SAML REST API. v1.0

Created Jan 16, 2024 at 02:01 PM

Overview

Resources

Auth_Mappings: Delete an auth mapping

Manage a single SAML attribute auth mapping.

```
DELETE https://{device}/api/cascade.saml/1.0/auth_mappings/{mapping_id}
```

Authorization

This request requires authorization.

Response Body

On success, the server does not provide any body in the responses.

Auth_Mappings: Add a new auth mapping

Mappings for SAML attributes to system roles and permissions.

```
POST https://{device}/api/cascade.saml/1.0/auth_mappings
```

Authorization

This request requires authorization.

Request Body

Provide a request body with the following structure:

JSON

```
{
 "attr_key": string,
 "attr_value": string,
 "user_role_map_id": number,
 "user_role_id": string
}

Example:
{
 "user_role_id": "administrator",
 "attr_key": "memberOf",
 "attr_value": "administrators"
}
```

Property Name	Type	Description	Notes
SamlAuthMapping	*<object>*	Object representing a single SAML attribute mapping.	
SamlAuthMapping.attr_key	*<string>*	SAML attribute key name.	
SamlAuthMapping.attr_value	*<string>*	SAML attribute value to match.	
SamlAuthMapping.user_role_map_id	*<number>*	ID of the mapping.	Optional
SamlAuthMapping.user_role_id	*<string>*	System role to grant (Profiler-only: event_viewer, dashboard_viewer, restricted, identity_enabled, traffic_filter).	Values: administrator, operator, monitor, event_viewer, dashboard_viewer, restricted, identity_enabled, traffic_filter, auto_resolution, edit_dashboards

Response Body

On success, the server returns a response body with the following structure:

JSON

```
{
 "attr_key": string,
 "attr_value": string,
 "user_role_map_id": number,
 "user_role_id": string
}

Example:
{
 "user_role_id": "administrator",
 "attr_key": "memberOf",
 "attr_value": "administrators"
}
```

Property Name	Type	Description	Notes
SamlAuthMapping	*<object>*	Object representing a single SAML attribute mapping.	
SamlAuthMapping.attr_key	*<string>*	SAML attribute key name.	
SamlAuthMapping.attr_value	*<string>*	SAML attribute value to match.	
SamlAuthMapping.user_role_map_id	*<number>*	ID of the mapping.	Optional
SamlAuthMapping.user_role_id	*<string>*	System role to grant (Profiler-only: event_viewer, dashboard_viewer, restricted, identity_enabled, traffic_filter).	Values: administrator, operator, monitor, event_viewer, dashboard_viewer, restricted, identity_enabled, traffic_filter, auto_resolution, edit_dashboards

Auth_Mappings: Get an auth mapping

Manage a single SAML attribute auth mapping.

```
GET https://{device}/api/cascade.saml/1.0/auth_mappings/{mapping_id}
```

Authorization

This request requires authorization.

Response Body

On success, the server returns a response body with the following structure:

JSON

```
{
 "attr_key": string,
 "attr_value": string,
 "user_role_map_id": number,
 "user_role_id": string
}

Example:
{
 "user_role_id": "administrator",
 "attr_key": "memberOf",
 "attr_value": "administrators"
}
```

Property Name	Type	Description	Notes
SamlAuthMapping	*<object>*	Object representing a single SAML attribute mapping.	
SamlAuthMapping.attr_key	*<string>*	SAML attribute key name.	
SamlAuthMapping.attr_value	*<string>*	SAML attribute value to match.	
SamlAuthMapping.user_role_map_id	*<number>*	ID of the mapping.	Optional
SamlAuthMapping.user_role_id	*<string>*	System role to grant (Profiler-only: event_viewer, dashboard_viewer, restricted, identity_enabled, traffic_filter).	Values: administrator, operator, monitor, event_viewer, dashboard_viewer, restricted, identity_enabled, traffic_filter, auto_resolution, edit_dashboards

Auth_Mappings: Add new auth mappings

Create multiple auth mappings.

```
POST https://{device}/api/cascade.saml/1.0/auth_mappings/bulk_create
```

Authorization

This request requires authorization.

