SharePoint Extranets

Peter Carson

March 11, 2015
Peter Carson

- President, Envision IT
- SharePoint MVP
- Virtual Technical Specialist, Microsoft Canada
- peter@envisionit.com
- http://blog.petercarson.ca
- www.envisionit.com
- Twitter @carsonpeter
- VP Toronto SharePoint User Group
Envision IT

Public Websites

Intranets / Staff Portals

Extranets / Member Portals

SharePoint
Office 365
Microsoft Azure
Extranet User Manager

- Easy delegation of user management to business
- Self-registration, approvals, forgotten password reset
- Simplified login for both internal and external users
Agenda

- What is an Extranet
- SharePoint Authentication
- Extranet Scenarios
- Licensing
- On-Premise
- Office 365
What is an Extranet

An **Extranet** is a web site that is accessible to users outside of the corporate network, which allows organizations to share information and collaborate with their customers, partners, and/or vendors in a secure and easy-to-use environment.

It may be delivered in a number of ways:

- As an extension of the public web site
- As a secure portion of the corporate Intranet
- As a standalone Extranet
Examples of Extranet Users

- Members
- Customers
- Vendors
- Suppliers
- Volunteers

- Board of Directors
- Citizens
- Researchers
- Tenants
- Partners
Considerations

- Who is coming into the Extranet?
- Does everyone see the same information?
- Is there a member database to interface with?
- Is it invitation only, or can people self-register?
- Who approves new registrations?
- Is it just the Extranet they will be accessing, or are there other systems?
Identity Management

- Process for managing the entire life cycle of digital identities, including the profiles of people, systems, and services
- For our purposes we are focused just on people
- Who creates and manages identities? The Extranet owner or the external users themselves?
- Are identities part of the Extranet or external to it?

Authentication and Authorization

- Authentication is the mechanism whereby systems may securely identify their users
- Authentication systems provide an answers to the questions:
  - Who is the user?
  - Is the user really who he/she represents himself to be?
- Authorization is the mechanism by which a system determines what level of access a particular authenticated user should have
  - Is user X authorized to access resource R?
<table>
<thead>
<tr>
<th>Technologies</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SharePoint</td>
<td>Microsoft’s collaboration platform that provides portals, document management, web content management, and much more</td>
</tr>
<tr>
<td>Office 365</td>
<td>Microsoft’s cloud hosted versions of Exchange (email), Lync (instant messaging), and SharePoint</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>Microsoft’s infrastructure and platform hosted services</td>
</tr>
<tr>
<td>Envision IT’s tool</td>
<td>Envision IT’s tool for managing users outside your organization</td>
</tr>
</tbody>
</table>
Poll 1

Which Version of SharePoint are you currently using?

- Office 365
- SharePoint Server 2013
- SharePoint Server 2010
- SharePoint Foundation (2010 or 2013)
- MOSS 2007 or WSS 3.0
Poll 2

How do you use SharePoint today?

- Internal collaboration
- Internal web publishing (Intranet)
- Extranets
- Public facing website
SharePoint Authentication
SharePoint On Premise Authentication Options

- **Windows Authentication**
  - Active Directory
  - Windows Claims
  - Or Classic Mode

- **Forms-Based Authentication**
  - .NET Providers
  - AD
  - SQL
  - Claims

- **Federated Identity**
  - Relying Party
  - Trusted Identity Provider
  - AD
  - User Store
  - Claims
Office 365 Authentication Options

Cloud Identity
- Windows Azure Active Directory
- No Integration

Directory and Password Synchronization
- Windows Azure Active Directory
- DirSync and Password Sync
- Integration with no federation

Federated Identity
- Windows Azure Active Directory
- Federation
- User Sync
- Single federated identity and credentials
Extranet Scenarios
SharePoint Extranet Scenarios

- Secure publishing portal
- Collaboration space

- Installed on premise in SharePoint Server, or in the cloud in Office 365
- Extranet User Manager installed on premise or hosted in Microsoft Azure
Office 365 External Sharing

- Up to 10,000 free external users in your Office 365 subscription through External Sharing
- Must use the Microsoft login form
- External users must have a Microsoft account, or be an Office 365 subscriber themselves
- No control over what account is used to accept the invitation
- “Light-weight solution”
  - Bill Baer – Microsoft Senior Product Marketing Manager and Microsoft Certified Master for SharePoint 2007 in the SharePoint product group
On Premises Forms-Based Authentication

- Add FBA login form to a SharePoint on premises installation
- Supports SharePoint 2010 and 2013, but not Office 365
- Deeply integrated into the SharePoint installation
- Earlier versions of EUM did this through an installation wizard
SharePoint Extranets - Federated Identities

- Works with both SharePoint on premises and in Office 365
- Light integration to either
- Trusted Identity Provider does the authentication
- Can be any SAML compliant provider
  - Active Directory Federation Services
  - Thinktecture Identity Server
    - [www.thinktecture.com](http://www.thinktecture.com)
  - Social identities
- Can be AD, SQL, or other user repository under the hood
- Relying parties (such as SharePoint) trust the SAML token and provide the authorization based off that identity
- Provides Single Sign-On to multiple systems
  - Can be any SAML claims compliant system, not just SharePoint
Extranet Licensing
# SharePoint 2013 Licensing

<table>
<thead>
<tr>
<th>2013</th>
<th>Intranet</th>
<th>Extranet</th>
<th>Internet Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Users</td>
<td>SharePoint Server + CAL</td>
<td>SharePoint Server + CAL</td>
<td>SharePoint Server</td>
</tr>
<tr>
<td>External Users*</td>
<td>N/A</td>
<td>SharePoint Server</td>
<td></td>
</tr>
</tbody>
</table>

- Also requires SQL Server and Windows Server licenses
- External users means users that are not either you or your affiliates’ employees, or you or your affiliates’ onsite contractors or onsite agents
Office Web Apps

- Web browser based versions of Word, Excel, and PowerPoint
- Not full versions, but main features for most users
- Allows viewing and editing without having Office installed
- Multiple people can co-author a document at the same time

- I have internal users who want to access Office documents via Office Web Apps, what licenses do I need to be compliant?

