AscenLink LinkOS V7.1 B5745

Release Notes

Table of Contents

Introduction

Summary

This LinkOS firmware V7.1 B5745 is the latest build for Fortinet AscenLink V7.1. To resolve the security vulnerabilities such as Heartbleed, Open SSL, PHP and key size for SSL certificates are upgraded in this release. Several system issues are also fixed in this release. This document provides a list of resolved issues, upgrade procedures and support information of AscenLink LinkOS V7.1 B5745. Please review all sections of this document prior to upgrading your device.

Supported Models

LinkOS **V7.1 B5745** is the latest AscenLink firmware version released for AscenLink-700, AscenLink-5000 and AscenLink-6000.

Compatibility

LinkOS **V7.1 B5745** provides basic support and is compatible with all versions of LinkReport. AscenLink-6000 requires LinkOS V6.1, or higher.

Resolved Issues in V7.1 B5745

Ticket 2805

Under AscenLink HA deployment, applying hundreds of NAT rules to the master unit caused the slave unit reboot abnormally.

Ticket 2823

AscenLink sometimes failed to establish secure connection (SSL) to AscenLink Web UI via Fire Fox or Google Chrome.

Ticket 2828

After firmware upgrading to an AscenLink which there have been policies configured in Multihoming, the Multihoming page of web UI was not shown correctly.

Ticket 2829

The function of disabling VRRP (System > Network setting > LAN Private Subnet) did not work. The checkbox could be “unchecked” but the process failed to disable VRRP.

Ticket 2851

PHP employed in AscenLink is upgraded to resolve a well-known threat CVE-2013-6420 (PHP function openssl_x509_parse memory vulnerability).

Ticket 2853

SSL certificates employed in AscenLink are upgraded to 2048-bit encryption to help preserve internet security.

Ticket 2866

A rule or filter of AscenLink’s services became ineffective if a FQDN that contained capital letters was employed for its source or destination settings. Impacted services were Firewall, Persistent Routing, Auto Routing, Bandwidth Management and Connection Limit.

Ticket 2883

Disabling Bandwidth Management (both inbound and outbound) without deleting all the user-

defined classes and filters caused abnormal effects on the traffic passing through AscenLink and related statistics.

Ticket 2897

Open SSL employed in AscenLink are upgraded to version 1.0.1g to resolve the threat CVE-2014_0160 (Open SSL Heartbleed vulnerability).

Firmware Upgrade Procedures

Upgrading Information

- Note that only versions V7.1 B5598, V7.0 B5526, V6.5 B3856, V6.5 B4038, V6.5 B4081 and V6.5 B4175 are supported for upgrade to V7.1 B5745. For previous V7.0 (B5338 and B5246), please update to V7.0 B5526 first before updating to V7.1 B5745.

- System with demonstration licenses cannot be upgraded to R7.1. Please contact Fortinet at ascenlink@fortinet.com for information on updating these systems to NFR units.

- Because of US Government export restrictions on Tunnel Routing technology, all upgrades From R7.0 or R6.5 to R7.1 **MUST** be "ordered" via your distributor and Fortinet Order Management. Upgrades for in-warranty systems will be at no charge, as usual, but Fortinet must have end-user visibility and update its databases in order to support AscenLink. The SKU for ordering a Release 7.1 upgrade is **AL-UPGD-R71**. This is a one-time requirement. Future upgrades will be automatically available to in-warranty customers via the FortiCare website, without the need for additional ordering.

Upgrade procedure

Upgrade from V6.5 or V7.0 B5526

After ordering the Upgrade License SKU, Fortinet will supply the License Key via email. Start the upgrade procedure as follow:

- Always back up your system configurations before upgrading.

- Log on to AscenLink as Administrator and go to [System > Administrator] page.

- Click Update to start the upgrade procedure

    - Click Browse to select the path where the new firmware image is saved

    - Enter the Update Key you received from Fortinet

    - Select Upload.

- Be patient while firmware is being upgraded. During the upgrade, do not turn off the system, unplug the power or repeatedly click the Submit button.

- The message “Update succeeded” will appear after the upgrade is completed. Please reboot the system afterwards for the firmware to take effect.

Upgrade from V7.1

Always back up your system configurations before upgrading.

- Log on to AscenLink as Administrator and go to [System > Administration] page.

- Click Update to start the upgrade procedure.
    - Click Browse to select the path where the new firmware image is saved.
    - Select Upload.
- Be patient while firmware is being upgraded. During the upgrade, do not turn off the system, unplug the power or repeatedly click the Submit button.

The message “Update succeeded” will appear after the upgrade is completed. Please reboot the system afterwards for the firmware to take effect.

Getting Help

For customer support of Fortinet's AscenLink products shipped **before** January 20, 2014, please contact your local Fortinet AscenLink channel partner or ascenlink@fortinet.com.

For customer support of Fortinet's AscenLink products shipped **after** January 20, 2014, please contact your local Fortinet AscenLink channel partner or http://www.fortinet.com/support/contact_support.html.

Patches and updates are regularly released for Fortinet's AscenLink products. For access, please register at https://support.fortinet.com/ or contact ascenlink@fortinet.com.