BV 204 - Extranets in SharePoint On Premises and Office 365

April 20, 2017

Peter Carson



- President, Envision IT
- SharePoint MVP
- Partner Seller,Microsoft Canada



- peter.carson@extranetusermanager.com
- http://blog.petercarson.ca
- www.envisionit.com
- Twitter @carsonpeter
- VP Toronto SharePoint User Group

Agenda

- Introduction to Extranets
- Scenarios
- Licensing
- Extranet User Manager
- Office 365 Demo
- Client Demos
- Wrap-Up and Q&A

What is an Extranet

- An <u>Extranet</u> 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?

Technologies

S > SharePoint	Microsoft's collaboration platform that provides portals, document management, web content management, and much more
Office 365	Microsoft's cloud hosted versions of Exchange (email), Lync (instant messaging), and SharePoint
Microsoft Azure	Microsoft's infrastructure and platform hosted services
ExtranetUserManager for SharePoint	Envision IT's tool for managing users outside your organization

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

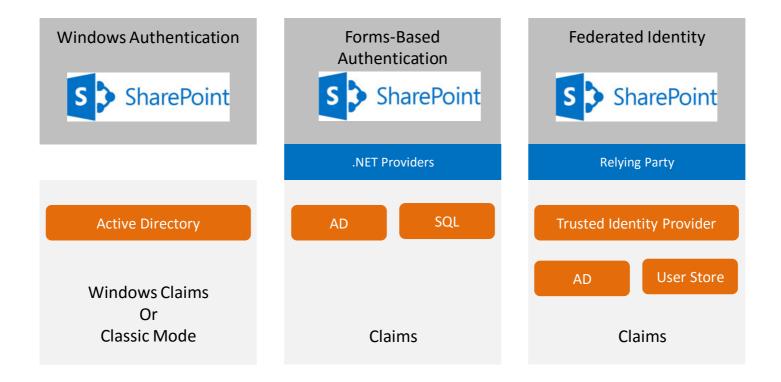
Poll 2

How do you use SharePoint today?

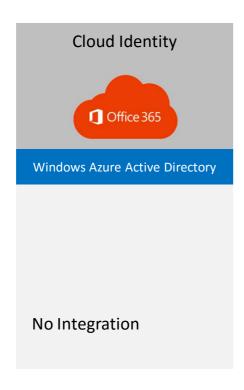
- Internal collaboration
- Internal web publishing (Intranet)
- Extranets
- Public facing website

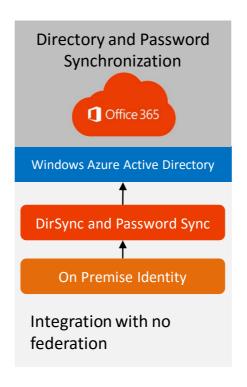
SharePoint Authentication

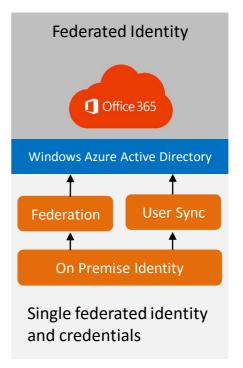
SharePoint On Premise Authentication Options