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Internal User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Office documents via Office Web Apps</td>
<td>Free, no Office client required</td>
</tr>
<tr>
<td>Edit Office documents via Office Web Apps</td>
<td>Requires Office 2013 Standard or Professional Plus</td>
</tr>
</tbody>
</table>

- Our company users (who are licensed for Office Client) are working with external users on projects, what licensing do those external users need to access Office documents via Office Web Apps?

<table>
<thead>
<tr>
<th>Scenario</th>
<th>External User*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Office documents via Office Web Apps</td>
<td>Free, no Office client required</td>
</tr>
<tr>
<td>Edit Office documents via Office Web Apps</td>
<td>Free, no Office client required</td>
</tr>
</tbody>
</table>

*External Users: defined as users that are not either your or your affiliates’ employees, or your or your affiliates’ onsite contractors or onsite agents.
# Office 365 Licensing

## Select a plan

<table>
<thead>
<tr>
<th></th>
<th>Business</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Office 365 Business Essentials</td>
<td>Office 365 Enterprise E1</td>
</tr>
<tr>
<td></td>
<td>Office 365 Business</td>
<td>Office 365 ProPlus</td>
</tr>
<tr>
<td></td>
<td>Office 365 Business Premium</td>
<td>Office 365 Enterprise E3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Individual services:
- Business-class email
- File storage & sharing
- Online meetings

<table>
<thead>
<tr>
<th>Plan</th>
<th>Price (User/month, 1 year)</th>
<th>Price (User/month, annual commitment)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Essentials</td>
<td>$5.10 user/month</td>
<td>$5.10 user/month, annual commitment</td>
</tr>
<tr>
<td>Business</td>
<td>$10.50 user/month</td>
<td>$10.50 user/month, annual commitment</td>
</tr>
<tr>
<td>Business Premium</td>
<td>$12.90 user/month</td>
<td>$12.90 user/month, annual commitment</td>
</tr>
<tr>
<td>Enterprise E1</td>
<td>$8.20 user/month</td>
<td>$8.20 user/month, annual commitment</td>
</tr>
<tr>
<td>ProPlus</td>
<td>$15.20 user/month</td>
<td>$15.20 user/month, annual commitment</td>
</tr>
<tr>
<td>Enterprise E3</td>
<td>$23.20 user/month</td>
<td>$23.20 user/month, annual commitment</td>
</tr>
</tbody>
</table>

### Additional options:
- [Learn more](https://products.office.com/en-ca/business/compare-more-office-365-for-business-plans)
- User maximum:
  - 300
  - 300
  - 300
  - Unlimited
  - Unlimited
  - Unlimited

SharePoint Online

Compare SharePoint options

<table>
<thead>
<tr>
<th>SharePoint Server</th>
<th>SharePoint Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>Plan 1</td>
</tr>
<tr>
<td>Enterprise</td>
<td>Plan 2</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Try now</td>
<td>$5.10 user/month</td>
</tr>
<tr>
<td>Buy now</td>
<td>$8.20 user/month</td>
</tr>
</tbody>
</table>

Licensing options

Plus applicable tax

https://products.office.com/en-ca/sharepoint/compare-sharepoint-plans
Comparison of Licensing

SharePoint On Premises
- Purchase of the Microsoft server licenses
  - SharePoint Server
  - SQL Server
  - Windows Server
- Purchase or hosted subscription of EUM

Office 365 and Federation
- Office 365 monthly subscriptions for each user, both internal and external
- Purchase or hosted subscription of EUM
Demo – Office 365

Registration through to Login

Office 365
Demo Scenario

- Office 365 sample site at [https://eumdev.sharepoint.com](https://eumdev.sharepoint.com)
  - SharePoint Online in Office 365
- EUM installed at [https://eum.eitdev.org](https://eum.eitdev.org)
- AD FS for internal users
- External users
  - In a separate AD or SQL Database
  - Authenticating through Thinktecture Identity Server
  - Managed with the Envision IT Extranet User Manager
Client Demos

- Public Health Ontario  
  - www.publichealthontario.ca
- Boys and Girls Clubs of Canada Members Portal  
  - www.bgccan.com
- Oakland County Government to Government Marketplace  
  - www.g2gmarket.com
- Supreme Court of Victoria Case Management  
  - www.redcrest.com.au
- Transamerica Life Canada Public Web Site and Advisors Portal  
  - www.transamerica.ca
- Kinross Gold Supplier Portal  
  - suppliers.kinross.com
- CAMH Problem Gambling Professionals  
  - www.problemgambling.ca
Ontario Association of Childrens Aid Societies

- Since 1912, Ontario Association of Children’s Aid Societies (OACAS) has represented Children’s Aid Societies in Ontario
- Provides service for government relations, communications, information management, education and training
- Advocates for the protection and well-being of children
- Voice of child welfare in Ontario
The Challenge

