Access rules

This article describes access rules used in Nexus Hybrid Access Gateway.

This article is valid from Nexus Hybrid Access Gateway 5.11.

What is an access rule?

Access rules consist of detailed requirements that users must conform to in order to be allowed access to resources and Single Sign-On (SSO) domains. They are also used in SAML 2.0 federation.

You can specify general access rules that can be reused in many places, as well as access rules that applies to a specific resource only. You can also specify a global access rule that automatically applies to all resources.

You can create access rules using different criteria. For example, access to a resource is allowed:

- if the user is authenticated with one or several authentication methods.
- if the user is member of one certain user group.
- if the incoming device/client comes from a specific IP address or IP address range.
- if the user uses a specific device.
- if the access occurs during a specified time period.
- if the client meets assessment requirement.
- if the user is stored in a specified user storage location.
- if the request is coming through a specified access point.
- if the user is authenticated by a registered SAML 2.0 identity provider.
- if the user is orchestrated to the remote system using an identity orchestration channel.
- if a HTTP header name and regular expression are matched.
- if the user conforms to a customized access rule, specified in separate XML files.

When adding access rules to a resource you can use the general access rules in combination with specific access rules, combined with AND. You can also combine specific rules with either AND or OR.

A custom-defined access rule is tailored to meet specific needs. The custom-defined access rules are specified in separate XML files and can only be updated by editing the corresponding XML file.

How can Single Sign-On (SSO) be used with access rules

For SSO you define how and when SSO should be used by protecting the SSO domain with access rules. The access rules specified for the SSO domain apply to the SSO functionality only, not to the resources in the SSO domain. For example, if a user successfully accesses a resource in the SSO domain but the SSO access rule fails, the user is still free to access resources in the domain. The user will be required to enter credentials for each resource, as if SSO was not applied.

How do I add an access rule?

Click here for information on how to add an access rule.

Related information

- Access point, add, set up and configure
- Add access rule
- Add identity orchestration channel and plugin
- Assessment
- Authentication methods
- Device definitions
- Identity orchestration
- Resources
- SAML 2.0 federation
- Single sign-on
- User groups