EnterpriseOne Single Sign-on (SSO) Options using JWT

P-051289

We help our customers realize IT

Cloud Hosting

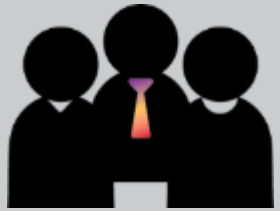
Public, private and hybrid cloud solutions

Managed Services

ERP system management with first-rate response times

AI & Generative AI

Integrating your business data with emerging technologies



JDE Consulting

Develop, implement, and support JDE applications

ERP Suites Products

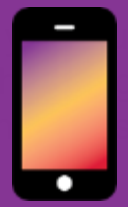
ORACLE
JD EDWARDS

Clarity

Synthetic monitoring and alerting to help JDE system admins

Scanability

Fast ROI with modern JDE barcode scanning



Mobility

JDE data and task management to mobile devices

ERP Suites Services

Business Advisory Services

- Project Management
- Technical Strategic Roadmapping
- Enterprise Architecture Strategy
- Systems Gap Analysis
- Process Engineering
- Organizational Change Management
- Digital Transformation
- Analytics & Insights Strategy

Functional Consulting Services

- JDE Distribution & Warehousing
- JDE Manufacturing
- JDE Financials
- JDE Human Capital Management
- Managed Services
- UXOne Expertise
- User Defined Objects
- Orchestration Design & Build

Technical & Infrastructure Services

- Technical Refresh
- Technical Upgrades
- Cloud Migrations
- IBM iSeries Administration
- Cloud Administration
- Networking & Server Infrastructure
- Identity Management
- Cybersecurity

Trusted Advisors

For JDE Users

unlocking efficiency | boosting profitability

ORACLE | Partner

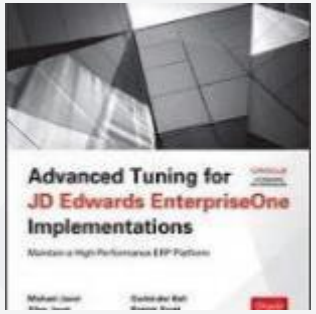
erp suites realize IT

Introduction

- **Frank Jordan** Director JD Edwards Technology

ERP Suites

- Works with ERP Suites Consulting, AI/ML, Cloud and Products divisions for products/services
- Over 28 years CNC experience with 350+ customers
- AI/ML, Orchestrations, AIS and E1/Composed Pages experience
- Private cloud (ERP Suites), Oracle Cloud, AWS and Azure
- Co-author Advanced Tuning for JD Edwards EnterpriseOne Implementations

