Multi-Zone SAML Single Sign-On

This describes how to use SAML/SSO for multi-zone environments.

> Prerequisites: You have Zone Administrator permissions for all zones that you want to manage in this configuration.

Automox supports multiple SAML configurations for all zones that you manage. Multi-zone SAML allows you to create a SAML configuration for each zone, providing specific access based on the zone and users.

Currently, multi-zone SAML only supports a one to one relationship with zones. Each zone will need its own configuration and its own SAML app.

Configuration

The process for configuring multi-zone SAML is the same as single-zone SAML. In any zone, follow single-zone SAML configuration steps to setup a SAML configuration.

Once configured, any user with an account in the zone with SAML enabled will be redirected to the IDP for login, unless they specify an zone at login.

Logging In

IDP-Initiated

IDP-initiated logins behave as expected. When a user clicks on a specific app in your IDP for a zone, they are redirected to that zone. After they log in, they can optionally navigate to another zone that they are part of if they use the Automox multi-zone drop-down menu.

SP-Initiated

SP-initiated logins behave in many different ways depending on how you want users to reach their specific zones:

Generic Login: If a user visits console.automox.com and attempts to log in, Automox defaults to the SAML configuration of the lowest zone ID that the specific user has access to. If zone A for the user has SAML, the SAML configuration for zone A is used. If zone A has password login, and zone B has SAML enabled, zone B's SAML configuration is used.

Define a Zone ID: Users can login directly to a specific zone if they specify a zone ID in the URL at login. If a user specifies zone A in their login URL, they will use zone A's SAML configuration to login.

Specify a zone ID in the login URL as follows:

- The zone ID for any given account can be found when logged into the console. The URL shows a parameter for “?o=XXXX,” where XXXX is the zone ID.
- Copy and paste the same “?o=XXXX” parameter into the login URL (https://console.automox.com/login) to force login to that specific zone.

Automox recommends bookmarking specific login URLs so that users can navigate directly to specific accounts.

Inviting and Provisioning Users

Inviting Users

With Multi-zone SAML enabled, users can be invited to other zones through the regular user invite workflow. If SAML is enabled in the zone that you are inviting them to, they will need appropriate access to the SAML app in your IDP.

Provisioning

Provisioning users from the IDP is only supported on IDP-initiated login. To provision a user to a specific zone, enable provisioning when setting up the SAML configuration and give the user access to the appropriate app in your IDP. When they attempt login, an account will be created for them in the appropriate zone.