The Case for Using Forms-Based Authentication (FBA) and the SQL Membership Provider for Implementing a SharePoint Extranet

PremierPoint
Solutions

Microsoft SharePoint is fast becoming the extranet platform of choice for companies worldwide.

Introduction

Increasingly, companies are discovering the many benefits of having an extranet. These benefits include:

- ✓ Streamlining communications and enabling companies to stay in closer contact with clients, vendors, and business partners
- ✓ Improving productivity and efficiency
- ✓ Enabling users to collaborate and share information more effectively, conveniently, and securely
- ✓ Giving companies the ability to update information instantly

Microsoft SharePoint is fast becoming the extranet platform of choice for companies worldwide. SharePoint has many built-in tools which enable collaboration and boost efficiency. Its versatility and extensibility make it an excellent choice for an extranet platform.

Once an organization determines it needs an extranet to collaborate with a trusted circle of people outside the company, a number of challenges arise when it comes to deploying and managing an extranet.

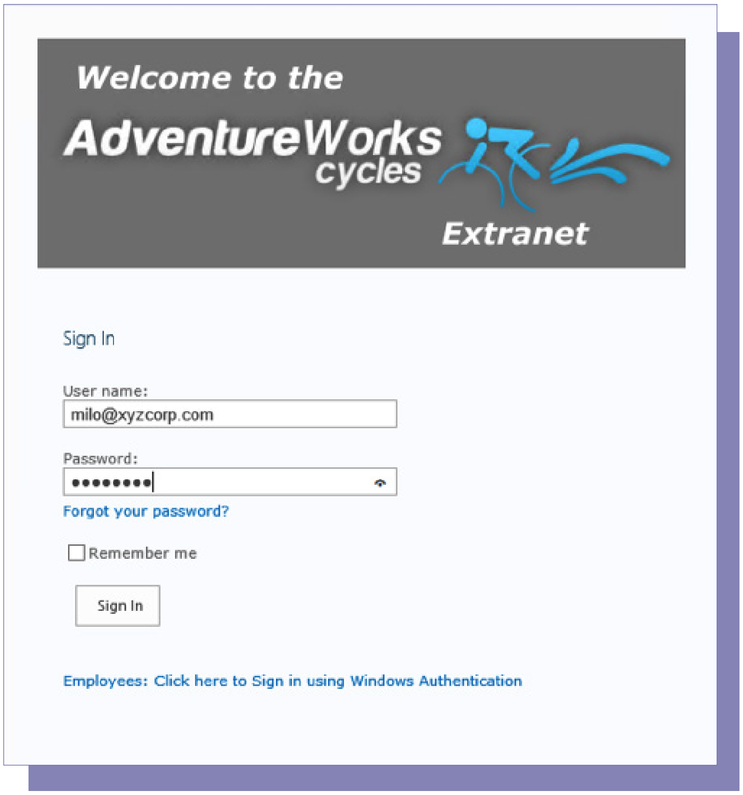
One of the biggest challenges is the need for **access security that is watertight but allows extranet users easy access** to the information they need. This paper will focus on the benefits of using FBA and the SQL Membership Provider in on-premises SharePoint to **achieve that iron-clad security.**

PremierPoint Solutions' Extranet Collaboration Manager for SharePoint Server and Foundation (ExCM) is a SharePoint add-in that provides the easy extranet collaboration and simplified extranet administration that SharePoint is missing in the out-of-the-box product. When ExCM is combined with FBA and SQL, the result is a comprehensive extranet solution.

Active Directory or FBA and SQL for Authentication?

Rather than using Active Directory for authenticating external users, PremierPoint Solutions believes that

Using a SQL Server-based Membership Provider with Forms-Based Authentication for logins is a **better solution**.



Sign In

User name:
milo@xyzcorp.com

Password:
••••••••

Forgot your password?

□ Remember me

Employees: Click here to Sign in using Windows Authentication

FBA gives a company a method to authenticate user credentials by having the user complete and submit an editable web form before logging into a system or service. FBA uses a custom database, which is created separately from Active Directory, to store user credentials. And the **FBA login screen is friendly to users, and not confusing or intimidating**, as AD login screens can sometimes be.

For instance, a custom-branded login screen like this could be provided for extranet users to login.

Using FBA and SQL Membership Provider together is fast, easy, secure, and extensible. Other solutions can be expensive and require separate hardware. They also are more difficult to implement and time consuming.