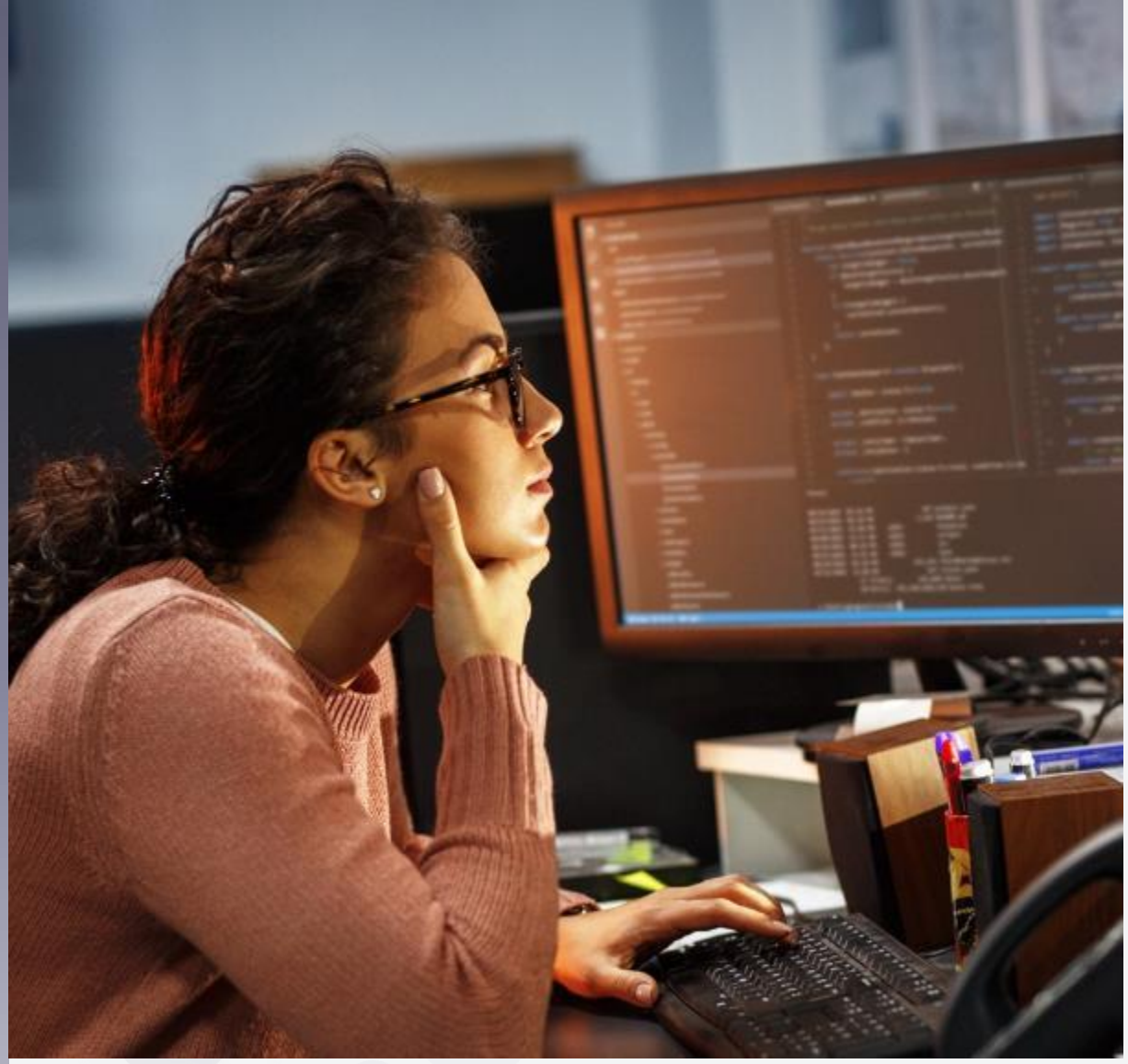


Agenda

- E1 Sign on Overview
- E1 default login options
- E1 LDAP
- E1 Single Sign on (SSO)
- E1 JSON Web Token (JWT) SSO
- Questions

E1 Sign on Overview Authentication Options

1. Base/Standard E1 Authentication (Default option using E1 user/password)
2. E1 LDAP authentication (Leverages a LDAP V3 compliant system such as Active Directory) All or nothing integration
3. Single Sign On (SSO)
    - Oracle Access Manager (OAM) or Oracle Identity Cloud Service (OICS) uses headers and certified by Oracle/JDE
    - Third party solutions – Everest International SSO, Okta application gateway, etc.
    - JSON Web Token (JWT) – OpenID Connect/OAuth 2.0 standards based (Microsoft Azure AD/Entra ID, Okta/Auth0, Oracle OAM/Identity Cloud Service IDCS, etc.)



E1 Default Login

E1 Default Options

1. Base/Standard E1 Authentication has short/long user and password options. Default legacy of 10-character user/password
2. E9.2 tools can provide long user/password which has case sensitive passwords and up to 40 characters Lower case long user storage (min 6/max 254 characters)
3. E1 roles and audit columns are still based on the short user id to maintain backward compatibility. Long user/password mainly for authentication purposes. Means you must always have a short user id and long user is optional unless you have authentication requirements for them
4. Once long user and/or password is enabled some security apps change such as P0092 to P0092L and P98OWSEC to P98LPSEC

E1 Default Options

1. E1 default login leverages the Enterprise server security kernel for authentication and verifies the encrypted user/database password. E1 LDAP and certain SSO options may not access the user password. This means that user password expiration may occur to disable the account for any of the authentication methods that allow the E1 user/password to be used. (E1 default and JWT SSO for example)
2. Global password policy available for items such as
    - Daily password change limit
    - Minimum password length
    - Minimum number of characters
    - Minimum number of numeric
    - Maximum number of consecutive characters
    - Minimum number of special characters

E1 Default Options

1. E1 default login can be an effective security framework in many customer situations
2. E1 security documentation and Oracle support has many additional details on the features. A good support document of E1: SEC: FAQ on User Profiles, System Users, Password, Global Password Policy and Sign-on Security (Doc ID 2236129.2) or the E1 Security document is an example
3. This security feature is the “tried and true” option that most customers begin with and is the foundation for other login options

E1 LDAP

E1 LDAP

