tsm authentication

You can use the `tsm authentication` commands to enable, disable, and configure user authentication options for Tableau Server.

- kerberos
  - configure
  - disable
  - enable
- list
- mutual-ssl
  - configure
  - disable
  - enable
- openid
  - configure
  - disable
  - enable
  - get-redirect-url
  - map-claims
- saml
  - configure
  - disable
  - enable
  - export-metadata
  - map-assertions
- sitesaml
  - disable
  - enable
- sspi
  - disable
  - enable
- trusted

tsm authentication kerberos <commands>

Enable, disable, and configure Kerberos user authentication on [Tableau Server]. See Configure Kerberos.

Synopsis

```
tsm authentication kerberos configure --keytab-file <keytab_file.keytab>
[global options]
```

```
tsm authentication kerberos enable [global options]
```

```
tsm authentication kerberos disable [global options]
```

Options for kerberos configure

-kt, --keytab-file <keytab_file.keytab>

: Required.

```
Specifies the service .keytab file used for requests to the KDC.
```

tsm authentication list

List the server's existing authentication-related configuration settings.

Synopsis

```
tsm authentication list [--verbose][global options]
```

Options

v, --verbose

Optional.

Show all configured parameters.

tsm authentication mutual-ssl <commands>

Enable, disable, and configure mutual SSL for user authentication on [Tableau Server]. To learn more about mutual SSL, see Configure Mutual SSL Authentication.

Before you enable mutual SSL, you must enable and configure SSL for external communication. For information, see Configure SSL for External HTTP Traffic to and from Tableau Server.

Synopsis

```
tsm authentication mutual-ssl configure [options] [global options]
```

```
tsm authentication mutual-ssl disable [global options]
```

```
tsm authentication mutual-ssl enable [global options]
```

Options

-cf, --ca-cert <certificate-file.crt>

Optional.

Specifies the location and file name for the certificate file. The file must be a valid, trusted certificate from a Certificate Authority (for example, Verisign).

-fb, --fallback-to-basic <true | false>

Optional.

Specifies whether Tableau Server should accept user name and password for authentication if SSL authentication fails.

Default value is false, to indicate that when configured for mutual SSL, Tableau Server does not allow a connection when SSL authentication fails. However, Tableau Serer accepts username and password authentication from REST API clients, even if this option is set to `false`.

-m, --user-name-mapping <upn | ldap | cn>

Optional.

Specifies the user name syntax (UPN, LDAP or CN) to retrieve from identity store or directory. The syntax must match the format for Subject or Subject Alternative Name on the user certificate.

-rf, --revocation-file <revoke-file.pem>

Optional.

Specifies the location and file name for the certificate revocation list file. This file can be a .pem or .der file.

tsm authentication openid <commands>

Enable, disable, and configure OpenID Connect (OIDC) user authentication on [Tableau Server].

Synopsis

```
tsm authentication openid configure [options] [global options]
```

```
tsm authentication openid disable [global options]
```

```
tsm authentication openid enable [global options]
```

```
tsm authentication openid get-redirect-url [global options]
```

```
tsm authentication openid map-claims [options] [global options]
```

Options for openid configure

-a, --client-authentication <string>

Optional.

Specifies custom client authentication method for OpenID Connect.

To configure Tableau Server to use the Salesforce IdP, set this value to `client_secret_post`.

-cs, --client-secret <string>

Optional.

Specifies the provider client secret. This is a token that is used by Tableau to verify the authenticity of the response from the IdP. This value is a secret and should be kept securely.

-cu, --config-url <CONFIG-URL>

Optional.

Specifies the provider configuration URL. The default value is constructed based on the name of the server (gateway.public.host), and the gateway port, if any(gateway.public.port). In addition, by default the protocol is set to https:// if SSL is enabled for the server.

-mf, --config-file <config-file.json>

Optional.

Specifies the local path to the static OIDC discovery JSON document.

-i, --client-id <CLIENT-ID>

Optional.

Specifies the provider client ID that your IdP has assigned to your application.

-id, --ignore-domain <true | false>

Optional. Default: `false`

Set this to `true` if the following are true:

- You are using email addresses as usernames in Tableau Server
- You have provisioned users in the IdP with multiple domain names
- You want to ignore the domain name portion of the `email` claim from the IdP

Before you proceed, review the user names that will be used as a result of setting this option to `true`. User name conflicts may occur. In the case of a user name conflict, the risk of information disclosure is high. See Requirements for Using OpenID Connect.

-if, --iframed-idp-enabled <true | false>

Optional. Default: `false`

Specifies if IdP is allowed inside of an iFrame. The IdP must disable clickjack protection to allow iFrame presentation.

-ij, --ignore-jwk <true | false>

Optional. Default: `false`

Set this to `true` if your IdP does not support JWK validation. In this case, we recommend authenticating communication with your IdP using mutual TLS or another network layer security protocol.