Request Body

Provide a request body with the following structure:

JSON

```
[
  {
    "attr_key": string,
    "attr_value": string,
    "user_role_map_id": number,
    "user_role_id": string
  }
]

Example:
[
  {
    "user_role_id": "administrator",
    "attr_key": "memberOf",
    "attr_value": "administrators"
  },
  {
    "user_role_id": "operator",
    "attr_key": "memberOf",
    "attr_value": "operators"
  }
]
```

Property Name	Type	Description	Notes
SamlAuthMappings	*<array of <object>>*	List of mappings from SAML attributes to system roles.	
SamlAuthMappings[SamlAuthMapping]	*<object>*	Individual SAML attribute mapping.	Optional
SamlAuthMappings[SamlAuthMapping].attr_key	*<string>*	SAML attribute key name.	
SamlAuthMappings[SamlAuthMapping].attr_value	*<string>*	SAML attribute value to match.	
SamlAuthMappings[SamlAuthMapping].user_role_map_id	*<number>*	ID of the mapping.	Optional
SamlAuthMappings[SamlAuthMapping].user_role_id	*<string>*	System role to grant (Profiler-only: event_viewer, dashboard_viewer, restricted, identity_enabled, traffic_filter).	Values: administrator, operator, monitor, event_viewer, dashboard_viewer, restricted, identity_enabled, traffic_filter, auto_resolution, edit_dashboards

Response Body

On success, the server does not provide any body in the responses.

Auth_Mappings: Update an auth mapping

Manage a single SAML attribute auth mapping.

```
PUT https://{device}/api/cascade.saml/1.0/auth_mappings/{mapping_id}
```

Authorization

This request requires authorization.

Request Body

Provide a request body with the following structure:

JSON

```
{
 "attr_key": string,
 "attr_value": string,
 "user_role_map_id": number,
 "user_role_id": string
}

Example:
{
 "user_role_id": "administrator",
 "attr_key": "memberOf",
 "attr_value": "administrators"
}
```

Property Name	Type	Description	Notes
SamlAuthMapping	*<object>*	Object representing a single SAML attribute mapping.	
SamlAuthMapping.attr_key	*<string>*	SAML attribute key name.	
SamlAuthMapping.attr_value	*<string>*	SAML attribute value to match.	
SamlAuthMapping.user_role_map_id	*<number>*	ID of the mapping.	Optional
SamlAuthMapping.user_role_id	*<string>*	System role to grant (Profiler-only: event_viewer, dashboard_viewer, restricted, identity_enabled, traffic_filter).	Values: administrator, operator, monitor, event_viewer, dashboard_viewer, restricted, identity_enabled, traffic_filter, auto_resolution, edit_dashboards

Response Body

On success, the server does not provide any body in the responses.

Auth_Mappings: List auth mappings

Mappings for SAML attributes to system roles and permissions.

```
GET https://{device}/api/cascade.saml/1.0/auth_mappings
```

Authorization

This request requires authorization.

Response Body

On success, the server returns a response body with the following structure:

JSON

```
[
  {
   "attr_key": string,
   "attr_value": string,
   "user_role_map_id": number,
   "user_role_id": string
  }
]

Example:
[
  {
   "user_role_id": "administrator",
   "attr_key": "memberOf",
   "attr_value": "administrators"
  },
  {
   "user_role_id": "operator",
   "attr_key": "memberOf",
   "attr_value": "operators"
  }
]
```

Property Name	Type	Description	Notes
SamlAuthMappings	*<array of <object>>*	List of mappings from SAML attributes to system roles.	
SamlAuthMappings[SamlAuthMapping]	*<object>*	Individual SAML attribute mapping.	Optional
SamlAuthMappings[SamlAuthMapping].attr_key	*<string>*	SAML attribute key name.	

SamlAuthMappings[SamlAuthMapping].attr_value	*<string>*	SAML attribute value to match.	
SamlAuthMappings[SamlAuthMapping].user_role_map_id	*<number>*	ID of the mapping.	Optional
SamlAuthMappings[SamlAuthMapping].user_role_id	*<string>*	System role to grant (Profiler-only: event_viewer, dashboard_viewer, restricted, identity_enabled, traffic_filter).	Values: administrator, operator, monitor, event_viewer, dashboard_viewer, restricted, identity_enabled, traffic_filter, auto_resolution, edit_dashboards

Settings: Apply settings

System settings for SAML authentication.

PUT https://{device}/api/cascade.saml/1.0/settings

Authorization

This request requires authorization.

Request Body

Provide a request body with the following structure:

