Access By Federation for Client Collaboration

INFO 1

i/+^ 2013
the catalyst

Introduction

- Holly Hanna, Microsoft Legal & Corporate Affairs
  hollyhan@microsoft.com
  @hollyhanna (Twitter)
- Karen Allen, Morgan Lewis & Bockius
  kallen@morganlewis.com

Authentication Issues – Fundamental Questions

- Authentication: “Who are you?”
- Authorization: “Are you allowed to do this?”

- AD Accounts – secure but a management nightmare
- Forms-based – easier to implement, but less secure

Microsoft Yesterday: Two Options, Neither Good

Option 1: Extranet

- Requires user to be set up in PARTNER domain
- Passwords need to be updated every 70 days
- Environment running on SharePoint 2007 – no way to collaborate in real time
- Management a constant headache for both administrator and user

Option 2: CorpNet Account

- 2+ week process for getting users set up in the system
- To remotely access the corporate network, external users must be approved for a smart card, requiring director-level approval
- Once remote access is approved, user must either visit a Microsoft location or send in picture and get a card mailed
- Once the user has access, they have access to the entire Microsoft corporate network – not just the matter they are working on

MorganLewis Extranet

- Requires user to be set up in AD domain
  - Used to limit access to sites and externally exposed applications
- Passwords complex, need to be updated every 90 days
- Environment running on SharePoint 2007 – no way to collaborate in real time
- Management a constant for both administrator and user
- Dedicated support team for password resets and other access issues

Circumventing the System

SkyDrive

i/+∧ 2013 the catalyst

IT Goal: Make It Easy

- When forced to choose between the right way to do something and the expedient way to do something, expedience wins every time
- Understand your security tradeoffs and undertake a solid risk analysis

Claims Authentication Fundamentals

6 Point ID
Document Selector

Secure Authentication Options

Claims-based = Authoritative Identity Source

- Microsoft Account
- ADFS
- OAuth

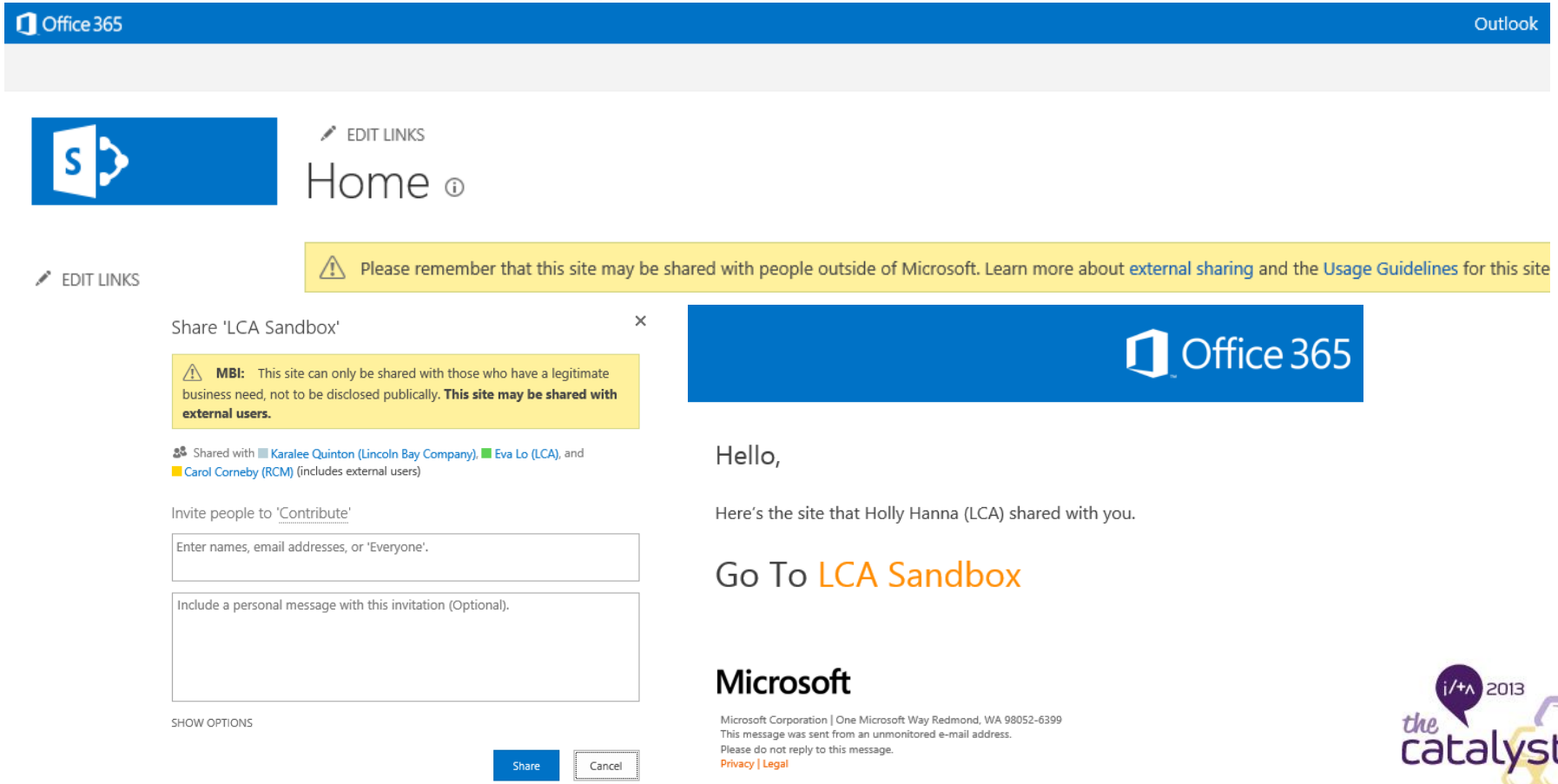
Microsoft Today: External Collaboration Made Easy

