AscenLink LinkOS V7.2.0 B6427

Release Notes

AscenLink Release Notes – LinkOS V7.2.0 B6427

December 12, 2014

Reversion 1

Table of Contents

Introduction

Summary

This LinkOS firmware V7.2.0 B6427 is the first build for Fortinet AscenLink V7.2. Several new features and updated features which are listed as follows are contained in this release:

- Support DNSSEC for Multihoming

- Support SRV records for Multihoming and Internal DNS

- Support multiple TXT records on one hostname

- Support IPv6/IPv4 dual stack for Bridge Mode: Multiple Static IP, Bridge Mode: One Static IP and Bridge Mode: PPPoE.

- Provide default IPv6 NAT rules for PPPoE V6 WAN links

- Support DSCP for Tunnel Routing

- Relocate the configuration panel of Threshold function

- Integrate the configuration pages of Inbound BM and Outbound BM into one page

- Support customer installation of SSL certifications for secure connections

- Add time zones for system date/time: United States and Canada

- Support SNMP counter64 for 32-bit LinkOS system and add new SNMP objects: ifHCInOctets and ifHCOutOctets

- Redefine version numbering for AscenLink LinkOS

- Support the specifying on default LAN port with IP address and netmask while resetting system to factory default via CLI

Moreover, several issues are resolved in this release including the fixes on Tunnel Routing and important updates for Bash and OpenSSL to fix security vulnerabilities. This document provides a list of resolved issues, upgrade procedures and support information of AscenLink LinkOS V7.2.0 B6427. Please review all sections of this document prior to upgrading your device.

Supported Models

LinkOS **V7.2.0 B6427** is the latest AscenLink firmware version released for AscenLink-700, AscenLink-5000 and AscenLink-6000.

Compatibility

LinkOS **V7.2.0 B6427** provides support and is compatible with all versions of

LinkReport. AscenLink-6000 requires LinkOS V6.1, or higher.

New Features in V7.2.0 B6427

Mantis ID 247090

AscenLink supports DNSSEC (Domain Name System Security Extensions) for Multihoming. One-key-pair (Key Sign Key, KSK) mechanism is employed here to sign and authenticate resource records for domains. RSASHA512 is the only algorithm used to generate the key pair, and the key size is 2048 bits. Note that DNSSEC is not supported for Multihoming's relay mode, and NSEC and NSEC3 records are not supported here.

Mantis ID 256243

AscenLink supports SRV records for Multihoming and Internal DNS.

Mantis ID 247165

IPv6/IPv4 dual stack is supported for deployments in WAN types: [Bridge Mode: One Static IP] and [Bridge Mode: Multiple Static IP]. Basic Subnet (in DMZ) and Static Routing Subnet (in DMZ) are supported for deployments of multiple IPv6 subnets. SLAAC and DHCPv6 are also supported for configuring IPv6 hosts.

Mantis ID 258214

PPPoE V6 is supported in AscenLink for the deployment of IPv6/IPv4 dual stack in WAN type: [Bridge Mode: PPPoE].

Mantis ID 247099

DSCP (Differentiated Services Code Point) is supported for Tunnel Routing. DSCP is a field in the IP headers for QoS purposes. The field becomes invisible for processing by the ISP if the transported IP packets are encapsulated in Tunnel Routing's GRE packets. Specifying the DSCP value in the GRE packets enables the QoS by DSCP for specific Tunnels (and thus all the traffic in those tunnels). Note that this is supported only for Tunnels established with static IP addresses. This will primarily be used for tunnels over MPLS networks.

Mantis ID 247687

Customers can install their own SSL certificate on AscenLink to perform a secure

connection (HTTPs) between AscenLink and a browser for Web UI. A CLI command was added for installation of SSL certificates.

Updated Features in V7.2.0 B6427

Mantis ID 246949

AscenLink's Multihoming and Internal DNS supports multiple TXT records on the same hostname.

Mantis ID 257674

AscenLink provides default IPv6 NAT rules for PPPoE WAN links. After a configuration of IPv6/IPv4 WAN link in Bridge Mode: PPPoE is applied, AscenLink generates a default NAT rule for IPv6 address translation.

Mantis ID 246008

The Threshold panel on the AscenLink's Web UI is removed from [Service / Auto Routing] and moved to [System / Network Settings / WAN Settings]. The inbound and outbound threshold values for each WAN link are used by both Auto Routing and Multihoming.

Mantis ID 247092

Configuration pages [Service/Inbound BM] and [Service/Outbound BM] on AscenLink's Web UI are integrated into one page [Service/Bandwidth Management] providing configuration panels for both inbound and outbound bandwidth management.

Mantis ID 247688

Two time zones: United States (Alaska, Aleutian, Arizona, Central, East-Indiana, Eastern, Hawaii, Indiana-Starke, Michigan, Mountain, Pacific, Samoa) and Canada (Atlantic, Central, East-Saskatchewan, Eastern, Mountain, Newfoundland, Pacific, Saskatchewan, Yukon) are added to AscenLink's Time/Date Setting.