Office 365 Authentication Options







On Premise Extranet Scenarios

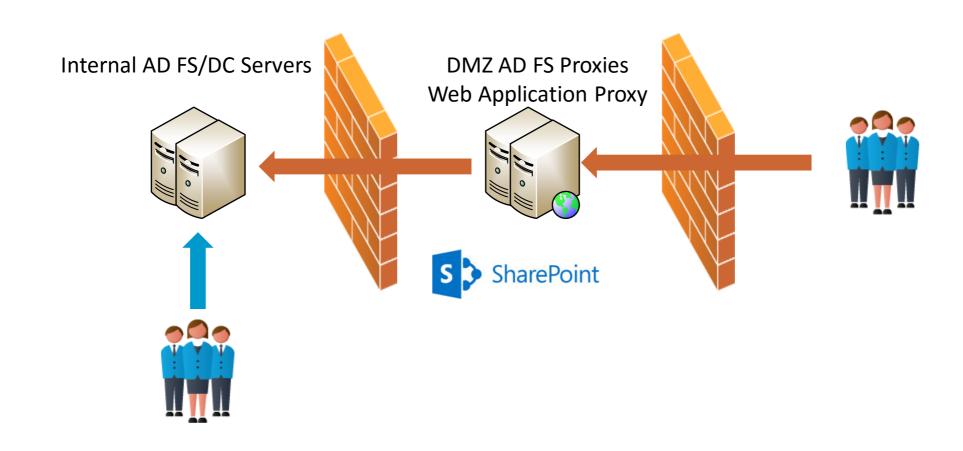
On Premises Forms-Based Authentication

- 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

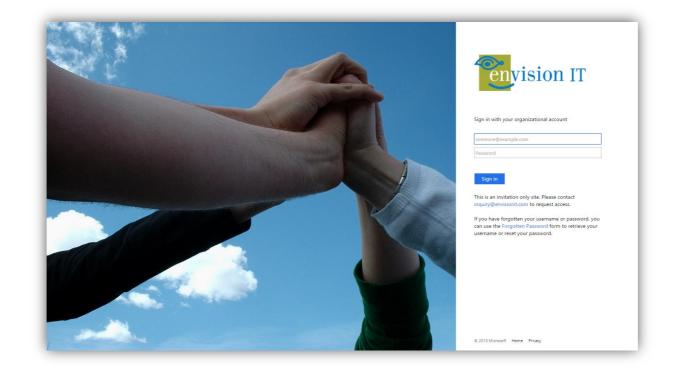
- Works with both SharePoint on premises and in Office 365
- Light integration to either
- Trusted Identity Provider does the authentication
- Can be any SAML compliant provider
 - Active Directory Federation Services
 - Thinktecture Identity Server
 - www.thinktecture.com
 - Social identities
- Can 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

AD FS Servers

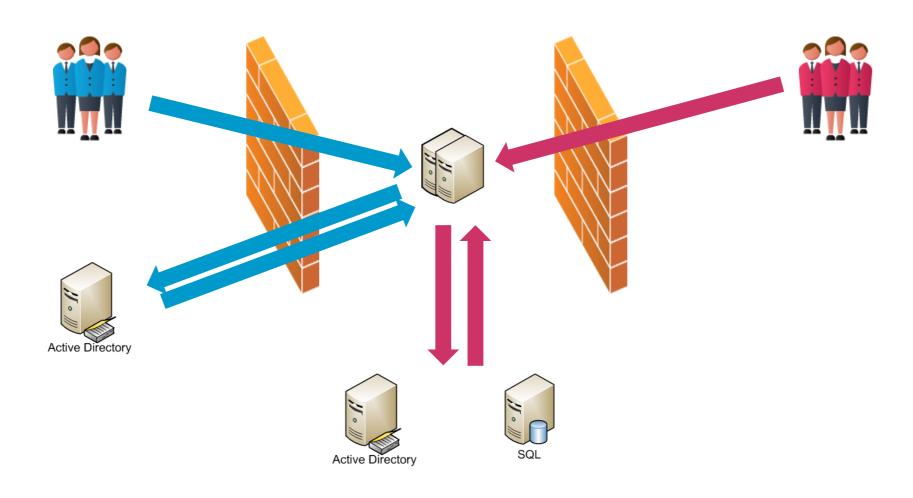


AD FS Login Form

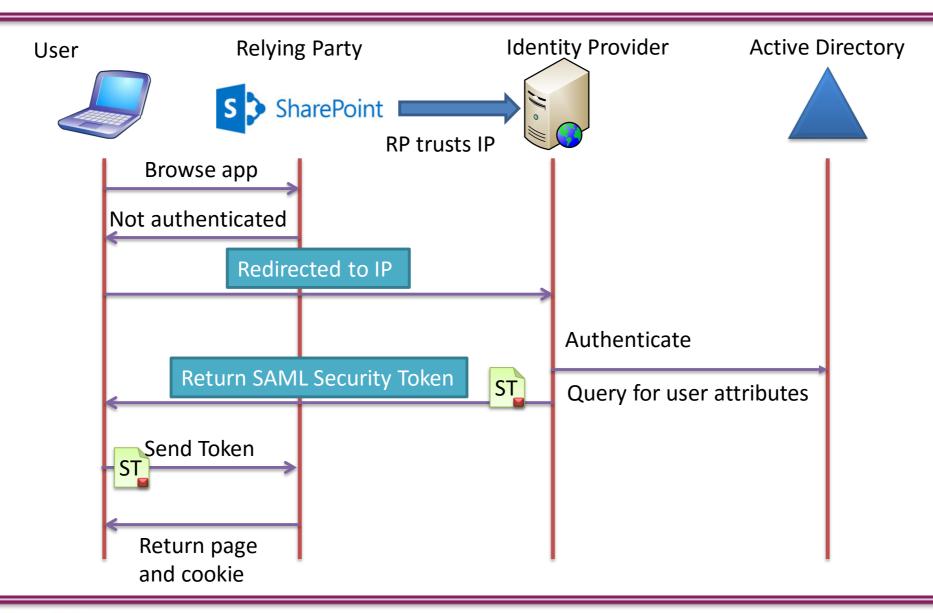
- Internal users shouldn't see this inside the network
- Can be branded, within limits



