-FL-SESC-ADD50-5YR - This license adds support for an additional fifty switches for five years. You can install any number of this license type on the controller.

Adding a new license to the SES controller requires the following information from the license certificate:

- ❒ Serial number
- ❒ Authentication key

To add SES controller licenses, perform the following procedure:

1. Select **System Settings** -> **System Information**.

   Licenses are managed in the Licenses section of the System Information window. Refer to Figure 32.

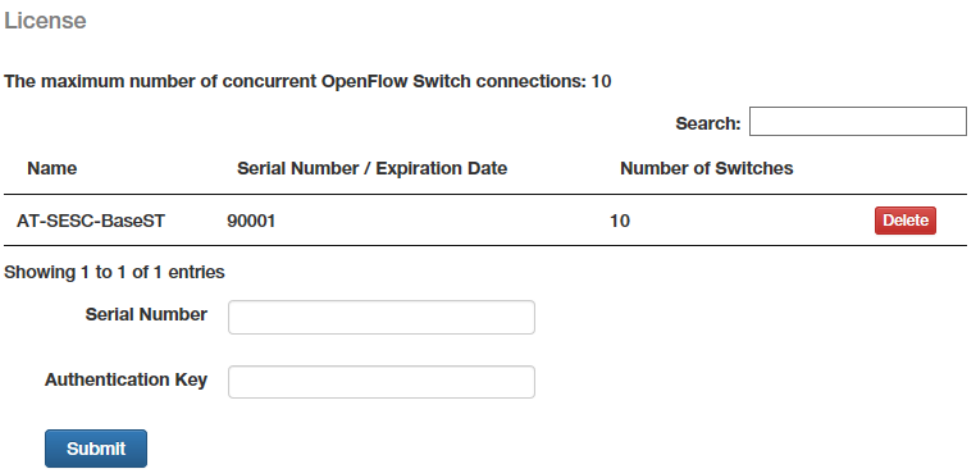


Figure 32. Licenses Section in the System Information Window

2. In the License section, click the **Serial Number** field and enter the serial number of the new license.
3. Click the **Authentication Key** field and enter the authentication key of the new license.
4. Click the **Submit** button to add the new license to the SES controller.

   The controller updates the table to include the new license.

To delete a license, perform the following procedure:

1. Select **System Settings** -> **System Information**.
2. In the License section of the window, click the **Delete** button of the expired license to be deleted.

   The SES controller displays a confirmation prompt.
3. Click the **OK** button to delete the license or the **Cancel** button to cancel the procedure.

Displaying the SES Controller Software Version Number

To view the version number and build date of the SES controller software, select **System Settings** -> **System Information**. The version information is displayed in the Software Information section at the top of the window. An example is shown in Figure 33.

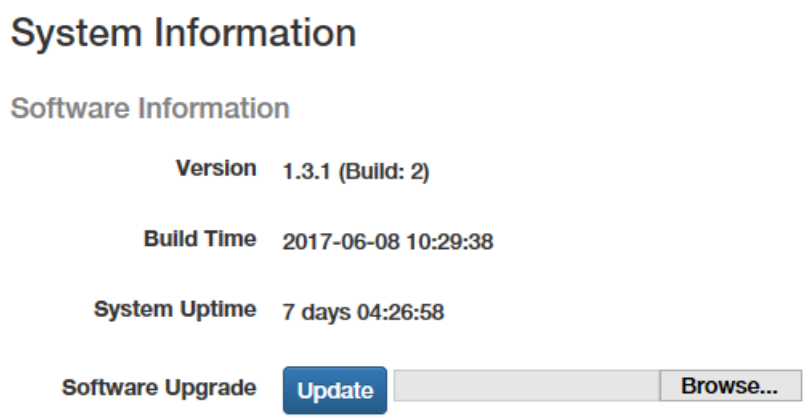


Figure 33. Software Information Section in the System Information Window

Installing New SES Controller Software

This procedure explains how to download new SES controller software to the server. It assumes you have obtained the new software from the Allied Telesis support web site and stored it on your workstation. Please review the following information before performing this procedure:

- ❒ The controller automatically resets after uploading new software. This may interrupt controller services.

- This procedure interrupts your management session. To resume managing the controller, start a new session at the completion of the procedure.
- Installing new software does not delete the existing licenses.

