Leveraging SSO with Ellucian CRM using Ellucian Ethos Identity

Introduction

Ellucian CRM applications can be included in an enterprise-wide SSO infrastructure

Doing so requires an understanding of the CRM authentication architecture and supported authentication options

Ellucian Ethos Identity is one option available to all CRM suite customers

Topics

1   Understanding Authentication

2   Authentication Options in Ellucian CRM

3   Ellucian Ethos Identity

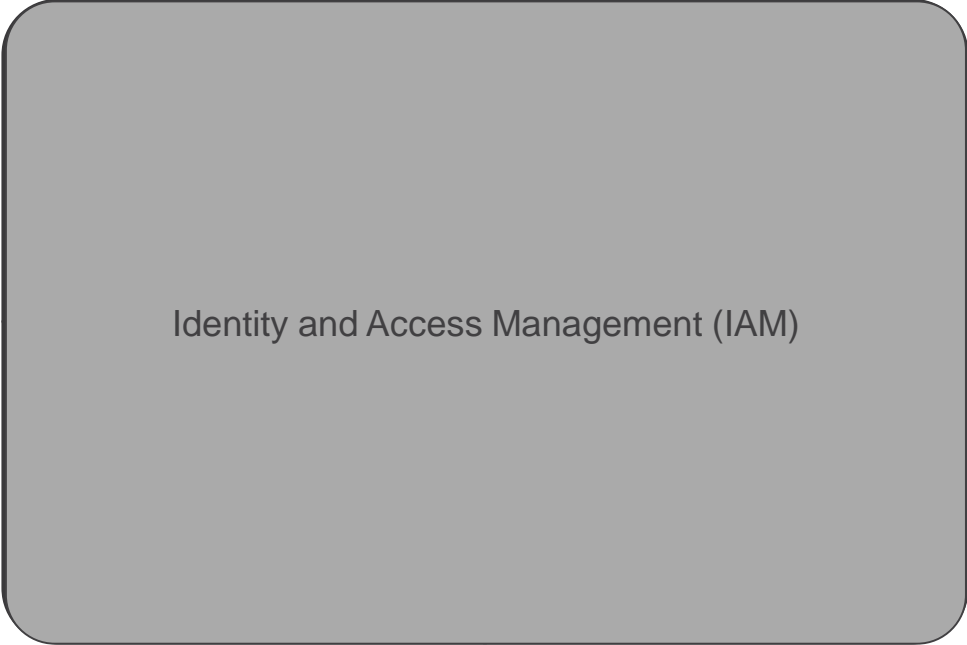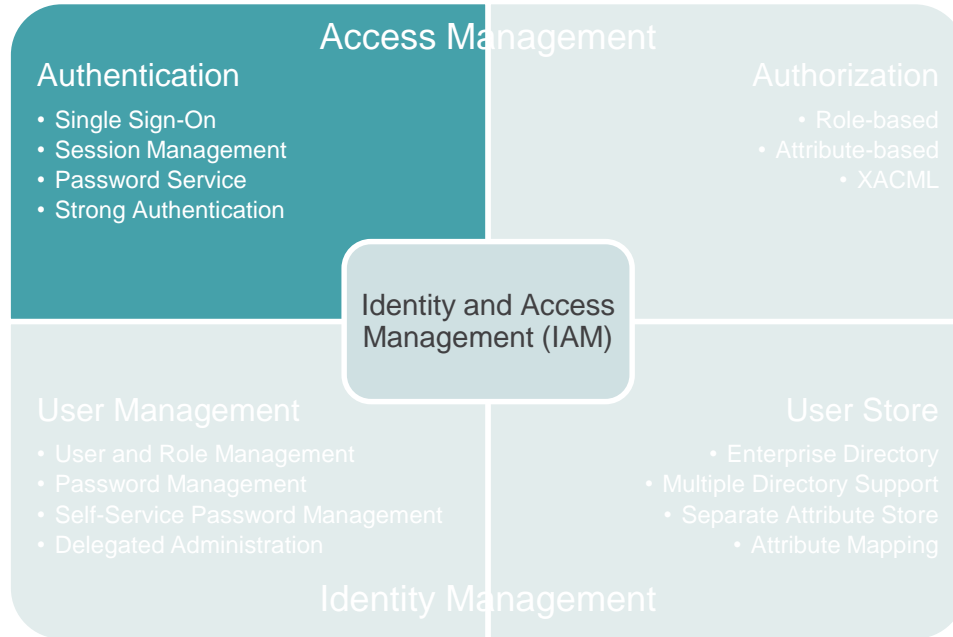**4**   Caveats/Considerations