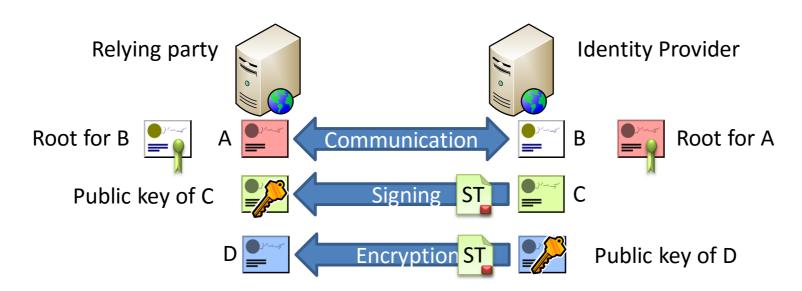
Federation



Authentication Process



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 Identity Server over ADFS?

- Thinktecture Identity Server is embedded in Extranet User Manager
- <u>www.thinktecture.com/identityAndAccessControl</u>
- 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 – SharePoint 2013

Registration through to Login



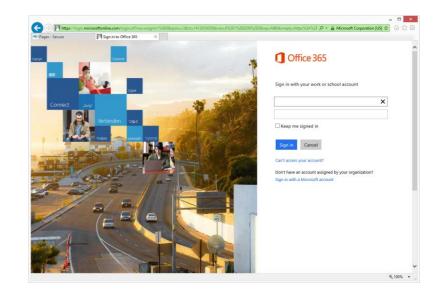
Demo Scenario

- SharePoint 2013 sample site at https://productdemo13.envisionit.com
- EUM installed at https://productdemo13eum.envisionit.com
- 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

Office 365 Extranet Scenarios

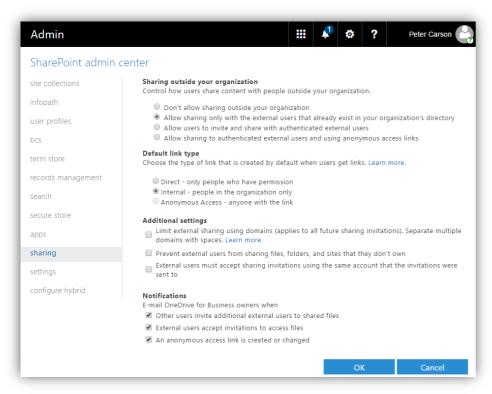
Office 365 External Sharing

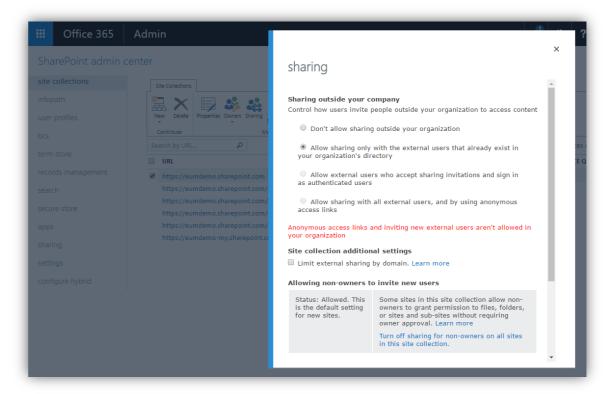
- Unlimited free external users in your Office 365 subscription through External Sharing
- Must use the Microsoft login form
- External users
 - Microsoft account
 - Office 365 subscriber
 - Azure AD tenant and account will be created
- "Light-weight solution"
 - Bill Baer Microsoft Senior Product Marketing
 Manager and Microsoft Certified Master for SharePoint
 2007 in the SharePoint product group



Enabling External Sharing in SharePoint Online

- Needs to be applied at the tenant and site collection level
- Managed through SharePoint admin center





Azure AD B2B



Simple

- Partners are invited into your Azure AD
- Each partner user uses an existing Azure AD account or one that is easily created during invitation acceptance
- Permissions can be managed through Azure AD groups

Secure

- All access is controlled through your Azure AD directory
- Partner users can be removed from your Azure AD and their access is immediately revoked
- When the partner user leaves the partner organization, access is lost automatically