- External users need a Microsoft Account (formerly Live ID or Passport), which can be easily created by the end user and associated with their email address
- Site owner sends an invitation from O365 site to the associated email address

What's a Microsoft Account?

- Single sign-on web service formerly known as Passport and Windows Live ID
- Available to anyone with an email address; automatic with a Hotmail.com or outlook.com address
- User is authenticated via SSL connection; if the user opts to have a site remember them, an encrypted time-limited cookie is stored on their computer and attached to a triple DES encrypted ID tag
- ID is sent to the web site, which then plants another time-limited HTTP cookie on the user's computer.

O365 External Collaboration

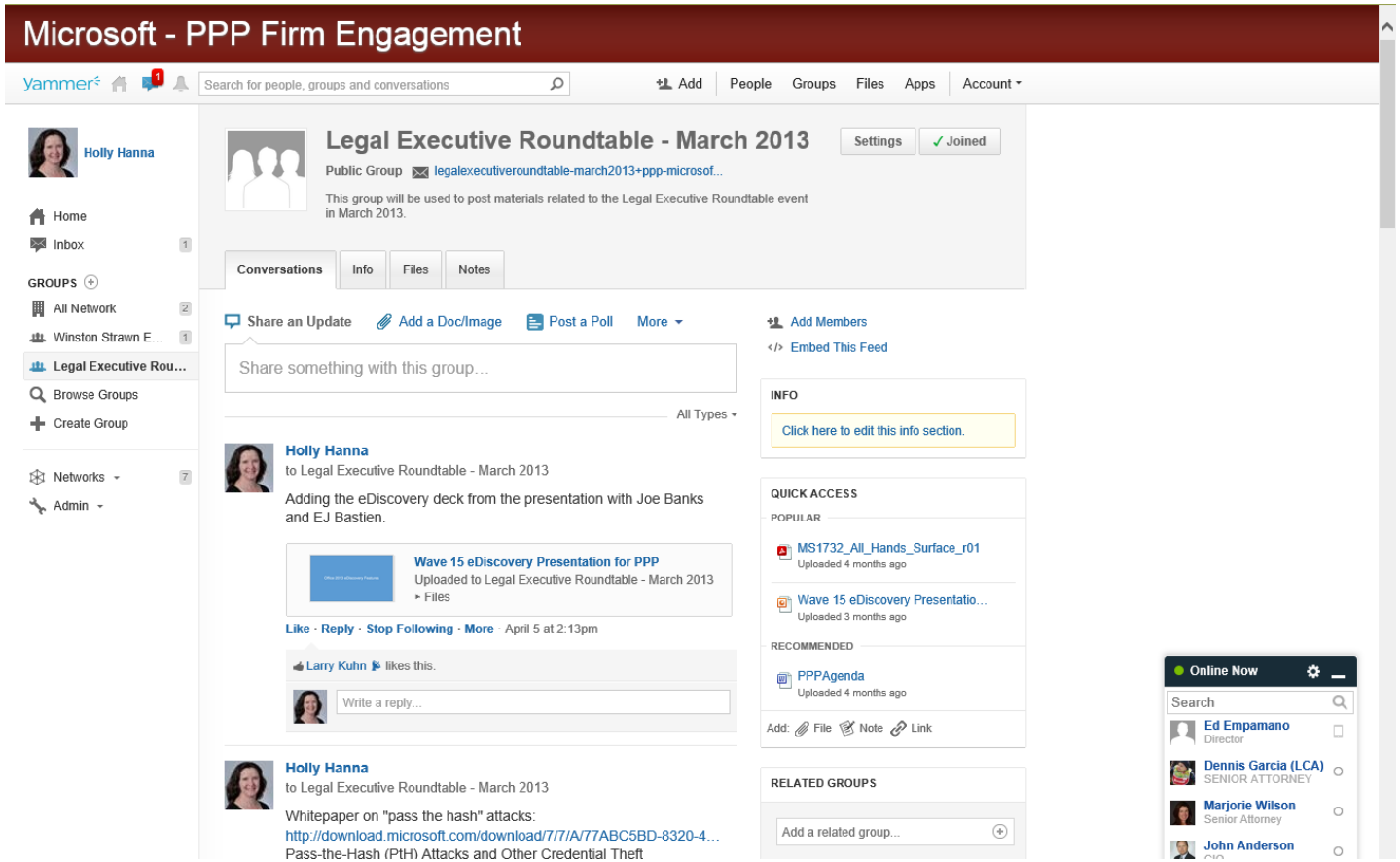


i/+∧ 2013 the catalyst

Securing O365 Collaboration

- Invitation is tokenized; cannot be forwarded or used by anyone who is not the intended recipient
- Link expires after one week for external users
- Only internal users can be owners and send invitations
- While individual items can be shared with non-site users by external users, site sharing is restricted to owners
- External users have access only to the sites they've been invited to and nothing else