- Current site users experienced challenges locating suitable content
  - No search engine functionality
  - Ever-growing archive of documents
- Maintaining an on premises SharePoint portal was complex and expensive
- Static web sites lack the dynamic functionality and features OACAS was looking for
The Solution

Office 365 + Windows Azure

SharePoint + Extranet User Manager for SharePoint
The Solution

- Self-service registration
- Approvals managed by the OACAS
- Everything is hosted in the cloud with minimal IT requirements
- Dynamic pages now automatically displaying “tagged” content
- Content authors can now simply upload content and “tag” it to appear within a desired section of the site
- Site navigation and search make it much easier to find information
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Network</td>
<td>The private network that all of the internal desktops, laptops, and most servers are connected to. This is a highly trusted, private network</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone&lt;br&gt;This is a less secure server area for resources that are going to be accessed from the Internet, such as an Extranet site</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory&lt;br&gt;The Microsoft directory service for both users and computers in a Windows Server network</td>
</tr>
<tr>
<td>One Way Trust</td>
<td>One AD trusts users and computers from another AD&lt;br&gt;Typically a DMZ AD would trust the Internal AD, but not the other way around</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IE</td>
<td>Internet Explorer</td>
</tr>
<tr>
<td>Windows Authentication</td>
<td>Logging into a resource using your Windows credentials (username and password you type in to log into your Windows PC) This often happens automatically in IE when properly configured</td>
</tr>
</tbody>
</table>
| FBA                         | Forms Based Authentication  
Logging in on an HTML login page. Typically this is done with a username and password, but may be other credentials such as email and password |
| Multi-Factor Authentication | Using additional factors for authentication, such as a hardware token, soft-token on a mobile device, text message, or phone call token |
## Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reverse Proxy</td>
<td>Takes requests from the Internet and forwards them to internal servers</td>
</tr>
<tr>
<td>Trusted Identity Provider</td>
<td>The identity provider trusted by the relying party</td>
</tr>
<tr>
<td>Relying Party</td>
<td>The system being accessed, such as SharePoint. It relies on the Trusted Identity Provider to authenticate the user requesting access</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Asset Markup Language specification</td>
</tr>
<tr>
<td>SAML Token</td>
<td>Token that is passed between the TIP and RP</td>
</tr>
<tr>
<td>JSON</td>
<td>JavaScript Object Notation format used to pass data to/from JavaScript</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>JWT</td>
<td>JSON Web Token. Similar to the SAML Token, used to pass security credentials between JavaScript and web services</td>
</tr>
<tr>
<td>Claim</td>
<td>A property in the SAML token, such as the email address or username of the user</td>
</tr>
<tr>
<td>Thinktecture Identity Server</td>
<td>Open source Identity Provider</td>
</tr>
<tr>
<td>Extranet Identity Server</td>
<td>EUM implementation of the Thinktecture Identity Server</td>
</tr>
</tbody>
</table>
SharePoint On Premises
Authentication
SharePoint On Premise Authentication Options

Windows Authentication

Active Directory

Windows Claims
Or
Classic Mode

Forms-Based Authentication

.NET Providers

AD
SQL

Claims

Federated Identity

Relying Party

Trusted Identity Provider

AD
User Store

Claims
Windows Authentication

- Supports Classic mode sites
- An advanced web gateway is recommended
  - Friendly web form is still presented
  - Can be customized
  - Single sign on can happen across multiple systems
- Gateway options
  - Microsoft Forefront UAG and TMG are now discontinued
  - Windows Server 2012 R2 Web Application Proxy
Forms Based Authentication

- Users can be stored in either SQL or AD
- Friendly, customizable web form for login
- Login with email address, even for AD users
- Requires a Claims mode site
Active Directory versus SQL

Active Directory
- Generally recommended that a separate AD forest is setup for the Extranet users
- May already exist in the DMZ to support the SharePoint farm
- Richer account policy control and audit capabilities

SQL
- No additional AD is required
- Standard Microsoft ASPNETDB database stores the credentials
- Encrypted passwords
SAML Federation

- Trusted Identity Provider does the authentication
- Can be any SAML compliant provider
  - Active Directory Federation Services
  - Thinktecture Identity Server
  - Social identities
- Can be AD or SQL user repository under the hood
- Relying parties (such as SharePoint) trust the SAML token and provide the authorization based off that identity
- Provides Single Sign-On to multiple systems
  - Can be any SAML claims compliant system, not just SharePoint
Claims Limitations

- **Claims to Windows Token Service (C2WTS)**
  - Can be mitigated through code
  - Power Pivot
  - SQL Server Reporting Services
  - Excel Services
  - PerformancePoint

- **InfoPath Forms Services**
  - Browser based forms not supported
  - Product is no longer part of Microsoft’s form strategy
Sample Architecture

- SharePoint Web Front Ends
- Office Web Apps Servers
- SharePoint Application Servers
- Active Directory
- Clustered or Always On SQL Server
Network Architecture
Four Categories of Users

- Internal Users
- Managed AD Users
- Managed SQL Users
- Federated Users
Site URLs

- Ensure that everyone is going to the same URL
- Don’t extend the site or use AAM
- Having different URLs for internal and external users causes confusion, particularly with email links
- Breaks features such as alerts and workflow tasks
  - SharePoint doesn’t know where to link people to
One Way Trust
Welcome to the Envision IT Extranet User Manager (with Thnkarchitecture Identity Provider). To enter this area of the site you must be an authenticated user.

If this is your first time visiting, please Register Here before logging in.

Email
Password

Remember me? 

Forgot Password?