5   Summary and Questions

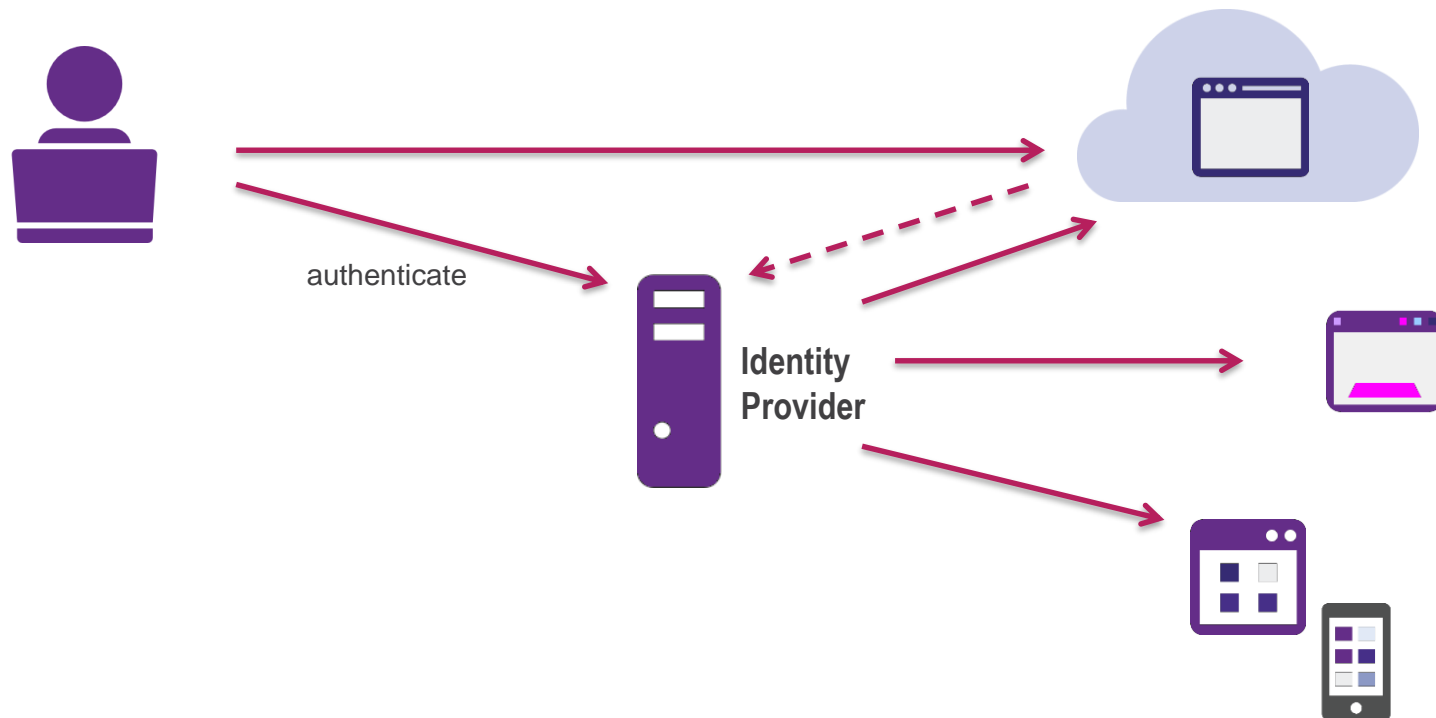# Understanding Authentication

Identity and Access Management

Identity and Access Management (IAM)

Identity and Access Management – Authentication

Access Management

Authentication

- Single Sign-On
- Session Management
- Password Service
- Strong Authentication

Authorization

- Role-based
- Attribute-based
- XACML

Identity and Access Management (IAM)

User Management

- User and Role Management
- Password Management
- Self-Service Password Management
- Delegated Administration

User Store

- Enterprise Directory
- Multiple Directory Support
- Separate Attribute Store
- Attribute Mapping

Identity Management

Generalized Authentication Flow

authenticate

Identity Provider

ellucian.

