Grass Valley
WE LOVE LIVE

WHITEPAPER

Single Sign On in AMPP

By Mike Owen, Ian Hawley, Will Molyneux, Chris Price and Vincent Trussart

Introduction

Virtually every business system our employees use to do their jobs is locked behind a username and password for authentication and security purposes. We then give them advice such as "Passwords must be secure," or "You need to use upper- and lower-case letters with punctuation and numbers," OR "Do not use your cat's middle name!" So our employees must remember countless meaningless passwords and which system they are for, which of course nobody can. The result then falls to one of the following:

- Paying for a secure third-party password manager
- A variation of forgot password, reset password, repeat
- A ticket to IT
- Using somebody else credentials
- Post it notes stuck to a monitor!

All the "solutions" either take time away from doing the core work that generates you real value or severely impair your security.

This is where Single Sign On comes in.

What is Single Sign On?

Single Sign On (SSO) is the ability to allow a user to sign into multiple systems with a single set of credentials. This is generally good for security posture as users only manage a single set of credentials that can be withdrawn and managed centrally, such as when an employee leaves. It also allows SSO users to have a single MFA/2FA solution linked to their provider rather than having to employ multiple solutions.

AMPP Supported Integrations

AMPP currently offers support for the following methods for providing SSO integration:

- ***Okta***

  Okta is an identity and access management system for helping customers integrate systems with other identity providers or using it as its own identity system.

- ***Azure Active Directory (Azure AD)***

  Azure AD is the Microsoft identity and access management system hosted in Microsoft's cloud offering, Azure.

- ***AWS Cognito***

  AWS Cognito is Amazon's cloud offering for an identity provider that can be used to manage users and their groups.

- ***OpenID Connect + OAuth 2.0***

  OpenID Connect and OAuth 2.0 are the protocols that we use when integrating with third-party providers such as the ones mentioned above. While we support these specifications, there are usually minor differences in some of the implementation details, which usually require a specific implementation tweak for the provider.

- ***SAML (coming soon)***

  SAML is a more legacy version of OpenID Connect, which is slowly becoming deprecated in favor of OpenID Connect. It is a protocol for allowing users from an external provider to be able to sign in to AMPP.

Integration Types

Grass Valley offer two types of SSO integration:

- Configuration only
- Requiring bespoke development

Generally, **Configuration Only** applies to **Okta** and **Azure AD,** but any specialization of these will require additional work that may be chargeable.

Providing integration via **OpenID Connect + OAuth 2.0** will require custom development to map elements within the external provider to AMPP roles.

Embedding AMPP or AMPP Components

AMPP can be embedded into any customer system for a unified user experience.

Providers must support embedding into I-Frames within AMPP to allow for SSO to work smoothly.

Embedding AMPP with SSO will therefore require professional services to confirm whether the provider can support AMPP. Grass Valley can work with customers to help them provide and validate such an integration.

Summary of SSO Support by AMPP

The following table describes the SSO providers supported by AMPP and the charging structure:

Provider	Type	Fee	Professional Services	Comments
Okta	Configuration	YES	NO	Configuration ~2 days
Azure AD	Configuration	YES	NO	Configuration 2-4 days*
OpenID Connect + OAuth 2.0	Bespoke	YES	YES	Requires both configuration and bespoke development
SAML	TBA	YES	TBA	Coming soon

* We support one single method of mapping roles, if this is different, bespoke integration is required.

Summary

SSO is becoming the standard method for dealing with increasing password complexity as systems become more decentralized. Integrating to an SSO system gives you a single way of managing user credentials, increases security, and decreases the IT burden so more time can be given to core tasks.