1. E1 Lightweight Directory Access Protocol (LDAP) has been available for many years to integrate with third party LDAP V3 compliant directory services (Such as Microsoft Active Directory)
2. E1 LDAP is an "all or nothing" authentication where ALL E1 users must be defined in the controlling LDAP. All accounts must be defined in the LDAP including those for the E1 services.
3. The E1 user definition and password is controlled in the LDAP. E1 LDAP will add a newly defined LDAP user to E1 with a default _LDAPDEFLT role. The security admin will then need to assign the desired E1 role(s) for that user.

E1 LDAP

1. The E1 user profile application P0092 will become disabled since user management occurs in the LDAP.
2. Roles can also be maintained in LDAP, but majority of E1 customers control this within EnterpriseOne since there is no ability to replicate changes or delete them from LDAP easily. Mainly just the user/password authentication is leveraged
3. One negative of E1 LDAP is that LDAP users are only added and no automated method to remove the E1 user without some workarounds such as a dedicated Enterprise server with LDAP Authentication disabled to allow the use of P0092. Other option is the Batch synchronization UBE R9200040 which removes/adds ALL the E1 users in the search.
4. The R9200040 UBE usage urges caution due to how it removes/adds users

E1 LDAP

1. Oracle generally recommends to disable E1 users instead of deleting them for several reasons such as audits, audit field data, etc.
2. E1 LDAP to Microsoft AD/LDAP is a common use case that many customers leverage with good success
3. E1 LDAP does not use/update the E1 security table password for the users which can be a concern if multiple Enterprise servers have a mix of LDAP enabled on production and disabled for non-production
4. E1 security documentation and Oracle support documents such as E1: LDAP: FAQs on LDAP (Lightweight Directory Access Protocol) Configuration with EnterpriseOne (Doc ID 2234115.2)

E1 Single Sign On (SSO)

E1 Single Sign On (SSO)

1. Oracle has SSO available and certified with Oracle Access Manager (OAM) and Oracle Identity Cloud Service (OICS).
2. Several third-party solutions are also available from OKTA/Auth0, Everest International (JDESSO), SSOGEN, OneLogin, Steltix Transparent Logon X10, etc.
3. Most of these solutions have some type of gateway/proxy server to work with the identity provider for an additional cost
4. The use of SSO provides a more centralized repository and ease of authentication for the users across multiple applications
5. May require additional expertise and time to implement these solutions depending on the identity provider software in use. There is usually increased complexity and effort to implement.