Authentication Implementation

Variety of protoocls

- SSO Protocols from/for Higher Education
  - CAS (formerly JASIG, now apereo)
  - CoSign (University of Michigan)
  - Kerberos (MIT)
  - Pubcookie (University of Washington)
- SAML 2.0 = SSO for enterprise apps such as Salesforce, Bb, Moodle, etc.
- WS-Federation/WS-Trust = SSO for Microsoft apps such as CRM, SharePoint, Office365, etc.
- OAuth 2.0 = API security such as Facebook, Amazon, LinkedIn, Box, etc.
- OpenID Connect = identity layer on top of OAuth 2.0
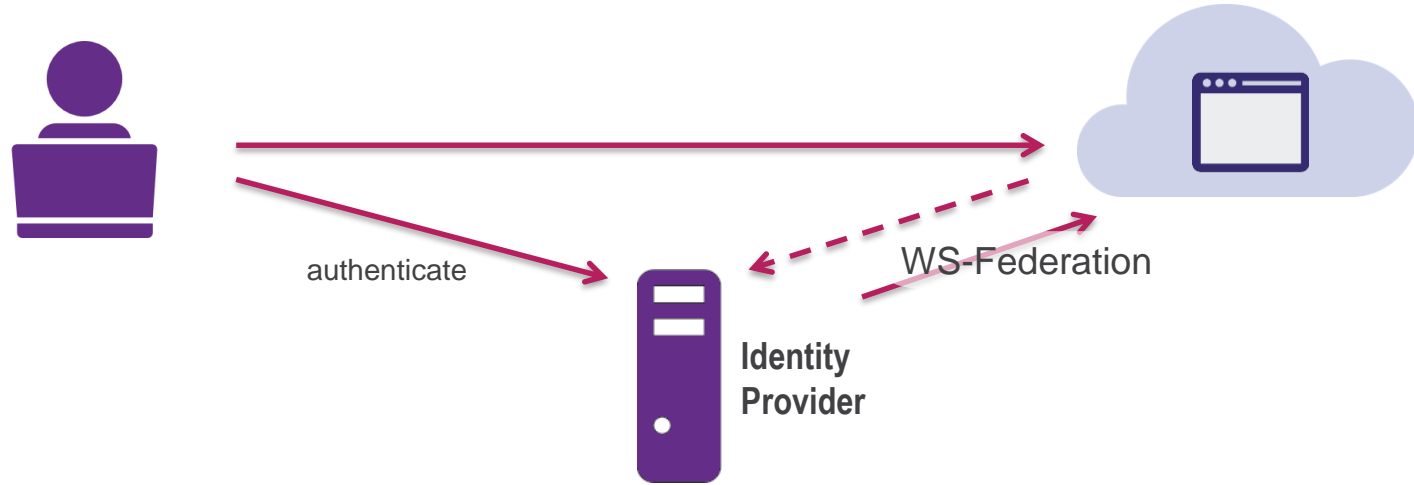
Authentication in Ellucian CRM Suite

ellucian.

Ellucian CRM

Dynamics CRM-based

Supported protocols:

- WS-Federation
  - aka passive-STS
  - Browser-based applications
- WS-Trust
  - aka active-STS
  - Non-browser applications (e.g., Outlook connector)

CRM Recruit	CRM Advise	CRM Advance
Ellucian CRM Core		
Microsoft Dynamics CRM		

ellucian.
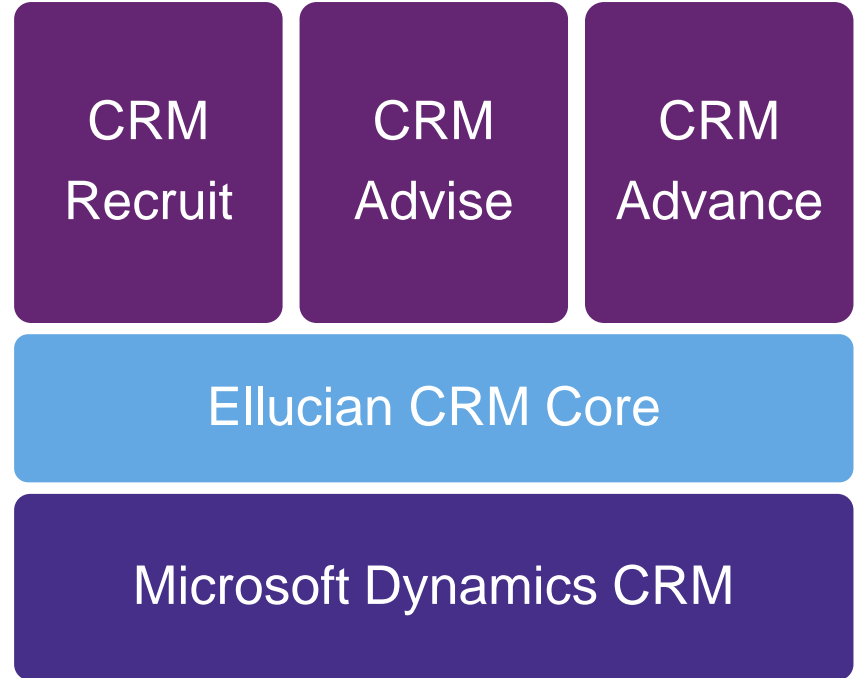
Identity Provider supporting WS-Federation

