



CLB379

# SharePoint 2010 Extranets and Authentication

Peter Carson  
President  
Envision IT

# Introduction – Peter Carson



- President, Envision IT
- SharePoint MVP
- Virtual Technical Specialist, Microsoft Canada
- Computer Engineering, UW
- [peter@envisionit.com](mailto:peter@envisionit.com)
- <http://blog.petercarson.ca>
- [www.envisionit.com](http://www.envisionit.com)
- Twitter @carsonpeter



# Agenda

- Authentication Background
- Preparing your site
- Setting up FBA
- ADFS Federation
- Windows Live ID Federation
- Combining it all together

# Four Categories of Users



Internal  
Users



Managed  
AD Users

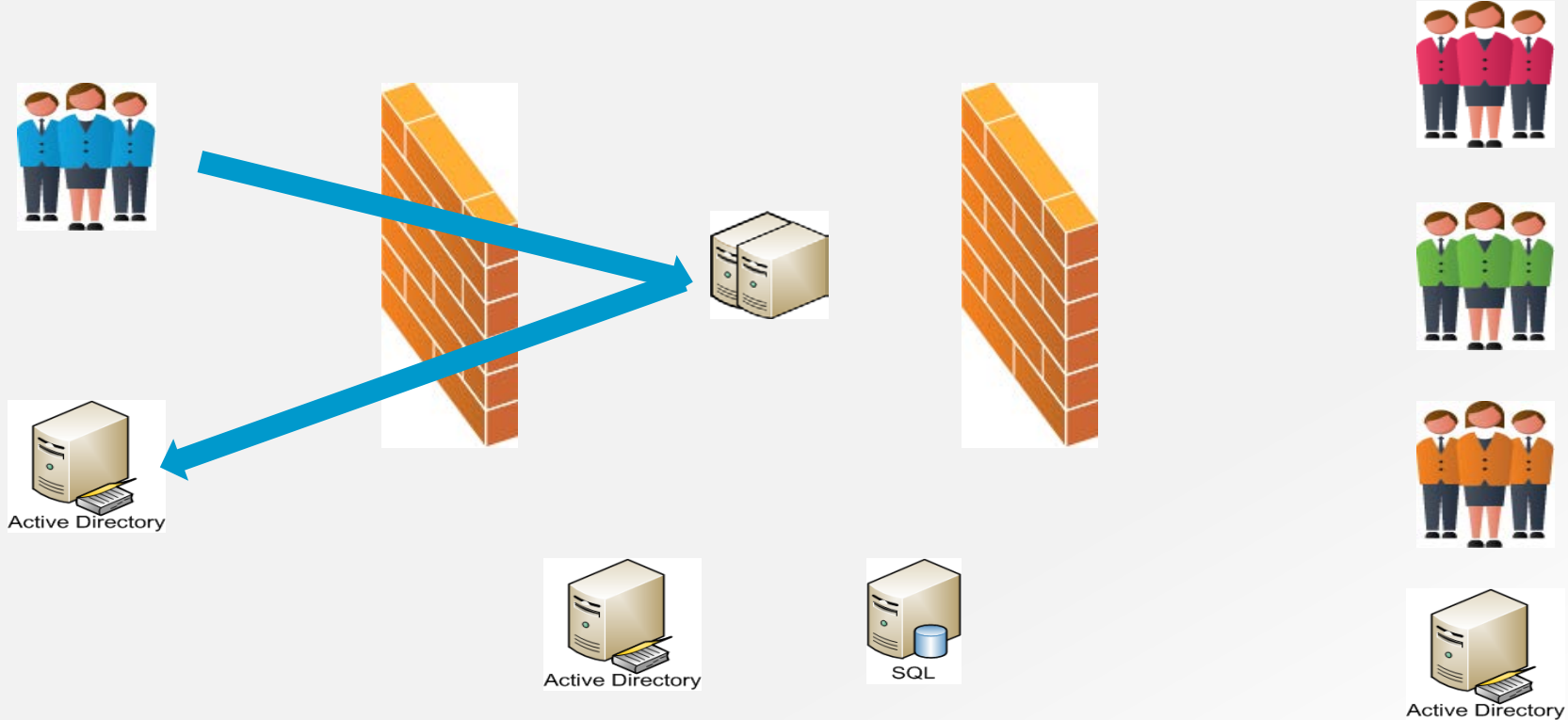


Managed SQL  
Users

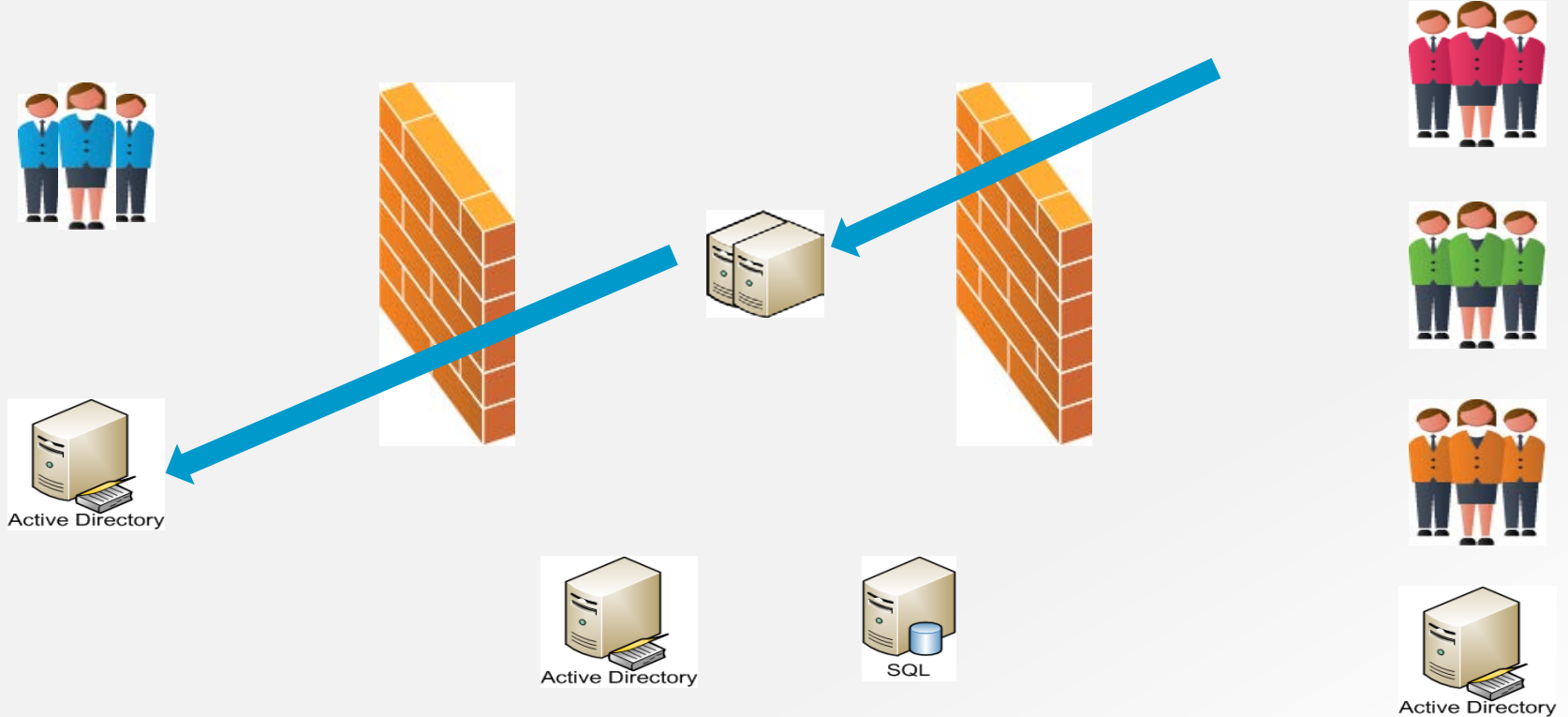


Federated  
Users

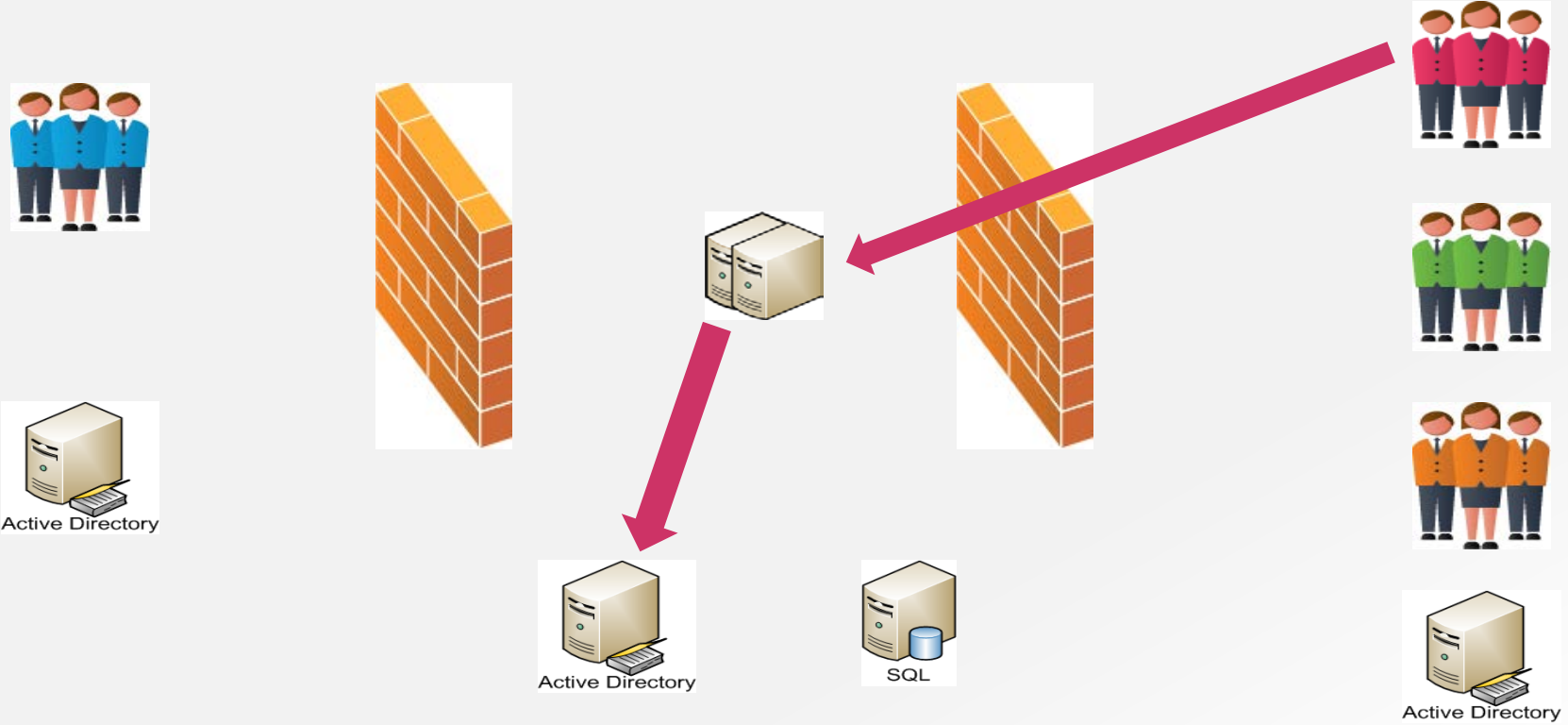
# Internal Users Accessing from Inside



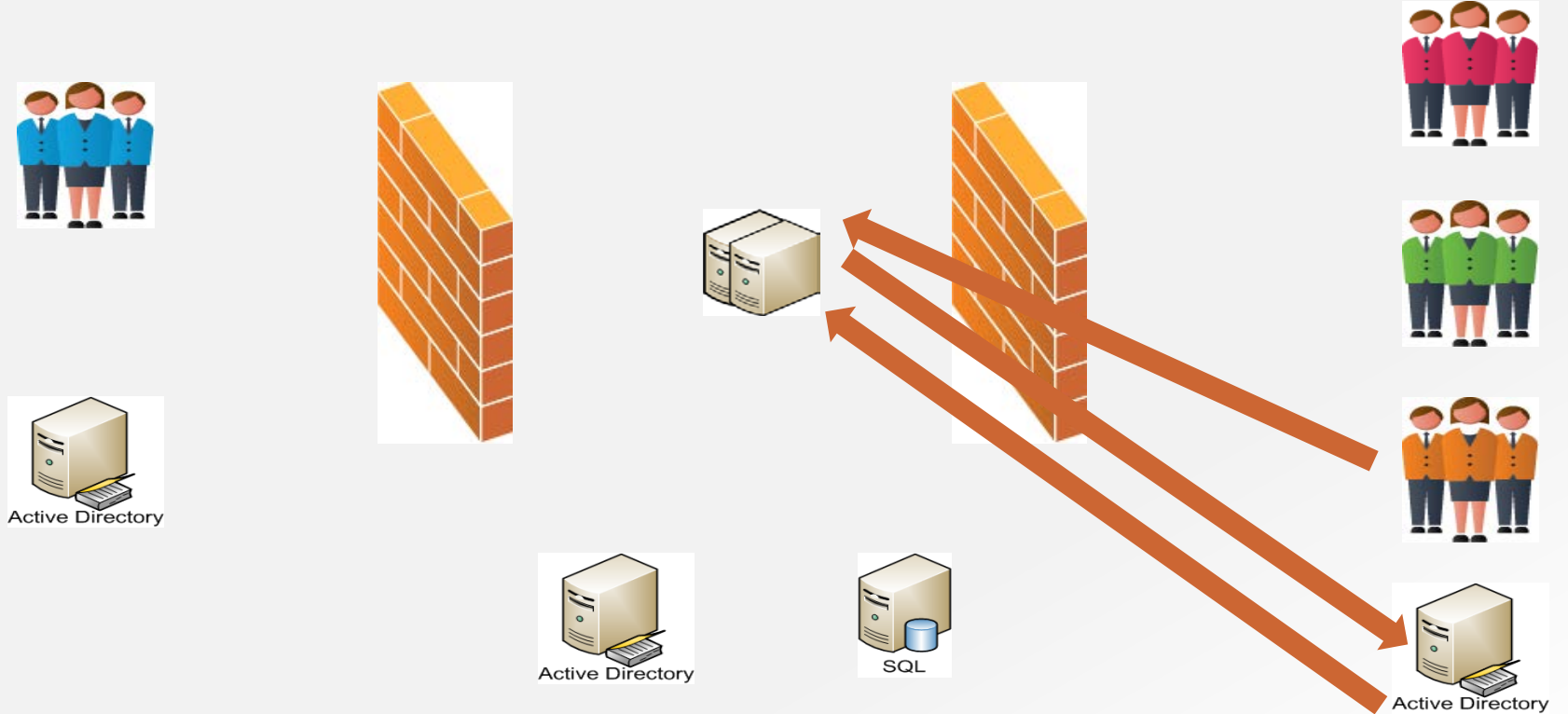
# Internal Users Working Remotely



# Managed Users



# Federated Users





# Preparing Your Site

- Ensure that the site is using Claims based security
  - If the site is Classic, there is a PowerShell script that will do a one-time conversion from Classic to Claims
    - > \$webapp = Get-SPWebApplication("<http://urlToWebApplication:Port>")
    - > \$webapp.UseClaimsAuthentication = 'True'
    - > \$webapp.Update()
    - > \$webapp.ProvisionGlobally()
- You need to have a default WA zone for the search crawler to work
- Extend the WA site to a new site for the Extranet zone
  - Generally you want to use SSL
- If the site is also going to be available anonymously you should extend it a third time for port 80 anonymous for the Internet zone

Site Actions ▾   Browse   Web Applications

New Extend Delete General Settings Manage Features Managed Paths Service Connections Authentication Providers Self-Service Site Creation Blocked File Types User Permissions Web Part Security User Policy Anonymous Policy Permission Policy

