ENTRÉ

REFERENCE GUIDE: SINGLE SIGN-ON AND ACTIVE DIRECTORY

DMP

LT-2002 20182

SINGLE SIGN-ON AND ACTIVE DIRECTORY OVERVIEW

Entré has the capability to control users' access to systems with single sign-on and Active Directory.

Single Sign-On (SSO) gives users the ability to log in to a system with one username and password that grants access to multiple parts of the system. For example, a user management system at a retail chain's corporate HQ allows employees to sign into a computer, then uses an authentication token to automatically sign them in to their email and programs.

Active Directory (AD) is a centralized user management feature included with Microsoft® operating systems that allows system administrators to manage users on a Windows® domain. For example, a college system administrator uses Active Directory to restrict access to specific network drives by assigning students to a pre-defined student user group.

How Does Single Sign-On Relate to Active Directory?

Active Directory is often used as a source for user credentials, which allows Single Sign-On services to integrate with systems already managing users with Active Directory. These integrations allow SSO to use AD information to control access to non-Windows products like web applications.

HOW ENTRÉ USES SINGLE SIGN-ON

In version 8.4.0 and higher, Entré supports using SSO to authenticate users for Entré and panel access.

Full Client

After the Entré full client is installed and a local Windows user is assigned an operator profile, the user is automatically logged in to the full client with their Windows credentials. The user may perform the functions allowed according to the operator profile assigned to them.

Web Client

Use PingFederate® or PingAccess® software from Ping Identity® to interact with Active Directory and create a certificate based on predetermined program access. The Entré application server uses the certificate sent from the Ping Identity server to allow users to log in to the web client without requiring them to re-enter their credentials. The user may perform the functions allowed according to the operator profile assigned to them.

When configuring SSO in Entré for use with the web client (**System Configuration > Single Sign On**), information about the Identity Provider (Entré) and Service Provider (Ping Identity) is required:

- **IdP Entity ID**—The Entré SSO Service Entity ID (URI)
- **IdP Redirect URL**—Entré web client server address and port number
- **Assertion Consumer Service URL**—The Ping authentication server address and port number
- **SP Entity ID**—The Ping connection ID (URI)

For more information about Ping Identity SSO software, refer to PingFederate and PingAccess.

HOW ENTRÉ USES ACTIVE DIRECTORY

The Entré NOC Active Directory Service allows organizations to deactivate personnel accounts in Entré for inactive users in the Active Directory. When personnel are disabled in the Active Directory, the Entré Active Directory Service queries both the AD and Entré databases, compares the information, then updates the appropriate table for that personnel record in Entré. The status of the associated personnel account and their badges is changed to inactive in Entré. For more information, refer to Entre NOC How-To: Active Directory Service (LT-1939).