Login
# Internal Firewall Port Requirements

## Windows Auth
- 123/UDP - W32Time
- 135/TCP - RPC Endpoint Mapper
- 464/TCP/UDP - Kerberos password change
- 49152-65535/TCP - RPC for LSA, SAM, Netlogon (*)
- 389/TCP/UDP - LDAP
- 636/TCP - LDAPS SSL
- 3268/TCP - LDAP GC
- 3269/TCP - LDAP GC SSL
- 53/TCP/UDP - DNS
- 49152-65535/TCP - FRS RPC (*)
- 88/TCP/UDP - Kerberos
- 445/TCP - SMB
- 49152-65535/TCP - DFSR RPC (*)

## FBA
- LDAP 389
- LDAPS 636
- SMB 445

## Federation
- No internal ports required
- Done through trusted, signed tokens passed through browser posts
- May still want to open port 443 for internal users to log in through ADFS externally

---

http://support.microsoft.com/kb/179442#method4
Forms Based Authentication

- HTML login form
- EZ-Login form that is part of EUM provides this
- Deeply wired into SharePoint
- Not easy to use for single sign-on for other systems
Windows Auth – Reverse Proxy

- Both internal and external users can log in externally through the reverse proxy
- The reverse proxy can present a customized HTML login form for the user
- From the internal server’s perspective, the user is logged in with Windows credentials
Sample Reverse Proxies

- Microsoft Forefront Threat Management Gateway (TMG)
  - Discontinued
- Microsoft Forefront Unified Access Gateway (UAG)
  - Discontinued
- Microsoft Web Application Proxy
  - Part of Windows Server 2012 R2
- Citrix NetScaler
- F5 Big-IP
Example Sites

- Forefront TMG
  - https://secure.envisionit.com
- Forefront UAG
  - https://secure.publichealthontario.ca
  - https://portal.calgaryunitedway.org
Internal Users - ADFS

- Internal users connect with their AD credentials through ADFS
- No trusts required between internal and DMZ AD
- No ports open from internal network to DMZ
Internal Users – ADFS with VPN

- No external publishing of internal ADFS externally
- Internal users working outside the internal network must VPN first to connect
- Typically the same requirement for all corporate resources
ADFS Federation – Internal with VPN
External Users - Federation

- External users use ADFS, Thinktecture, or another Trusted Identity Provider to access the Relying Party, such as SharePoint
Federation – External Users

Active Directory

Active Directory

SQL
All Relying Parties use Thinktecture Identity Server as their Trusted Identity Provider

TIS is a Relying Party for ADFS for internal users

Allows more sophisticated login and home realm discovery to improve the user experience
Federation – External Users

Active Directory

Thinktecture Identity Server

Active Directory
Federation – Internal Users
Federation – Internal Users External

Thinktecture Identity Server

Active Directory

Active Directory
/_layouts/15/Authenticate.aspx
/_login/default.aspx  - Home Realm Discovery
/_trust/default.aspx
Sign In

Select the credentials you want to use to logon to this SharePoint site:

- Windows Authentication
- Thinktecture IP-018
/issue/wsfed - Posts the SAML in wresult hidden field

/account/signin
/account/signin

- Customized Login page
Why Thinktecture over ADFS?

- Open source allows any customization
- Fully brandable (ADFS allows branding within very particular parameters)
- Login with email address instead of AD username
- Use SQL instead of AD as the underlying user repository
- Ability to incorporate the home realm discovery into the login form
Federated Identity

- Trusted Identity Provider does the authentication
- Can be any SAML compliant provider
  - Active Directory Federation Services
  - Thinktecture Identity Server
    - [www.thinktecture.com](http://www.thinktecture.com)
  - Social identities
- Can be AD, SQL, or other user repository under the hood
- Relying parties (such as SharePoint) trust the SAML token and provide the authorization based off that identity
- Provides Single Sign-On to multiple systems
  - Can be any SAML claims compliant system, not just SharePoint
Trusted Identity Providers

- Active Directory Federation Services (ADFS)
- Thinktecture Identity Server
- Social Identities
  - Facebook
  - Linkedin
  - Microsoft Account
  - Google+
Summary

- **Internal Users**
  - Windows Auth
  - ADFS
  - ADFS and Thinktecture

- **External Users**
  - FBA
  - Reverse Proxy
  - Federation
Active Directory Federation Services

- **ADFS 1.0**
  - Windows Server 2003
- **ADFS 1.1**
  - Windows Server 2008
- **ADFS 2.0**
  - Minimum to be used with SharePoint
  - Free download
  - Windows Server 2008 SP2 minimum
  - ADFS Proxy is used in the DMZ to expose externally
- **ADFS 2.1**
  - Windows Server 2012 Role
  - ADFS Proxy is used in the DMZ to expose externally
- **ADFS 3.0**
  - Windows Server 2012 R2 Role
  - Web Application Proxy is used in the DMZ to expose externally
ADFS Login Form

- Internal users shouldn’t see this inside the network
- Can be branded, within limits
Thinktecture Identity Server

- Open source project available on GitHub
- Integrated into the Extranet User Manager V3 installer
- Customized to work with both on premises SharePoint and Office 365
Authentication Process

User

Browse app

Not authenticated

Redirected to IP

Return SAML Security Token

Send Token

Return page and cookie

Relying Party

SharePoint

Active Directory

Identity Provider

Authenticates

Query for user attributes

RP trusts IP

Active Directory trusts RP

User

Browser

Not authenticated

Redirected to IP

Return SAML Security Token

Send Token

Return page and cookie

Active Directory

RP trusts IP

Active Directory trusts RP
PKI SSL encryption is used for communication
- Token can be self-signed by the Identity Provider
- Token can also be encrypted with a self-signed certificate from the Identity Provider
Authentication Providers

Edit Authentication

Claims Authentication Types

Choose the type of authentication you want to use for this zone.

- Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.

- Basic authentication method exchanges users’ credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

- Enable Windows Authentication
  - Integrated Windows authentication
  - NTLM

- Basic authentication (credentials are sent in clear text)

- Enable Forms Based Authentication (FBA)
  - ASP.NET Membership provider name
  - ASP.NET Role manager name

- Trusted Identity provider
  - Trusted Identity Provider: Thinktecture IP-STS
SharePoint Infrastructure

- SharePoint Farm (one or more servers)
  - Web Application
    - Site Collection
      - Subsites
        » Lists and Libraries
  - Application Pools
  - IIS Sites
  - Content Databases
Web Application Zones

- Authentication methods are defined for each zone of a web application
- Each web app can have up to five zones
  - Default
  - Intranet
  - Extranet
  - Internet
  - Custom
- Multiple authentication methods can be applied to a single zone
When to Use Zones

- In general we recommend not to use multiple zones.
- Everyone (internal and external users) should share a single https url (https://portal.contoso.com)
- Confusion results otherwise
  - Emailed links are broken for some of your users
  - Workflows, tasks, and alerts point to the wrong URL (unless you are in the Default zone)
- The only exception is where you also need an anonymous http zone
  - Mixed public and private sites
  - This is the only scenario that Microsoft recommends
  - Secure https zone should always be the default zone
Authentication Chooser

- Users decides what method to use to authenticate
- Goal should be to hide this from the user
  - Use the IP address
  - Check the email domain of the login email address
AD FS and SharePoint On Premises
AD FS and SharePoint On Premises

- Same AD FS infrastructure is needed as Office 365
- Complete the AD FS Configuration Checklist
- Export the token signing certificate
- Setup the Relying Party (SharePoint) in AD FS
- Run the PowerShell to configure SharePoint to trust AD FS as an identity provider
- Select the Trusted Identity Provider in Central Admin
# AD FS Configuration Checklist

<table>
<thead>
<tr>
<th>Relying Party Definition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Extranet</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://adfsportal.eitdev.org/_trust/">https://adfsportal.eitdev.org/_trust/</a></td>
</tr>
<tr>
<td>Identifier</td>
<td>extranet</td>
</tr>
<tr>
<td>Full Identifier</td>
<td>urn:extranet:sharepoint</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Claim Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Attribute</td>
</tr>
<tr>
<td>E-Mail Addresses</td>
</tr>
<tr>
<td>Token Groups - Unqualified Names</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SharePoint Trusted Identity Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token Issuer</td>
</tr>
<tr>
<td>Certificate File</td>
</tr>
<tr>
<td>Certificate Name</td>
</tr>
<tr>
<td>Realm</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>ADFS Signin URL</td>
</tr>
</tbody>
</table>
Token Signing Certificate
Relying Party Trust

Add Relying Party Trust Wizard

Welcome

Steps
- Welcome
- Select Data Source
- Choose Issuance
- Authorization Rules
- Ready to Add Trust
- Finish

Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.
Relying Party Trust
Relying Party Trust
Relying Party Trust

Configure Certificate

Steps:
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse.

- Issuer:
- Subject:
- Effective date:
- Expiration date:

View... Browse... Remove...
Relying Party Trust

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 Web SSO protocols for relying parties. If WS-Federation, SAML or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:
https://adfsportal.exceler.org/:trust/

Example: https://fs.contoso.com/adfs/ls/

Enable support for the SAML 2.0 Web SSO protocol

The SAML 2.0 single sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Web SSO protocol.

Relying party SAML 2.0 SSO service URL:

Example: https://www.contoso.com/adfs/ls/

Previous Next Cancel Help
Relying Party Trust

Configure Identifiers

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Relying party trust identifier:

Example: https://fs.contoso.com/sdfs/services/trust

https://offportal.mdeou.org/trust/

Remove

Add

Previous  Next  Cancel  Help
Relying Party Trust

Choose Issuance Authorization Rules

- Permit all users to access this relying party
  - The issuance authorization rule will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.
- Deny all users access to this relying party
  - The issuance authorization rule will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
Relying Party Trust

The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.

- Open the Edit Claim Rules dialog for this relying party trust when the wizard closes.
Relying Party Trust

Add Transform Claim Rule Wizard

Select Rule Template

Steps
- Choose Rule Type
- Configure Claim Rule

Claim rule template:
Send LDAP Attributes as Claims

Claim rule template description:
Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.
Relying Party Trust
PowerShell to Configure SharePoint

```powershell
$TokenIssuer = "ADFS LAB LOCAL"
$CertFile = "C:\Install\ADFS\adfs.cer"
$CertName = "Token Signing Cert Lab Local"
$realm = "urn:extranet:sharepoint"
$descript = "SharePoint secured by SAML (ADFS) Lab Local"
$ADFSSigninURL = "https://adfs.eitdev.org/adfs/ls"

if ($args[0] -eq "-Install")
{
    write-host "INSTALL Certificate - $CertName"
    New-SPTtrustedRootAuthority -Name $CertName -Certificate $cert

    write-host "INSTALL Token Issuer - $TokenIssuer"
    $map = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -IncomingClaimTypeDisplayName "EmailAddress" -SameASIncoming;
    $map2 = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.microsoft.com/ws/2008/06/identity/claims/role" -IncomingClaimTypeDisplayName "Role" -SameASIncoming;

    $ap = New-SPTtrustedIdentityTokenIssuer -Name $TokenIssuer -Description $descript -realm $realm -IdentifierClaim "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress";
}
elseif ($args[0] -eq "-Uninstall")
{
    write-host "UNINSTALL $TokenIssuer and $CertName"

    Remove-SPTtrustedIdentitytokenissuer $TokenIssuer
    Remove-SPTtrustedRootAuthority -Identity $CertName
}
```
Select the Trusted Identity Provider
EUM and SharePoint
EUM and SharePoint

