Extranet Identity Management and Authentication for SharePoint On Premise, Office 365 and Beyond

Presented by Peter Carson
President, Envision IT

October, 2014
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
Hugh Davidson

Business Development Manager, Product Sales

- e: hdavidson@envisionit.com
- p: (905) 812-3009 x222
Denesh Sohan

Director of Products

• e: dsohan@envisionit.com
• p: (905) 812-3009 x298
Corey Thokle

Project Manager

• e: cthokle@envisionit.com
• p: (905) 812 3009 ext.248
• Envision IT Overview
• Extranet Scenarios
• Extranet User Manager Overview
• SharePoint On Premises Demo
• Federation
• Office 365 Demo
• Wrap-Up and Q&A
Focused on complex SharePoint solutions, Envision IT is the “go-to” partner for Microsoft SharePoint, building integrated public web sites, Intranets, Extranets, and web applications that leverage your existing systems anywhere over the Internet.
Public Web Sites

We create interactive, content-rich customer-facing web sites that are able to grow and transform with changing needs.
Collaboration Portals

Our Collaboration Portals provide a secure space for teams to share knowledge and resources.
Intranets

Our Intranet Sites connect people to information, expertise and key business applications, and SharePoint provides a broad set of Enterprise Content Management features.
Extranets

Envision IT has a wealth of experience building Corporate Extranets that allow you to securely connect with customers and partners.
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.

• The Extranet may be added as a module into the Intranet site to only allow external users into specific sub-sites of the Intranet.
Poll 1

Which Version of SharePoint are you currently using?

• SharePoint Server 2013
• Office 365
• 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
Extranet Scenarios
SharePoint On Premise Authentication Options

Windows Authentication
- 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
• On premises SharePoint can be published externally through SSL
• Unless an additional reverse proxy is used, the login experience is very basic
• No forgotten password, change password, or self-registration
• IT needs to setup and manage external users
• No mechanism for getting credentials to users
SharePoint Extranets – Office 365

• 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
SharePoint Extranets – Forms Based Authentication

• Branded and friendly login form is possible
• Requires custom development
• Users can be stored outside of the corporate Active Directory
• Installation is manual and requires re-configuring numerous config files on the SharePoint servers
• Previous releases of Extranet User Manager (Version 2.6 and prior) addressed the login form, branding, installation, self-registration, forgotten password, and user management delegation issues
SharePoint Extranets - Federation

- Supports SharePoint 2010 and 2013 on premises, and Office 365
- Fully branded user experience
- Friendly customizable login form
- Login with email address
- Automatic login for internal users
- Customizable self-registration with approvals
- Welcome email to set credentials
- Forgotten password reset
- Delegation of user management to business or externally
- Delegated group management simplifies permissions
- Supports single sign-on to other claims-aware applications
- Improved governance over your Extranet
• Easy delegation of user management to business
• Self-registration, approvals, forgotten password reset
• Simplified login for both internal and external users
Main Components

• Administration console
  ▪ Used by IT to configure EUM
  ▪ Used by the business to manage users and groups

• End User
  ▪ Components that the Extranet users see
  ▪ Login, disclaimer, change password, forgotten password

• Registration
  ▪ Allow users to self-register
  ▪ Support approval workflows
Full pricing details available at www.envisionit.com/eum

- Standard edition $8,000 USD per production farm
  - No limits on the number of SharePoint web front ends
  - 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
Registration Form Customizations
A pending approval account has been created for TestUser1 with the username @envisionit.com.

In order to activate the user, Edit Their Record and set their status to Active.

This e-mail is intended only for the named recipient(s) and may contain information that is privileged or confidential. Any unauthorized use is strictly prohibited. If you have received this e-mail in error, or are not named as a recipient, please immediately notify the sender and destroy all copies of this e-mail.
Approve the User
Welcome Peter Carson 2,

Welcome to the Envision IT Extranet.

Your username is pcarson2.

As part of the sign-up process for this site you will be required to Set a Password before Tuesday March, 25 2014 4:52pm.

If you have not selected a password by this time you will have to Restart the Password Change Process.

You can access your sites at https://eum.eitdov.org

This e-mail is intended only for the named recipient(s) and may contain information that is privileged or confidential. Any unauthorized use is strictly prohibited. If you have received this e-mail in error, or are not named as a recipient, please immediately notify the sender and destroy all copies of this e-mail.
Forgotten Password

Forgot your password?

