3.2 Release Notes

Release Features

This Unbox release 3.2 includes a diagnostics view, Multi-Factor Authentication, SFP Port enablement, recovery mode alternative, an Inventory View, Downloadable Audit Logs, the ability to manage the Uplevel NAS from an AD, and more. These features help MSP's manage customers, troubleshoot issues, and increases the size of business MSP's can manage with Uplevel. This creates more control and visibility in the dashboard and broadens the reach and value that MSP's can provide to their small business customers.

Diagnostics View

The new diagnostics view in the dashboard allows partners to directly troubleshoot ISP bandwidth and Wifi interference issues. This view allows partners the ability to directly run speed and interference tests on the equipment directly from the internet links or access points. This means partners will have a direct view into the customers network and their issues without having to be onsite. These tests include:

Short Bandwidth Test: Measures the upload and download speeds directly from the WAN port of the gateway for one minute and presents the results in a graphical form on the dashboard or the option to download the raw data to a csv.

Long Bandwidth Test: Measures the upload and download speeds directly from the WAN port of the gateway for either 12 hours, 24 hours, 2 days, 3 days, 5 days, or 1 week at intervals of 5 minutes, 15 minutes, 1 hour, or 3 hours. The results will be presented graphically on the dashboard or the raw data can be downloaded to a csv.

Wi-Fi Scans: Scans from all access points in the area that are broadcasting signals and which channels they are broadcasting on. These scans will occur directly from all access points connected to the gateway in question and include the channel they are heard on and the signal strength they are heard at. Devices on the same or overlapping channels or at a very high signal strength may be causing interference issues with the Uplevel access points.

Top Talkers test: Measures the top communicators on the Primary internet connection, secondary internet connection, or any of the created VLAN's. This will capture the next 10,000 packets sent and received and display the top sources and/or destinations. Depending on the amount of traffic flowing capturing 10,000 packets can vary greatly in the amount of time it takes to complete. The more traffic on the network the faster the 10,000 packets will be captured.

The Devices view now has the addition of an “alert if offline” checkbox. This will generate alerts when specific devices go on or offline to the email addresses specified in the “Notifications” tab of the account settings. This is on a per account level and will only be true for the account that is currently logged in. Now MSP’s can be alerted when critical devices go offline on the network and when there may be a critical issue on the LAN.

Multi-Factor Authentication

Now you can enable Multi-Factor Authentication using any authenticator of your choice. The initial configuration of this will be done out of the Uplevel dashboard Settings tab. Once MFA is enabled you will be logged out of the dashboard and be prompted to log back in where you will see a QR code. This code can be used with your favorite MFA authenticator including, but not limited to, Google Authenticator, Authy, Microsoft Authenticator, and Duo Mobile. The recovery code should also be noted, as this configuration screen is the only place this emergency code will appear.

Once MFA has been configured all subsequent logins will prompt the user to enter their MFA code which can always be found in their chosen MFA authenticator. Once an account has been associated to an authenticator this authenticator must be used every time moving forward or the recovery code. If the account is ever deleted out of the authenticator this does not disable MFA from the dashboard. This could result in a user being unable to login.

Once the recovery code is entered the user will be prompted to re-scan a QR code and generate a new recovery code.

To disable MFA you can at any point log into the dashboard and again, under settings, turn MFA off.

SFP Ports as Uplink on Switches

The SFP ports on both 8 and 22 Port switches have been enabled and can now be used as an alternative uplink port. Now, you are able to use the SFP ports as fiber uplink ports when connecting switches together. This is commonly seen in offices that have fiber runs connecting different buildings or different offices together. Only one uplink port can be used at a time. If more than one uplink port is attached a loop will occur. An alert in the dashboard will notify the user of this issue, however loops should attempt to be avoided to reduce further issues on the network.

Ability to abort recovery mode during boot up

A gateway in recovery mode can now be pulled out of recovery mode using the reset button during the boot up. Recovery mode occurs when the gateway fails to complete a bootup sequence. If a gateway is in recovery mode the “C” light on the back of the gateway will light up green. In order to get the gateway out of recovery mode and the LAN to be operational the gateway requires an internet connection. To avoid the gateway requiring an internet connection to resume LAN communications users can now press and hold the reset button for 60 seconds while the gateway is powering on. This will bypass the recovery image and boot up with the full firmware image available. As the gateway completes its 60 second boot up the status light will turn on and the "C" light will turn off. This indicates the reset button can be released, recovery mode is no longer present, and the gateway is operational on the LAN with its previous firmware image.

Inventory View

In the Settings option of the dashboard users will now be able to view all hardware currently associated with their dashboard. This includes the customer it is connected to, the site it is located at, and the factory name of the Gateway, AP, or Switch. This will help MSP's to better manage the equipment at each customer and correlate this to their monthly bills.

Downloadable Audit Logs for HIPAA compliance

Now MSP's can directly download HIPAA compliance Audit Logs directly from the dashboard. In the site settings option of any customer there is now a "Security Audit Logs" button which will download a .gz file containing a "VCIOAudit.log" this is a file showing all of the dashboard activity for all customers. There will also be a "customers" folder created which will contain a subsequent folder for each customer containing a "backendLogs.tar.gz" file containing several management audit logs for each customer.

Using the Uplevel NAS with an onsite Active Directory (AD) Server

An Active Directory server can now be used in combination with the Uplevel NAS. For customers who have existing Active Directory or Domain Controller servers they can now have this domain controller manage the permissions of the integrated file server on the Uplevel gateway. This is done by mapping the Samba3 drive to the Domain Controller (DC) and creating a VHD image for emulating the native NTFS file system. This allows customers the ability to use their existing domain policies and infrastructure along to manage the permissions of the Uplevel NAS along with the integrated local and cloud backup replication.

Other Bug fixes

Other bug fixes that have been included in this release include additional backend data collection, adjustment to the data and presentation of monthly reports, reduction of the health checks frequency, dynamic client count ability, warning text for paid for features, confirmation boxes when making configuration changes across multiple sites, and a change in the ISP out and unstable limits.