- Full details in the Deployment and Configuration Guide
- High-level steps
  - Create an IIS site to install into
  - Run the installer
  - Configure the Extranet Identity Server
  - Complete the EUM configuration
  - Add SharePoint as a Relying Party
  - Integrate AD FS as an Identity Provider
  - Configure other Relying Parties
Claims Augmentation
Claims Augmentation

- The provisioning of additional custom claims for the user being authenticated
- Can come from any data source
  - Line of business system
  - SQL database
- Provides additional information about the user that can be used for security or audience targeting
TMX Group

- Toronto Stock Exchange
  - Largest stock exchange in Canada, the third largest in North America and the seventh largest in the world
  - World leader in the mining and oil and gas sector
  - As of March 2014, TSX had 1515 listed companies with a combined market capitalization of CAD $2,457 billion

- TSX Venture Exchange
  - Public venture capital marketplace for emerging companies
  - As of March 2014, TSXV had 2109 listed companies with a combined market capitalization of CAD $37 billion

- Numerous other holdings, products, and services

www.sharepointeurope.com
Issuer Portal

- Authenticated, targeted portal
- Multi-way conversations
- Product offerings, events, postings
- Internal and external forms
- English and French
- Agile project methodology
- Launch target of Q4 2014

“I Envision the issuer portal becoming the main point of contact with TMX, making it easier to do business with us, building engagement and stickiness with our clients, and creating a community for our staff, clients, and third parties.”

Based on conversations with Loui Anastasopoulos and the TMX team

www.sharepointeurope.com
Custom Claims in TMX

- **Company**
  - May be more than one
  - Company Type
  - Exchange (TSX or TSX Venture Exchange)
  - Sector
  - Role at company
- **Primary Company**
- **Primary Exchange**
- **Portal Roles**
- **Compound combinations of the above**
- **Used both to secure sections of the portal, and to target content to specific audiences**
Custom Claims in SharePoint

1. Access application
2. Redirect to identity provider
3. Authenticate
4. Return token
5. Return SAML Token
6. Authenticate user
7. Augment claims (By Custom Claims Provider)
8. Accept passport

Identity Provider:
- ADFS
- ACS
- [other]

TMX Gateway
SharePoint-hosted web application

SharePoint STS
Custom Claims with EUM

User

Relying Party

Identity Provider

Active Directory

Claims DB

Browse app

Not authenticated

Redirected to IP

Return SAML Security Token

Send Token

Return page and cookie

SharePoint

RP trusts IP

Authenticate

Query for user attributes

Retrieve custom claims
Office 365
Office 365 Authentication Options

**Cloud Identity**
- Windows Azure Active Directory
- No Integration

**Directory and Password Synchronization**
- Windows Azure Active Directory
- Integration with no federation
- DirSync and Password Sync
- On Premise Identity

**Federated Identity**
- Windows Azure Active Directory
- Single federated identity and credentials
- Federation
- User Sync
- On Premise Identity
ADFS Servers

Internal ADFS/DC Servers  →  DMZ ADFS Proxies

https://login.thinktecturedev.com
ADFS Server Considerations

- Should have at least two each of ADFS and ADFS Proxy Servers
- If there is only one Internet connection, consider putting them in Azure
- Having Lync and Exchange in the cloud and not being able to authenticate because your Internet pipe is down is a problem
ADFS Proxy

- ADFS Proxy role is part of ADFS 2.0 and 2.1
  - Windows Server 2008 SP2 or 2012
- Replaced with WAP in ADFS 30
  - Windows Server 2012 R2
  - Web Application Proxy
  - Reverse Proxy replacement for the discontinued Microsoft Forefront UAG and TMG
Setting Up Your Domain With Office 365

- DirSync is still used to create the shadow WAAD accounts
- Set up a trust between ADFS and Windows Azure AD
  - Setup through PowerShell
  - Requires you to setup some TXT DNS records to prove you own the domain
- Accounts need to be licensed in the Office 365 portal
- Useful links
Setting Up Your Domain With Office 365

1. Open the Windows Azure Active Directory Module.
2. Run $cred=Get-Credential. When the cmdlet prompts you for credentials, type your cloud service administrator account credentials.
3. Run Connect-MsolService –Credential $cred. This cmdlet connects you to Windows Azure AD. Creating a context that connects you to Windows Azure AD is required before running any of the additional cmdlets installed by the tool.
4. Run Set-MsolAdfscontext -Computer <AD FS primary server>, where <AD FS primary server> is the internal FQDN name of the primary AD FS server. This cmdlet creates a context that connects you to AD FS.
5. Run New-MsolFederatedDomain –DomainName <domain>, where <domain> is the domain to be added and enabled for single sign-on. This cmdlet adds a new top-level domain or subdomain that will be configured for federated authentication.
6. Using the information provided by the results of the New-MsolFederatedDomain cmdlet, contact your domain registrar to create the required DNS record. This verifies that you own the domain. Note that this may take up to 15 minutes to propagate, depending on your registrar. It can take up to 72 hours for changes to propagate through the system. For more information, see Verify a domain at any domain name registrar.
7. Run New-MsolFederatedDomain a second time, specifying the same domain name to finalize the process.
Example PowerShell

```powershell
import-module MSOnline
$msolcred = get-credential
connect-msolservice -credential $msolcred
Get-MsolUser
Get-MsolDomain
Get-MsolDomainVerificationDns -DomainName envisionit.com
```
Demo 1 Scenario