E1 Single Sign On (SSO)

1. Some solutions can handle web, AIS, fat clients while most are web-based solutions.
2. OAM and OICS per the E1 security document provide both authentication and authorization services. Using authorization services has OAM/OICS examine each URL submitted by the user which does have additional overhead/performance implications. ERP Suites typically suggests leveraging just the authentication services to eliminate this overhead unless there are business/security requirements
3. Third party solutions are typically not certified by Oracle, but they can leverage the SSO configuration support used for OAM/OICS if they have http header-based authentication at the web level

E1 Single Sign On (SSO)

1. There are many customers that use SSO for the E1 web and additional security features such as multi-factor authentication (MFA) or conditional access the IDP can provide
2. E1 security documentation and Oracle support documents such as E1: LDAP: Frequently Asked Questions on Configuration of Single Sign On (SSO) Through Oracle Access Management (OAM) with EnterpriseOne (Doc ID 2157524.1) provide good suggestions and information
3. The E1 Security document also has extensive configuration information for OAM as well

E1 JSON Web Token (JWT SSO)

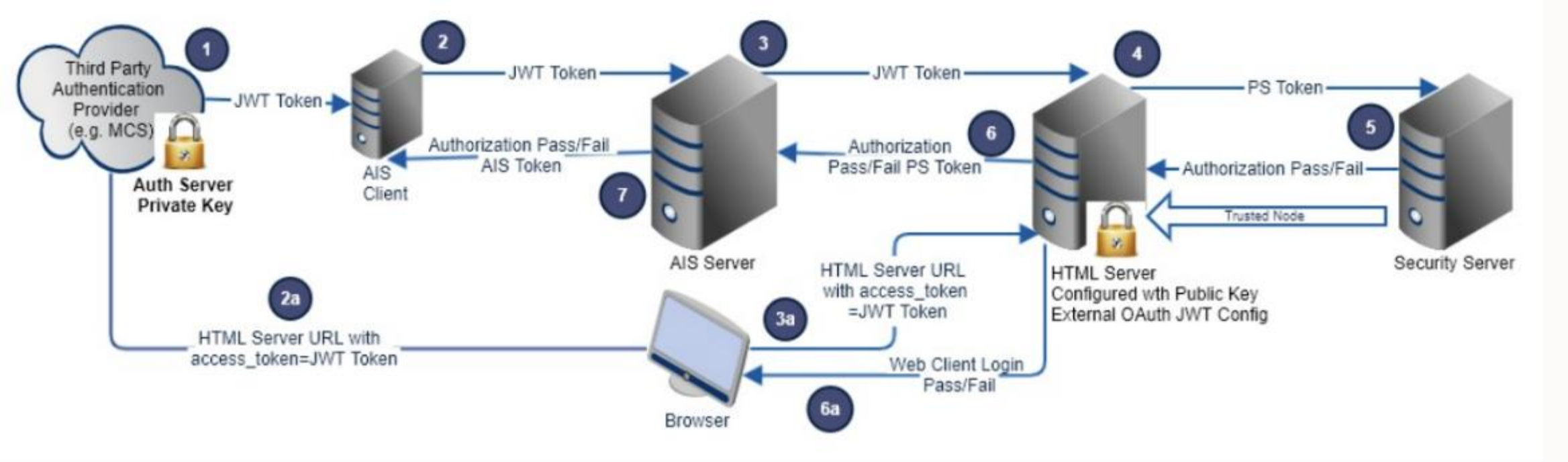
E1 JSON Web Token (JWT SSO)

1. E1 has the capability of using JSON Web Token authentication based on OAuth2.0 or OpenID Connect standards
2. Application Interface Services (AIS) has included the JWT option since early E1 tools 9.2.0.5 with several enhancements along the way. AIS is used for Orchestrations
3. Java Application Server (JAS/HTML) has the JWT option since tools 9.2.5.4 and later. This is a key enhancement to allow various identity providers (IDP's) such as Microsoft Azure AD, Okta/Auth0 and others to provide authentication services to E1 authorized resource

E1 JSON Web Token (JWT SSO)

1. E1 JWT leverages an Identity Provider (IDP) that can generate an OAuth2.0 JSON Web Token such as Microsoft Entra ID/Azure AD, OKTA/Auth0, etc.
2. The IDP presents a sign-on page based on the URL provided that will authenticate the user. It then passes a JWT access token to E1 HTML in the URL that is encrypted with the verification of a valid user
3. Once logged in the E1 application behaves like traditional E1 default login
4. Some IDP systems provide a certain time frame where future logins can occur without signing in again (Cached). Example Microsoft Entra ID/Azure AD with Office 365 login process

E1 JWT Authentication Flow example



(Release 9.2.5.4 and later) The following steps describe the HTML authentication flows:

1. A third party authentication provider generates a JWT with private key.

2a. The JWT is sent in the access token URL parameter of the HTML server (E1Web Client) URL.