Mantis ID 256358

AscenLink supports SNMP counter64 for 32-bit LinkOS system (AscenLink 700) in this release. Two SNMP objects are supported: ifHCInOctets and ifHCOutOctets.

Mantis ID 256359

AscenLink LinkOS's version numbering is redefined in this release. This version number is composed of three components and follows the format: [Major Version].[Minor Version].[Revision Number]. The version number is displayed in [System / Summary] from Web UI.

Mantis ID 254588

A function to specify an IP address and netmask to AscenLink's default LAN port is added to the CLI command "resetconfig". Administrators can assign an appropriate IP (rather than the default 192.168.0.1) to the LAN port while resetting AscenLink to factory default via the command, so that AscenLink's Web UI can be accessed directly via the LAN port from the current network after the system reboots. Note that resetting system with specification on LAN port disables all the WAN links by default.

Resolved Issues in V7.2.0 B6427

Mantis ID 253812

A mistake of identifying Remote Host ID caused function failure on Tunnel Routing if multiple TR groups are deployed over more than two units and are established with only one static IP.

Mantis ID 254240

The performance of Tunnel Routing transmission over multiple WAN links was worse than over only one WAN link.

Mantis ID 256702

Users failed to query Multihoming for A/AAAA records and CNAME records after restoring a configuration file which contains enabled settings of Multihoming via the Web UI page [System / Administrator].

Mantis ID 257676

The slave unit under deployment of Multihoming Backup did not function correctly.

Mantis ID 257898

IP Conflict Test in Diagnostic Tools made misjudgments of detecting IP conflict for the WAN links deployed in [Bridge Mode: Multiple Static IP] and with DHCP Range enabled for hosts in the DMZ.

Mantis ID 257899

An error message was displayed while executing IP Conflict Test in AscenLink's Diagnostic Tools via a Monitor account.

Mantis ID 257901

The Bash module employed in AscenLink was updated to the latest version which contains fixes for vulnerabilities related to Shellshock: CVE-2014-6271, CVE-2014-6273,

CVE-2014-6277, CVE-2014-7169, CVE-2014-7186 and CVE-2014-7187.

Mantis ID 257902

OpenSSL employed in AscenLink was updated to version 1.0.1j which contains fixes for vulnerabilities CVE-2014-3513, CVE-2014-3568 and CVE-2014-3567.

Mantis ID 258039

CLI command failed to enable SIP gateway module in AscenLink.

Mantis ID 258040

IPv6 rules for Virtual Server could not be disabled.

Mantis ID 258198

The DHCP function enabled for subnets deployed to a DMZ port was still detected after the associated WAN link was disabled (only happened on WAN links in Bridge Mode: One Static IP and Multiple Static IP). This mistake caused a failure to enable DHCP on the same DMZ port for other Bridge Mode WAN links; an error message "Found multiple DHCP in one port" was displayed.

Mantis ID 258209

DNAME record was not contained in the type list for Nslookup query via [System > Diagnostic Tools].

Mantis ID 258373

DHCPv6 lease information failed to display on page [Statistics > DHCP Lease Information].

Mantis ID 258374

Hosts using DHCPv6 failed to get DNS information.

Mantis ID 258827

An abnormal system reboot occurred intermittently by a particular Tunnel Routing application.

Mantis ID 263095

The load balancing algorithms "By Upstream Traffic" failed in Tunnel Routing.

Firmware Upgrade Procedures

Upgrading Information

- Note that only versions later than V6.5 B4175 (V6.5 B4175 is included) are supported for upgrade to V7.2.0 B6427. For V7.0 (B5338 and B5246), please update to V7.0 B5526 **first** before updating to V7.2.0 B6427.

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

- AscenLink's firmware image and upgrade license key are available from FortiCare at https://support.fortinet.com once customer's AscenLink Serial Number is registered. However, because of US Government export restrictions on Tunnel Routing technology, all registration to FortiCare for customers using V7.0 or V6.5 **MUST** be "ordered" via your distributor and Fortinet Order Management. Registrations 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 Registration is **AL-REGI-FC**. 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, V7.0 B5526 or V7.1

After registering to FortiCare, the License Key can be generated inside FortiCare (for in-warranty Serial Number).

Start the upgrade procedure as follow:

- Always back up your system configurations and store in a save place before upgrading (and downgrade).

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

- Click Update to start the upgrade procedure
  - o Click Browse to select the path where the new firmware image is saved
  - o Enter the Update Key you received from Fortinet
  - o 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, please contact your local Fortinet AscenLink channel partner or http://www.fortinet.com/support/contact_support.html. AscenLink system must be registered to FortiCare to receive support.

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.