- Sample sites at https://envisionit.sharepoint.com/sites/eumwebinar
- Internal user in authenticated automatically through the ADFS Server
- Normally needs to go through the Microsoft home realm discovery page
  - This has been overridden for the tenant to go to AD FS
Microsoft Home Realm Discovery
Smart Links

- Run Fiddler as you are logging in
- Capture the 302 redirect
  - https://fedsrv.envisionit.com/adfs/ls/?cbcxt=&popupui=&vv=&username=peter%40envisionit.com&mkt=&lc=1033&wfresh=&wa=wsignin1.0&wtrealm=urn:federation:MicrosoftOnline&wctx=wa%3Dwsignin1%252E0%26rpsnv%3D3%26ct%3D1395748967%26rver%3D6%252E1%26wp%3DMBI%26wreply%3Dhttps%253A%252F%252Fenvisionit%252Esharepoint%252Ecom%252F%255Fforms%252Fdefault%252Easpx%2526lc%3D1033%26id%3D500046%26bk%3D1395748967%26LoginOptions%3D3
- Remove the highlighted text
- Add the desired URL as double-encoded text
Smart Links

https://fedsrv.envisionit.com/adfs/ls/?wa=wsignin1.0&wtrealm=urn:federation:MicrosoftOnline&wctx=wa%3Dwsignin1%252E0%26rpsnv%3D3%26ct%3D1395748967%26rver%3D6%252E1%252E6206%252E0%26wp%3DMBI%26wreply%3Dhttps%253A%252F%252Fenvisionit%252Esharepoint%252Ecom%252Fsites%252Feumwebinar%

<table>
<thead>
<tr>
<th>Character</th>
<th>Double-Encoded Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>:</td>
<td>%253A</td>
</tr>
<tr>
<td>.</td>
<td>%252E</td>
</tr>
<tr>
<td>/</td>
<td>%252F</td>
</tr>
</tbody>
</table>

- A friendly URL and redirect can be setup to hide the complex URL
- Our Custom 404 product is a good option for this
- https://productdemo.envisionit.com/eumwebinar
Extranets in Office 365

- External sharing using Microsoft accounts or other federated users
- Licensing of external users as subscribers
External Sharing

Pros
- Supported by default by Office 365
- Up to 10,000 external users can access a SharePoint Online site for free using Microsoft accounts
- Also works for other federated users with subscriptions

Cons
- Need to enable external sharing
- Email invitations are sent out
- Can be authenticated or anonymous
- Hard to hide the Microsoft experience
- No groups or central management
Licensed External Users

Pros
- Centrally managed
- Group permissions
- Full control over the login experience

Cons
- Need to pay for a subscription
Why Thinktecture over ADFS?

- Open source allows any customization
- Fully brandable (ADFS allows branding within very particular parameters)
- Login with email address instead of AD username
- Use SQL instead of AD as the underlying user repository
- Ability to incorporate the home realm discovery into the login form
Authentication Process

- Active Directory
- Thinktecture
- Office 365
Managing Your External O365 Users with EUM

- Delegate user management internally or externally to your organization
- Self-registration and approvals
- Full control over the accounts and login experience
- Delegated group management simplifies permissions
- Lost password reset
- Improved governance over your Extranet
Demo 3

- Self-registration and approval of a new external user
- [https://eum.eitdev.org/landing/register/register.aspx](https://eum.eitdev.org/landing/register/register.aspx)
- Uses the Graph API to setup the users in Office 365
Windows Azure AD Graph API

- Provides programmatic access to Azure AD through REST API endpoints
  - Create a new user in a directory
  - Get a user’s detailed properties, such as their groups
  - Update a user’s properties, such as their location and phone number, or change their password
  - Check a user’s group membership for role-based access
  - Disable a user’s account or delete it entirely
- Assigning subscriptions has been the challenge
Apps and Office 365
Apps and Office 365

- Three main types of Apps
  - SharePoint Hosted
    - Client side code only
  - Auto Hosted
    - Server code runs in an Azure instance provided by Office 365
    - No longer available as Preview has been ended by Microsoft
  - Provider Hosted
    - Use your own server environment to host your server side code
    - Doesn’t need to be Microsoft technology
No App code ever runs on the SharePoint farm
Apps are selected and installed by the end user
Need to explicitly trust the app to allow it to run
OAuth is used to provide the end-user’s authentication to the app and back to SharePoint
Challenges with SharePoint Apps

- For full functionality, apps need to be installed in each site where they are being used
- No way to programmatically install them
- This is a problem for apps that are used on many sites
Alternative App Model

- Client side code and REST APIs is the direction Microsoft is taking in general
- Use this approach for Apps too
- If Office 365 is authenticated using Thinktecture, that can be leveraged to authenticate provider hosted apps too
- Thinktecture can provide a JSON Web Token (JWT) to the client-side code
  - Similar to a SAML token
  - It is the model going forward with WebAPI
- This can be passed to and trusted by the REST API for authentication
App Authentication Process with JWT