3a. The JWT is forwarded to the EnterpriseOne HTML by the browser through the URL parameter.

4. The JWT is validated against the public key, the token timeout is validated, and the principal (user) is extracted from the JWT payload. A PSToken is generated for that user and sent for authorization by the Security Server (EnterpriseOne Enterprise Server).

5. The Security Server checks the PS token with SSO node trust, and then an authorization response is returned to the EnterpriseOne HTML Server.

6a. The authorization response is returned to the browser, and user is logged in to the Web Client or the login has failed.

7. The authorization response is returned to the AIS client (third-party). If passed, for a token request the response includes an AIS token.

E1 JSON Web Token (JWT SSO) Requirements

1. E1 Apps 9.2 with Tools 9.2.5.4 and later
2. E1 Long userid support enabled since typical user will be an e-mail name. E1 user should be created/configured with an associated long userid which maps to a claim of upn, sub or prn.
3. E1 SSO node lifetime for GLOBALNODE record must be configured
4. Identity provider (IDP) is needed to create the token and has private/public key. IDP can also provide MFA feature since E1 does not have this capability
5. AIS and HTML typically need web instance SSL ports configured due to security requirements. If E1 has references to non-SSL URL's some issues may occur getting to that link

E1 JSON Web Token (JWT SSO) Advantages

1. Both JWT SSO and E1 default login can be used.
2. JWT SSO and E1 LDAP is also a configuration option as well.
3. JWT SSO typically does not require any gateway/proxy server like OAM/OICS provides
4. OAuth2.0/OpenID Connect web framework is used by many companies.
5. Allows you to leverage additional features of your identity provider such as MFA or conditional access
6. Since most IDP's are cloud service the complexity is significantly reduced to configure and implement
7. Microsoft Entra ID/Azure AD is used by many companies for their LDAP services so E1 can become just another custom application (If you have Office 365 that usually implies Entra ID/Azure AD is present)
8. Can be used with default *ALL role or role chooser (HTML instance decision)

E1 JWT SSO Microsoft Entra ID/Azure AD Caveats

1. Entra ID/Azure AD custom application registrations by default leverage a public rolling key provided by Microsoft. These signing keys can change without notice and current E1 JAS/HTML instance external keystore does not dynamically update/support new public keys without an instance recycle. This can create some user frustration when a rolling public key changes and the JAS external keystore must be manually updated/recycled
2. In November 2023 Microsoft published documentation regarding the use of a custom signing key instead of the public rolling keys. This feature allows the customer to create a self-signed certificate that is loaded into the custom app registration service principal object that can have the certificate expiration set between 1 to 10 years. This private/public key is only used by the custom app registration and the E1 JAS instances that have the public key loaded. No more rolling key and the customer owns the private/public key used for this specific purpose. The details are at https://learn.microsoft.com/en-us/entra/identity-platform/jwt-claims-customization?WT.mc_id=Portal-Microsoft_AAD_IAM#security-considerations
3. ERP Suites has been able to test and implement custom signed keys for many customers using Entra ID/Azure AD E1 JWT SSO. The results have been very positive and stable.
4. Other business partner solutions add some complexity with a certificate proxy server to handle the public rolling key instead of the custom signing key option.
5. An enhancement request into Oracle has also been submitted to provide an external keystore cache refresh command via Server Manager to eliminate the need to recycle the E1 HTML instance. No ETA date currently known

E1 JSON Web Token (JWT SSO) Disadvantages

1. Only works for E1 web applications such as AIS/Orchestrations and HTML users. No fat clients, but E1 default login/LDAP can be used outside of web or other use cases such as a Scheduler and integrations
2. The E1 user may need to maintain their E1 password unless the password is hidden, and a limited knowledge strong password is used with no password expiration. It can be same as the Windows/IDP password in most situations, but potentially confusing to the user.
3. E1 LDAP uses the password from your LDAP so no expiration present
4. Shortcut or Parameterized URL's are not currently supported for JWT SSO Traditional E1 login needed. Workaround is to login to E1 BEFORE clicking on the shortcut/parameterized URL
5. No automated method currently available to update the external Java store HTML SSL certificates used by JWT so manual process/updates are needed at least yearly unless you craft a custom signed key with a longer expiration such as 10 years

E1 JWT/OAuth2 Implementations

- Some JDE Business partners have also implemented JWT for AIS or HTML
- Fusion5 with Shannon Moir has a CNC blog article with some ideas https://shannonscncjdeblog.blogspot.com/2022/02/using-oauth-jwt-to-log-into-jde.html
- Circular Edge presented at InFocus 2022 regarding JWT for HTML linking to Microsoft Azure AD
- ERP Suites has customers in Production using JWT for AIS or HTML using OKTA/Auth0 and Azure AD in cloud
- The general process flows for JWT/OAuth2.0 is similar, but there are differences for each identity provider

Why use E1 JWT SSO?

It makes financial sense.

You can maintain the password in one place instead of E1. Less maintenance involved with an identity provider

It improves performance.

E1 user login can be streamlined depending on the Identity provider options

It provides options.