Note

Installing new software does not affect the system or authentication configuration information. However, Allied Telesis recommends backing up the system configuration information before performing the procedure. For instructions, refer to “Backing Up System Information” on page 70.

To install new SES controller software, perform the following procedure:

1. Select **System Settings** -> **System Information**.
2. In the Software Information section of the window, click the Software Update **Browse** button and locate the file with the new SES controller software on your workstation. Refer to Figure 33 on page 77.
3. Click the Software Upgrade **Update** button.

   The SES controller uploads the firmware file and the server writes it to its storage disk. Afterwards, the controller automatically reboots with the new software.
4. To resume managing the controller, wait two minutes and then start a new management session.

Downloading the Technical Support Information File

You might be asked to perform the following procedure if you contact Allied Telesis Technical Support for assistance. It downloads a technical support file from the SES controller to your computer. The file is used in troubleshooting problems with the controller. It is TAR Archive file, with a TGZ filename extension. Do not make any changes to the file prior to sending it to Allied Telesis Technical Support.

To download the technical support information file, perform the following procedure:

1. Select **System Settings** - > **Maintenance**.
2. Scroll down to the Technical Support Information section at the bottom of the Maintenance window. Refer to Figure 34.

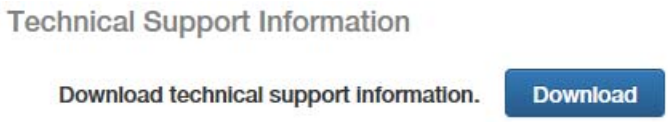


Figure 34. Technical Support Information Section in the Maintenance Window

3. Click the **Download** button.

   The SES controller displays a confirmation prompt.

4. Click the **OK** button to download the file or the **Cancel** button to cancel the procedure.

   When you click OK, the SES controller generates the file. This may take from a few seconds to several minutes, depending on the size of the database.

5. After the SES controller generates the file, follow the prompts to save it on your computer.

   Note
   Do not change the TGZ filename extension.

6. Send the file to Allied Telesis Technical Support.

Restarting the SES Controller

This section contains the procedure for restarting the SES controller's operating system.

Note

This procedure does not reboot the controller's server. To reboot or shut down the server, refer to "Rebooting or Shutting Down the SES Controller's Server" on page 81.

To restart the SES controller's operating system, perform the following procedure:

1. Select **System Settings** - > **Maintenance**.
2. Scroll down to the System Start/Stop section in the Maintenance window. Refer to Figure 35.

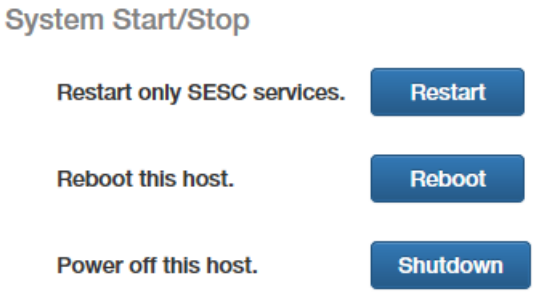


Figure 35. System Start/Stop Section in the Maintenance Window

3. Click the Restart only SESC services **Restart** button.

   The SES controller displays a confirmation prompt.

4. Click the **OK** button to reset the SES controller or the **Cancel** button to cancel the procedure.

Caution

This procedure is disruptive to network operations. The SES controller does not respond to queries from OpenFlow switches as it reinitializes its operating system.

The SES controller resumes normal operations after 30 to 60 seconds.

Rebooting or Shutting Down the SES Controller's Server

To reboot of shutdown the SES controller's server, perform the following procedure.

1. Select **System Settings** - > **Maintenance**.
2. Scroll down to the System Start/Stop section in the Maintenance window. Refer to Figure 35 on page 80.
3. Click the Reboot this host **Reboot** button or the Power off this host **Shutdown** button.

   The SES controller displays a confirmation prompt.
4. Click the **OK** button to reboot or shutdown the controller's server or the **Cancel** button to cancel the procedure.

Caution

Rebooting or shutting down the SES controller's server is disruptive to network operations. When rebooted, the controller requires approximately two minutes to initialize its operating system.