-r, --return-url <return-url>

The URL of your server. This is typically is the public name of your server, such as `"http://example.tableau.com"`.

-sn, --custom-scope-name <string>

Optional.

Specifies a custom scope user-related value that you can use to query the IdP. See Requirements for Using OpenID Connect.

Options for openid map-claims

Use these options to change the default OIDC claims Tableau Server will use when communicating with your IdP. See Requirements for Using OpenID Connect.

-i, --id <string>

Optional. Default: `sub`

Change this value if your IdP does not use the `sub` claim to uniquely identify users in the ID token. The IdP claim that you specify should contain a single, unique string.

-un, --user-name <string>

Optional. Default: `email`

Change this value to the IdP claim that your organization will use to match user names as stored in Tableau Server.

tsm authentication saml <commands>

Configure [Tableau Server] to support single-sign on using the SAML 2.0 standard, enable or disable SAML for a site, map assertion attribute names between [Tableau Server] and the identity provider (IdP).

Available commands

`tsm authentication saml configure [options] [global options]`

`tsm authentication saml disable [options] [global options]`

`tsm authentication saml enable [options] [global options]`

`tsm authentication saml export-metadata [options] [global options]`

`tsm authentication saml map-assertions [options]`

tsm authentication saml configure

Configure the SAML settings for the server. Specify the SAML certificate and metadata files, provide additional required information, set additional options.

If you are configuring SAML for the first time or have previously disabled it, you must run this command with `tsm authentication saml enable`. For more information, see Configure Server-Wide SAML.

Synopsis

`tsm authentication saml configure [options] [global options]`

Options

-e, --idp-entity-id <id>

Required for initial SAML configuration; otherwise optional. IdP entity ID value.

Typically this is the same as the Tableau Server return URL (specified in the `--idp-return-url` parameter). The entity ID that you enter is used as a base for generating site-specific entity IDs. For example, if you enter the following:

http://tableau-server

A site configured for SAML might display the following entity ID:

http://tableau-server/samlservice/public/sp/metadata?alias=48957410-9396-430a-967c-75bdb6e002a0

To find a site's entity ID, go to the site's [Settings] page, and select the [Authentication] tab. When SAML is enabled, the entity ID is shown under the first step for configuring site-specific SAML, exporting metadata.

-r, --idp-return-url <idp-return-url>

Required for initial SAML configuration; otherwise optional. The SAML return URL configured in the IdP. This is typically the Tableau Server external URL; for example, https://tableau-server.

Notes

- http://localhost does not work for an external server.
- Adding a trailing slash to the URL (https://tableau-server/) is not supported.

-i, --idp-metadata <idp-metadata.xml>

Required for initial SAML configuration; otherwise optional. Provide the location and name of the XML metadata file you exported from the IdP's settings.

For example, `C:\ProgramData\Tableau\Tableau Server\data\saml\<metadata-file.xml>`

-cf, --cert-file <certificate.crt>

Required for initial SAML configuration; otherwise optional. The location and file name for the x509 certificate file for SAML. For requirements for the certificate file, see SAML Requirements.

For example, `C:\ProgramData\Tableau\Tableau Server\data\saml\<file.crt>`

-kf, --key-file <certificate.key>

Required for initial SAML configuration; otherwise optional. Location and name of the key file that goes along with certificate.

For example, `C:\ProgramData\Tableau\Tableau Server\data\saml\<file.key>`

-a, --max-auth-age <max-auth-age>

Optional. Default value is 7200 (2 hours).

The maximum number of seconds allowed between a user's authentication and processing of the AuthNResponse message.

-d, --desktop-access <enable | disable>

Optional. Default value is enable.

Use SAML to sign in to the server from Tableau Desktop. If single sign-on from Tableau client applications does not work with your IdP, you can set this to `disable`.

-m, --mobile-access <enable | disable>

Optional. Default value is enable.

Allow using SAML to sign in from older versions of Tableau Mobile app. Devices running Tableau Mobile app version 19.225.1731 and higher ignore this option. To disable devices running Tableau Mobile app version 19.225.1731 and higher, disable SAML as a client login option on Tableau Server.

-so, --signout <enable | disable>

Optional. Enabled by default.

Enable or disable SAML sign out for Tableau Server.

-su, --signout-url <url>

Optional. Enter the URL to redirect to after users sign out of the server. By default this is the Tableau Server sign-in page. You can specify an absolute or a relative URL.