You can have more consistent policies with authentication being controlled within an identity provider such as multi-factor authentication (MFA)

Assess and form a strategic plan

- *Do you need to update your E1 system to a level that supports JWT on HTML? Long userid, tools 9.2.5.4, etc.*
- *What identity provider is in use? (Microsoft Entra ID/Azure AD, Okta/Auth0, OAM/IDCS, etc.) Older IDP's can be higher cost/complexity to implement*
- *What are your security policies and features available/desired?*

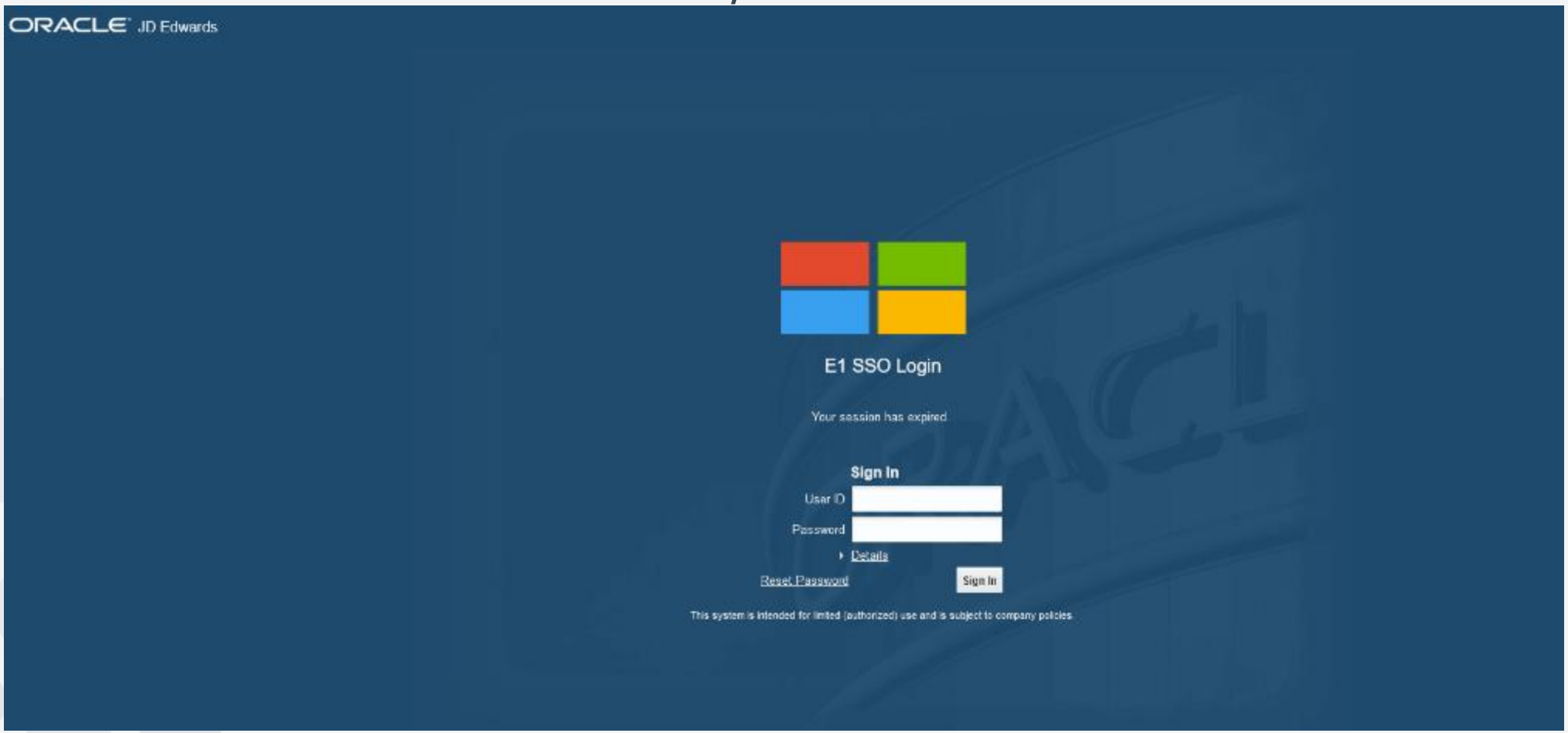
Summary

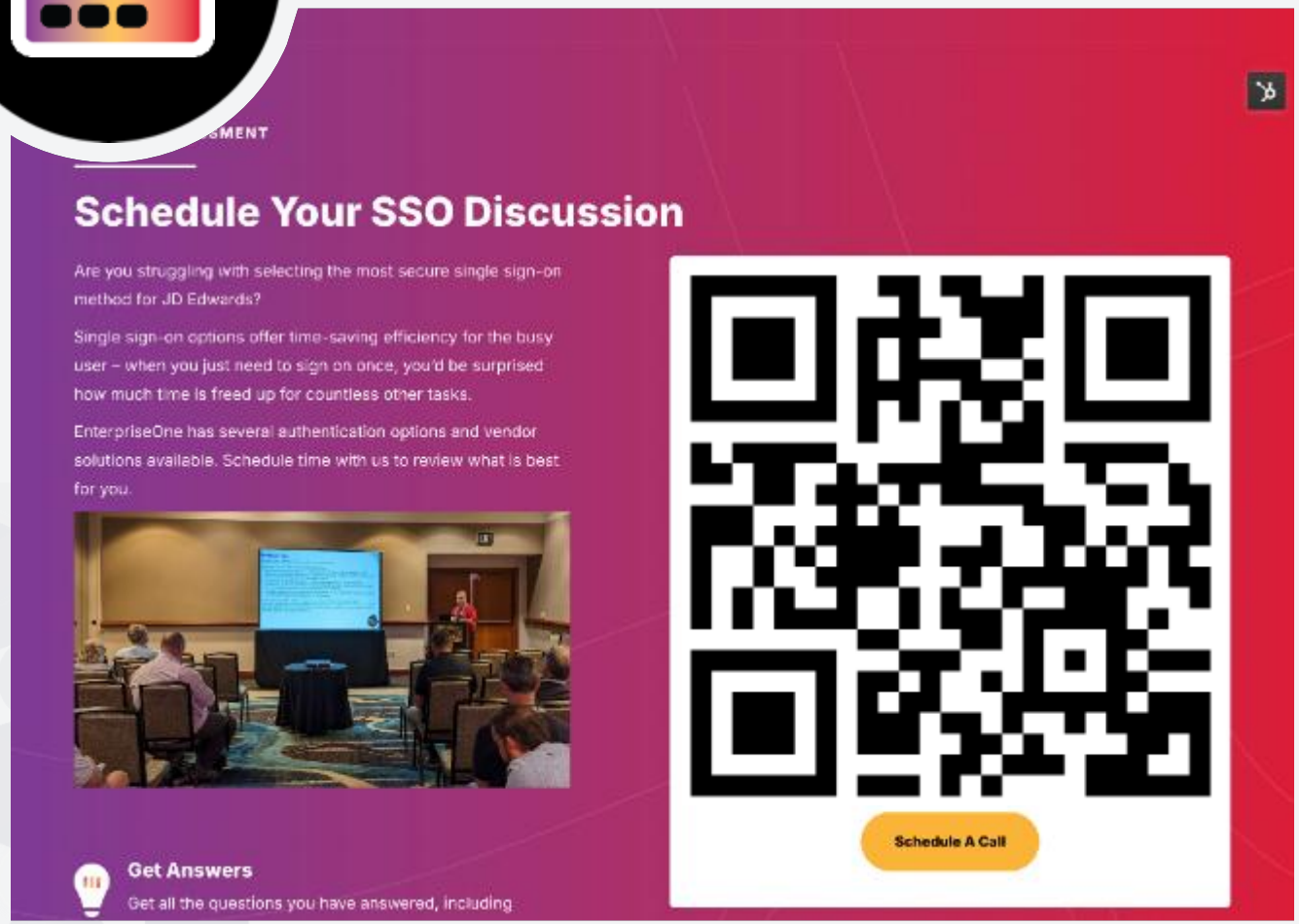
- EnterpriseOne has several authentication options and vendor solutions available
- The newer JWT option provides a very good single sign-on (SSO) option for many companies that can be very cost effective.
- Most E1 customers leverage Microsoft AD or ADFS/Active Directory for Office 365 and with JWT this opens the door for SSO/MFA through Entra ID/Azure AD

erp suites
realize IT

Demo

- Demo of E1 JWT SSO with Entra ID/Azure ID





Schedule SSO Discussion

Get answers about JDE SSO

- Requirements
- Do you need to upgrade
- How much it could cost
- What identity providers
- Security features desired
- and more

