

Adtran

Adtran Switch Engine (ASE)

20.12-3 Release Notes

Release Notes

6AMCRN20123-40A

October 2022



To the Holder of this Document

The contents of this manual are current as of the date of publication. Adtran reserves the right to change the contents without prior notice.

Trademark Information

“Adtran” and the Adtran logo are registered trademarks of Adtran, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by Adtran’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with Adtran that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall Adtran be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

Be advised that certain security risks are inherent in the use of any telecommunications or networking equipment, including but not limited to, toll fraud, Denial of Service (DoS) attacks, loss or theft of data, and the unauthorized or illegal use of said equipment. ADTRAN OFFERS NO WARRANTIES, EITHER EXPRESSED OR IMPLIED, REGARDING THE PREVENTION, DETECTION, OR DETERRENCE OF TOLL FRAUD, NETWORKING ATTACKS, OR UNAUTHORIZED, ILLEGAL, OR IMPROPER USE OF ADTRAN EQUIPMENT OR SOFTWARE. THEREFORE, ADTRAN IS NOT LIABLE FOR ANY LOSSES OR DAMAGES RESULTING FROM SUCH FRAUD, ATTACK, OR IMPROPER USE, INCLUDING, BUT NOT LIMITED TO, HUMAN AND DATA PRIVACY, INTELLECTUAL PROPERTY, MATERIAL ASSETS, FINANCIAL RESOURCES, LABOR AND LEGAL COSTS. Ultimately, the responsibility for securing your telecommunication and networking equipment rests with you, and you are encouraged to review documentation regarding available security measures, their configuration and implementation, and to test such features as is necessary for your network.



901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000

Copyright © 2022 Adtran, Inc.
All Rights Reserved.

Table of Contents

1. Introduction	4
2. Supported Platforms	4
3. Features and Enhancements	4
4. Fixes	6
5. Errata	9
6. System Notes	9
7. Warranty and Contact Information	10

1. Introduction

Release 20.12-3 is a major system release that adds new features and addresses customer issues that were uncovered in previous releases for the Adtran Switch Engine (ASE) switches.

This release is generally available code. Results obtained during internal testing have been evaluated and the code has been determined to be ready for general availability. Caveats discovered during testing but not addressed in this build are listed in [Errata on page 9](#).

Configuration guides, white papers, data sheets, and other documentation can be found on Adtran's Support Community, <https://supportcommunity.adtran.com>. The contents of these release notes will focus on the platforms listed in [Supported Platforms on page 4](#).

2. Supported Platforms

[Table 1](#) lists the platforms that are supported in ASE firmware release 20.12-3.

Table 1. Supported Platforms

Platform	Part Number
NetVanta 1760-12F	17101763F1
NetVanta 1570-24-370W	17101574PF1

3. Features and Enhancements

This section highlights major features, commands, and behavioral changes for all products running ASE version 20.12-3:

- Cable diagnostic results for the 10G copper module interface have been disabled, and the running state and display results for this interface are not displayed.
- Enabled the **ip https** and **http-redirect** features in the default switch configuration.
- Added DHCP server support to the switch functionality. Devices can act as a DHCP server and can support configurable DHCP options. In addition, DHCP server IP assignments based on Client Identifier values and device MAC addresses are now supported, without client-provided Option 61 values.
- Added support for the Adtran 10G copper SFP to ASE devices.
- BSW-100
BSW-99 Updated the options in the **no radius-server** CLI configuration to match those available in the Web GUI, and added the **attribute** parameter to the **no-radius server** command set.
- BSW-10
BSW-536
BSW-537
BSW-539
BSW-540 Added support for Telnet and SSH client functionality in the ASE CLI.
- BSW-119 Added the **write** command to the switch CLI; this command acts similarly to the **copy run start** command.
- BSW-120 Added the **copy tftp://x.x.x.x/filename flash** command to the switch CLI; this command performs the same function as the older **copy tftp://x.x.x.x/filename flash:filename** command.