authenticate

WS-Federation

Identity Provider

Protocol bridge supporting WS-Federation

authenticate

SAML

WS-Federation

Identity Provider

Protocol Bridge
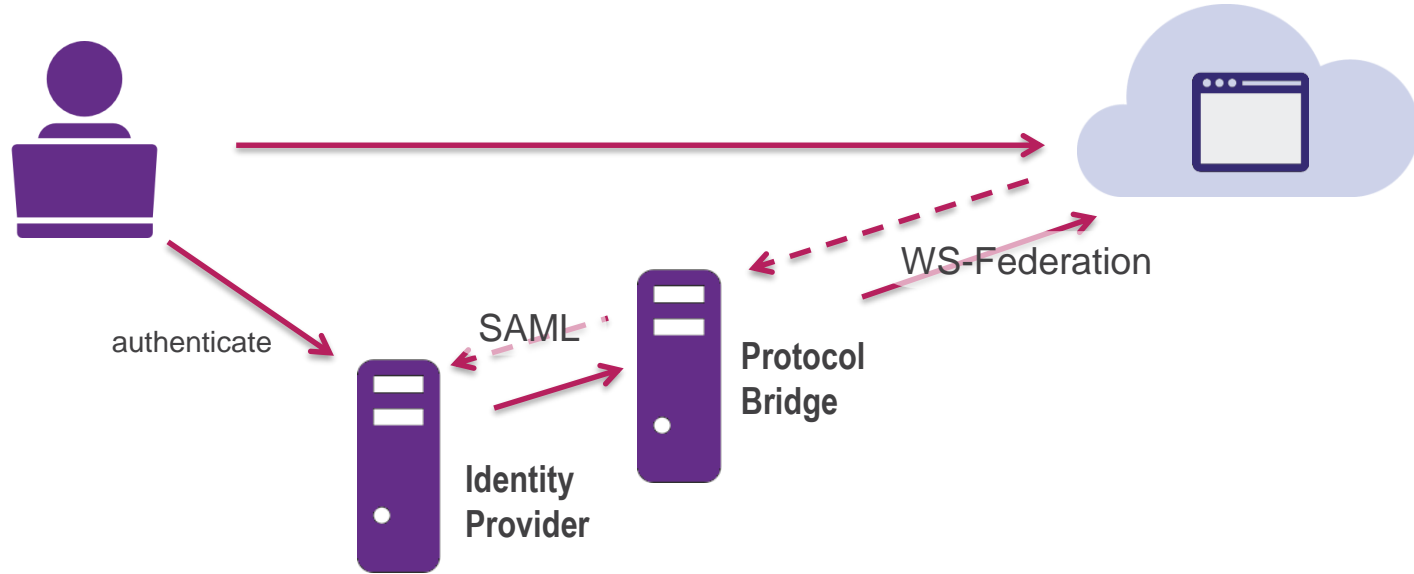
Supported Options

Active Directory Federation Services (AD FS)

- developed by Microsoft

- can be installed on Windows Server operating systems

- provides users with single sign-on access to systems and applications

- claims-based access control authorization model

Ellucian Ethos Identity

- Ellucian-branded version of WSO2 Identity Server

- Multi-platform Java application with embedded Tomcat server

- Supports multiple SSO protocols

- Primary IdP or protocol bridge

Ellucian Ethos Identity

What It's Not

Don't call it "EIS" or "Ellucian Identity Services"