Seamless

- Partner companies who need access do not need to have Azure AD
- Azure AD B2B collaboration provides a simple user sign-up experience for these partners

Azure AD B2B and Office 365





- Partner users can be granted access to any part of your SharePoint Online
- Considered external users by Microsoft
- No Office 365 subscription is required for the partner users
- Permissions in SharePoint Online can be applied to Azure AD groups
- Site owners can manage the Azure AD group membership through EUM

B2B Experiences

User Type	Experience
Existing Office 365 or Azure AD user	Logs in with their Azure AD credentials to accept the invitation
Business email not in Azure AD	Azure AD tenant is created behind the scenes User creates a password Can provide their name and country Azure AD manages the password reset requirements Tenant can be converted to a fully managed Azure AD tenant later
Consumer email (Gmail, Hotmail, etc.)	Account is converted to a Microsoft account in the background

Azure B2B Current Preview Limitations

- Delegation of user management is supported, but it is all or nothing
 - No way to restrict access to users in a group
- Managed through the Azure portal
 - Can be overwhelming for business users
- No self-registration or approval process
- No integration to other line of business systems
 - Profile management, CRM integration, account verification
- No integration to on premises AD
 - This can be used with Azure Application Proxy to provide access to on premise systems through
 B2B single sign on

Quick Win Scenarios

- Development tenants
 - Typically one user account shared by multiple people
 - Use Azure B2B to invite the full development and client teams
 - No need for In Private browser windows and additional logins
- Small Extranets
 - Board of Director portals
 - Smaller organizations
 - POC
 - Centrally managed invitations

Guest Inviter Role

- Initially you had to be a global admin in Azure to invite users
- Guest Inviter role can be delegated to other users
- Applied through PowerShell

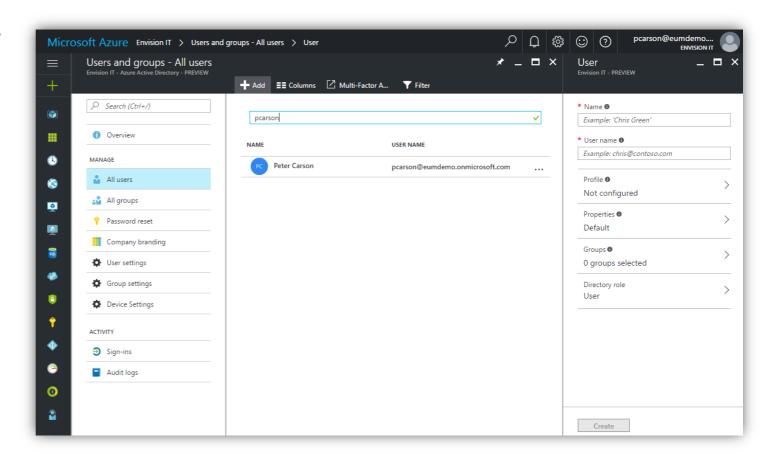
```
$inviter = get-msolUser -UserPrincipalName alias@domain.com $inviterRole = get-msolRole
-RoleName 'Guest Inviter'

Add-MsolRoleMember -RoleName 'Guest Inviter' -RoleMemberObjectId $inviter.ObjectId

Get-MsolRoleMember -RoleObjectId $inviterRole.ObjectId
```

