Ecessa Firmware Release Notes

Version: 11.0.0
Release: 2019.03.18
Revision 1.0: 2019.03.18

New Features

System

- **Ability to capture device crash reports**

Additional Information

This feature should only be enabled if the device is rebooting for unknown reasons. When this feature is enabled and the device gets into a failed state it will attempt to save the crash report.

Disk

- **SSD drives support swap which allow part of the drive to be used for memory when system memory is not available**

Improvements

WAN

- **PPPoE WAN's will use a default MTU of 1452**

SSL

- **Ability to set Diffie-Hellman key size to be used for web server HTTPS**

Additional Information

The default Diffie-Hellman key size for HTTPS is 1024. This change allows 2048 to be used for the key size.

DNS

- **Add support for DNS CAA records**

SNMP

- **Add IPv6 support to the Ecessa SNMP MIB**

Additional Information

The Ecessa MIB has been updated to version 2 to support IPv6 using the InetAddress convention. For SNMP monitoring purposes, users will need to update to ECESSA-MIB-v2.

DHCP-Helper

- **Allow DHCP Relay to be used when LAN DHCP servers are configured on the device as long as they use different LANs**

Changes

VPN

- **Add ability to configure Diffie Hellman key size for SSL VPN connections, either 1024 or the default 2048**

Update

- **Firmware update user interface updated to show more information about available versions**

Additional Information

The user interface for firmware updates now displays information about why a version is not available based on the firmware device

Partitions

- **Devices with SSD drives now support multiple firmware versions on the device as well as a recovery firmware**

Fixes

System

- **Maximum number of sessions are not set correctly for PL1200 and PL4000 models**

WAN Virtualization

- **WAN Virtualization sites using double digit site ID's can result in extra PPP connections staying around after tunnels bounce**
- **Disabling WAN Virtualization, or a hardware failover occurring when WAN Virtualization is enabled, on a busy system can result in a software deadlock**
- **WAN Virtualization static route tunnels were not being configured correctly using the CLI**
- **WAN Virtualization compression can cause traffic to be dropped when a tunnel bounces**

  Additional Information

  The compression feature was previously removed due to it causing traffic to stall when the master tunnel went down. That problem has been fixed and the feature added again
- **A WAN Virtualization site can get in to a state where a tunnel appears to repeatedly come up and go back down but never actually connects**

  Additional Information

  This problem can be seen when a site remains up but one or more of its tunnels is bouncing repeatedly.

  Workaround

  Disable WAN Virtualization and re-enable it to correct the problem. To prevent it from happening again, increase the tunnel tests and/or timeout values to avoid bouncing.

VPN

- **VPN non-legacy autostart does not work correctly in firmware 11.0.0+ after WAN changes are made**

  Additional Information

  Issue seen with Autostarting VPNs in older firmwares is no longer present in this firmware, so the default value has been changed. If you have legacy-autostart disabled via the CLI, and upgrade to 11.0+ firmware, legacy-autostart will now be enabled.
- **Some SSL clients running new software versions will not connect to SSL VPN due to weak message digest algorithm**

  Additional Information

  A user that creates a new certificate authority will be able to choose the digest, which defaults to sha256. The self certificate authority can be configured to use the following message digests: sha1, sha256, sha384, sha512, md5, and mdc2
- **CLI diagnostics iperf will not initially connect over a site-to-site IPSec VPN connection**
- **Clients which do not support 'comp-lzo' setting may be unable to connect to a SSL VPN**

  Additional Information

  This affects clients which do not support the 'comp-lzo' option. In this version Ecessa uses the 'compress' option to choose compression. Additionally add support for the LZ4 compression algorithm for use in SSL VPNs.

Virtual Product

- **Virtual Product has a missing log file**

  Additional Information

  Via CLI: log view main or via web interface: (View Log -> Main Tab) will not display on the virtual product.
- **Registering a virtual machine with a group name that is more than 24 characters will report that the group does not exist even if it does**

  Additional Information

  The new error message about this will state that the group name provided was too long

  Workaround

  Create another group to place the VM into which has a name which is 24 characters or less.

VTI

- VPN IPSec VTI connections now require wide open traffic selectors in order to allow routed traffic through

DNS

- Authoritative DNS zone may load improperly on config load
- CLI command dns notify does not work

SNMP

- 'View Ecessa Mib' does not include the beginning section in the web interface

Statistics

- Web links to statistics on QoS page go to the wrong page

Known Issues

System

- Ports can become disabled on legacy 600 product (7568c) when pulling a cable during traffic flow

Additional Information

Ports can become disabled on legacy 600 family of products (7568c) when pulling cables during traffic flow. The device will have to be manually rebooted in order to get the port into a working state.