A cloud-based SSO or Identity as a Service (IDaaS) solution

An identity/user-account provisioning agent

An identity governance solution

Ethos Identity Composition

Ellucian Ethos Identity

Ellucian Extensions

- CAS protocol support
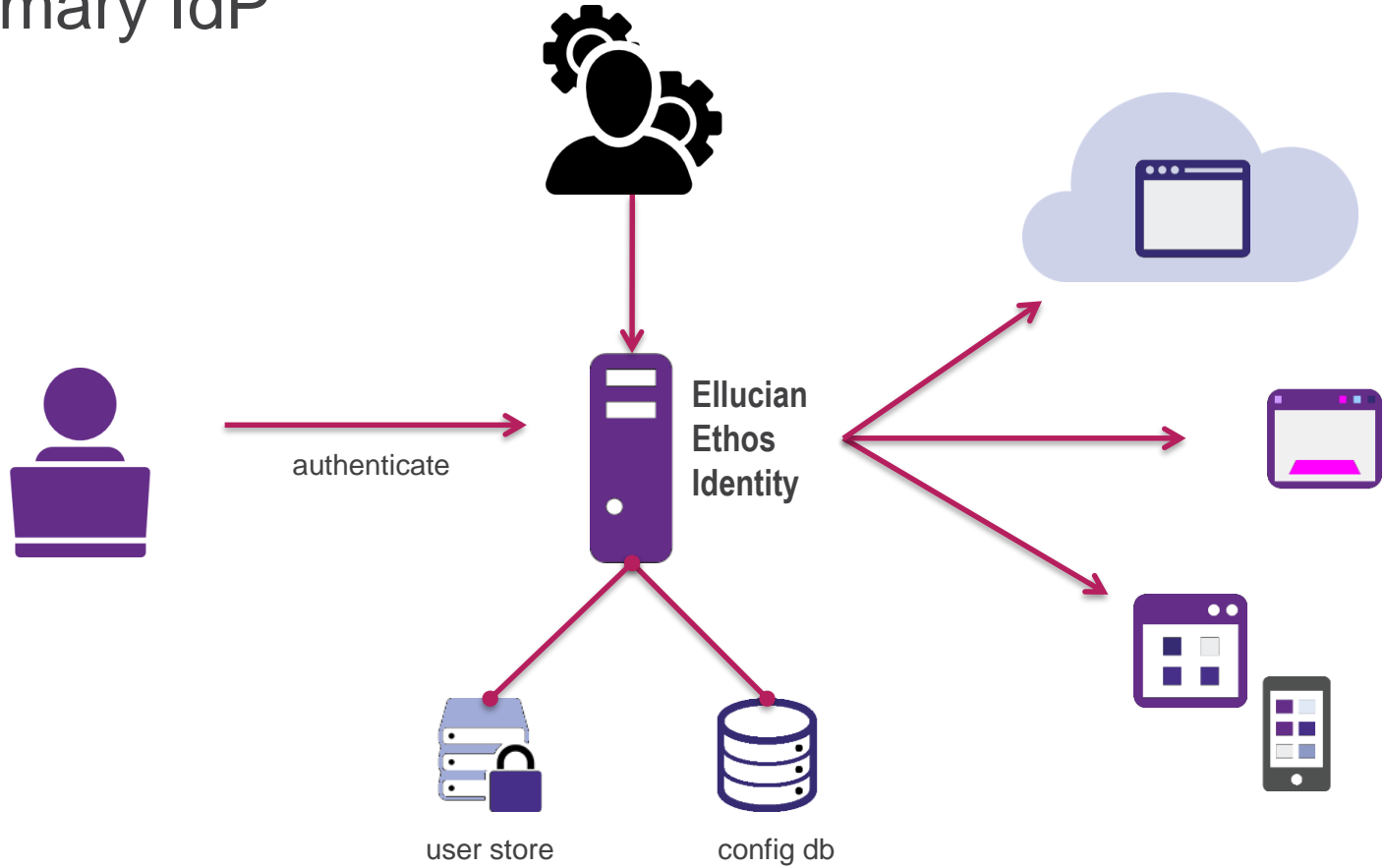- Attribute store support

WSO2 Identity Server

- Administrator Console
- Login pages
- End User Dashboard
- Multi-protocol support
- User store support
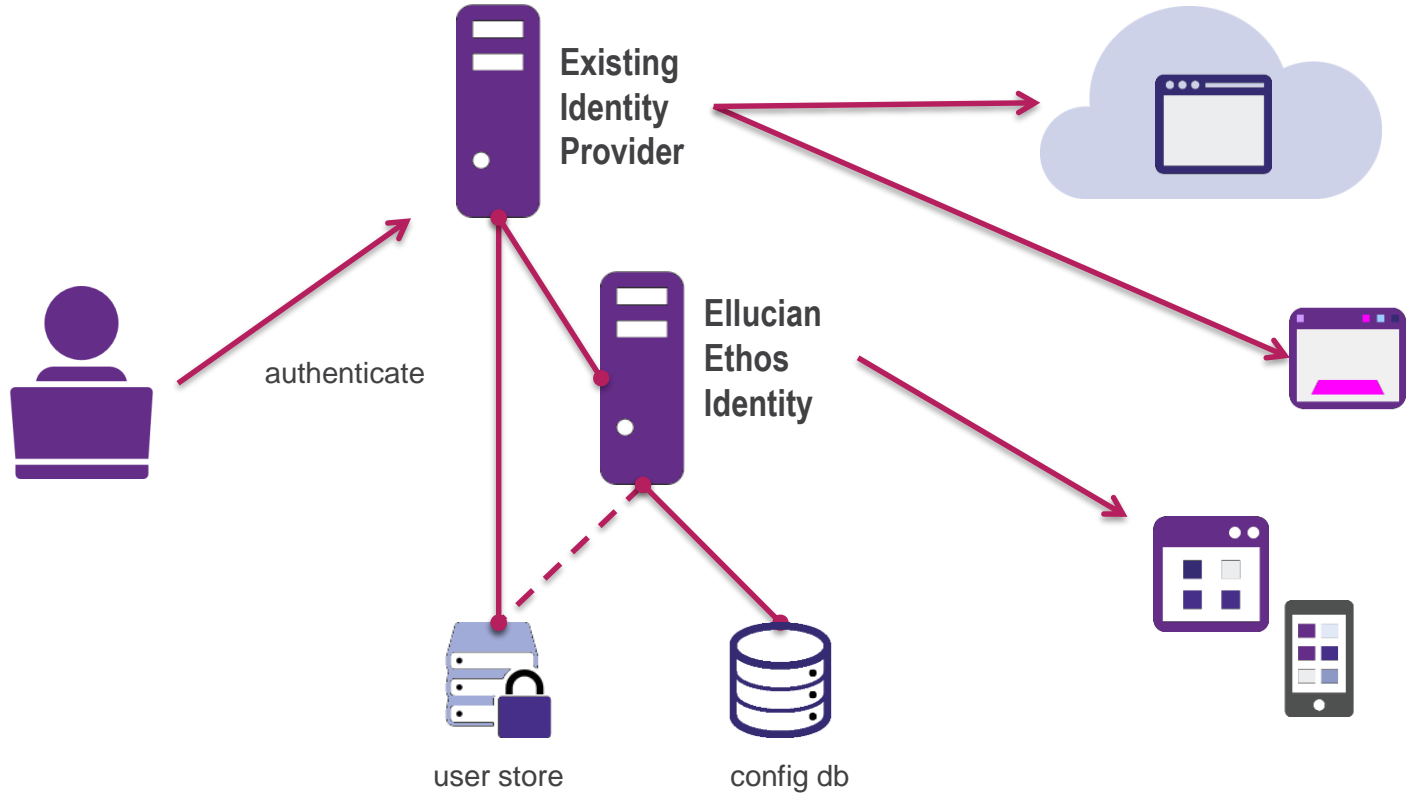- User and Groups Management