- BSW-121 Updated the switch function when firmware upgrades are completed so that the switch does not reboot automatically. Instead, when a firmware upgrade is completed, the following message appears and no reboot takes place: *File transfer completed, reload the device to activate the firmware*. The new firmware will be used until the device is rebooted, but no firmware swaps are allowed until after a reboot has been performed. Once the device is rebooted, it will use the new firmware specified in the upgrade procedure, and future firmware swaps will be allowed.
- BSW-127 Added the switch serial number to the output of the **show version** command.
- BSW-150 Increased the switch banner size to **1520** characters.
- BSW-152 Added support for custom remarks in management ACL configurations. The remarks can be used to add a description to each ACL rule.
- BSW-153 Added the ability to add, view, and modify VLAN interface descriptions in both the CLI and Web GUI.
- BSW-156 BSW-480 Added support for Enable mode TACACS+ authentication. The **aaa authentication enable local** feature has been added to the default switch configuration.
- BSW-216 Added the ability to view and modify port descriptions in the Web GUI.
- BSW-218 Added the ability to use the CLI to view users currently connected to the device in the Web GUI
- BSW-270 Added the ability to specify a 31 bit netmask in an IP Address configuration for a port.
- BSW-299 Added support for specifying additional SNMP server parameters in the **snmp-server** configuration, such as contact name, phone, email, and additional location and chassis-id information.
- BSW-302 Added support for LLAG interface descriptions in both the CLI and Web GUI.
- BSW-341 Added support for hostnames to be specified with a numeral as the first character and to include additional special characters.
- BSW-346 Added a confirmation step when entering the **reload defaults** command. Updated prompts appear as follows when the **reload defaults** command is entered:


```
# reload defaults
Do you want to save the configuration to default settings (y/n)? n
Give up to do reload default.
```
- BSW-366 Added support for the new **show tech** command. When entered, this command displays output from various other **show** commands, and produces an output file which can be downloaded via HTTP. Information included in the **show tech** command output includes:


```
#show version
#show interface * [status | capabilities | statistics]
#show logging
#dir
#show running-config
#show spanning-tree
#show ip [arp | interfaces | route | statistics]
#show access management
#show system cpu status
```
- BSW-428 Updated the **show vlan** command output to include access ports configured with the voice VLAN enabled.
- BSW-49 Updated the SNMP server state to be disabled by default.
- BSW-97 BSW-290 Added enhancements to the **reload** command. The additional **in <time>** parameter allows a reload to be scheduled on a delay, and the additional **cancel** parameter allows a scheduled reload to be canceled.

- PM2022032401 Added two messages to indicate the progress when saving configuration files to Flash memory. The first message (*Please do not power off*) indicates that the file is being saved, and not to power down the device while the file is saving. The second message (*Saving flash memory is done*) indicates the write process is complete.
- W1101235 Added a field for device part numbers in the ASE CLI and Web GUI.
- W1110416 Added support for auto-link capabilities between ASE devices and n-Command MSP.
- W1110416 Added the ability to specify group descriptions when configuring LACP groups.

4. Fixes

This section highlights major bug fixes in ASE release 20.12-3.

- Fixed an issue in which a description for the LACP max-bundle parameter was missing in the CLI.
- BSW-214 Fixed an issue in which the backspace key would not function in SSH/telnet sessions.
- BSW-267 Fixed an issue in which, when entering the **no ip name-server** command, the command would accept a number value outside of the valid preference range.
- BSW-363 Fixed an issue in which the ASE device would remove VLAN tags on access ports with **voice vlan** enabled.
- BSW-365 Fixed an issue in which Link OAM MIB retrieval did not function properly when using the GUI. In addition, updated the wording of Link OAM error messages in both the CLI and Web GUI. Error messages now indicate the type of problem experienced, and appear as either *OAM port configuration is not appropriately configured* or *OAM link partner is disconnected*.
- BSW-370 Fixed an issue in which 2.5Gb SFP (P/N 1200482G1) would not function properly on an ASE device.
- BSW-377 Fixed an issue in which the **show ip ospf interface** command would display an incorrect state for VLANs.
- BSW-408 Fixed an issue in which the **Reset** button for the **Add Route** configuration option was not functioning correctly in the **IP Configuration** page of the GUI (**Configuration > System > IP**),.
- BSW-421 Fixed an issue in which an unsupported speed option was able to be specified for Gigabit Ethernet ports.
- BSW-430 Fixed an issue in which the syslog server mode could not be disabled via the web GUI.
- BSW-431 Fixed an issue in which using the syslog **reset** button in the web GUI would disable the server mode.
- BSW-432 Fixed an issue in which some QoS drop precedence level configuration options were missing from the web GUI.
- BSW-435 Fixed an issue in which the **inner-tag vid** parameter for QoS Control List entries would not function properly.
- BSW-438 Fixed an issue in which the wrong help text was displayed for the QoS control list IPv6 configuration in the CLI.
- BSW-443 Fixed an issue in which some rate type configurations were missing for some queues in the **QoS Egress Port Shapers** GUI menu.
- BSW-444 Fixed an issue in which **QoS Ingress Map** and **QoS Egress Map** configurations were not available in the web GUI.
- BSW-446 Fixed an issue in which an IPv6 address could not be specified for the VLAN interface in the web GUI.