Contribute   Manage   Security   Policy

	Name	URL	Port
Central Administration			
Application Management	SharePoint - blog.joeseguini.ca80	http://blog.joeseguini.ca/	80
System Settings	SharePoint - blog.petercarson.ca80	http://blog.petercarson.ca/	80
Monitoring	SharePoint Central Administration v4	http://webserver2010:19000/	19000
Backup and Restore	SharePoint - 8080 - Previous Envision IT Public Site	http://webserver2010:8080/	8080
Security	SharePoint - www.holocausttohope.ca80	http://www.holocausttohope.ca/	80
Upgrade and Migration	SharePoint - www.miltonmasters.ca80	http://www.miltonmasters.ca/	80
General Application Settings	SharePoint - wwwa.envisionit.com80	http://wwwa.envisionit.com/	80
Configuration Wizards	SharePoint - hsfoboard.envisionit.com80	https://hsfoboard.envisionit.com/	443

### Authentication Providers

Zone	Membership Provider Name
Default	Claims Based Authentication
Internet	Claims Based Authentication
Extranet	Claims Based Authentication

# Tips to be Aware of

- If you want search to work anonymously, you need to enable anonymous access on your Windows Authentication zone
- SharePoint won't let you disable all authentication, but you can enable WA for the Internet zone, and then disable it in IIS
- SharePoint will let you configure a zone for SSL, but you still need to go into IIS to setup the certificate and bindings

# Setting up FBA

- Decide on where your users are going to be stored
  - SQL or AD are the two common choices
- Setup the store
- Configure the authentication type for the Extranet zone
- Update web.configs for SharePoint web app, Central Admin, and Security Token Service

# SQL versus AD Authentication

## AD

- Requires a separate set of domain controllers
  - These may already be in place to support the SharePoint farm
- Provides richer policy and audit controls
- Single URL inside and outside if not using FBA

## SQL

- Can use email address as the username
- Simpler to implement

# Setting up the ASPNETDB Database

- C:\Windows\Microsoft.NET\Framework64\v2.0.50727\aspnet\_regsql.exe -E -S *ServerName* -d *DatabaseName* -A all
- You need to have the -A all option to have Role support setup

# Plan your Settings

- It is critical that web.config updates are correct
- If they are wrong, SharePoint may not authenticate (without guidance as to why), or it may “blow up” entirely
- Use Envision IT’s planning worksheet to ensure no steps are missed

# Plan your Settings

Key information is

- Membership, role, and profile provider names
- Connection string name
- Provider definitions
- Connection string definition
- Custom login form URL

Excel Planning Spreadsheet helps you plan and calculate these



### 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 passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA) for this Web application. After you create an FBA Web application, additional

Enable Windows Authentication

If Windows authentication is not selected on any Zone of this Web application, crawling for this Web application will be disabled.

Integrated Windows authentication

NTLM

Basic authentication (credentials are sent in clear text)

Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name

MembershipProvider

ASP.NET Role manager name

RoleProvider

Trusted Identity provider

There are no trusted identity providers defined.

# ADFS Federation

- Delegates the authentication role to a remote domain
- On the partner side you need the following
  - Domain controller running Windows Server 2008 or 2008 R2
  - ADFS 2.0 installed and wizard run
  - STS login page secured and published externally

# ADFS Federation – Partner Side

- Setup the relying party trust in ADFS on the partner server
- You will need the published URL for your site, and create a realm that uniquely identifies your site with this ADFS
- Setup a claim rule to map LDAP (AD) attributes to the claim
  - At a minimum you'll likely want email address and groups mapped to the claim
- Export the certificate for use in SharePoint

# ADFS Federation – SharePoint Side

- SharePoint configuration is done through PowerShell
- Import the certificate from the ADFS server
- Setup the claim's attribute mapping to SharePoint
- Create the SPTrustedIdentityTokenIssuer to tie it all together
- Now it shows up as a Trusted Identity Provider in Central Admin

## Edit Authentication

Client Object Models used by some parts of the UI. Enabling this prevents users from performing some tasks using the UI if they do not have the Use Remote Interfaces permission.

### 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 passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

ASP.NET membership and role provider are used to

Enable Windows Authentication

If Windows authentication is not selected on any Zone of this Web application, crawling for this Web application will be disabled.

