

Uplivra is in beta and online purchasing is paused. [Apply to test it](#): testers get a license on request and 10% off when purchasing opens.

INSTALL GUIDE · ADMINISTRATORS AND BUYERS

Supported devices, protocols and connectors

Which makers, protocols and connectors Uplivra supports, and which are tested on real equipment.

Uplivra Technologies LLC · Guide for Uplivra 26.10 · Updated 4 October 2026 · Latest version:
<https://uplivra.com/guides/support-matrix.html>

- "Lab-tested" means checked against real equipment or a real service account.
- Unless a row says so, **support is implemented and tested against simulators or mocks, not yet on real equipment**.

1. Devices and makers

Key:

- **Y**: vendor-specific support.
- **G**: generic (standard MIBs, or guided steps without vendor code).
- **—**: none.

What each column covers:

- **Firmware**: Uplivra copies the image over SFTP/SCP and shows the maker's install commands. It never installs or reboots the device itself.

Maker / OS	SNMP	Config backup	Firmware	Vulnerability matching	Port profiles	AAA templ
Cisco IOS / IOS-XE	Y	Y + restore	Y	Y	IOS-XE	TACACS+ RADIUS 802.1X

Maker / OS	SNMP	Config backup	Firmware	Vulnerability matching	Port profiles	AAA templ
Cisco NX-OS	Y	Y	Y	Y	—	TACAC
Cisco ASA	G	Y	Y	Y	—	—
Cisco IOS XR	G	—	version only	Y	—	—
Juniper Junos	G	Y + restore	Y	Y	EX	TACAC 802.1X
Arista EOS	G	Y + restore	—	—	—	TACAC
Aruba AOS-CX	G	Y	Y	Y	Y	TACAC 802.1X
ArubaOS-Switch / ProCurve	Y	Y	Y	Y	—	TACAC
ArubaOS controllers	G	—	version only	Y	—	—
Fortinet FortiOS	Y	Y	Y	Y	—	TACAC FortiS 802.1X
Palo Alto PAN-OS	Y (version)	Y	Y	Y	—	TACAC
MikroTik RouterOS	Y	Y	Y	Y	—	RADIUS 802.1X

Maker / OS	SNMP	Config backup	Firmware	Vulnerability matching	Port profiles	AAA templ
Ubiquiti EdgeOS / VyOS	G	Y	version only	EdgeOS only	—	—
Ubiquiti UniFi	G	Y	version only	—	—	—
SonicWall SonicOS	G	Y	version only	Y	—	—
pfSense / OPNsense	G	Y	version only	Y	—	—
Ruckus / Brocade FastIron	G	custom command	version only	Y	—	TACACS
Extreme EXOS	G	—	version only	Y	—	—
Dell OS10	G	—	version only	—	—	TACACS
Huawei VRP	G	—	—	—	—	TACACS
VMware ESXi	G	—	version only	Y	—	—

Maker / OS	SNMP	Config backup	Firmware	Vulnerability matching	Port profiles	AAA templ
Other SNMP devices (Meraki, Netgear, TP-Link, APC and Eaton UPS)	G (APC UPS: Y)	—	version only	—	—	—
Windows servers	WinRM/WMI; PowerShell over SSH	—	version only	—	—	—
Linux servers	SSH (/proc, df)	key files	version only	—	—	pam-r

Not matched for vulnerabilities: Windows, Linux, Arista EOS, VyOS.

2. Protocols

Protocol	Direction and port	Notes
ICMP	out	Availability, latency, loss; traceroute
SNMP v1, v2c, v3	out UDP 161	v3 auth: MD5, SHA, SHA-224/256/384/512. Privacy: DES, AES-128/192/256.
SNMP traps and informs	in UDP 162	Only from a known community or v3 user

Protocol	Direction and port	Notes
Syslog	in UDP and TCP 514 (port per site)	RFC 3164 and 5424. No TLS on the way in.
Syslog forwarding	out UDP, TCP or TLS (514/6514)	TLS 1.2 or later
NetFlow v5/v9, IPFIX	in UDP 2055	
sFlow v5	in UDP 6343	
SSH	out TCP 22	Config backup, config restore, SSH checks, firmware copy and the browser terminal all check the device's SSH host key. The first key seen is remembered; if it changes, Uplivra stops before signing in until an administrator accepts the new key.
SFTP/SCP (firmware)	out 22; optional read-only pull service on 2022	TFTP, FTP, HTTP and Telnet are refused
WinRM	out TCP 5985/5986	NTLM/Negotiate. HTTPS uses TLS 1.2 or later, with an optional pin. No Kerberos.
HTTP/S, DNS, NTP and certificate checks	out	Certificate checks support STARTTLS and report TLS 1.0/1.1
DHCP	rogue-server check out UDP 67; optional DHCP server in UDP 67	