- BSW-449 Fixed an issue in which traffic would flow through the wrong CoS queue, even when the CoS value was specified correctly in the QoS ingress map.
- BSW-452 Fixed an issue in which the **QoS Ingress Map** and **QoS Egress Map** configurations could not be edited from the web GUI.
- BSW-453 Fixed an issue in which the **Cancel** button did not function correctly in the **QoS Egress Port Scheduler** GUI menu.
- BSW-459 Fixed an issue in which the **QoS Control List** GUI menu would not function properly if an out-of-range entry was specified.
- BSW-461 Fixed an issue in which the QoS control list was not functioning properly in the device GUI.
- BSW-466 Fixed an issue in which interface VLAN IP configurations were being deleted when running configurations were uploaded from the CLI.
- BSW-467 Fixed an issue in which **QoS Ingress Map** and **QoS Egress Map** configurations could be saved with an invalid **Map ID** in the web GUI.
- BSW-468 Fixed an issue in which some LACP Group configuration parameters were missing from the device GUI.
- BSW-469 Fixed an issue in which the help text for the **interface-llag** command would display twice.
- BSW-470 Fixed an issue in which ingress traffic was being filtered when the LACP max-bundle parameter was set to 1.
- BSW-471 Fixed an issue in which the LACP system priority configuration was missing in the GUI.
- BSW-475 Fixed an issue in which the LACP group range configurations were different between the CLI and web GUI.
- BSW-490 Fixed an issue in which the **Reset** button was not functioning correctly in the **Authentication Method** GUI menu.
- BSW-494 Fixed an issue in which the **Reset** button was not functioning correctly in the **Access Management** GUI menu.
- BSW-525 Fixed an issue in which the SNMP mode would display as enabled in the output of the **show snmp** command, even when SNMP was disabled.
- BSW-535 Fixed an issue in which the **telnet** command was only available in the configuration menu. This command is now available in the Enable mode.
- BSW-560 Fixed an issue in which, in some cases, the auto-link feature stopped working until the device was rebooted and displayed a status of **Error: Stopped by user**, even when auto-link was enabled.
- BSW-561 Fixed an issue in which **restore job** operations would fail when using n-Command MSP with the ASE device.
- BSW-565 Fixed an issue in which the **LLDP-MED Neighbor** GUI menu would display incorrect characters along with actual values.
- BSW-566 Fixed an issue in which VLAN translation configuration options were missing from the ASE Web GUI.
- BSW-568 Fixed an issue in which the ASE device firmware version, size, and Device Type descriptions were displayed incorrectly in n-Command MSP.
- BSW-571
- BSW-575 Fixed an issue in which the number of entries displayed in management ACLs were incorrect (only displaying 16 entries instead of 64).
- BSW-582 Fixed an issue in which firmware upgrades would fail when using n-Command MSP.