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

SAML Provider

# ADFS Permission Assignments

- ADFS only allows you to perform authentications, it doesn't allow you to do lookups against the remote AD
- When assigning permissions in SharePoint, SharePoint has no way of validating whether ADFS users or roles are valid
- People picker will match anything you type in as an ADFS match; you need to know if it is valid before choosing it

# Windows Live ID Integration - Test

- Configure Microsoft Services Manager
  - <https://msm.live.com/>
  - Use your Live ID to login
- Register and manage your site
- Retrieve the certificate and import into SharePoint
- Use PowerShell to create the SPTrustedIdentityTokenIssuer (similar to ADFS)

# Windows Live ID Integration - Prod

- Submit for a compliance review
- In MSM, submit the site for Production
- Retrieve the production certificate
- Repeat the import and `SPTTrustedIdentityTokenIssuer` process on the SharePoint server



# Combining It All Together

- Part of Envision IT's Extranet User Manager is our Hydra provider and EZLogin form
  - Hydra is a single provider that can sit on top of multiple providers
  - Internal AD, DMZ AD, SQL, ADFS, and Live ID can all coexist on one site
  - Allows login by email address, which determines which provider to use
  - Internal AD users are automatically logged in

# Resources



- <http://blog.petercarson.ca>
- Steve Peshka's Configuring SharePoint 2010 and ADFS v2 End to End
  - <http://blogs.technet.com/b/speschka/archive/2010/07/30/configuring-sharepoint-2010-and-adfs-v2-end-to-end.aspx>
- Hiran Salvi's Configuring Windows Live ID as Trusted Identity Provider for SharePoint 2010
  - <http://blogs.msdn.com/b/hsalvi/archive/2010/09/01/configuring-windows-live-id-authentication-provider-as-federated-identity-provider-for-sharepoint-2010.aspx>

# related sessions



- CLB271 – Practical Tips for SharePoint Governance: Oct 25, 10:30am
- CLB376 – Upgrading and Migrating to SharePoint 2010 On-Premise and in the Cloud: Oct 25, 1:00pm
- CLB277 – Why SharePoint Data Protection is Not as Easy as it Looks: Oct 26, 10:30am

# Remember To Complete Your Evaluations!

You could WIN a Samsung Focus Windows Phone 7!

Let us know what you liked & disliked!

Remember, 1=Bad, 5=Good 😊

Please provide comments!



No purchase necessary. The contest is open to residents of Canada (excluding government employees). The Toronto Tech-Days evaluation form contest begins on October 25<sup>th</sup>, 2011 and ends on October 26<sup>th</sup>, 2011. The Vancouver Tech-Days evaluation form contest begins on November 15<sup>th</sup>, 2011 and ends on November 16<sup>th</sup>, 2011. The Montreal Tech-Days evaluation form contest begins on November 29<sup>th</sup>, 2011 and ends on November 30<sup>th</sup>, 2011. Participants can enter the contest in one of two ways: (1) complete and submit an evaluation form by the contest close date; or (2) provide contact information by the contest close date. The draw for Toronto will take place on October 31<sup>st</sup>, 2011. The draw for Vancouver will take place on November 21<sup>st</sup>, 2011. The draw for Montreal will take place on December 5<sup>th</sup>, 2011. The chances of being selected depend upon the number of eligible entries. Selected participants will be contacted by phone and/or e-mail and will be required to answer correctly a time-limited skill-testing question. There are three (3) prizes available to be won. One (1) prize will be given away for each Tech-Days event in Toronto (October 25-26 2011), Vancouver (November 15-16 2011) and Montreal (November 29-30 2011). The prize consists of a Samsung Focus Windows Phone 7 (handset only; voice and/or data plan not included) (approximate retail value of \$499 CAD). The prize will be delivered to the shipping address designated by the winner within 6-8 weeks. The winner may be required to sign a declaration and release form. For full contest rules, please see a Microsoft Tech-Days representative.

**You can email any additional comments directly to  
[td\\_can@microsoft.com](mailto:td_can@microsoft.com) at any time.**

**Q & A**

***Microsoft***<sup>®</sup>