Ellucian Extras

- Installer
- Configuration Utility
- Migration Utility
- WSO2 Liaison
  - Patches
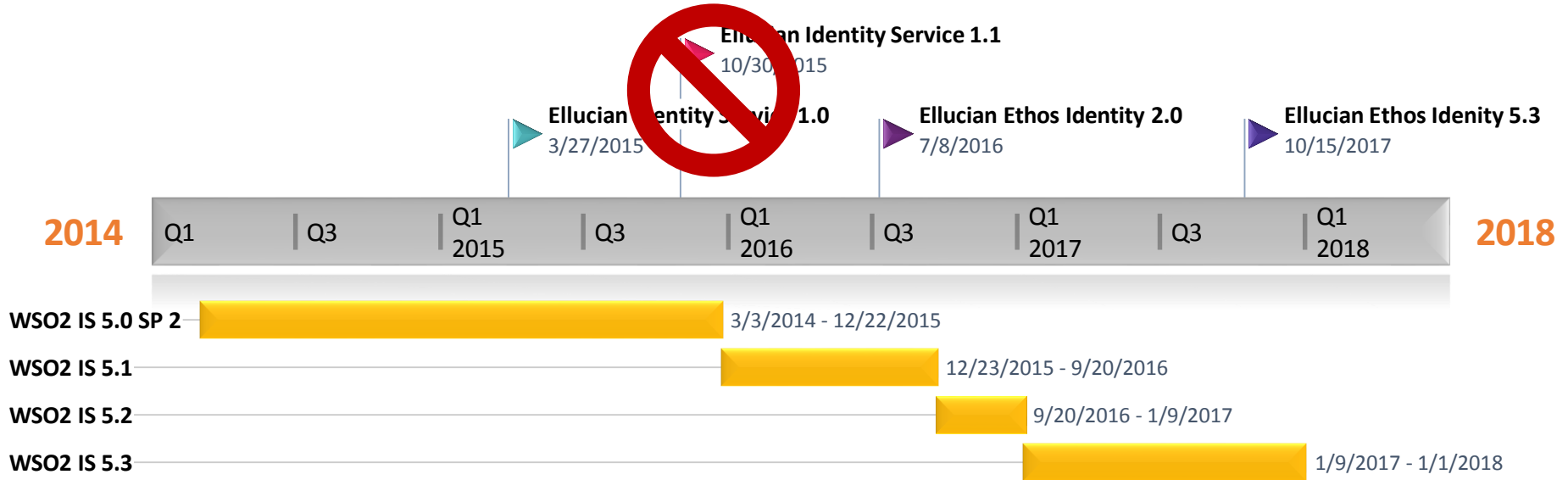 - Testing
  - Bug fixes

As a Primary IdP

authenticate

Ellucian Ethos Identity

user store

config db

ellucian.

As a Protocol Bridge

Existing Identity Provider

Ellucian Ethos Identity

authenticate

user store

config db

ellucian.

Ethos Identity Release History

Ellucian Identity Service 1.1
10/30/2015

Ellucian Identity Service 1.0
3/27/2015

Ellucian Ethos Identity 2.0
7/8/2016

Ellucian Ethos Idenity 5.3
10/15/2017

2014

| Q1 | Q3 | Q1 2015 | Q3 | Q1 2016 | Q3 | Q1 2017 | Q3 | Q1 2018 |

2018

WSO2 IS 5.0 SP 2 — 3/3/2014 - 12/22/2015

WSO2 IS 5.1 — 12/23/2015 - 9/20/2016

WSO2 IS 5.2 — 9/20/2016 - 1/9/2017

WSO2 IS 5.3 — 1/9/2017 - 1/1/2018

Key Enhancements in Ellucian Ethos Identity 5.3.x

Upgrade to WSO2 Identity Server 5.3

- Various security fixes and enhancements
- HTML support for email templates, template internationalization and dynamic properties for email templates
- Upload/Download of SAML Metadata
- SSO Protocols:
  - SAML2
  - CAS
  - WS-Trust
  - WS-Federation
- Enhanced Caching