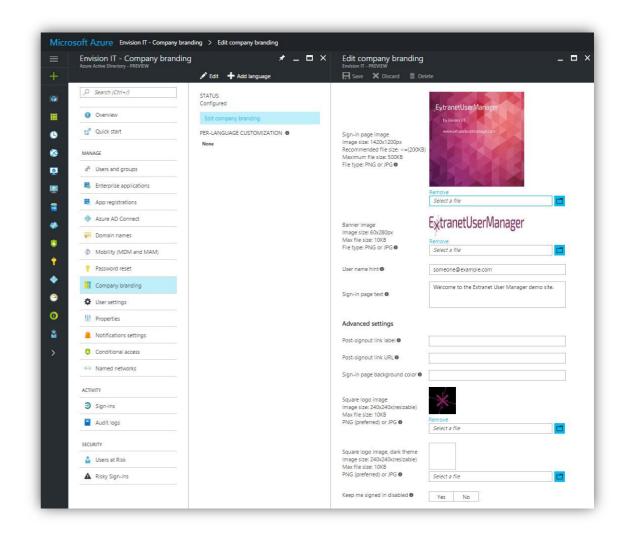
Managing External Users

- Managed through the new Azure portal
- https://portal.azure.com



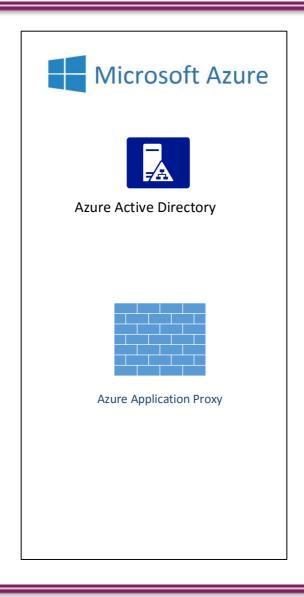
Azure AD Branding

- Images, logos, and text for sign-in page
- Managed through the new Azure portal
- https://portal.azure.com

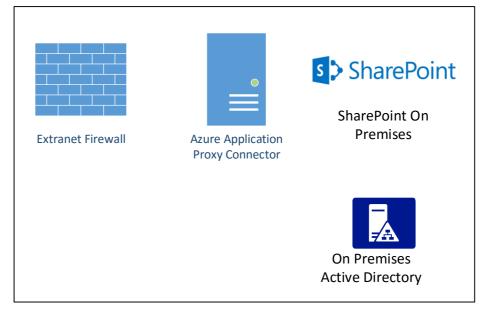


Office 365 and On Premises SharePoint Hybrid Extranet

Azure Application Proxy







Extranet Licensing

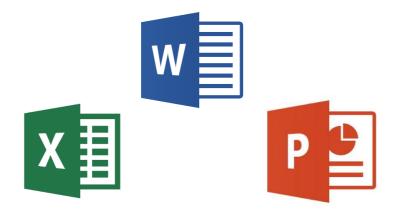
SharePoint 2013 Licensing

2013	Intranet	Extranet	Internet Sites
Internal Users	SharePoint Server + CAL	SharePoint Server + CAL	Chana Daint Camuan
External Users*	N/A	SharePoint Server	SharePoint Server

- 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?

Scenario	Internal User
Read Office documents via Office Web Apps	Free, no Office client required
Edit Office documents via Office Web Apps	Requires Office 2013 Standard or Professional Plus

 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?

Scenario	External User*
Read Office documents via Office Web Apps	Free, no Office client required
Edit Office documents via Office Web Apps	Free, no Office client required

^{*}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

	Business		Enterprise			
See options for: Education Government Nonprofit Home	Office 365 Business Essentials	Office 365 Business	Office 365 Business Premium	Office 365 Enterprise E1	Office 365 ProPlus	Office 365 Enterprise E3
	Learn more →	Learn more →	Learn more →	Learn more →	Learn more →	Learn more →
Individual services: Business-class email File storage & sharing Online meetings	\$5.10 user/month (annual commitment) 1 year \$5.10 user/month	\$10.50 user/month (annual commitment) 1 year \$10.50 user/month	\$12.90 user/month (annual commitment) 1 year \$12.90 user/month	\$8.20 user/month (annual commitment)	\$15.20 user/month (annual commitment)	\$23.20 user/month (annual commitment)
Plus applicable tax	Buy now	Buy now	Buy now	Buy now	Buy now	Buy now
User maximum	300	300	300	Unlimited	Unlimited	Unlimited

https://products.office.com/en-ca/business/compare-more-office-365-for-business-plans

SharePoint Online



Compare SharePoint options

SharePoi	nt Server	SharePoint Online		
Standard	Enterprise	Plan 1	Plan 2	
Licensing options →	Try now Licensing options →	\$5.10 user/month Buy now	\$8.20 user/month	

Plus applicable tax

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

SharePoint Online External Users

- External users invited through SharePoint or Azure AD B2B
- No license required for SharePoint Online
- Must be external to your organization can't use it for staff
- Each paid Azure AD Basic or Premium also allows five equivalent Azure AD licenses for external users

Client Demos

- Public Health Ontario
 - www.publichealthontario.ca
- Ontario Association of Children's Aid Societies
 - <u>oacas.sharepoint.com</u>
- 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
- ivari Public Web Site and Advisors Portal
 - www.ivari.ca
- Kinross Gold Supplier Portal
 - <u>suppliers.kinross.com</u>
- CAMH Problem Gambling Professionals
 - www.problemgambling.ca