Workaround

Reboot the device.

WAN

- Creating a WAN using the CLI, with an alias of 24 characters, causes a software restart
- The DHCP service can stop unexpectedly

Additional Information

The DHCP service stopping will cause DHCP WAN lines to miss IP Address updates.

Workaround

If a DHCP WAN does not properly update its IP Address then reboot the device.

- When a DHCP WAN is given a very short lease time by the modem the Ecessa device can become unresponsive

Additional Information

The duration of a lease is typically at least several hours. When the duration of the lease is less than a minute this problem can occur.

Workaround

Verify that the ISP modem is providing the DHCP WAN with a proper lease time.

WAN Virtualization

- Creating a WAN Virtualization site with a name longer than 22 characters causes a software restart
- When a device is running a configuration which has WAN Virtualization sites and loads a configuration which does not have WAN Virtualization sites configured the device software may restart

Additional Information

This is only a factor if the device has a product key which supports less WAN Virtualization sites then the configuration that is currently running

- Adding an encrypted WAN Virtualization site using the CLI may not work as expected

Additional Information

Using the CLI to add an encrypted WAN Virtualization site, and setting global WAN Virtualization options at the same time, will result in no VPN entry being created for the site.

Workaround

Using the CLI, commit global WAN Virtualization changes separately from committing the added site. Alternatively, add the site using the web interface.

- Enabling WAN Virtualization encryption using the CLI without specifying a VPN name will create an IPSec VPN entry with no name

Additional Information

Once an entry with no name is created, the user will then have no way to delete the entry.

Workaround
Make sure to specify the 'vpn-name' in the CLI command, or use the web interface to enable encryption for WAN Virtualization sites.

● WAN Virtualization which is using non base IP addresses can not route as expected when a static route is in place which applies to all traffic
Additional Information
WAN Virtualization feature which is setup to use non base IP addresses can have issues when there is a static route that is in place which is setup to apply to all traffic.

Workaround
There are several ways to address this issue:
1. If possible use the base IP addresses for WAN Virtualization.
2. Change the static route so that it only applies to the traffic that is necessary.

● WAN Virtualization hub location cannot have a site number that is greater than 127
Additional Information
When a WAN Virtualization site is created, the hub site (which is defined as the site with the lower site ID number) must be 127 or lower. If the value is greater than 127 then the associated site will be unable to connect. This does not affect the remote site IDs, which can be greater than 127. This does not affect the total number of sites allowed.

Workaround
Set the associated hub site to have a lower site number.

Hardware Failover

● Using Hardware Failover with high traffic throughput can cause excessive loading of the device
Additional Information
Hardware Failover is by default stateful, and a very high number of TCP sessions can cause excessive loading of the device.

Workaround
If a Hardware Failover device becomes slow to respond, turn off the stateful option in Hardware Failover using the following CLI command: 'hwfo set stateful disable; commit save'

Virtual Product

● Virtual Product may boot slowly
Additional Information
Slow boot sequence has been observed. Infrequently the Virtual Product will take around four minutes to boot. Upon boot everything functions normally.

Workaround
Force reset the device.

SIP Proxy

● Phone calls made within a short time after enabling the VoIP feature may not choose the Primary WAN
Workaround
Wait at least 10 seconds after initially enabling the VoIP feature before making phone calls.

DNS

● DNS Reverse Zone may not work correctly for load-balanced hosts
Additional Information
DNS Reverse Zone information for load-balanced hosts may be set up incorrectly with PTR option.

Workaround
Remove the load-balanced host, activate changes, then add the load-balanced host again.

LCD

● The LCD display can become stuck and not display new information when keys are pressed
Workaround
Reboot the device.

Aliases

● Using the CLI to create an alias with multiple addresses will reorder the

addresses and remove duplicates, making the alias unusable for firewall forwarding rules

Additional Information

If creating aliases to use for firewall WAN to LAN one-to-one forwarding rules, the CLI will not create them properly.

Workaround

Use the web interface to create aliases where the order of the addresses, and preservation of duplicates is important.

Static Routes

- **Failback static route over WAN Virtualization doesn't fail back after failing over to a WAN**