- Bug 22350 Updated the mode setting from **Enable/Disable** to **On/Off** in the **DHCP > Server > Configuration** GUI menu.
- Bug 22352 Updated the **Event Notification > SNMP Trap** GUI menu to include the ability to delete a notification.
- Bug 22353 Updated the **APS > Configuration** GUI menu to include the Working, Protection Port, SF Type, Domain, Service, and MEPID parameters.
- Bug 22354 Fixed an issue in which the **firstttl** parameter was missing from the IPv6 traceroute feature.
- Bug 22355 Fixed an issue in which, in the **Detailed Link OAM Statistics** GUI menu (**Port Management > Link OAM > Detailed Link OAM Statistics**), when clearing the statistics for Port 1 only, the OAM statistics for all ports were cleared.
- Bug 22356 Fixed an issue in which the Link OAM variable retrieval option was available on the web GUI even though the feature is not supported.
- Bug 22357 Fixed an issue in which SNMP would not accept a subsequent view entry used to exclude a specified OID subtree in certain **snmp** commands.
- Bug 22360 Fixed an issue where, after the DHCP client ID was updated, the Option 61 parameter of Discover packets remained unchanged.
- Bug 22362 Fixed an issue in which the **Refresh** button of the **Multicast > IGMP Snooping > VLAN Configuration** GUI menu did not function.
- Bug 22363 Fixed an issue in which the QCE configuration GUI menu would not return a warning when incorrect IPv4 settings were specified in the entry.
- Bug 22479
Bug 22503
Bug 22505 Fixed several issues related to PoE use in the ASE device, including an issue in which powered device class information would not display correctly, an issue where power allocation and power required values were not the same, and an issue in which selecting **PoE Management** functions in the **PoE Firmware Upload** GUI menu would display an incorrect upload path.
- Bug 22500 Fixed an issue in which the 10G interface port configuration options did not match with expected functionality.
- Bug 22506 Fixed an issue in which selecting MRP functions in the **MVRP Statistics** or **MVRP Statistics** GUI menus would display incorrectly.
- Bug 22509 Fixed an issue in which the ASE device web GUI displayed functions that were not supported in the device.
- Bug 22516 Fixed an issue in which the ASE device fan did not operate correctly.
- Bug 22517 Fixed an issue in which the **copy** command would not transfer configuration files to a TFTP server.
- Bug 22518 Fixed an issue in which the web GUI would not properly display descriptions entered for interfaces via CLI.
- Bug 22520 Fixed an issue in which the IP address entries were displayed incorrectly in the **Advanced Settings** page of IP address configuration in the web GUI.
- Bug 22609 Fixed an issue in which device temperature detection information was not displaying correctly in the **show system** output.

5. Errata

The following is a list of errata that still exist in ASE release 20.12-3.

- Spanning-tree may incorrectly prevent Link Aggregation Group (LAG) links from becoming active when **max-bundle** is set to **1**. **Workaround:** Set the **max-bundle** to a value higher than **1**.
- BSW-286 When support was added for TACACS+ authentication of Enable mode logins, the default Enable mode login authentication behavior was changed. Previously, the default authentication database was set to the local database. With the addition of the TACACS+ authentication support, you must now specify the database to be used for authentication. If the local database is to be used for Enable mode login and authentication, you must enter the **aaa authentication enable local** command when accessing the switch. The entire login procedure includes the following commands:
 - ◆ **#username test privilege 0 password encrypted <string>**
 - ◆ **#enable secret 5 level 15 <string>**
 - ◆ **#aaa authentication enable local**
- BSW-544 In some cases, SSH/Telnet features will not function with non-Adtran devices.

6. System Notes

The following are important notes about the ASE 20.12-3 release:

- For ASE system compatibility with n-Command MSP, the ASE device must be running version 20.12-3 or later.
- Due to key exchange algorithms and encryption ciphers, telnet/SSH access for the NetVanta 1760-12F may be limited when accessing non-Adtran devices using this feature. In some cases, when logged into an ASE device via telnet, and then using SSH to access a non-Adtran device, the connection may be successful but limited to enable mode access on the non-Adtran device.
- On a NetVanta 1760-12F, if upgrading from ASE 20.12-1 to 20.12-3, the changes included in 20.12-3 for SNMP server enable/disable functions, AAA authentication, or auto-link configurations may cause issues if these features have been configured previously. If problems are encountered after a device upgrade to 20.12-3, it is recommended to reload the device with the factory default settings.
- Updated SNMP configuration commands for the 20.12-3 release include:
 - ◆ **no snmp-server**
 - ◆ **snmp-server community [writecommunity | readcommunity] disable**
 - ◆ **no snmp-server security-to-group model [v1 | v2c] name [public | private]**
- Updated AAA authentication commands for the 20.12-3 release include:
 - ◆ **aaa authentication enable local**
 - ◆ **aaa authentication login http redirect**
 - ◆ **aaa authentication login https local**
- Updated auto-link commands for the 20.12-3 release include:
 - ◆ **auto-link recontact-interval 3600**
 - ◆ **auto-link penalty 0**
 - ◆ **auto-link https srv https**

7. Warranty and Contact Information

Warranty information can be found online by visiting www.adtran.com/warranty-terms.

To contact Adtran, choose one of the following methods:

Department	Contact Information	
Customer Care	From within the U.S.:	(888) 4ADTRAN ((888)-423-8726)
	From outside the U.S.:	+1 (256) 963-8716
Technical Support	Support Community:	www.supportcommunity.adtran.com
	Product Support:	www.adtran.com/support
Training	Email:	training@adtran.com
	Adtran University:	www.adtran.com/training
Sales	For pricing and availability:	1 (800) 827-0807