Extranet User Manager

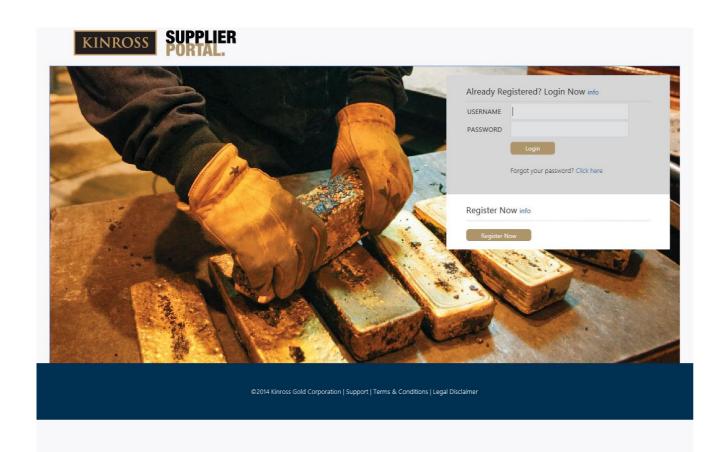




- Easy delegation of user management to business
- Self-registration, approvals, forgotten password reset
- Simplified login for both internal and external users

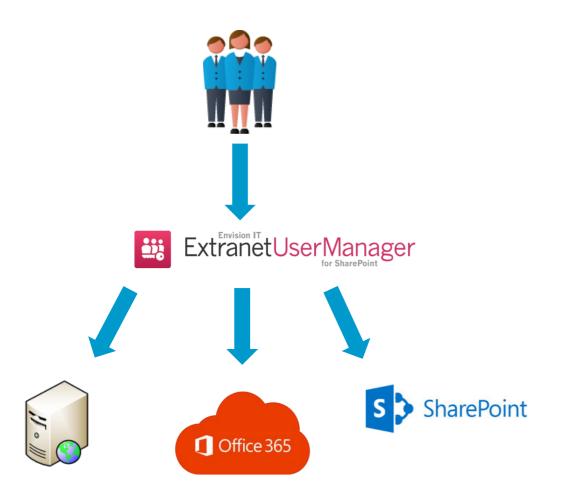
Extranet User Manager Features

Branded Experience



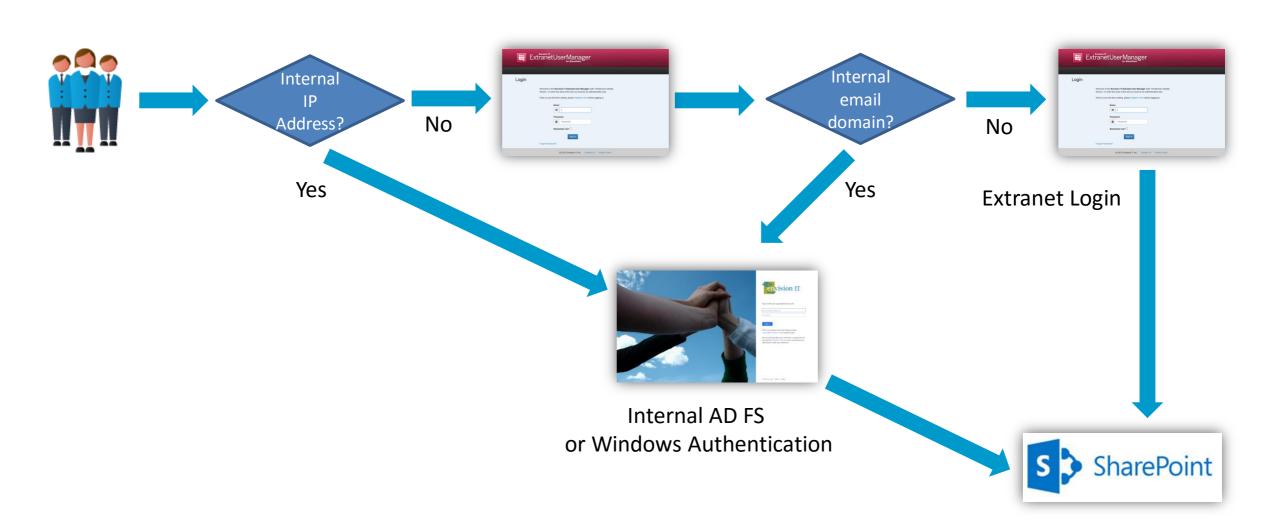
- Maintain your corporate brand throughout the entire user experience
 - Registration
 - Login
 - Approval and welcome emails
 - All end-user pages