Advantages of FBA and SQL

Companies typically don't want to add external users to their Active Directory for two important reasons:

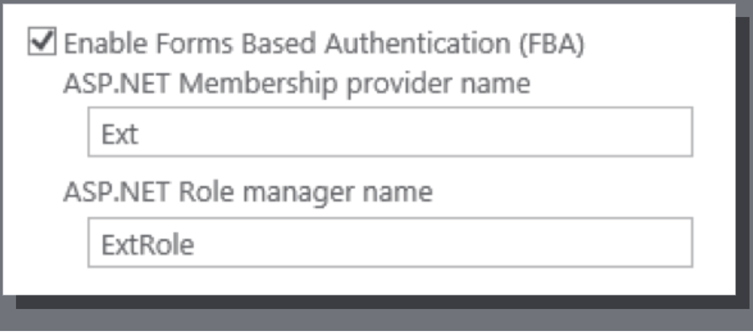
1. it requires too much administrative overhead to manage user accounts, passwords, and profile information on top of their company's Active Directory users, and

2. most would want to have a security separation to keep non-employees out of their company's Active Directory, which means a place would be required to store these external users

The good news is that FBA is built into SharePoint, and a company only needs to check a box and fill in two boxes to enable FBA in a SharePoint environment.

Here is a screenshot of the Authentication Providers screen for a SharePoint web application:

The combination of FBA and SQL utilizes the SQL Membership Provider for both **ease** and **security**.



☑ Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name

Ext

ASP.NET Role manager name

ExtRole

Internal users continue to use their Active Directory credentials to log in to the extranet, while external users are stored securely in SQL. Because the SQL Membership Provider is from Microsoft, a good deal of documentation about the schema is available online.

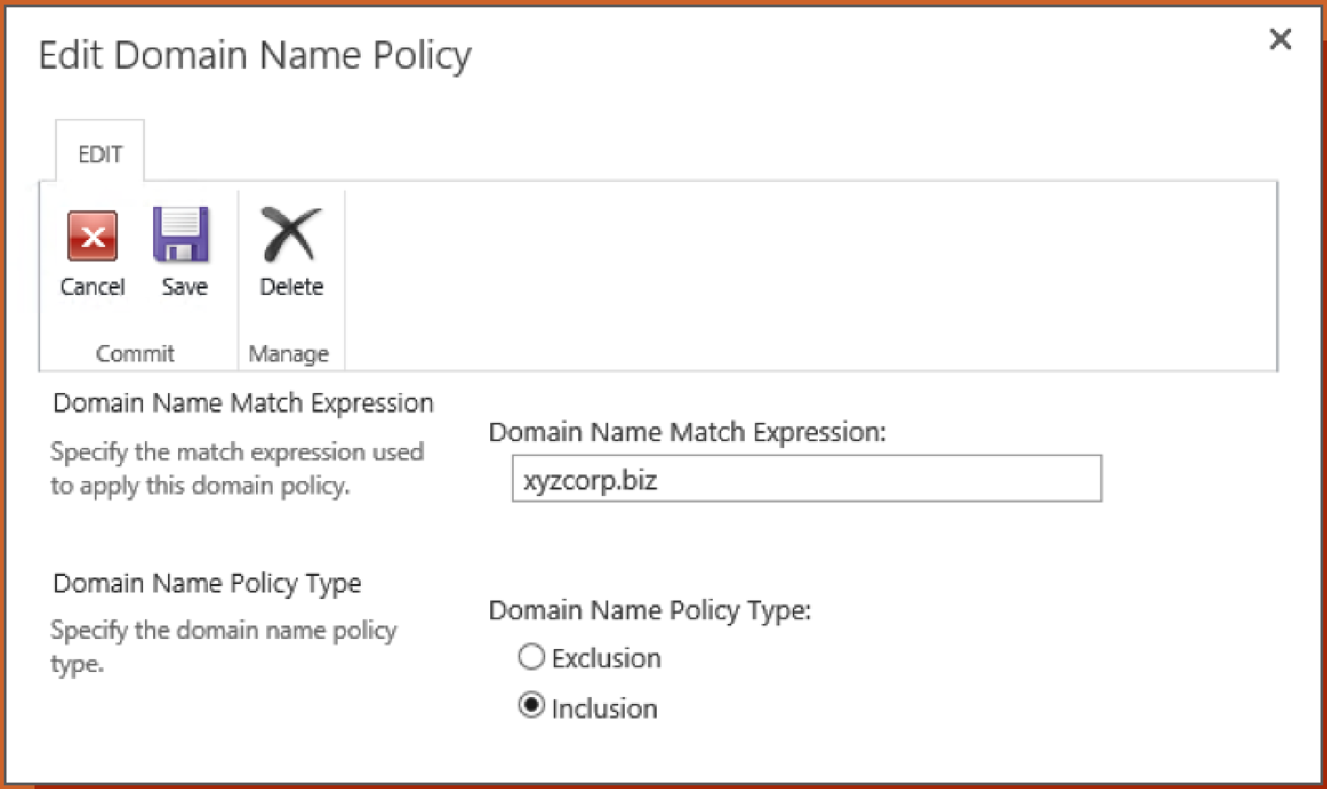
With this approach, external users use their email address as their account username,

▶ which is easy to remember

▶and ensures uniqueness

▶as well as security.

