CENSITRAC™ SAML INTERFACE SPECIFICATION

Overview

CensiTrac™ supports external authentication and single sign-on (SSO) using SAML 2.0. CensiTrac can be configured to require a SAML 2.0 session, redirecting unauthenticated users to an Identity Provider (IdP). To enable this configuration, CensiTrac and the IdP must exchange metadata and identify the IdP attribute that will be used to provide user identity. Once enabled, users will authenticate with the IdP, and then be redirected to the CensiTrac application as an authenticated user.

Sign-On Workflow

CensiTrac supports a Service Provider (SP) initiated SSO where CensiTrac is the SP and an external resource on a customer's local network is the IdP. The standard flow is:

1. User requests access to CensiTrac application server, either via a browser or the CensiTrac executable.
2. CensiTrac inspects the call and if the user is not authenticated redirects the request to the SSO server.
3. SSO server authenticates the user with the IdP and redirects the user back to CensiTrac with additional credentials.
4. CensiTrac attempts to match the provided credentials for the authenticated user with an existing user in CensiTrac, and, if found, allows access as that CensiTrac user.

Configuration

The SAML configuration requires three items:

1. Censis will generate a SAML 2.0 complaint metadata file. This file should contain the information needed to create a partner entry for CensiTrac at the IdP. This information is valid for the lifetime of the CensiTrac server; if the server is replaced, Censis will supply a new metadata file if needed.
2. The customer will supply Censis with either metadata or a URL for the IdP metadata needed for Censis to create a matching entry. If the metadata frequently changes, a URL should be used to ensure updates without impacting user access.
3. The customer will provide the name of the attribute that is shared when a user is authenticated. This attribute is used to match a user id in CensiTrac to an authenticated user.

User Provisioning

When using the SAML interface, users in CensiTrac are provisioned via the normal user creation workflow in CensiTrac. However, there is no option to enter a password. Authentication for the users is performed via the SAML interface. User access is controlled using the standard CensiTrac access level controls and restrictions.

Censis Technologies, Inc.
830 Crescent Centre Drive, Suite 610
Franklin, TN | **www.censis.com**

615-468-8000
888-877-3010 Toll-Free
615-468-8003 Fax