Additional Bug Fixes from WSO2

Ellucian value-added features

Feature	In IS 5.3?	Part of Ellucian Extensions?
CAS protocol support	🔴	🟢
Change password	🟢	No
Reset password	🟢	No
Full Office 365 support	🟢	No
Dynamics CRM support	🟢	Patch from WSO2
Secondary attribute store	🔴	🟢
ANT configuration scripts	🔴	🟢
Migration from EEId 2.0.x to 5.3	🔴	🟢
End user page internationalization; Translations; RTL support	🔴	No
Clustering	🟡	Documentation

End User Dashboard
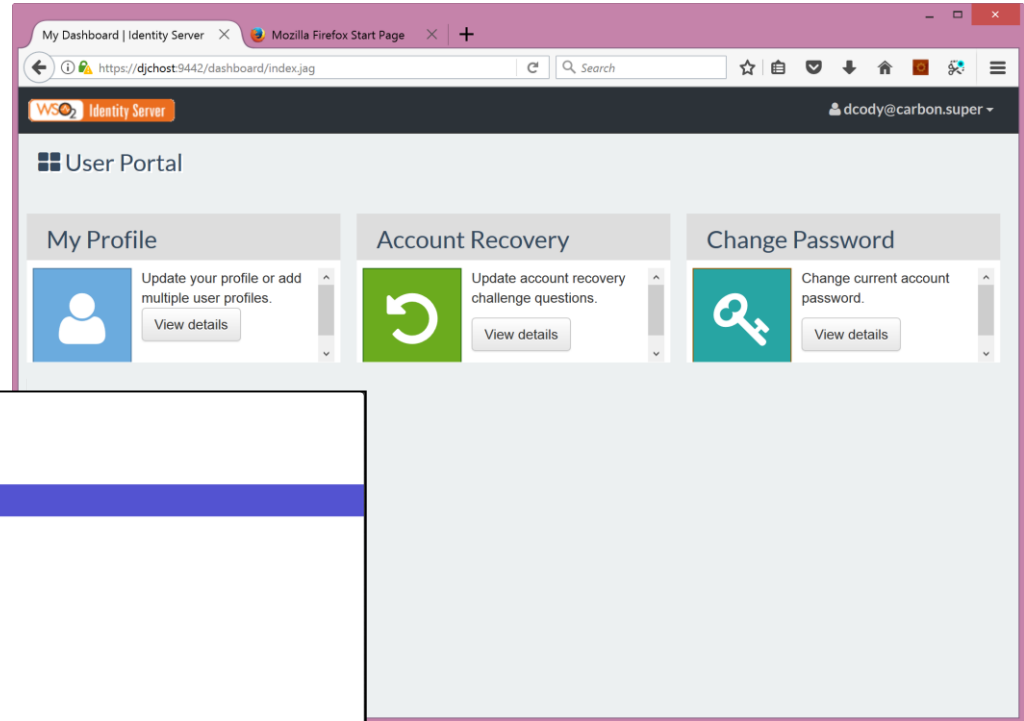
Account Management Enhancements
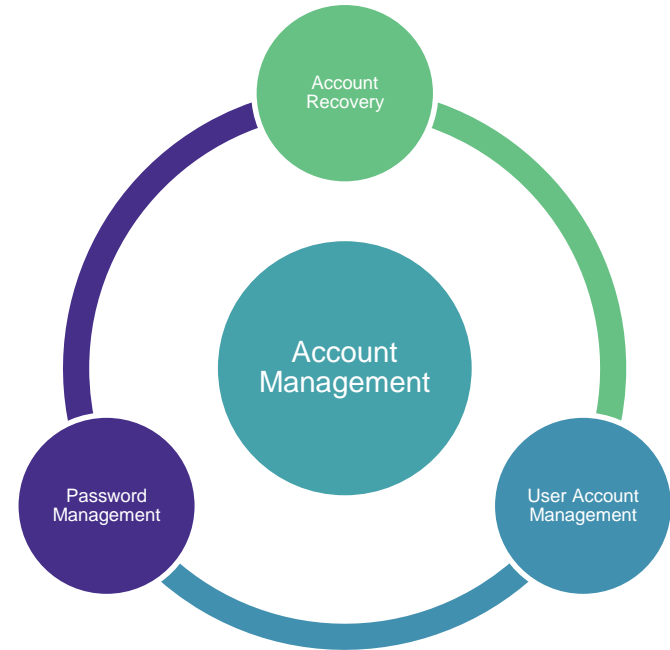
Account Recovery

- Password Recovery
- Username Recovery

Password Management

- User Initiated
- Admin Initiated (Forced password reset)
- Password History
- Password Complexity