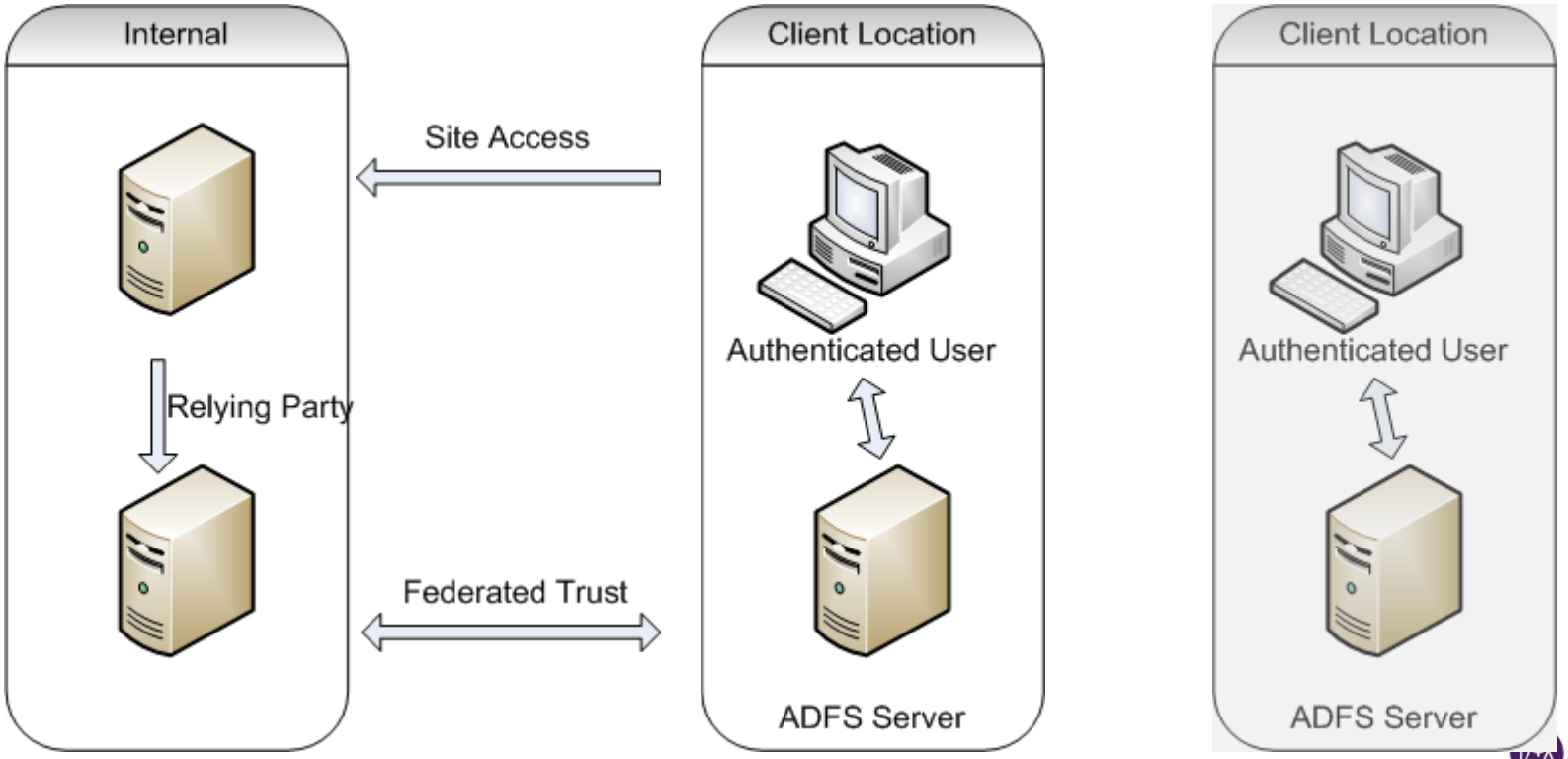
Yammer External Collaboration



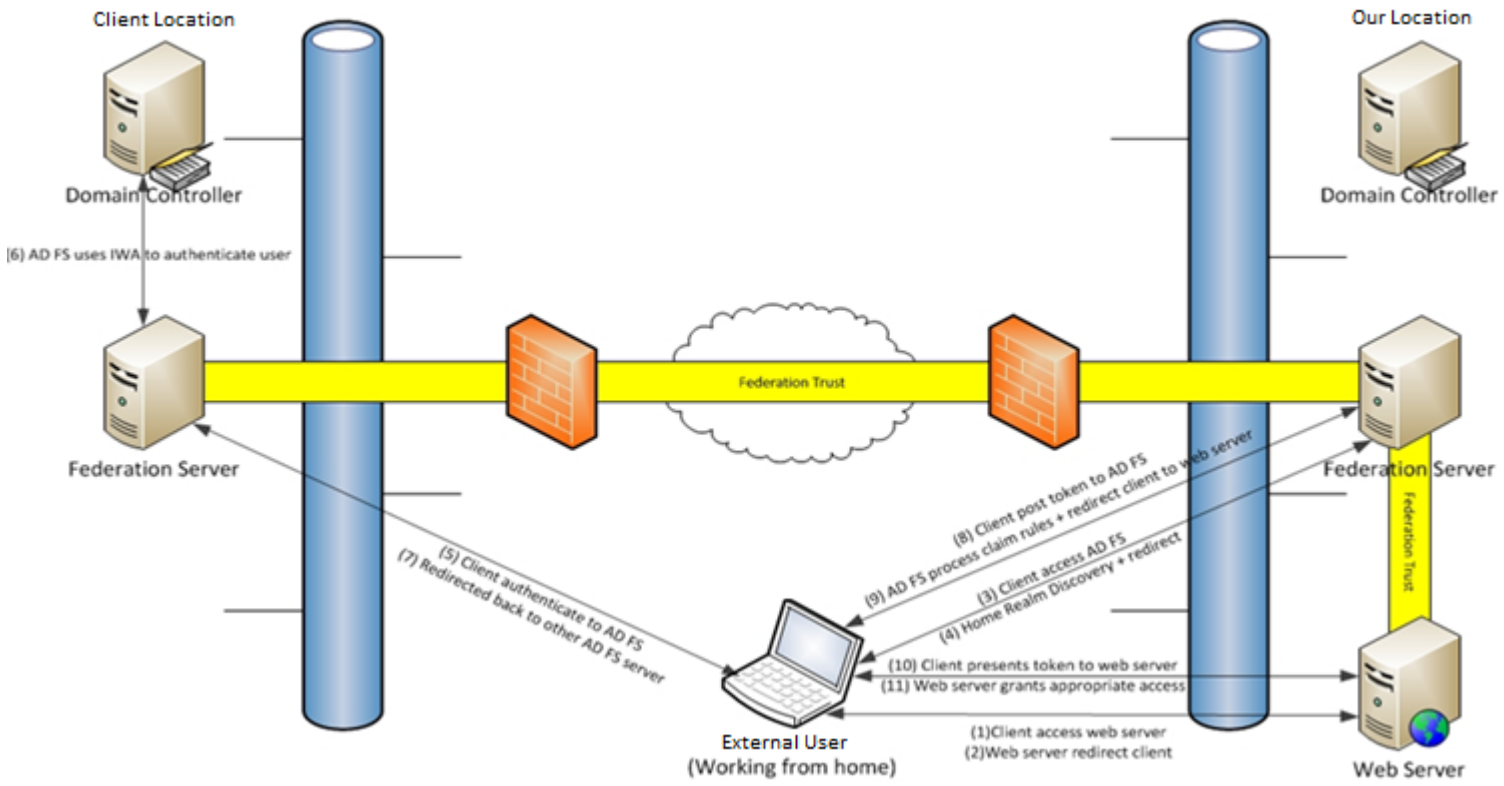
Single Sign-On via ADFS

- Client Request for single sign-on to SharePoint extranet site
- Client's AD configured as Claims Provider
- Configured SharePoint to trust the claims coming from ADFS for authentication
- Management
  - Defined groups and roles within SharePoint to match the client's AD group name
  - Linked the groups to Policies in SharePoint
  - Group Membership in AD is managed in the client's AD
  - Allows the client to add users as necessary

ADFS Architecture
Simple View

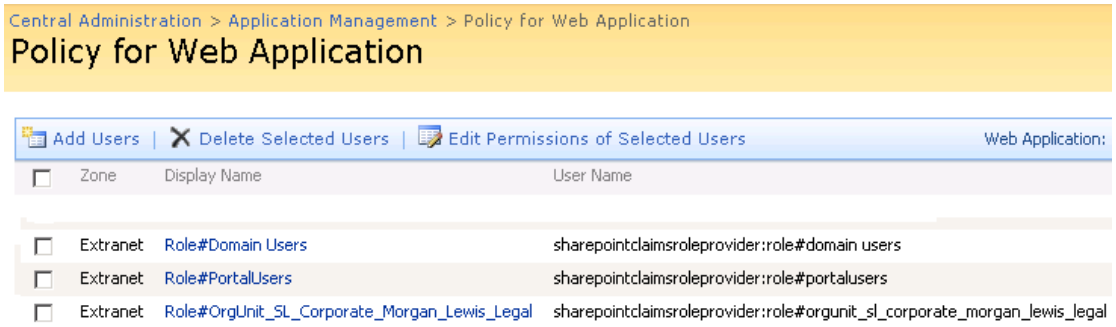


ADFS Architecture
Detail View