JSON

```
{
  "enabled": string,
  "sign_auth_requests": string,
  "fqdn": string,
  "idp_metadata": string,
  "nameid_attr": string,
  "want_assertions_signed": string,
  "allow_local_login": string
}

Example:
{
  "sign_auth_requests": true,
  "enabled": true,
  "fqdn": "",
  "nameid_attr": "NameID",
  "idp_metadata": "<?xml version=\"1.0\"?><md:EntityDescriptor xmlns:md=\"urn:oasis:names:tc:SAML:2.0:metadata\"
xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\" entityID=\"https://cam-tarpon22:8443/simplesaml/saml2/idp/metadata.php\">
<md:IDPSSODescriptor protocolSupportEnumeration=\"urn:oasis:names:tc:SAML:2.0:protocol\">    <md:KeyDescriptor
use=\"signing\">      <ds:KeyInfo xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\">        <ds:X509Data>
<ds:X509Certificate>aaaaaaa</ds:X509Certificate>        </ds:X509Data>      </ds:KeyInfo>    </md:KeyDescriptor>
<md:KeyDescriptor use=\"encryption\">      <ds:KeyInfo xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\">        <ds:X509Data>
<ds:X509Certificate>aaaaa</ds:X509Certificate>        </ds:X509Data>      </ds:KeyInfo>    </md:KeyDescriptor>
<md:SingleLogoutService Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\" Location=\"https://cam-
tarpon22:8443/simplesaml/saml2/idp/SingleLogoutService.php\"/>    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>    <md:SingleSignOnService Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\"
Location=\"https://cam-tarpon22:8443/simplesaml/saml2/idp/SSOService.php\"/>  </md:IDPSSODescriptor></md:EntityDescriptor>",
  "want_assertions_signed": true,
  "allow_local_login": true
}
```

Property Name	Type	Description	Notes
SamlSettings	*<object>*	System settings for SAML authentication.	
SamlSettings.enabled	*<string>*	SAML currently enabled.	
SamlSettings.sign_auth_requests	*<string>*	Flag indicating that SAML requests must be signed.	Optional
SamlSettings.fqdn	*<string>*	Fully qualified domain name of this device. The IdP server will redirect all users to this domain name.	Optional
SamlSettings.idp_metadata	*<string>*	XML metadata for identity provider.	Optional
SamlSettings.nameid_attr	*<string>*	Attribute to map to NetProfiler username (blank to use IdP-provided value from metadata).	Optional
SamlSettings.want_assertions_signed	*<string>*	Flag indicating that SAML assertions must be signed.	Optional
SamlSettings.allow_local_login	*<string>*	Flag to allow local login authentication via special URL: /local_login.php when SAML is enabled. It allows recovering bad SAML settings.	Optional

Response Body

On success, the server returns a response body with the following structure:

JSON

```
{
  "enabled": string,
  "sign_auth_requests": string,
  "fqdn": string,
  "idp_metadata": string,
  "nameid_attr": string,
  "want_assertions_signed": string,
  "allow_local_login": string
}
```


Example:


```
{
  "sign_auth_requests": true,
  "enabled": true,
  "fqdn": "",
  "nameid_attr": "NameID",
  "idp_metadata": "<?xml version=\"1.0\"?><md:EntityDescriptor xmlns:md=\"urn:oasis:names:tc:SAML:2.0:metadata\"
xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\" entityID=\"https://cam-tarpon22:8443/simplesaml/saml2/idp/metadata.php\">
<md:IDPSSODescriptor protocolSupportEnumeration=\"urn:oasis:names:tc:SAML:2.0:protocol\">    <md:KeyDescriptor
use=\"signing\">      <ds:KeyInfo xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\">        <ds:X509Data>
<ds:X509Certificate>aaaaaaa</ds:X509Certificate>        </ds:X509Data>      </ds:KeyInfo>    </md:KeyDescriptor>
<md:KeyDescriptor use=\"encryption\">      <ds:KeyInfo xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\">        <ds:X509Data>
<ds:X509Certificate>aaaaa</ds:X509Certificate>        </ds:X509Data>      </ds:KeyInfo>    </md:KeyDescriptor>
<md:SingleLogoutService Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\" Location=\"https://cam-
tarpon22:8443/simplesaml/saml2/idp/SingleLogoutService.php\"/>    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>    <md:SingleSignOnService Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\"
Location=\"https://cam-tarpon22:8443/simplesaml/saml2/idp/SSOService.php\"/>  </md:IDPSSODescriptor></md:EntityDescriptor>",
  "want_assertions_signed": true,
  "allow_local_login": true
}
```


Property Name	Type	Description	Notes
SamlSettings	*<object>*	System settings for SAML authentication.	
*SamlSettings.*enabled	*<string>*	SAML currently enabled.	
*SamlSettings.*sign_auth_requests	*<string>*	Flag indicating that SAML requests must be signed.	Optional
*SamlSettings.*fqdn	*<string>*	Fully qualified domain name of this device. The IdP server will redirect all users to this domain name.	Optional
*SamlSettings.*idp_metadata	*<string>*	XML metadata for identity provider.	Optional
*SamlSettings.*nameid_attr	*<string>*	Attribute to map to NetProfiler username (blank to use IdP-provided value from metadata).	Optional
*SamlSettings.*want_assertions_signed	*<string>*	Flag indicating that SAML assertions must be signed.	Optional
*SamlSettings.*allow_local_login	*<string>*	Flag to allow local login authentication via special URL: /local_login.php when SAML is enabled. It allows recovering bad SAML settings.	Optional

Settings: Show current settings

System settings for SAML authentication.

```
GET https://{device}/api/cascade.saml/1.0/settings
```

Authorization

This request requires authorization.

