

Zero Trust Access: Single Sign-On (SSO)

Integrating SSO for a Zero Trust Campus

The Nile Access Service is built on the principles of a "Zero Trust Campus," ensuring that no user or device is implicitly trusted. As part of this security model, the Nile Access Service supports the integration of Single Sign-On (SSO) to streamline user authentication and authorization across multiple applications and resources.

[diagram required]

By implementing SSO, organizations can leverage their existing identity providers (IdPs) to centrally manage user credentials and enforce consistent access policies. This approach aligns with the Zero Trust principle of verifying user identity or device before granting access, reducing the risk of unauthorized access and enhancing overall security.

Why Use SSO with the Nile Access Service?

The Nile Access Service's support for SSO integration offers several key benefits:

1. **Improved User Experience:** SSO allows users to access multiple applications and resources with a single set of credentials, reducing password fatigue and improving productivity.
2. **Centralized User Management:** By integrating with existing IdPs, the Nile Access Service enables organizations to manage user identities and access privileges from a central location, simplifying user provisioning and deprovisioning.

3. **Consistent Policy Enforcement:** SSO integration ensures that access policies defined within the IdP are consistently applied across the Nile Access Service, ensuring a unified security posture.
4. **Enhanced Security:** The Nile Access Service's SSO integration, combined with its Zero Trust principles, helps mitigate the risks of password-based authentication by verifying user identity and device posture before granting access.

Integrating Identity Providers with Nile Access Service

The Nile Access Service supports integration with various identity providers (IdPs) using the SAML protocol. This allows users to authenticate to the Nile platform using their existing corporate credentials, providing a seamless single sign-on experience.

The general steps to integrate an IdP with the Nile Access Service are as follows:

1. Configure the IdP Application:

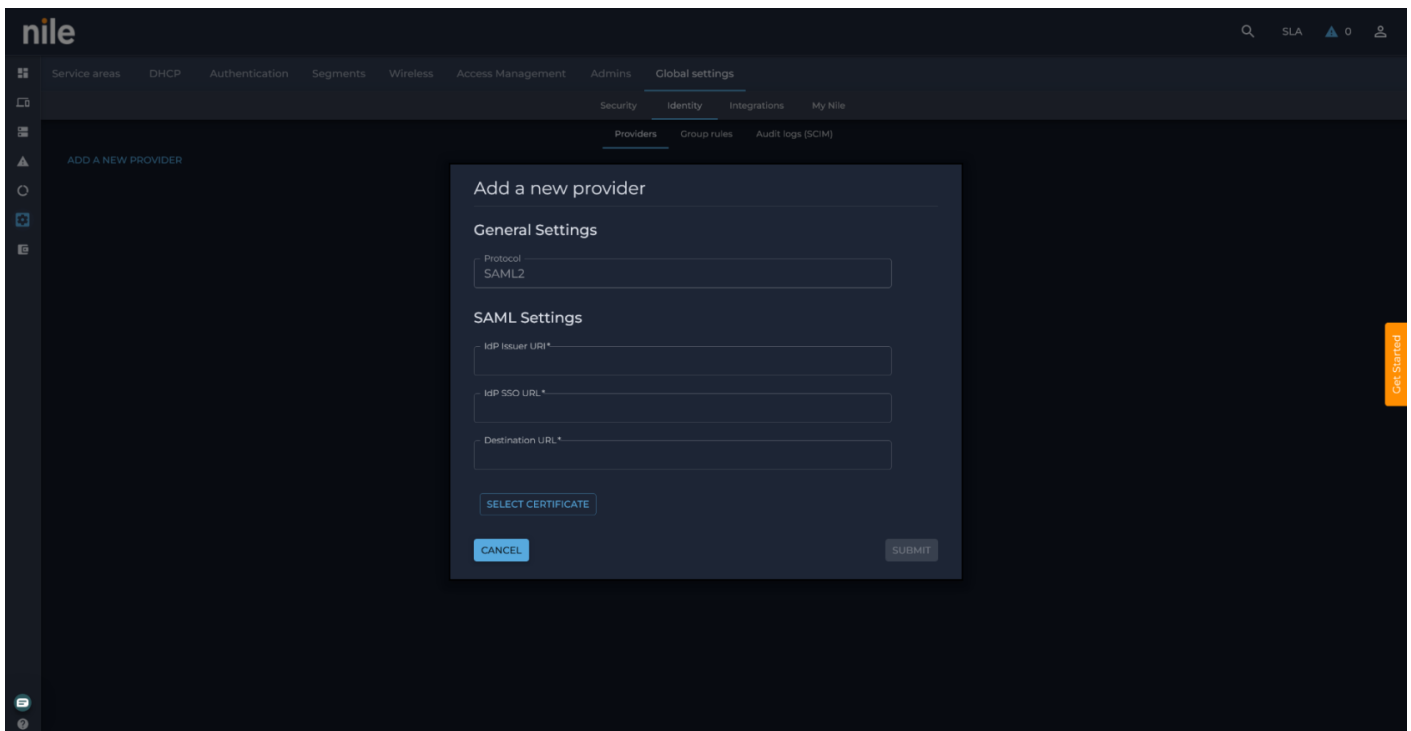
- Log in to the administration portal of your IdP (e.g., Azure AD, Google Workspace, Okta, OneLogin).
- Create a new SAML application or custom integration for the Nile Access Service.
- Provide the necessary configuration details, such as the Assertion Consumer Service (ACS) URL and Entity ID.
- Download the IdP's SAML signing certificate.

