

3.5 VPN Access Procedure

Effective Date: October 27, 2025

Revised Date: October 27, 2025

1. Purpose

This document establishes a standardized guideline for remote access to Arkansas State University - Jonesboro (A-State) Virtual Private Network (VPN).

2. Scope

These guidelines apply to all employees, students and all authorized third parties (contractors or consultants) that will utilize VPN to access the A-State Network.

3. Definitions

- **VPN** – A Virtual Private Network that establishes a secure connection between two trusted locations (your computer and the A-State network) via an insecure, public network (the Internet).
 - **Geo Blocked** – Restricting access to the network by the user's geographic location.
-

4. Guidelines

VPN access allows users unrestricted access to the Arkansas State University computer network from locations external to the Jonesboro campus. This unrestricted access to the network could increase the University's exposure to viruses, malware, and could allow hackers using compromised accounts greater access to the A-State network. These guidelines should be followed to lessen the security risk of the campus at large.

- Standard VPN access will be approved by the Security Division if Chair/Dean/Dept. Head approval is not available. If Chair/Dean/Dept. Head approval is available, then VPN access will be granted without further approval from ITS.
 - **Service:** [A-State VPN Access Request](#)
- VPN access is geo-blocked to the United States and Canada.
- International VPN access is permitted on a per-user and per-country basis. This requires a separate set of approvals as well as standard VPN access. This access must be approved by the Security Division and the Networking Division.
 - **Service:** [International VPN Access Request](#)

- Devices failing security scans may be denied VPN access.
 - Access may be suspended/terminated by ITS at any time if access could cause a security issue.
 - VPN access is logged, and the logs will be retained for one year.
 - Logging includes:
 - Connection/disconnection times
 - IP address received from DHCP
 - Connecting IP address
 - IP address(es) accessed
 - Username that opened the connection
 - ITS may require devices connecting via VPN to be scanned for up-to-date OS and software patches and/or versions, current antivirus software, or other security related issues.
 - 3rd party vendors may apply for VPN access but require a sponsored A-State user account.
-

5. Approved VPN Clients

To ensure secure and supported remote connectivity to the A-State network, only University-approved Virtual Private Network (VPN) client software may be used to establish VPN connections. Use of unsupported or unauthorized VPN clients is prohibited.

The following VPN clients are approved for use on A-State managed and personal devices when connecting to the University network:

- **GlobalProtect VPN (Palo Alto)** - This client is the primary supported VPN solution for faculty, staff, and authorized contractors requiring secure access to A-State resources. Instructions for obtaining, installing, configuring, and using GlobalProtect are maintained by IT Services and available here: [How to Download VPN](#)
- **FortiClient VPN (Fortinet)** - The FortiClient VPN client is approved for use where GlobalProtect is unavailable or not appropriate (primarily for mobile VPN use). FortiClient may be required for access to specific systems, departments, or research environments that depend on Fortinet VPN infrastructure.
- **Extreme ZTNA (Extreme Networks) [LIMITED USE WITH ITS APPROVAL]** - A-State is implementing Extreme ZTNA to provide identity-based, "least-privilege" access to specific University applications. This solution may be required for access to certain high-security systems or cloud-based resources. During the current implementation phase, its use is restricted to authorized testing groups and specific departmental workflows as directed by IT Services.

Requirements & Restrictions

Approved VPN clients must be obtained directly from official University distribution points or the respective vendor's official repositories. **The above VPN clients are the only approved platforms to be used to connect to the A-State network unless otherwise authorized by Information Technology Services.**

VPN clients must be kept up to date with the latest security patches and versions supported by A-State Information Technology Services.

Use of third-party VPN technologies/clients not explicitly approved in this section is not permitted and may result in loss of VPN privileges and further institutional sanctions.

6. Standards Review

This document will be reviewed and reaffirmed annually, or upon significant changes to university IT governance, systems, or regulatory requirements.

Effective Date: October 27, 2025

Next Review Date: October 27, 2026

Version: 1.1

Revision #7

Created 2025-10-31 02:07:55 UTC by Christopher Boothman

Updated 2026-07-28 19:17:33 UTC by Jacob Weaver