Uploading the Trap Monitoring Rule File

This procedure explains how to upload the trap monitoring rule file from Allied Telesis to the SES controller, for the enhanced firewall protection feature. The controller uses the file to monitor the syslog messages from firewalls for warnings of possible threats on their WAN ports. The following procedure assumes you have already obtained the file from Allied Telesis and stored it on your computer. For instructions on obtaining the file, contact an Allied Telesis sales representative.

To upload the rule file to the SES controller, perform the following procedure:

1. Select **System Settings** - > **Maintenance**.
2. Scroll down to the Trap Monitor section in the Maintenance window. Refer to Figure 36.

Figure 36. Trap Monitor Section in the Maintenance Window

3. Click the **Browse** button and locate the rule file on your computer.
4. Click the **Upload** button.

   The SES controller uploads the file to the server.
5. If you have not already configured the SES controller's trap monitoring settings, go to "Configuring the Enhanced Firewall Protection Feature" on page 83

Configuring the Enhanced Firewall Protection Feature

The enhanced firewall protection feature is configured with the fields in the Trap Monitor Settings window in the System Settings menu. For background information, refer to “Enhanced Firewall Protection Feature” on page 20. Not all the fields are used by the feature. Some are reserved for future development. Table 10 lists the required fields. They are defined in Table 11 on page 85.

Table 10. Configuring the Trap Monitor Settings Window for the Enhanced Firewall Protection Feature

Window Section	Field
Protocols	Syslog Port Number
Networks	Monitoring Networks Excluding Networks (optional) Syslog Forwarding Targets (optional)
AMF Masters	IP address Username Password These parameters are used only when the control plane is using AMF. They are not used with the OpenFlow protocol.
Rules - AMF Action	Drop Packets Link-Down
Rules - Palo Alto Network tab	Enable the Monitoring of Traps from this Host Host Addresses Trap Action

1. To display the Trap Monitor Settings window, select **System Settings - > Trap Monitor Settings**.

   The window is shown in Figure 37 on page 84.

