

Uplevel Systems Service Agreement

This Service Agreement governs the deployment, configuration, maintenance and use of equipment and services provided by Uplevel Systems, Inc (“Uplevel”) to _____ (“MSP”), in connection with a Business Associate Agreement (“BAA”) to be executed and set in place between Uplevel and MSP.

SERVICES COVERED

The following Uplevel services are covered under this Service Agreement:

Category	Remarks
Firewall	The Firewall functionality contained within the Uplevel UG-101 and UG-101A gateways may be used
Ethernet	The Ethernet LAN switching functionality contained within the Uplevel UG-101/UG-101A and the Uplevel ULS-101 and ULS-102/ULS-102A may be used
Wireless	The Wi-Fi® functionality contained within the Uplevel UAP-101/UAP-101A may be used
VPN	The Site-to-Site and Remote Access VPN functionality implemented by the Uplevel UG-101/UG-101A gateways may be used
Dual-WAN	The Dual-WAN functionality supported by the Uplevel UG-101/UG-101A gateways may be used
DHCP/DNS	The DHCP and DNS functionality supported by the Uplevel UG-101/UG-101A gateways may be used
Configuration & Monitoring	The configuration and monitoring dashboard provided by Uplevel to set up, manage, and monitor the Uplevel system may be used

Any Uplevel service not listed in the above table is not covered under this Service Agreement, and must not be enabled or used. Use of a service that is not covered under this Service Agreement shall result in MSP being regarded as not adhering to the terms of this Service Agreement. In particular, the Storage and Backup functionality of the Uplevel system is specifically excluded from this Service Agreement.

SERVICE USAGE LIMITATIONS

The following requirements and limitations are placed on the installation of the Uplevel system into the premises of a Covered Entity (as defined by 45 C.F.R. § 160.103 of the Health Information Portability and Accountability Act of 1996), as well as the configuration of the Uplevel services that may be used and covered under this Service Agreement.

1. Ethernet switches that are not provided by Uplevel shall not be used to connect workstations or devices to a LAN containing a UG-101/UG-101A gateway, or to connect a UAP-101/UAP-101A Access Point.

2. Each workstation/device that is connected via an Ethernet connection shall be connected to a separate port of an Uplevel UG-101/UG-101A gateway or ULS-101/ULS-102/ULS-102A switch.
3. A Boss group must be created, and an SSID must be assigned to the group. This SSID must be available to the administrator for emergency access.
4. If the Remote Access VPN service is used, then the Boss group must be provided with an administrator account for remote access VPN.
5. The password be assigned for any Wi-Fi SSID shall have a minimum of 8 characters with at least 2 special characters plus a mixture of uppercase and lowercase letters and numbers.
6. If a Guest SSID is used, it must have a password assigned, and the password must follow the rules above.
7. The IDS/IPS service must be subscribed to and enabled on the Uplevel system.
8. Neither the Storage nor the Backup services can be enabled.
9. The Firewall service within the UG-101/UG-101A must be used, and ports may not be opened on the Firewall to devices or systems having known vulnerabilities.
10. The Uplevel system must be running Release 3.1 or higher