Single Sign-On

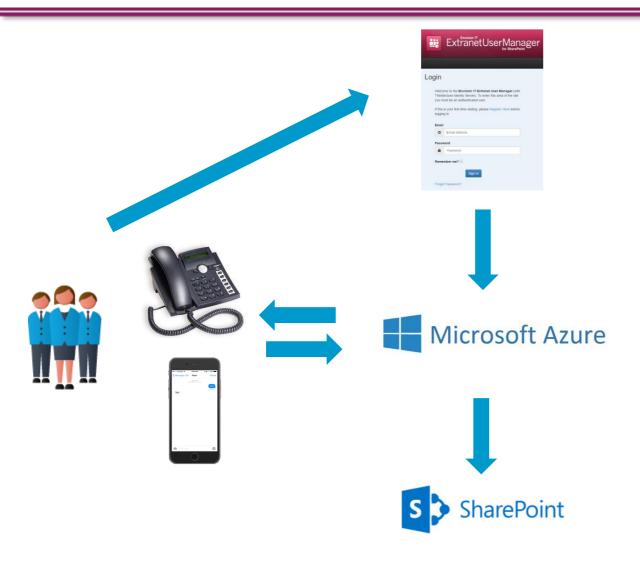


- Users sign in once
- As they move to other systems, they are automatically logged in
- Securely managed through SAML tokens

ezRealm Home Realm Discovery

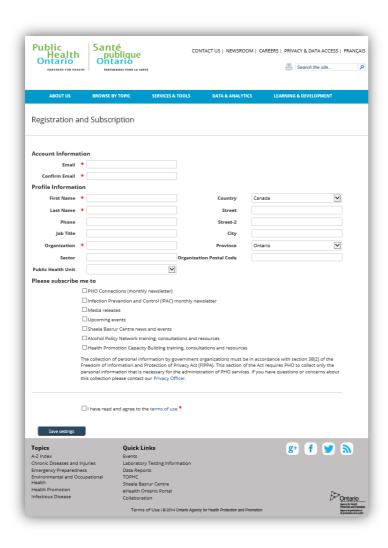


Multi-Factor Authentication



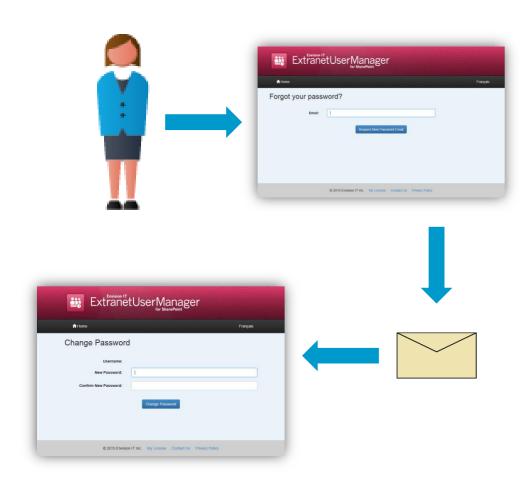
- Second factor authentication through a phone call or text message
- Infrastructure provided by Azure
 MFA service

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, 2013, and 2016



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

Office 365



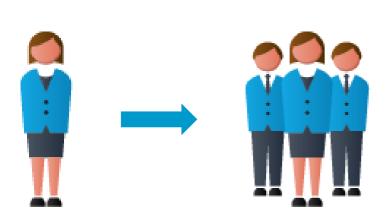
- PowerShell script setups up the trust
- Hosted outside of Office 365
- Office 365 tenant can be set to automatically redirect to the EUM login page

Adaptive Design



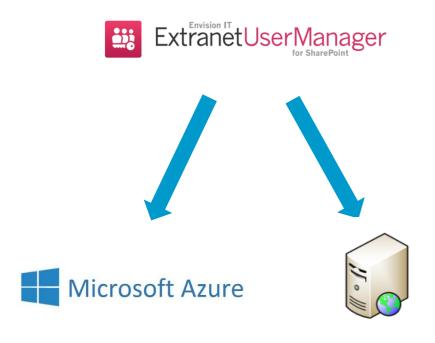
- Leverages the Twitter Bootstrap framework
- All end-user pages adapt to smartphone, tablet, or desktop experiences