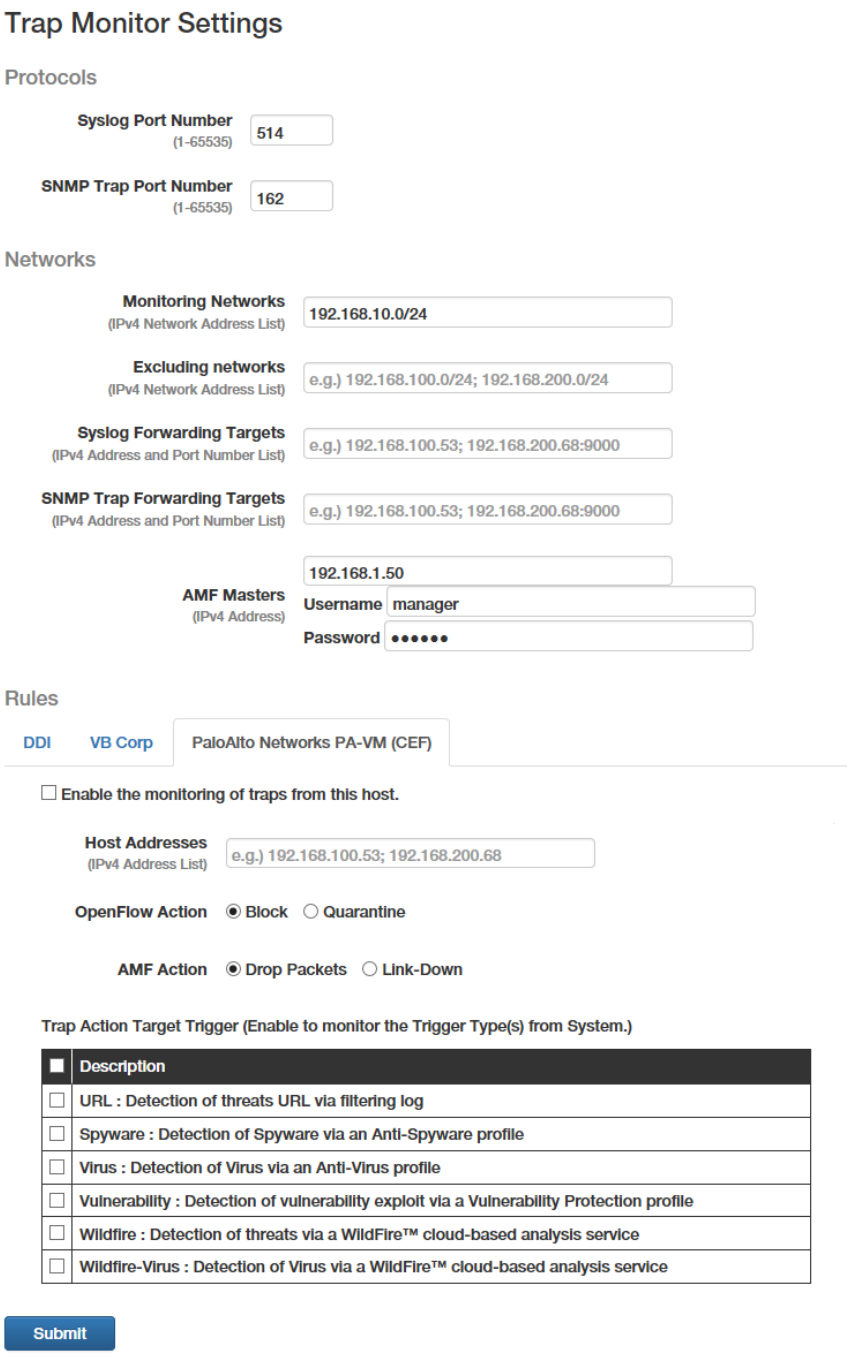


Figure 37. Trap Monitor Settings Window

Note

If the Rules section at the bottom of the window does not include the Palo Alto network tab, you need to upload the trap monitoring rule file to the SES controller. For instructions, refer to “Uploading the Trap Monitoring Rule File” on page 82.

2. Configure the fields. They are described in Table 11.

Table 11. Trap Monitor Settings Window

Field	Description
Protocols Section	
Syslog Port Number	Enter the UDP port number of a syslog server that is to receive syslog messages relayed by the SES controller from firewalls. You can enter only one port number. The range is 1 to 65535. The default value is 514. This field is used together with the Syslog Forwarding Targets field.
SNMP Trap Port Number	This parameter is reserved for future development.
Networks Section	
Monitoring Networks	Enter the IPv4 addresses of networks, subnets (i.e., intranets), or hosts to protect behind the firewall with the enhanced firewall protection. Here are the guidelines: - The list should only include addresses of networks behind the firewall. Do not include networks in front of the firewall (for example, the Internet). - You can enter multiple IPv4 addresses. Separate addresses with semi-colons. - Subnet masks are entered as decimal numbers representing the number of bits, from left to right, that constitute the network portions of the addresses. For example, the decimal masks 16 and 24 are equivalent to 255.255.0.0 and 255.255.255.0, respectively. Here is an example of an address and subnet mask: 10.41.28.0/24. - If you omit the subnet mask, the SES controller adds “/32” as the mask.

Table 11. Trap Monitor Settings Window (Continued)

Field	Description
Monitoring Networks (continued)	- For addresses of specific hosts, enter them without the subnet mask (for example, 10.12.171.12) or with the “/32” mask (for example, 10.12.171.12/32. - The enhanced firewall protection feature is inactive if you leave this field empty.
Excluding Networks	Enter the IPv4 addresses of subnets or hosts to be excluded from the enhanced firewall protection feature. You can use this option to prevent the feature from blocking switch ports of critical hosts, such as servers, because of threats detected on a firewall WAN port. Here are the guidelines: - The IPv4 addresses should be subnets or hosts within the networks specified in the Monitoring Network field. - You can leave this field empty. For other guidelines, refer to the Monitoring Networks field.
Syslog Forwarding Targets	Enter the IPv4 addresses of destination syslog servers. The SES controller relays syslog messages from firewalls to the designated servers. To be part of the enhanced firewall protection feature, firewalls have to send their syslog messages to the SES controller, which uses them to determine when threats are detected on firewall WAN ports. By entering the addresses of syslog servers in this field, you can have the controller relay the messages to servers, for storage. This is useful in saving syslog messages from firewalls that support only one IPv4 address of a syslog server.

