Single Sign-on in Security

Single sign-on (SSO) is an identification system that allows users to access multiple applications and websites with one set of login credentials. SSO is a key weapon in the battle for security in the enterprise. A successful implementation of SSO reduces the opportunities for hackers and cybercriminals to access your sensitive corporate data.

The benefits of using SSO include:

- Reduce the risk of accessing third-party websites (user passwords are not stored, or managed externally).
- Reduce password fatigue from different username and password combinations.
- Reduce the time spent re-typing passwords for the same identity.
- Reduced IT costs due to fewer password-related calls to the IT help desk.

Security and compliance benefits of SSO

Usernames and passwords are the main target of cybercriminals. Every time a user logs in to a new application, it's an opportunity for hackers. SSO reduces the number of attack surfaces because users only log in once each day and only use one set of credentials.

Reducing login to one set of credentials improves enterprise security. When employees have to use separate passwords for each app, they usually don't. In fact, 59% use the same or similar passwords on multiple accounts. Thus, if a hacker gets access through one poorly secured website, they are likely to be able to access other corporate systems.

SSO helps with regulatory compliance, too. Regulations, such as Sarbanes-Oxley, require that IT controls are documented and that organizations prove that adequate methods are in place to protect data. SSO is a way to meet requirements around data access and antivirus protection.

SSO can also help with regulations, like HIPAA, that require effective authentication of users who are accessing electronic records or who require audit controls to track activity and access. Regulations, like HIPAA, also require automatic logoff of users, which most SSO solutions enable.

When SSO is part of an identity and access management (IAM) solution, it utilizes a central directory that controls user access to resources at a more granular level. This allows organizations to comply with regulations that require provisioning users with appropriate permissions. UAM systems enable SSO with role-based access control (RBAC) and security policies. This type of SSO solution also deprovisions users quickly—or even automatically—another common compliance requirement meant to ensure that former employees, partners, or others can't access sensitive data.

How Yealink use SSO to provide secure solution?

There are many usage scenarios for SSO: Both C/S and B/S architecture systems can be used, which usually support quick configuration and use. On the Yealink device management platform, Yealink uses OAuth2 and CAS protocols to realize the single sign-on function and provide customers with device security management solutions.

OAuth2

OAuth2 is an authorization protocol that allows third parties (clients) to access

content owned by a user (hosted in trusted applications, server resources) without them having to drive or know the user's credentials. That is, third-party applications can access content owned by the user, but these applications do not know the authentication credentials.

CAS

Centralized Authentication Service (CAS) is a SSO protocol for the World Wide Web. Its purpose is to allow a user to access multiple applications while providing credentials (such as username and password) to the authentication server only once. In this way, not only does the user not need to repeatedly authenticate when logging in to the web application, but also these applications cannot obtain sensitive information such as passwords. "CAS" also refers to software packages that implement the protocol.

If you have any security-related queries or requests, feel free to contact the Yealink security team at security@yealink.com