Application Configuration

- Extend Webapp to SSL site (extranet zone)
- Requires Federation Extensions for SharePoint
- Add external groups as Roles via WebApp policy



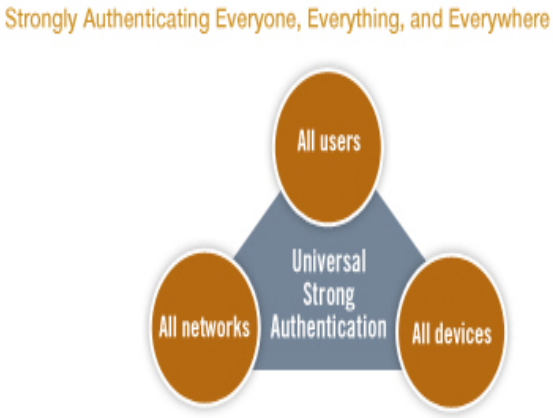
Microsoft Account Pros & Cons

- Advantages
  - Makes it easy for attorneys to collaborate in real time with outside counsel
  - Available for any device, anywhere; offline sync to local machine
  - With Windows 8, user is already signed in; when accessing a collaboration site, pass-thru of credentials is seamless
- Disadvantages
  - If user's Microsoft account is compromised, shared documents could be at risk
  - No IT control over who has access to what data

ADFS Pros & Cons

- Advantages
  - Shifts burden of authenticating users to the identity provider
  - Vendor neutral SAML-based token
  - Seamless for end users
- Disadvantages
  - More complex configuration
  - Support issues for end-users
    - Troubleshooting on both sides

Coming Attractions
Open Authentication



- Industry Standard Protocol
- Used by Citrix FileStream, Box.com, Windows Live, and others

Further Reading

- Claims-Based Identity Term Definitions
  http://msdn.microsoft.com/en-us/library/ee534975.aspx
- Open Authentication (OAuth) Overview
  http://en.wikipedia.org/wiki/OAuth
- Microsoft Account
  https://signup.live.com
- ADFS Concepts
  http://technet.microsoft.com/en-us/library/cc776617(v=ws.10).aspx