Get Started

erpsuites.com/SSO

sales@erpsuites.com

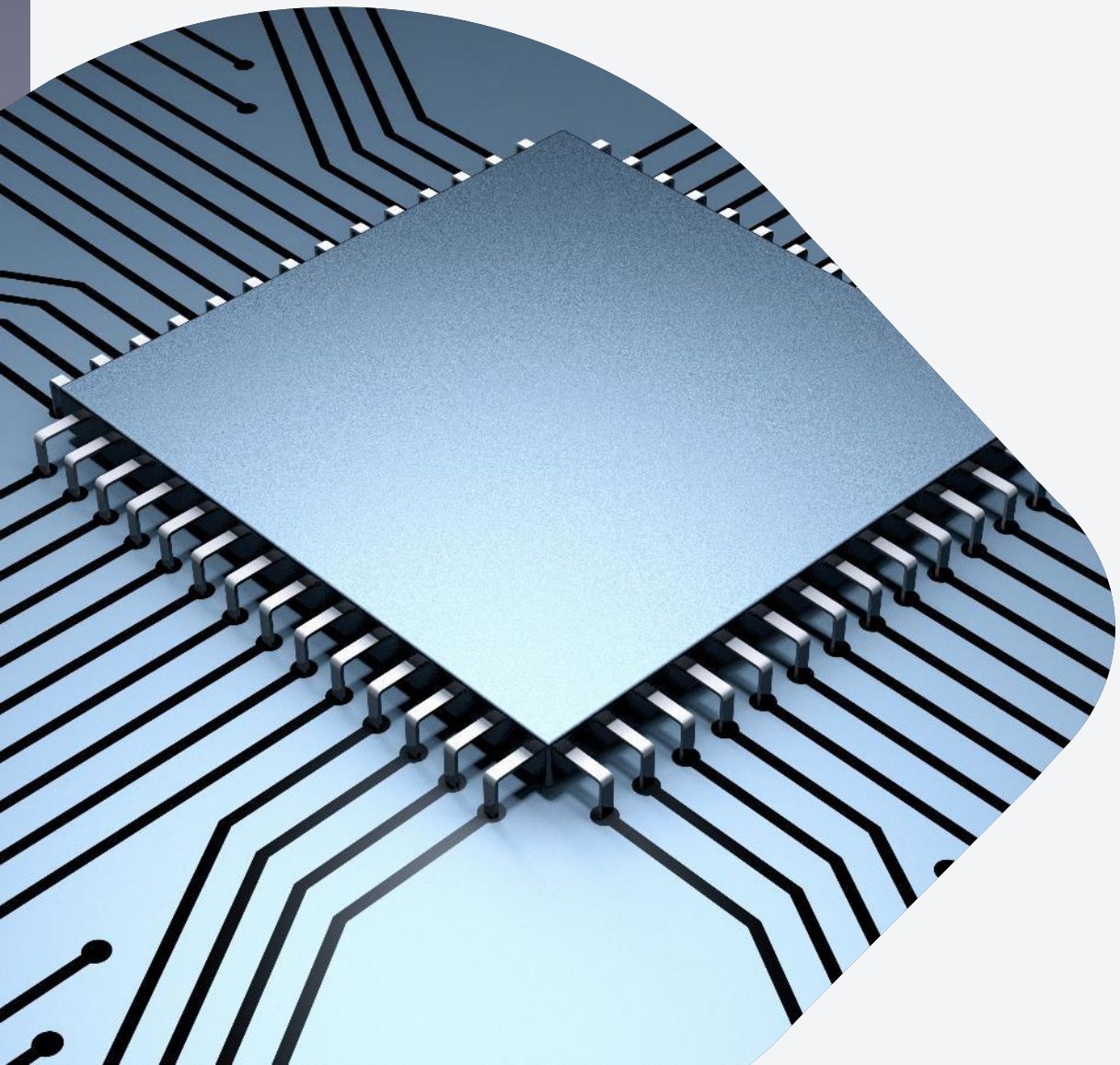
erp suites

realize IT

Questions?

- fjordan@erpsuites.com

- Session ID: P-051289



erp suites

realize IT

LOVE THIS SESSION?

COMPLETE AT LEAST **3 SESSION SURVEYS** PER DAY AND GET ENTERED INTO THE DAILY DRAWINGS TO WIN A **$500** GIFT CARD!

Bibliography

- E1 documentation, Oracle support documents, learnjde.com
- Fusion5 with Shannon Moir has a CNC blog article with some ideas https://shannonscncjdeblog.blogspot.com/2022/02/using-oauth-jwt-to-log-into-jde.html
- Circular Edge presented at InFocus 2022 regarding JWT for HTML linking to Microsoft Azure AD

ERP Suites In Numbers

realize IT

Our Team:

500+ Years of Experience

Our team consists of some of the best in the industry. We are the experts who have actually written the book on the many domains we serve.

100+ People Dedicated to You

Our team numbers over 100 people across all of our domains. With 24/7 operations for your most critical enterprise technology, the ERP Suites team has your back.

17+ States With our Presence

Headquartered in Cincinnati, OH, our team is spread across 17 states within the US, providing the coverage of a national firm with the presence and attention of a local office

Our Growth:

23+ Years & Counting

For over 23 years we have been serving the Oracle, Microsoft, IBM, and AWS communities with best-in-class services across the United States

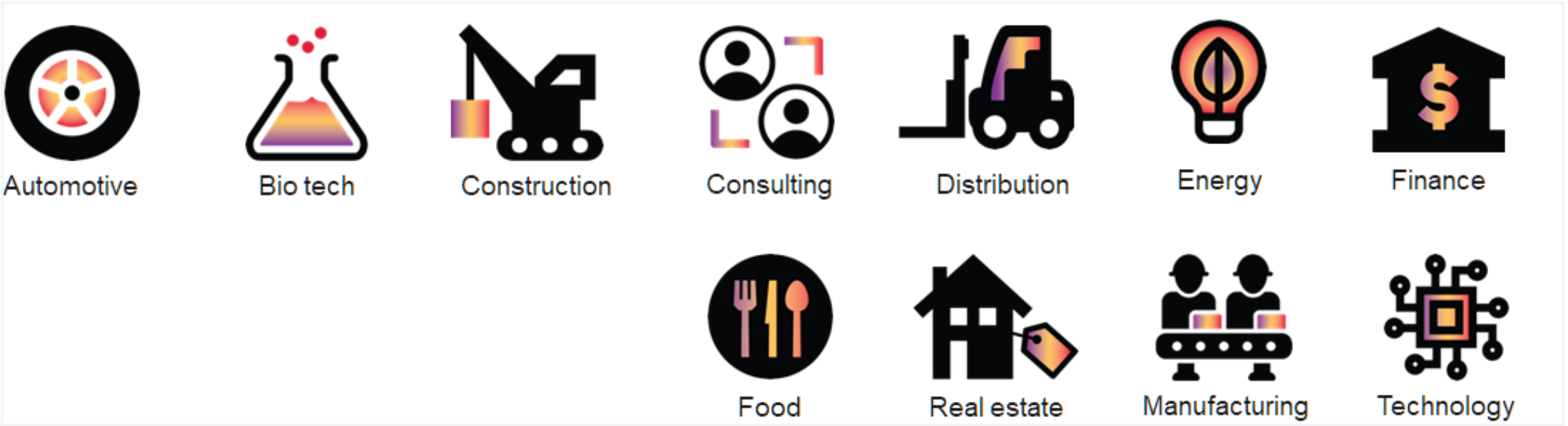
26% YoY Revenue Growth

Our customers continue to trust us with their most critical business applications with a majority of that growth coming from existing customers

18% Headcount Growth

We continue to invest in our people and expand our team in existing and new service areas using our best-in-class talent acquisition methodology

Over 300 companies have trusted us to help them grow



erp suites
realize IT

“…we found that ERP Suites had a reputation of having some of the best JDE resources available.”