Protocol	Direction and port	Notes
TACACS+	in TCP 49	Unencrypted packets rejected
RADIUS	in UDP 1812/1813; CoA out UDP 3799	PAP, CHAP, MAB, EAP
RadSec	in TCP 2083 (off by default)	Mutual TLS, 1.2 or later
802.1X	through RADIUS	EAP-TLS only (certificates). PEAP and EAP-TTLS are not supported.
Access Control node pairs	TCP between nodes	Mutual TLS 1.3
LDAP / LDAPS	out 636, or 389 with StartTLS	Plain LDAP refused unless allowed explicitly
OIDC single sign-on	out HTTPS	Authorization code with PKCE
SAML	—	Not supported
SMTP (alerts)	out 587/465/25	STARTTLS or TLS; username and password (no OAuth2)
IMAP (Service Desk mail-in)	out 993/143	Username and password (no OAuth2)
Webhooks	out HTTPS	HMAC-SHA256 signatures
MCP (connect your own AI)	in HTTPS 443	Read only; one token per connection, limited to what an administrator ticked

Protocol	Direction and port	Notes
Collector to server	out HTTPS 443	TLS 1.3 with X25519 + ML-KEM-768 by default, pinned certificate or CA
Web interface and API	in HTTPS 443	TLS 1.2 or later by default ("compatible"); TLS 1.3 only when set to "modern"
Collector site tests	UDP 4717	HMAC-signed; open only during a test
Shared site address	UDP 4718; gratuitous ARP	HMAC-signed heartbeats
ACME certificates	out 443	Let's Encrypt; Cloudflare DNS-01
Licensing, updates, vulnerability feed	out 443	licensing.uplivra.com; NVD 2.0 and CISA KEV

3. Connectors

System	How	Access	Tested against
ServiceNow	Table and Service Catalog APIs; basic auth	Creates incidents and changes; reads approvals	mock
Jira Service Management	Service desk REST API; email + API token	Write, read approval	mock

System	How	Access	Tested against
Freshservice	API v2; API key	Write, read	mock
Zendesk	API v2; email + token	Write, read	mock
Generic ticket webhook	JSON POST with HMAC; inbound decision callback	Write	mock
ConnectWise, HaloPSA, Autotask	—	Not built	—
AWS	STS (role + external ID), EC2, RDS, ELBv2, Lambda, CloudWatch, Health; Uplivra's own SigV4 signing	Read only	fake
Azure	ARM, Resource Graph, Monitor metrics, Resource Health; service principal	Read only	fake
Microsoft 365 service health	Microsoft Graph service announcements	Read only	fake
LDAP / Active Directory	LDAP v3 (own client), simple bind	Read	fake server
OIDC (Entra ID, Google, Okta and others)	Discovery, authorization code, PKCE	Sign-in only	fake
Entra ID / Okta directory lookups	—	Not built (planned)	—
HashiCorp Vault	KV v2; token or AppRole, optional client certificate	Read	mock

System	How	Access	Tested against
CyberArk CCP	AIMWebService; AppID + client certificate	Read	mock
Log forwarding	Syslog UDP/TCP/TLS; HTTPS JSON lines; Splunk HEC; S3 (with Object Lock); Azure Blob	Write	mock
Email	SMTP	Write	fake SMTP server
Slack, Microsoft Teams	Incoming webhooks (Teams Adaptive Card 1.4)	Write	delivery not tested
PagerDuty	—	Not built. Reach it through a generic webhook.	—
SMS	—	Not built (low priority)	—
Local AI model	OpenAI-style chat API, private network addresses only	Read	mock
ISE / ClearPass / NPS import	CSV upload	Import	no test. NPS's own export is XML, so it needs converting first.
Windows DHCP, ISC Kea	PowerShell over WinRM; Kea Control Agent	Read	mock

System	How	Access	Tested against
Stripe (portal only)	Customers, checkout, subscriptions; signed webhooks	Write	mock

No connector has been tested against a live third-party service yet. The only optional real-host tests are WinRM interop, Let's Encrypt Pebble and the PostgreSQL test database.