Table 11. Trap Monitor Settings Window (Continued)

Field	Description
Syslog Forwarding Targets (continued)	Here are the guidelines: - You can specify multiple destination syslog servers. Separate the server IPv4 addresses with semicolons. Here is an example: 10.122.67.2;10;122.101.90 - You can include a secondary syslog port number with an IPv4 address if a destination syslog server uses a different port number than the value in the Syslog Port Number field in this window. Separate the IPv4 address from the port number with a colon. Here is an example: 10.122.67.2:9000 - The SES controller changes the sender's IPv4 address in syslog messages to its own address. However, the information inside the syslog messages themselves are not changed.
SNMP Trap Forwarding Targets	This parameter is reserved for future development.
AMF Masters	Enter the IPv4 address of the AMF master, with the AMF application proxy. You can specify only one IP address.
Username	Enter the username of the privileged user on the AMF master. It is case-sensitive.
Password	Enter the password of the privileged user on the AMF master. It is case-sensitive.
Rules Section - AMF Action	
Drop Packets	Drop the ingress packets of hosts that the firewall has identified as the possible source or target of a network threat.
Link-Down	Disable the switch ports of hosts that the firewall has identified as the possible source or target of a network threat.
Rules Section - Palo Alto Networks Tab	

Table 11. Trap Monitor Settings Window (Continued)

Field	Description
Enable the monitoring of traps from this host.	Enable or disable the enhanced firewall protection feature. The feature is enabled when the check box has a check mark. The default value is disabled.
Host Addresses	Enter the IPv4 addresses of the firewalls. You can enter multiple addresses.
OpenFlow Action	Not applicable to the AMF application proxy.
AMF Action	Select the action of a switch when notified that a host is the source or target of a malware attack. The choices are listed here: - Drop packets: Drop the ingress and egress packets of the host. - Link-Down: Disable the host's port.
Trap Action	Enable or disable the network threats that the enhanced firewall protection feature is to monitor from the firewall. Threats are enabled when their check boxes have check marks. The default setting for all threats is enabled. The threats are listed here: - URL - Spyware - Virus - Vulnerability - Wildware - Wildfire-Virus

Note

The DDI and VB Corp tabs in the Rules section at the bottom of the Trap Monitor Settings window are reserved for future development.

3. Click the **Submit** button to add your changes to the SES controller.

Viewing or Restoring Isolated Hosts

This section contains instructions on how to view or restore hosts that the controller has disconnected, blocked, or quarantined. The action the SES controller performs in restoring a host depends on the type of isolation, as outlined here:

- Restoring a disconnected host- The SES controller instructs the switch to activate the host's port, allowing the host to forward traffic.
- Restoring a blocked host - The controller instructs the switch to unblock the host's traffic, allowing the host to forward traffic.
- Restoring a quarantined host - The controller restores the host to its original VLAN assignment.

To restore isolated hosts from the Action List window in the Policy Settings window, perform the following procedure:

1. Select **Policy Settings** -> **Action List**.

   The SES controller displays the isolated hosts in the Active Device List window. An example is shown in Figure 38.

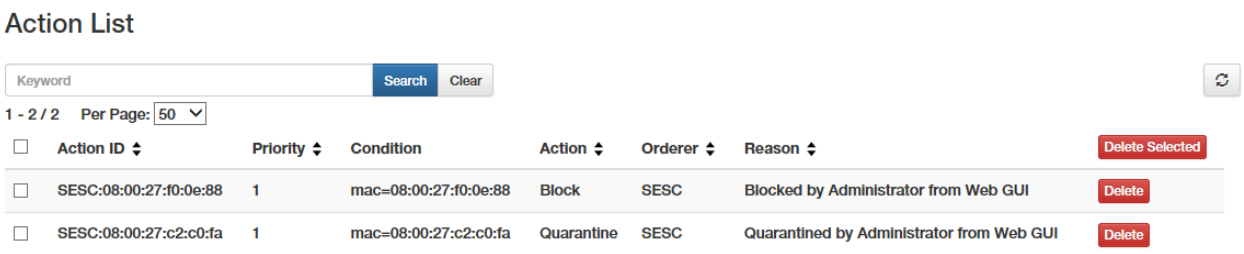


Figure 38. Action List Window

The columns in the window are described in Table 12.

Table 12. Action List Window

Column	Description
Action ID	Displays the MAC address of the isolated host, preceded by "SESC:".
Priority	Displays the priority number.
Condition	Displays the MAC address of the isolated host, preceded by "mac:".