Response Body

On success, the server returns a response body with the following structure:

JSON

```
{
  "enabled": string,
  "sign_auth_requests": string,
  "fqdn": string,
  "idp_metadata": string,
  "nameid_attr": string,
  "want_assertions_signed": string,
  "allow_local_login": string
}

Example:
{
  "sign_auth_requests": true,
  "enabled": true,
  "fqdn": "",
  "nameid_attr": "NameID",
  "idp_metadata": "<?xml version=\"1.0\"?><md:EntityDescriptor xmlns:md=\"urn:oasis:names:tc:SAML:2.0:metadata\"
xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\" entityID=\"https://cam-tarpon22:8443/simplesaml/saml2/idp/metadata.php\">
<md:IDPSSODescriptor protocolSupportEnumeration=\"urn:oasis:names:tc:SAML:2.0:protocol\">    <md:KeyDescriptor
use=\"signing\">      <ds:KeyInfo xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\">        <ds:X509Data>
<ds:X509Certificate>aaaaaaa</ds:X509Certificate>        </ds:X509Data>      </ds:KeyInfo>    </md:KeyDescriptor>
<md:KeyDescriptor use=\"encryption\">      <ds:KeyInfo xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\">        <ds:X509Data>
<ds:X509Certificate>aaaaa</ds:X509Certificate>        </ds:X509Data>      </ds:KeyInfo>    </md:KeyDescriptor>
<md:SingleLogoutService Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\" Location=\"https://cam-
tarpon22:8443/simplesaml/saml2/idp/SingleLogoutService.php\"/>    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>    <md:SingleSignOnService Binding=\"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect\"
Location=\"https://cam-tarpon22:8443/simplesaml/saml2/idp/SSOService.php\"/>  </md:IDPSSODescriptor></md:EntityDescriptor>",
  "want_assertions_signed": true,
  "allow_local_login": true
}
```

Property Name	Type	Description	Notes
SamlSettings	*<object>*	System settings for SAML authentication.	
SamlSettings.enabled	*<string>*	SAML currently enabled.	
SamlSettings.sign_auth_requests	*<string>*	Flag indicating that SAML requests must be signed.	Optional
SamlSettings.fqdn	*<string>*	Fully qualified domain name of this device. The IdP server will redirect all users to this domain name.	Optional
SamlSettings.idp_metadata	*<string>*	XML metadata for identity provider.	Optional
SamlSettings.nameid_attr	*<string>*	Attribute to map to NetProfiler username (blank to use IdP-provided value from metadata).	Optional
SamlSettings.want_assertions_signed	*<string>*	Flag indicating that SAML assertions must be signed.	Optional
SamlSettings.allow_local_login	*<string>*	Flag to allow local login authentication via special URL: /local_login.php when SAML is enabled. It allows recovering bad SAML settings.	Optional

Error Codes

In the event that an error occurs while processing a request, the server will respond with appropriate HTTP status code and additional information in the response body:

```
{
    "error_id":   "{error identifier}",
    "error_text": "{error description}",
    "error_info": {error specific data structure, optional}
}
```

The table below lists the possible errors and the associated HTTP status codes that may returned.

Error ID	HTTP Status	Comments
INTERNAL_ERROR	500	Internal server error.
AUTH_REQUIRED	401	The requested resource requires authentication.
AUTH_INVALID_CREDENTIALS	401	Invalid username and/or password.
AUTH_INVALID_SESSION	401	Session ID is invalid.
AUTH_EXPIRED_PASSWORD	403	The password must be changed. Access only to password change resources.
AUTH_DISABLED_ACCOUNT	403	Account is either temporarily or permanently disabled.
AUTH_FORBIDDEN	403	User is not authorized to access the requested resource.
AUTH_INVALID_TOKEN	401	OAuth access token is invalid.
AUTH_EXPIRED_TOKEN	401	OAuth access token is expired.
AUTH_INVALID_CODE	401	OAuth access code is invalid.
AUTH_EXPIRED_CODE	401	OAuth access code is expired.

RESOURCE_NOT_FOUND	404	Requested resource was not found.
HTTP_INVALID_METHOD	405	Requested method is not available for this resource.
HTTP_INVALID_HEADER	400	An HTTP header was malformed.
REQUEST_INVALID_INPUT	400	Malformed input structure.
URI_INVALID_PARAMETER	400	URI parameter is not supported or malformed.
URI_MISSING_PARAMETER	400	Missing required parameter.