1. User
2. Client Side Code
   - Browse app
   - No JWT
   - Redirected to IP
3. Provider App
   - App trusts IP
   - Return JWT Security Token
4. Thinktecture
   - JWT
5. User
   - JWT
   - Save Token in session
   - REST call with Token
   - Return JSON data
   - Return page
App Development Architecture

- Client side development done in AngularJS
  - Open-source platform originally developed by Google
  - Visual Studio support is being built in by Microsoft
  - Ideal for presentation logic

- Provider-hosted server side code REST APIs
  - Built in Visual Studio as a WebAPI project
  - Best place to put business logic and data access
  - Can be a high-trust app using certificates to authenticate to SharePoint
Extranet User Manager

- Easy delegation of user management to business
- Self-registration, approvals, forgotten password reset
- Simplified login for both internal and external users
Extranet User Manager Features
Branded Experience

- Maintain your corporate brand throughout the entire user experience
  - Registration
  - Login
  - Approval and welcome emails
  - All end-user pages
Single Sign-On

• Users sign in once
• As they move to other systems, they are automatically logged in
• Securely managed through SAML tokens
Self-Registration

- Fully customizable registration experience
- Fields can be added or removed
- Can be integrated into back-end systems
- Customizable approval workflow
- Full Visual Studio source code project provided
Forgotten Password

- Request a password reset by email
- Passwords themselves are never sent through email
  - One-time use, time expiring token sent
Works with SharePoint 2010 and 2013

- Does not need to be installed on the SharePoint Server
- PowerShell script setups up the trust
Office 365

- PowerShell script sets up the trust
- Hosted outside of Office 365
- Office 365 tenant can be set to automatically redirect to the EUM login page
Adaptive Design

- Leverages the Twitter Bootstrap framework
- All end-user pages adapt to smartphone, tablet, or desktop experiences
Delegated User Management

- Management of the Extranet users is delegated to the business
- IT doesn’t need to manage accounts
- Can also be delegated securely to the external organizations themselves
Azure Hosted or On Premise

- Can be installed on an on-premises server
  - SharePoint Server
  - IIS Server
- Hosted in Azure
  - Secure multi-tenant hosting
  - Managed by Envision IT
  - 7x24 monitoring and remediation
Multi-Lingual Support

- Full multi-lingual support for end user pages
- Resource files for easy translation and updating of text
Full pricing details available at www.envisionit.com/eum

- **Standard edition** $8,000 USD per production farm
  - Four hours of Premium Software Support

- **Enterprise Edition** $13,000 USD
  - Unlimited SSO authentication to claims aware applications
  - Eight hours of Premium Software Support

- 20% annual Software Assurance provides all product updates

- Dev and QA farm licenses provided with up to date Software Assurance

- Additional support packages available

- Azure hosted monthly subscription plans coming next month
# Extranet Clients

## Non-Profit
- Boys & Girls Clubs of Canada
- Centre for Addiction and Mental Health (CAMH)
- United Way of Calgary
- Heart & Stroke Foundation of Ontario
- YMCA of Greater Toronto

## Government/Public Organizations
- State of Colorado
- Supreme Court of Victoria
- Redland City Council
- National Physical Laboratory (NPL) (UK)

## Utilities
- Alberta Utilities Commission (AUC)
- Fortis Alberta
- Ontario Power Generation (OPG)

## Health Care
- Public Health Ontario
- SickKids Hospital
- Tecumseh RCT

## Education
- Education Quality and Accountability Office (EQAO)
- Blue Water District School Board

## Legal
- Stikeman Elliott

## Real Estate/Retail
- Cadillac Fairview Corporation
- LNR Property LLC
- Land Securities
- Loyalty One

## Financial
- Citi
- Transamerica Life
- Lombard Canada

## Manufacturing/Construction/Mining
- Idemitsu Kosan
- Alcan Cable
- Johnson Outdoors

## Aviation
- Montreal Airport
- Los Angeles World Airports
- NAV CANADA

## Technology
- The SCE Group
- Mercury Systems
- Restaurant Sciences
- Sony Mobile Communications

## Utilities
- Alberta Utilities Commission (AUC)
- Fortis Alberta
- Ontario Power Generation (OPG)

## Health Care
- Public Health Ontario
- SickKids Hospital
- Tecumseh RCT

## Education
- Education Quality and Accountability Office (EQAO)
- Blue Water District School Board

## Legal
- Stikeman Elliott

## Real Estate/Retail
- Cadillac Fairview Corporation
- LNR Property LLC
- Land Securities
- Loyalty One

## Financial
- Citi
- Transamerica Life
- Lombard Canada

## Manufacturing/Construction/Mining
- Idemitsu Kosan
- Alcan Cable
- Johnson Outdoors

## Aviation
- Montreal Airport
- Los Angeles World Airports
- NAV CANADA

## Technology
- The SCE Group
- Mercury Systems
- Restaurant Sciences
- Sony Mobile Communications

---

**collabcon**

---

**envision IT**
Links

- www.envisionit.com
- blog.petercarson.ca
- www.envisionit.com/eum

- Video and presentation deck will be at www.envisionit.com/events

- Customer sites
  - www.publichealthontario.ca
  - www.bgccan.com
  - www.g2gmarket.com
  - www.redcrest.com.au
  - www.transamerica.ca
  - suppliers.kinross.com
  - www.problemgambling.ca
Session Evaluations

- Go to Evaluations on the home page of [www.collabcon.org](http://www.collabcon.org)
- It is important to get your feedback
- Please fill out evaluations for all the sessions you attend
- Following the conference, a random drawing from all completed evaluations will be selected
- The winner will receive a $250 Future Shop gift card, valid online or in store