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

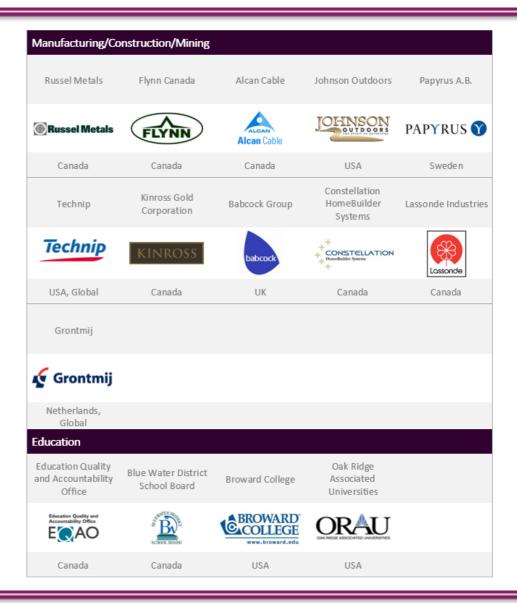
Extranet User Manager Licensing

Version	On Premise	Hosted
Standard Edition	\$8,000	\$850 / month
Enterprise Edition	\$13,000	\$1,070 / month
Annual Software Assurance	20%	Included

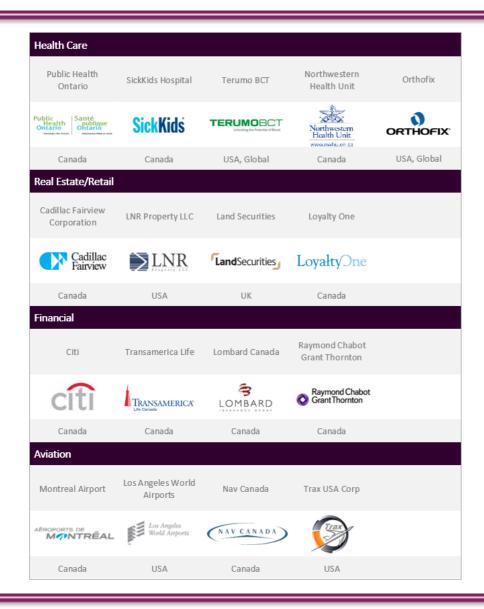
 Full pricing details available at <u>https://www.extranetusermanager.com/Pricing</u>

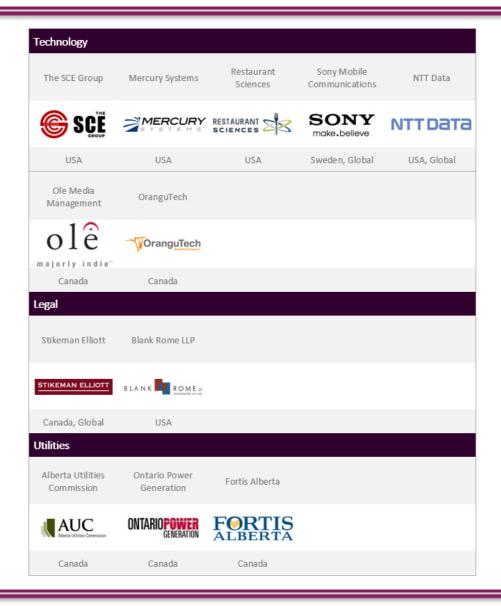
Extranet Clients

Non-Profit				
Boys and Girls Clubs of Canada	Centre for Addiction and Mental Health	United Way of Calgary	Heart and Stroke Foundation of Ontario	YMCA of Greater Toronto
Boys & Girls Clubs of Canada Clubs Garçons et Filles du Canada	camh Centre for Addiction and Mental Health	United Way Calgary and Area	HEART&* STROKE FOUNDATION	YMCA GRATIA IGROVIO
Canada	Canada	Canada	Canada	Canada
Ontario Association of Children's Aid Societies	Canadian Agency for Drugs and Technologies in Health			
Ontario Association of Children's Aid Societies the ease of total authors is Origin	CADTH			
Canada	Canada			
Government/Publi	c Organizations			
State of Colorado	Supreme Court of Victoria	Redland City Council	National Physical Laboratory	International Development Research Centre
	Terrorit	Redland CITY COUNCIL	NPL () National Physical Laboratory	IDRC 💥 CRDI
USA	Australia	Australia	UK	Canada
City of Charlotte	Oakland County	Islington Council		
CHARLOTTE.	OAKIAND COUNTY	* ISLINGTON		
USA	USA	UK		



Extranet Clients





Links

- www.envisionit.com
- blog.petercarson.ca
- www.envisionit.com/eum
- Video and presentation deck will be at <u>www.envisionit.com/events</u>
- Customer sites
 - www.publichealthontario.ca
 - www.bgccan.com
 - www.g2gmarket.com
 - www.redcrest.com.au
 - www.ivari.ca
 - suppliers.kinross.com
 - www.problemgambling.ca

Questions?