2. Configure the Nile Identity Provider:

- Log in to the Nile Customer Portal as an administrator.
- Navigate to the "Settings" > "Global Settings" > "Identity" page.
 - Click "Add a New Provider" and fill out the form with the details from the IdP configuration:
 - IdP Issuer URI
 - IdP SSO URL
 - Destination URL
 - Upload the IdP's SAML signing certificate.
 - Configure any necessary group mapping rules to assign users to segments based on IdP group membership.

3. Test the SSO Integration:

- Verify that users can successfully log in to the Nile Access Service using their IdP credentials.
- Ensure that the user is being placed in the correct segment based on your configured policies.



Refer to the provider-specific integration guides for detailed steps on configuring Azure AD, Google Workspace, Okta, and OneLogin as identity providers for the Nile Access Service.

Links to individual config guides will be added

Unique Passphrase (UPSK) + SSO

Unique Passphrase (UPSK) is a feature of the Nile Access Service that enhances the security of traditional pre-shared key (PSK) wireless networks. Unlike a typical PSK network, where a single key is shared among all devices, UPSK assigns a unique key to every authenticated user.

To use UPSK, follow these steps:

1. **Create a UPSK-enabled SSID:**

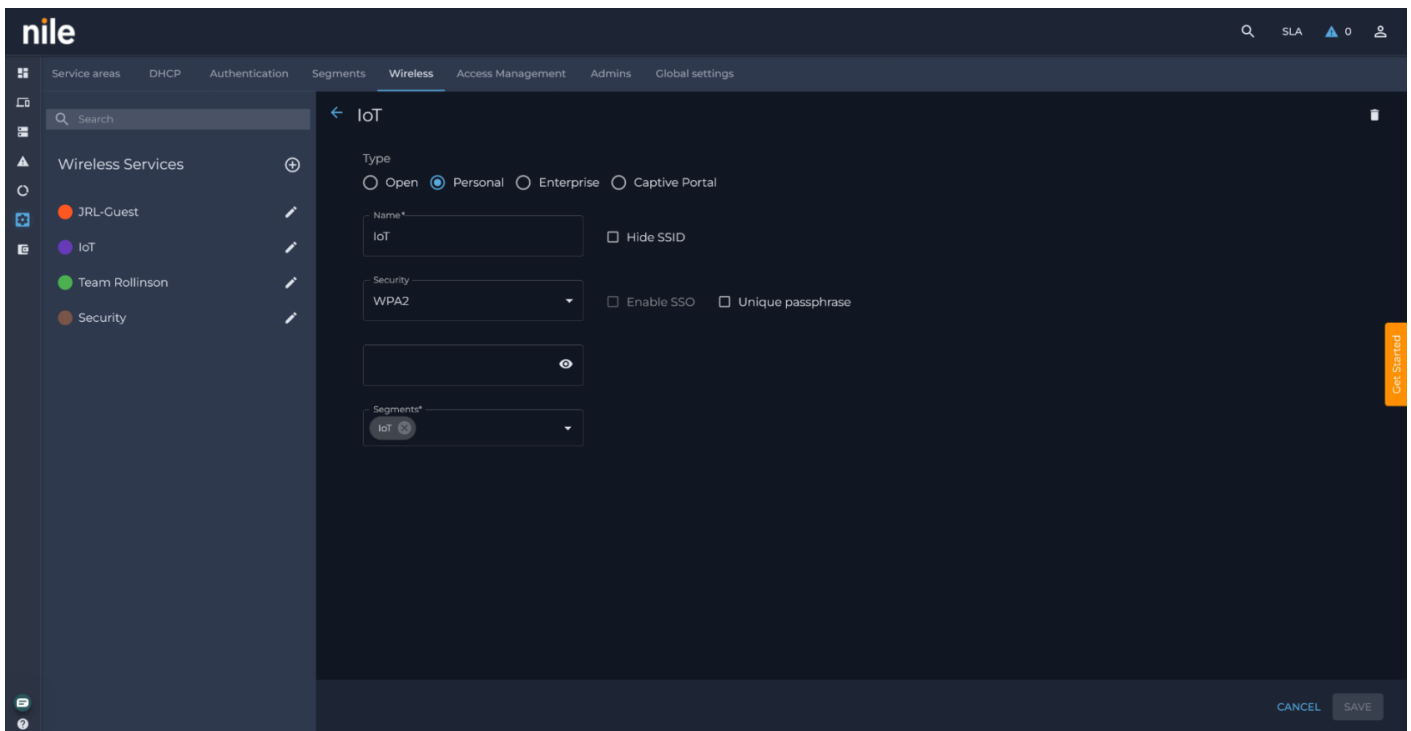
- In the Nile Customer Portal, navigate to "Settings" > "Wireless".
- Select the "Personal" SSID type and enable the "Enable SSO" option.
- Enter a pre-shared key and select the appropriate network segment.

2. **Register Devices:**

- Provide users with a unique registration link, which can be obtained from the Nile Customer Portal or the my.nilesecure.com website.
- Users will be redirected to an SSO login page to authenticate.
- After successful login, users can generate a unique passphrase for their device.

3. **Connect Devices to the UPSK SSID:**

- Users can connect their devices to the UPSK-enabled SSID using the generated passphrase.
- Alternatively, users can scan a QR code from the self-registration page to automatically connect their device.



The UPSK feature ensures that each user and device has a unique set of credentials, enhancing the overall security of the wireless network and aligning with the Nile Access Service's zero-trust principles.

For more information on configuring identity provider integration or the Unique Passphrase feature, refer to the provider-specific guides and the Nile Access Service documentation.

Read Next

[MAd Authentication Bypass](#)

Revision #7

Created 20 March 2024 18:21:32 by JR

Updated 28 March 2024 21:53:20 by JR