SOLUTION NOTE

NIOS 8.4: STREAMLINING NETWORK SERVICE ADMINISTRATION WITH SINGLE SIGN-ON INTEGRATION

OVERVIEW

As its name implies, single sign-on (SSO) enables secure, authenticated access to many systems and resources using a single login/password facility.

Through SSO, individuals gain access to different applications without the burden of multiple logins, multiple user IDs, password proliferation and the associated overhead.

The widespread use of web-based applications drove the definition and acceptance of the Security Assertion Markup Language (SAML), the language protocol that enables access through SSO. Optimized for the web, SAML is an XML framework for securely exchanging authentication and identity information. It is managed by the Organization for the Advancement of Structured Information Standards (OASIS).

SAMLarticularly SAML 2.0, increases security by reducing login transaction volume, lowers barriers to resource use and cuts administrative overhead. Many vendors now offer SAML-based single sign-on as web-based services and organizations are widely adopting it.

THE INFOBLOX – SSO INTEGRATION

SSO is commonly used to expedite access to enterprise and web-based business applications, not to access IT infrastructure. But because the access challenges facing network professionals mirror those of business users, Infoblox has created a pathway for integrating SSO into NIOS 8.4. NIOS 8.4 is the operating system that powers the Infoblox platform for core network services, including DNS, DHCP and IP address management. Integration of SSO is now possible in NIOS 8.4 through the added support for SAML 2.0, enabling organizations to use an SSO service to access NIOS 8.4 and all its capabilities.

NIOS 8.4 conforms to the SAML architecture. Within that architecture, NIOS 8.4 is categorized as a Service Provider (SP) the catchall term used in SAML for applications and resources.

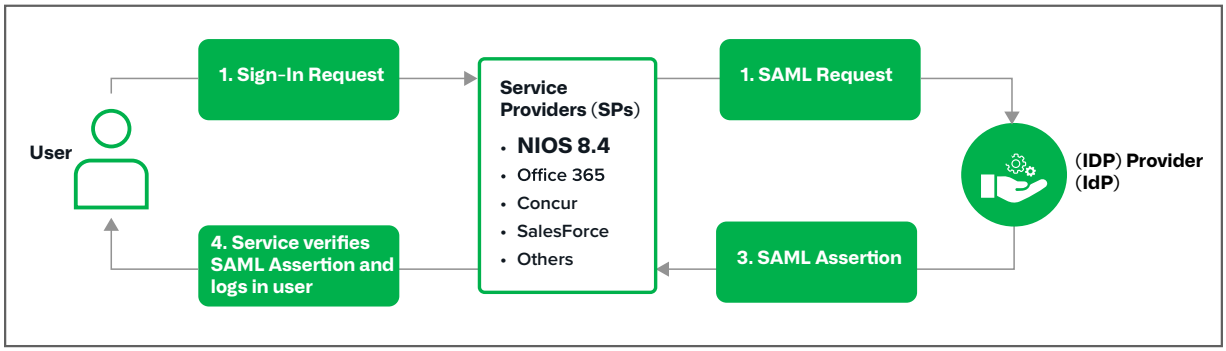

Figure 1: How NIOS 8.4 enables SSO integration through support of SAML 2.0

When a User signs into an SP, an encrypted SAML Request is sent to an Identity Provider (IDP). The IDP authenticates the user and provides identity information (such as groups or memberships). If the User is authenticated successfully and authorized, the IDP responds with an encrypted SAML Assertion. The SP(s) verifies the Assertion and the user gains access to all appropriate SPs.

SAML 2.0-based IDPs can manage access to NIOS 8.4. Some of the common IDPs that are compatible with NIOS 8.4 include:

- Okta
- Azure SSO
- Ping Identity
- Shibboleth SSO

BENEFITS

SSO support in NIOS 8.4 using SAML 2.0 helps organizations:

- **Make Users More Productive** – Access to NIOS 8.4 employs the same steps and tools for accessing mainstream production applications. Using NIOS is faster, simpler and less prone to errors.
- **Improve Security** – SSO greatly decreases the number of sign-on transactions and the attendant security exposures.
- **Increase Administration Efficiency** – Calls, email and messages to the support desk asking for help reaching NIOS and any SP are reduced.
- **Leverage Existing Investments** – An organization that uses a SAML-based SSO today can readily fold in NIOS 8.4, making DDI and DNS security services accessible through their existing SSO service.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20230919v1