BrassCraft®

Mark Labadie, Vice President

erp suites

realize IT

“… working with you all is an absolute delight compared to any experience we ever had with OMCS.”

COLAS

IT Manager

erp suites

realize IT

“A huge differentiator between my previous partner and ERP Suites is the personal interaction.”

WEITZ

Steve McClure, Senior IT Manager

erp suites

realize IT

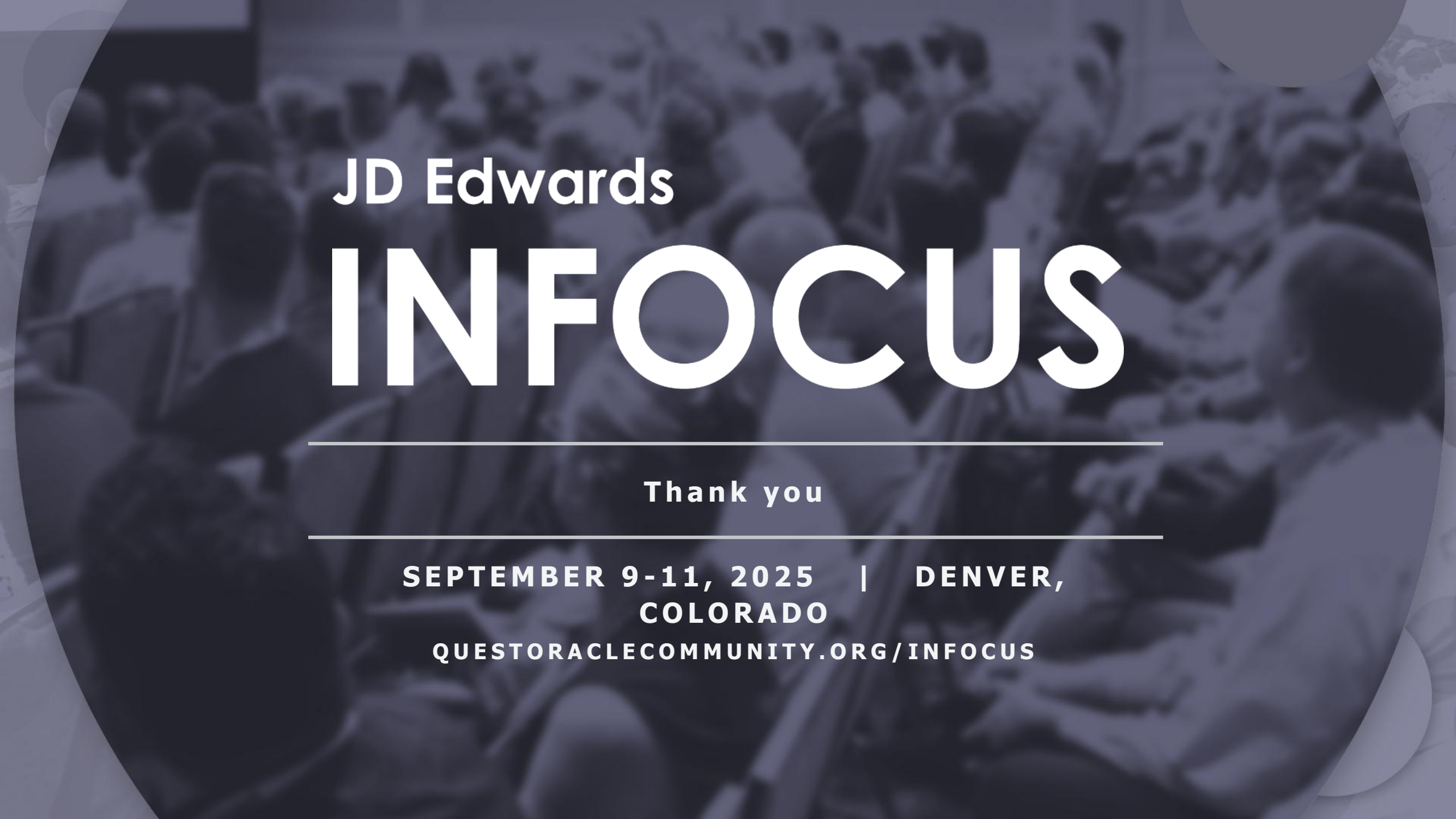
“A huge differentiator between my previous partner and ERP Suites is the personal interaction.”

WEITZ

Steve McClure, Senior IT Manager

erp suites

realize IT


JD Edwards
INFOCUS
Thank you
SEPTEMBER 9-11, 2025 | DENVER, COLORADO
QUESTORACLECOMMUNITY.ORG/INFOCUS