Email:  

Request New Password Email

© 2013 Envision IT Inc. | My License | Contact Us | Privacy Policy
Demo One – On Premises

Registration through to Login

SharePoint
Demo Scenario

- Sample site at [https://productdemo13.envisionit.com](https://productdemo13.envisionit.com)
- SharePoint 2013 on premises
- ADFS for internal users
- External users
  - In a separate AD
  - Authenticating through Thinktecture Identity Server
  - Managed with the Envision IT Extranet User Manager
**Single Sign-On**

- [https://productdemo13eum.envisionit.com](https://productdemo13eum.envisionit.com)
  - Extranet User Manager
  - Installed in its own IIS site outside of SharePoint
- [https://productdemo13sample.envisionit.com](https://productdemo13sample.envisionit.com)
  - Sample ASP.NET 4.5 Visual Studio application
  - Displays the claim information for the logged in user
Managing Your External Users with EUM

- Supports SharePoint 2010 and 2013 on premises, and Office 365
- Fully branded user experience
- Friendly customizable login form
- Login with email address
- Automatic login for internal users
- Customizable self-registration with approvals
- Welcome email to set credentials
- Forgotten password reset
- Delegation of user management to business or externally
- Delegated group management simplifies permissions
- Supports single sign-on to other claims-aware applications
- Improved governance over your Extranet
Technical Advantages

- Fully supported by Microsoft with minimal changes to the SharePoint farm
  - PowerShell script installs the required certificates into SharePoint
- No open firewall ports from DMZ to internal required
  - If internal users should be able to login externally without VPN, then ADFS needs to be published externally on port 443
- External users can be stored in a separate DMZ AD, or in a SQL database
- IT no longer needs to manage the external users, or reset their passwords
Poll 3

When would you like us to follow up?

• Right away
• November / December
• January
Single Sign-On and Federated Identities

• Trusted Identity Provider does the authentication
• Can be any SAML compliant provider
  ▪ Active Directory Federation Services
  ▪ Thinktecture Identity Server
    o 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
ADFS Servers

Internal ADFS/DC Servers

DMZ ADFS Proxies
Web Application Proxy

SharePoint

Envision IT

Leaders in SharePoint Solutions
ADFS Login Form

- Internal users shouldn’t see this inside the network
- Can be branded, within limits
Authentication Process

User

Relying Party

Identity Provider

Active Directory

Browse app

Not authenticated

Redirected to IP

Return SAML Security Token

Send Token

Return page and cookie

Authenticate

Query for user attributes

User

Relying Party

Identity Provider

Active Directory

SharePoint

RP trusts IP

Active Directory

Authenticate

Query for user attributes

Return SAML Security Token

Send Token

Return page and cookie

Browse app

Not authenticated

Redirected to IP

Send Token

Return page and cookie
Certificates

- 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
Why Thinktecture over ADFS?

- Thinktecture Identity Server is embedded in Extranet User Manager
- [www.thinktecture.com/identityAndAccessControl](http://www.thinktecture.com/identityAndAccessControl)
- 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
Demo Two – Office 365

Registration through to Login
Demo Scenario

• Sample site at https://eumdev.sharepoint.com
• EUM installed at https://eum.eitdev.org
• SharePoint Online in Office 365
• ADFS for internal users
• External users
  ▪ In a separate AD
  ▪ Authenticating through Thinktecture Identity Server
  ▪ Managed with the Envision IT Extranet User Manager
Next Steps

• Reach out to Hugh Davidson, Sales
  e: hdavidson@envisionit.com
  p: (905) 812-3009 x222

• Installation Support on Premise

• Minimum 30 day evaluation with all features enabled
Pricing

- Full pricing details available at [www.envisionit.com/eum](http://www.envisionit.com/eum)
- Standard edition $8,000 USD per production farm
  - No limits on the number of SharePoint web front ends
  - 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
Product Roadmap

- SQL User Store
- Office 365 Support
- Azure Support
- Responsive design
- Quick spin-up demo environment**
- Multifactor Authentication
- Social Identity Integration
Upcoming Events

• EIT Webinar – Oct 21st
• ESPC Webinar – Oct 30th 9am EST
  ▪ Link for registration
• Collabcon Toronto – November 24th – 25th
  ▪ www.collabcon.org
  ▪ Use the discount code ENVISIONIT for a 10% discount
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
Questions?