

[DEPRECATED] Building a Zero Trust Campus: Authentication

Shiv> Zero Trus Campus has three sections, This section falls under Zero Trust Access.

Authentication Methods in the Nile Access Service: Building a Zero Trust Campus

The Nile Access Service is built on the principles of the "Zero Trust Campus," ensuring that no user or device is implicitly trusted. By implementing strong authentication methods and granular access controls, the Nile Access Service helps organizations secure their network resources and protect against unauthorized access.

The following authentication methods are supported within the Nile Access Service, each playing a crucial role in establishing a Zero Trust Campus:

1. Wired and Wireless 802.1X
2. Single Sign-On (SSO)
3. MAC Authentication Bypass (MAB)

Let's review each of these in more detail.

Wired and Wireless 802.1X: Strong Authentication for Zero Trust

802.1X is an IEEE standard for port-based network access control, providing strong authentication and encryption for both wired and wireless connections. By implementing 802.1X, organizations can ensure that only authenticated users and devices can access network resources, aligning with the principles of the Zero Trust Campus.

Nile's implementation of 802.1X offers:

- Support for various EAP methods (PEAP, EAP-TLS, EAP-TTLS) to accommodate different security requirements
 - **Shiv> We are transparent to EAP methods as we pass through the packets to a RADIUS server. So the EAP method support is more specific to the RADIUS sever.**
- Integration with existing RADIUS infrastructure for centralized authentication and authorization

- Granular access control based on user identity and device posture [Shiv> We dont do device posture. However we plan to integrate with Crowdstrike in the futre to offer device posture based access](#)
- Centralized policy management through the Nile Customer Portal

[Learn more](#) about configuring 802.1X in the Nile Access Service to strengthen your Zero Trust Campus.

Single Sign-On (SSO): Streamlining Zero Trust Access

Single Sign-On allows users to access multiple applications with a single set of credentials, streamlining the user experience while maintaining the principles of the Zero Trust Campus. By integrating SSO with the Nile Access Service, organizations can enforce consistent authentication and authorization policies across their network resources.

Nile's SSO integration provides:

- Support for popular SSO protocols (SAML, OAuth, OpenID Connect) to ensure compatibility with leading identity providers [Shiv> I know we def support SAML not sure of thers. We do support SCIM protocol now.](#)
- Granular access control based on user attributes and group membership [Shiv> We are not doing this today but are working on it as part of microsegmentaiton phase 2 scheduled for fall 2024](#)
- Centralized SSO configuration through the Nile Customer Portal

[Discover how SSO](#) can be seamlessly integrated into the Nile Access Service to enhance your Zero Trust Campus.

MAC Authentication Bypass (MAB): Securing Devices in a Zero Trust Campus

MAC Authentication Bypass is an authentication method that grants network access based on a device's MAC address. While MAB is useful for devices that don't support 802.1X, it's essential to implement additional security measures to maintain the integrity of the Zero Trust Campus.

Nile's MAB implementation includes:

- Quarantine all new devices by default
- Centralized MAB configuration through the Nile Customer Portal
- Create custom rules based on MAC OUI [Shiv> We support the following match criterias](#)
 - Exact MAC address
 - Fingerprint
 - MAC OUI
- [Optionally](#) Integration with external MAC address databases (e.g Aruba ClearPass and Cisco ISE)for granular access control

Explore the configuration and best practices for MAB in the Nile Access Service to secure devices within your Zero Trust Campus.

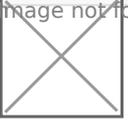
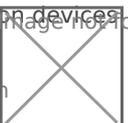
By leveraging these authentication methods and following best practices, organizations can build a robust Zero Trust Campus with the Nile Access Service, ensuring secure access to network resources and protecting against unauthorized access.

Authentication Comparison

image not found or type unknown



Shiv> I did not follow why there is an  under considerations. That symbol means something is not good. Maybe we dont need that column?

Authentication Method	Description	Zero Trust Campus Benefits	Considerations
 <p>Wired and Wireless 802.1X</p>	<p>IEEE standard for port-based network access control</p> <ul style="list-style-type: none"> - Supports various EAP methods (PEAP, EAP-TLS, EAP-TTLS) - Provides strong authentication and encryption 	 Ensures only authenticated users and devices access network resources  Enables granular access control based on user identity and device posture  Integrates with existing RADIUS infrastructure for centralized management	 Requires careful planning and configuration  Necessitates compatible client software on devices  May introduce additional authentication latency

Authentication Method	Description	Zero Trust Campus Benefits	Considerations
 <p>Single Sign-On (SSO)</p>	<p>Allows users to access multiple applications with a single set of credentials</p> <ul style="list-style-type: none"> - Supports popular SSO protocols (SAML, OAuth, OpenID Connect) - Reduces password fatigue and improves user experience 	<p>Enforces consistent authentication and authorization policies</p> <p>Provides granular access control based on user attributes and group membership</p> <p>Streamlines user experience while maintaining Zero Trust principles</p>	<p>Requires integration with identity providers (IdPs)</p> <p>IdP becomes a critical component, necessitating high availability</p> <p>May require additional attribute mapping and user provisioning</p>
 <p>MAC Authentication Bypass (MAB)</p>	<p>Authenticates devices based on their MAC address</p> <ul style="list-style-type: none"> - Useful for devices that don't support 802.1X (printers, IoT devices) 	<p>Provides network access for devices that can't support 802.1X</p> <p>Serves as a fallback method to ensure maximum device coverage</p> <p>Centralized configuration through the Nile Customer Portal</p>	<p>Less secure than 802.1X, as it relies on MAC addresses</p> <p>Vulnerable to MAC spoofing attacks</p> <p>Requires additional measures to maintain Zero Trust principles</p>

Revision #13

Created 13 March 2024 19:17:31 by JR

Updated 28 March 2024 21:53:20 by JR