User Account Management

- User Account Locking
- User Account Disabling
- User Account Suspension

Account Recovery

Account Management

Password Management

User Account Management

Caveats/Considerations

Authentication in Ellucian CRM

Important Distinctions

- Applications are not monolithic

- Include browser-based and non-browser-based components, requiring different SSO protocols

  - WS-Federation

  - WS-Trust

Examples have been browser-based apps to this point

- Non-browser applications (e.g., Outlook connector) must be addressed

CRM Recruit	CRM Advise	CRM Advance
Ellucian CRM Core		
Microsoft Dynamics CRM		
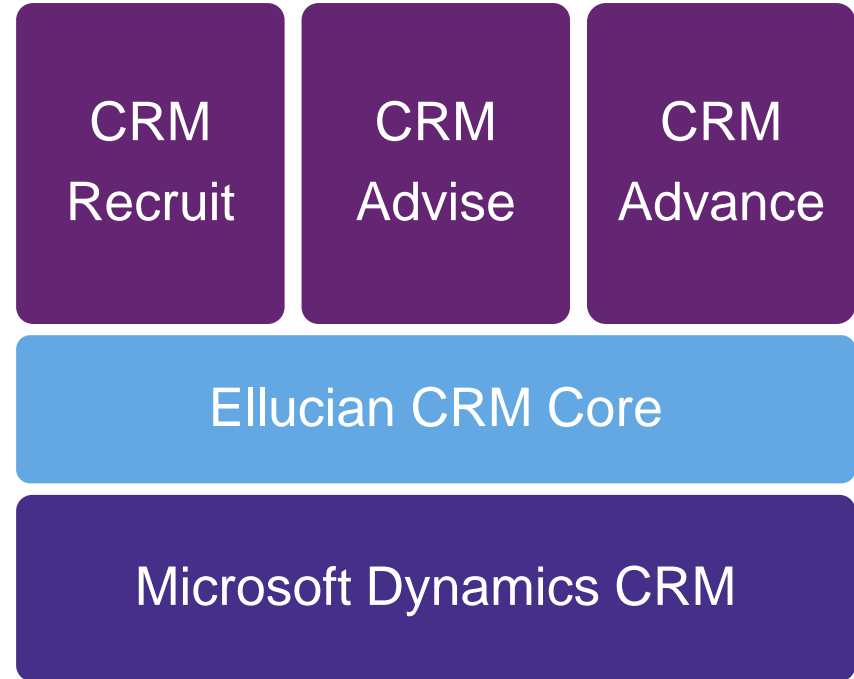
Compatibility Matrix

	Browser-based CRM Console (admin user)	Regular portal non-CX based (Advise)	Outlook connector	SDK (CX sites, installer, other utilities)	CX sites using ADFS for constituent logins	Student or constituent logins to CX sites	Externally controlled authentication
Ethos Identity 2.x (non-federated)	Tested – works	Tested – works	Tested – works	Tested – works	Future development and testing	n/a	n/a
Ethos Identity 5.3 (non-federated)	Tested – works	Tested – works	Tested – broken, working to resolve	Tested – broken, working to resolve	Future development and testing	n/a	n/a
EEId with federated IdP (Shib, etc.)	Tested – works	Tested – works	Tested – does not work	Tested – does not work	Depends on federated IdP	n/a	n/a
AD FS	Tested – works	Tested – works	Tested – works	Tested – works	Future development and testing	n/a	n/a
AD FS federated with IdP (Shib, etc.)	Not tested	Not tested	Not tested	Not tested	Future development and testing	n/a	n/a
Azure AD Premium	Under testing	Under testing	Under testing	Under testing	Future development and testing	n/a	n/a

Summary and Questions

Summary

Ellucian CRM applications support the WS-Federation and WS-Trust protocols

Including them in institution-wide SSO requires an IdP or protocol bridge that supports these protocols

Two supported options currently: AD FS and Ellucian Ethos Identity

Ethos Identity helps institutions establish or improve single sign-on across applications that support disparate protocols

Ethos Identity is available to all Ellucian customers as an entitlement

WSO2 Identity Server 5.3 is the core of Ellucian Ethos Identity, providing enhanced capabilities that institutions have requested

Resources

Ellucian Customer Support Center

- Downloads, documentation, articles, global search

  - https://ellucian.okta.com/app/UserHome > Support Center tile or Download Center tile

  - https://resources.elluciancloud.com/category/identity

eCommunities Identity and Access Management space

- Announcement, discussions, peer support

  - https://ecommunities.ellucian.com/community/identity-and-access-management

WSO2 Identity Server documentation

- Detailed feature documentation and configuration examples

  - https://docs.wso2.com/display/IS530/Introduction

Ellucian Professional Services

- Ethos Identity installation and service provider configuration

Need Help?

Contact your CSM

Include Justin Duffell
to support the effort

Questions

ellucian.

ellucian.

Thank you.