Example

```
tsm authentication saml configure --idp-entity-id https://tableau-server --idp-metadata
"C:\ProgramData\Tableau\Tableau Server\data\saml\<metadata.xml>" --idp-return-url
https://tableau-server --cert-file "C:\ProgramData\Tableau\Tableau Server\data\saml\
<file.crt>" --key-file "C:\ProgramData\Tableau\Tableau Server\data\saml\<file.key>"
```

tsm authentication saml enable and saml disable

Enable or disable server-wide SAML authentication. In this context, all sites and users that you enable for SAML go through a single identity provider.

Synopsis

`tsm authentication saml enable [global options]`

`tsm authentication saml disable [global options]`

tsm authentication saml export-metadata

Export the Tableau Server .xml metadata file that you will use to configure the SAML IdP.

Synopsis

`tsm authentication saml export-metadata [options] [global options]`

Options

-f, --file [/path/to/file.xml]

Optional.

Specifies the location and file name in which the metadata will be written. If you don't include this option, `export-metadata` saves the file to the current directory, and names it `samlmetadata.xml`.

-o, --overwrite

Optional.

Overwrites an existing file of the same name specified in `-f`, or of the default name if `-f` is not included. If a file specified in `-f` exists, and `-o` is not included, the command does not overwrite the existing file.

tsm authentication saml map-assertions

Maps attributes between the IdP and Tableau Server. Provide the name that the IdP uses for the attribute specified in each argument.

Synopsis

`tsm authentication saml map-assertions --user-name <user-name> [global options]`

Options

-r, --user-name <user-name-attribute>

Optional. The attribute in which the IdP stores the user name. On Tableau Server this is the display name.

-e, --email <email-name-attribute>

Not implemented. Do not use.

-o, --domain <domain-name-attribute>

Optional. The attribute in which the IdP stores the domain name.

-d --display-name <display-name-attribute>

Not implemented. Do not use.

Example for saml map-assertions

`tsm authentication saml map-assertions --email=Email --user-name=DisplayName`

tsm authentication sitesaml enable and sitesaml disable

Set the server to allow or disallow SAML authentication at the site level. Enabling site-specific SAML gives you access to the [Settings] > [Authentication] tab in the [Tableau Server] web UI. The [Authentication] tab contains the site-specific SAML configuration settings.

Use the `sitesaml enable` command with `saml configure` if you haven't yet configured the server to allow site-specific SAML. For more information, see Configure Site-Specific SAML.

Synopsis

```
tsm authentication sitesaml enable [global options]
```

```
tsm authentication sitesaml disable [global options]
```

tsm authentication sspi <commands>

This command will only work on Tableau Server on Windows. If you attempt to enable SSPI on Tableau Server on Linux, an error will be returned.

Enable or disable automatic sign-in using Microsoft SSPI.

If you use Active Directory for authentication, you can optionally enable automatic logon, which uses Microsoft SSPI to automatically sign in your users based on their Windows username and password. This creates an experience similar to single sign-on (SSO).

Do not enable SSPI if you plan to configure Tableau Server for SAML, trusted authentication, a load balancer, or for a proxy server. SSPI is not supported in these scenarios.

Synopsis

```
tsm authentication sspi disable [global options]
```

```
tsm authentication sspi enable [global options]
```

As with all authentication commands, you must run `tsm pending-changes apply` after running this command.

tsm authentication trusted <commands>

Configure trusted authentication (trusted tickets) for user authentication on [Tableau Server].

Synopsis

```
tsm authentication trusted configure [options] [global options]
```

Options

-th, --hosts <string>

Optional.

Specifies the trusted host names (or IPv4 addresses) of the web servers that will be hosting pages with Tableau content.

For multiple values, enter the names in a comma-separated list where each value is encapsulated in double-quotes.

For example:

```
tsm authentication trusted configure -th "192.168.1.101", "192.168.1.102",
"192.168.1.103"
```

or

```
tsm authentication trusted configure -th "webserv1", "webserv2", "webserv3"
```

-t, --token-length <integer>

Optional.

Determines the number of characters in each trusted ticket. The default setting of 24 characters provides 144 bits of randomness. The value can be set to any integer between 9 and 255, inclusive.

Global options

-h, --help

Optional.

Show the command help.

-p, --password <password>

Required, along with `-u` or `--username` if no session is active.

Specify the password for the user specified in `-u` or `--username`.

If the password includes spaces or special characters, enclose it in quotes:

`--password "my password"`

-s, --server https://<hostname>:8850

Optional.

Use the specified address for Tableau Services Manager. The URL must start with `https`, include port 8850, and use the server name not the IP address. For example `https://<tsm_hostname>:8850`. If no server is specified, `https://<localhost | dnsname>:8850` is assumed.

--trust-admin-controller-cert

Optional.

Use this flag to trust the self-signed certificate on the TSM controller. For more information about certificate trust and CLI connections, see Connecting TSM clients.

-u, --username <user>

Required if no session is active, along with `-p` or `--password`.

Specify a user account. If you do not include this option, the command is run using credentials you signed in with.