Table 12. Action List Window (Continued)

Column	Description
Action	Displays the action, which can be disconnect, block, or quarantine. The actions are described in “Viewing or Restoring Isolated Hosts” on page 89.
Orderer	Displays who ordered the action. “SESC” indicates the SES controller.
Reason	Displays the reason for the isolation.

2. To remove a host from its isolated status and return it to its normal status, do one of the following:

   - To restore a single isolated host, click its **Delete** button in the right column.
   - To restore multiple hosts, click their check boxes in the left column and then the **Delete Selected** button at the top of the right column.

   The SES controller displays a confirmation prompt.

3. Click the **OK** button to restore the host or **Cancel** to cancel the procedure.

Appendix A
Configuring Your Web Browser

This chapter contains instructions on how to configure your web browser for the SES controller. The chapter includes the following sections:

Enabling JavaScript on Your Web Browser

Your web browser has to have JavaScript to support the browser windows in the SES controller. The following procedure explains how to enable JavaScript in Microsoft Windows Internet Explorer. If you are using a different web browser, refer to the appropriate documentation for instructions.

To enable JavaScript in Microsoft Windows Internet Explorer, do the following:

1. Open the Windows Internet Explorer.
2. Click **Tools** from the menu bar.
3. Select **Internet options** from the drop-down menu.

   The Internet Options window is displayed.
4. Click the **Security** tab on the Internet Options window.

   The Internet Options window is shown in Figure 39.

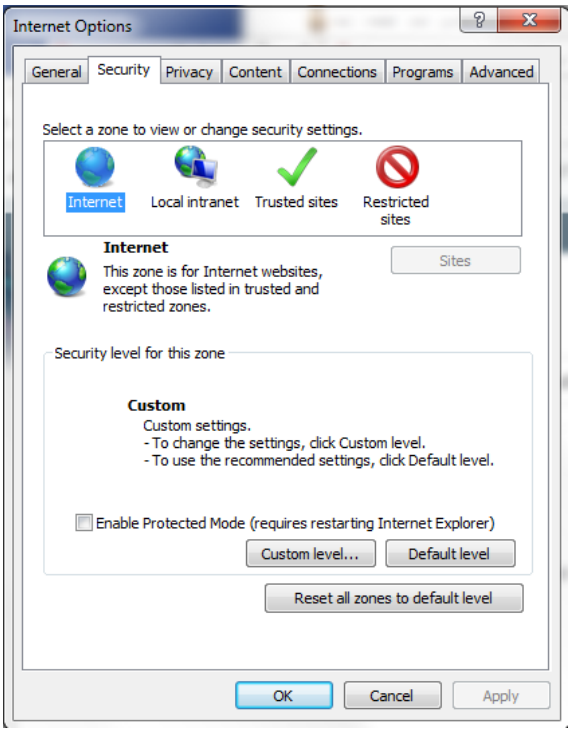


Figure 39. Security Tab in the Internet Options Window

5. Click the **Custom Level...** button.

The Security Settings Internet Zone window is shown in Figure 40.

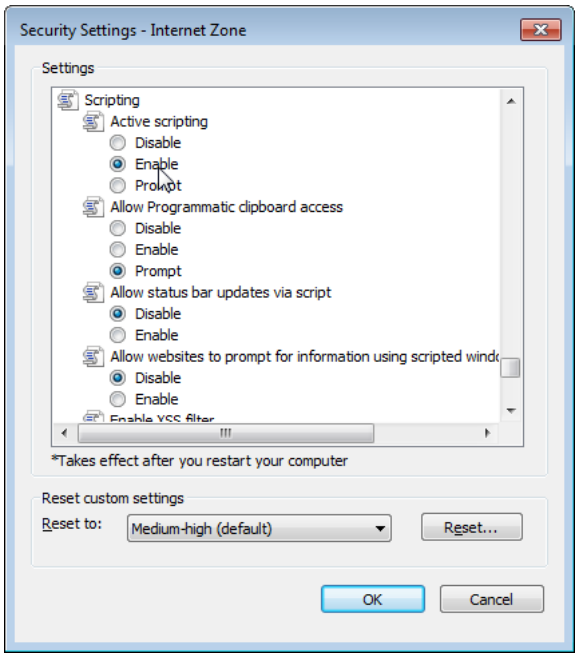


Figure 40. Security Settings Window

6. Scroll down to the Scripting section and Active scripting subsection.
7. Change the setting of Active scripting to **Enable**.
8. Click **OK**.
9. Restart the Internet Explorer.

