Single sign-on

This article describes Single Sign-On and how it is used in Nexus Hybrid Access Gateway.

What is Single Sign-On (SSO)

Single Sign-On (SSO) permits users to enter their credentials once, which then gives them access to several resources without the need to re-authenticate later on. Policy expressions help and assist the user with internal credentials. When using the system for the first time, users might be prompted for internal credentials as additional user ID and password. But the system administrators have the possibility to pre-populate this and even make a dynamic lookup to get the values. If the user has been prompted to add individual SSO credentials, they are then stored per user account and retrieved whenever the user accesses resources registered in an SSO domain. If credentials are invalid or changed, the user will be prompted to enter them again.

Where can SSO be used?

The system administrators can enabled SSO for web based access including HTML5 clients and some TCP protocols using the Access Client. Almost any web resource requiring additional user information can benefit and use SSO. SSO can also be used for well defined protocols as Microsoft Terminal server (RDP), Secure Shell (SSH) and Telnet.

How does web based SSO work?

When SSO is enabled and used, it performs a POST or a GET request to a URL:

- POST requests supply additional data from the client (browser) to the server in the message body.
- GET requests include all required data in the URL.

The form data usually contains a user name and a password together with some static fields. The variables [$username], [$password], and [$domain] are replaced by the stored user name, password and NTLM domain from the SSO database. If the back-end server requires the logon request to contain specific headers, these can be supplied as additional headers.

How is SSO used?

There are two methods of using SSO:

- Persistent SSO - Access to several resources without the need to re-authenticate for each resource.
- Session-based SSO - Enables one-time-logon: users do not have to re-authenticate for each request.

What is SSO domains?

In Hybrid Access Gateway, SSO domains are configured to enable Single sign-on for resources using the same user credentials. The SSO domain specifies how SSO will be used for the resources included in the domain. When user credentials are modified, the changes apply to all resources in the SSO domain.

SSO domains are available in two domain types (authentication):

- Text (default)
- Cookie

Depending on which domain type you choose, different domain attributes can be associated with the SSO domain. Both domain types can be protected by access rules.

Related information

- Access Client
- Add Single Sign-On domain
- Resources
- SAML 2.0 federation
- Single sign-on script in Hybrid Access Gateway
- User accounts
- Users
- Web resources

Domain type Text

Text-based authentication is used to send authentication information as text, with different attributes defining the information needed.

For the domain type text, the available domain attributes are:

- User name
- Password
- Domain
- Ticket

Which domain attributes you add to the domain type Text depends on the authentication method used. The domain attributes normally used for the different authentication methods are described below.

Internal authentication protocols supported:

- Web based NTLM
  When using the Microsoft authentication method NTLM, all domain attributes for the domain type Text (user name, password, and domain) are added.
- Web based Basic
  When using the authentication method Basic, the attributes user name and password are added. Basic is the most commonly used authentication method for web environments.
- Web Form-based
  When using form-based logon for an SSO domain, the attributes user name and password are added. To use form-based logon for an SSO domain, you need to design a web form for access to each resource in the SSO domain. This is done when adding or editing a resource. Selecting form-based SSO will provide the logon form and form response configuration.

  The logon form is added to the resource host to enable form-based SSO. Configuration of the logon form includes whether SSO should perform POST or GET when triggered, the URL to GET or POST data to, as well as form data sent to the server. A form response message can be used to determine whether a logon was successful or not. Configuration of the form response message, that will appear when the user has logged on or failed to log on, includes a URL to which the response from the form should be sent, and a text string form response used to decide if the authentication is successful or unsuccessful.

- Web Adaptive Single-Sign On
  Adaptive SSO is a new version of Form Based SSO that does not need to be configured but learns it's configuration by itself. You only need to apply it on a resource and choose a SSO-domain to use.
- RDP via Access Client
- SSH via Access Client
- Telnet via Access Client

SSO to cloud applications

- SAML 2.0
- OAuth 2.0

Domain type Cookie

Cookie-based authentication is used to send authentication information in HTTP headers. A common use of cookie SSO is when back-end applications only want to read the authentication information at the very first request.

For the domain type cookie, the available domain attributes are:

- Cookie name
- Cookie value
- Cookie secure
- Cookie domain

See Add Single Sign-On domain for more information.