   JavaScript is now enabled on your web browser. For instructions on how to start a management session, refer to “Starting a Management Session” on page 49.

Making the SES Controller a Trusted Website

If you manage the SES controller with the secure HTTPS mode and the Allied Telesis SSL certificate, your web browser will display a website security certificate message at the start of your management sessions. You can avoid this message by making the SES controller a trusted web site in your web browser. The following instructions are for the Microsoft Windows Internet Explorer. For instructions on how to add a trusted web site to a different web browser, refer to the appropriate documentation. The procedure requires knowing the IPv4 address of the controller.

To make the SES controller web site a trusted site in Microsoft Windows Internet Explorer, perform the following procedure:

1. Open Windows Internet Explorer.
2. Click **Tools** from the menu bar.
3. Select **Internet options** from the drop-down menu.

   The Internet Options window is displayed.
4. Click the **Security** tab on the Internet Options window. Refer to Figure 39 on page 92.
5. Click the **Trusted sites** icon in the box. Refer to Figure 41.

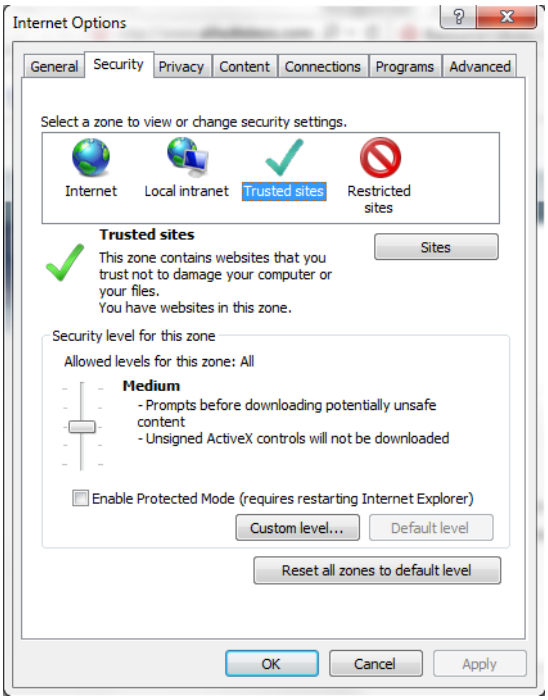


Figure 41. Security Tab in the Internet Options Window

6. Click the **Sites** button.

   The Trusted sites window is displayed. Refer to Figure 42.

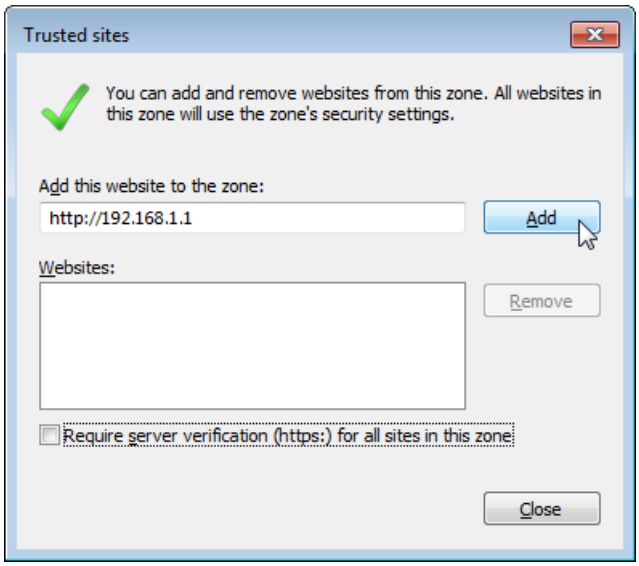


Figure 42. Trusted Sites Window

7. In the “Add this website to the zone” field, enter “https://” followed by the IP address of the SES controller.

   The default IP address for the controller is 192.168.1.1.

8. Verify that the checkbox for “Require server verification (https:) for all sites in this zone” has a check mark. If the checkbox does not have a check mark, click the box to add it.

9. Click the **Add** button.

10. Click the **Close** button.