When used in conjunction with ExCM from PremierPoint Solutions, **this approach gains additional security through the use of domain-name policies**, which can be "inclusions" or "exclusions." These can be set globally, per site, or per site collection.



Edit Domain Name Policy

Domain Name Match Expression

Specify the match expression used to apply this domain policy.

Domain Name Match Expression: xyzcorp.biz

Domain Name Policy Type

Specify the domain name policy type.

Domain Name Policy Type:

○ Exclusion

● Inclusion

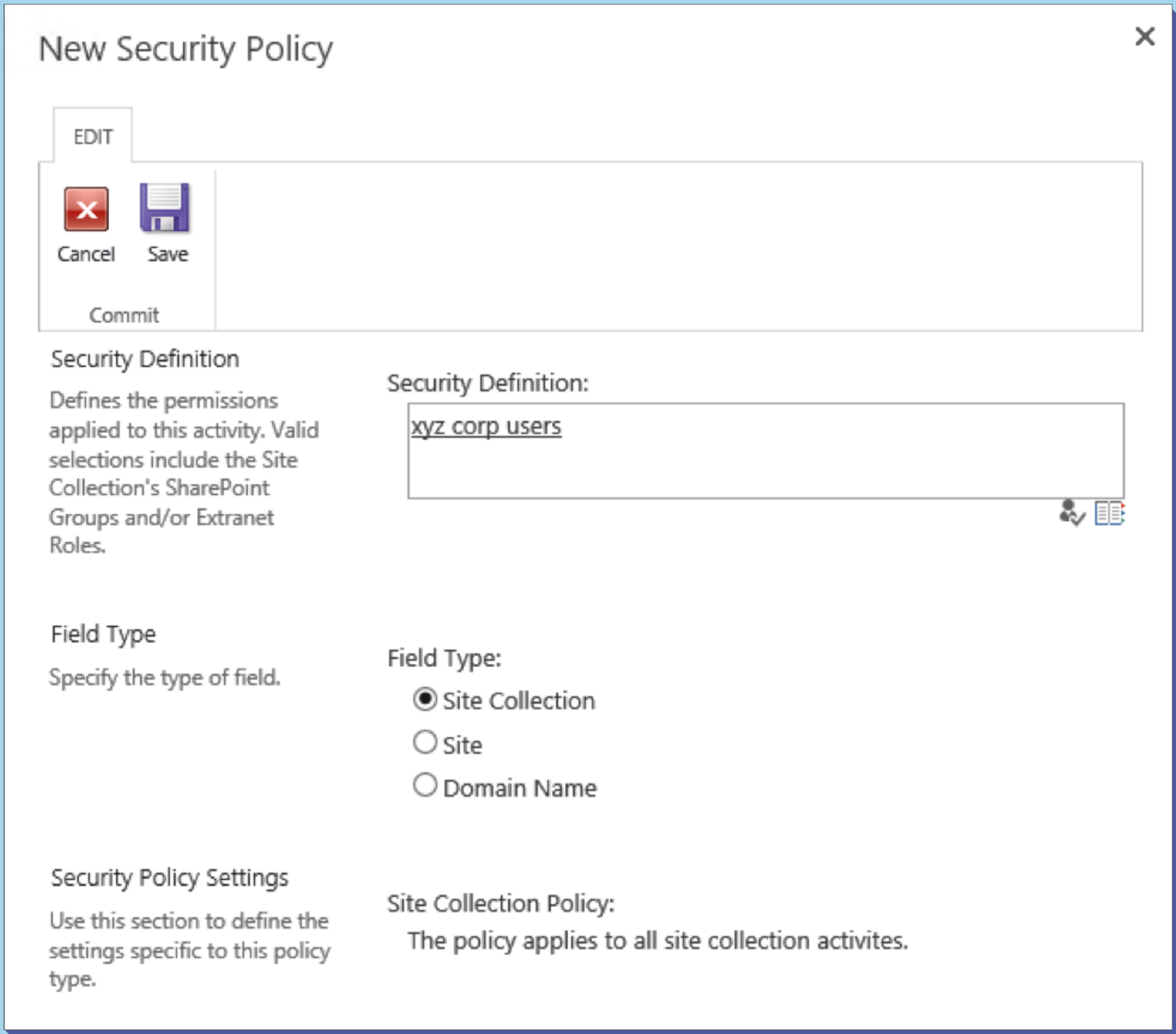
A company might set an exclusion policy, for example, specifying that no one is allowed to register for an extranet account with a "generic" Internet mail address such as @yahoo.com, @gmail.com, or @hotmail.com. Or, conversely, the company might set an inclusion policy specifying that the site must only contain users with @companyB.com email addresses.

Domain name policies are one of many completely configurable options ExCM provides to help secure an extranet to specific requirements.

Other examples are site-security policies; password strength requirements; account expiration and lockout policies; customizable approval workflows; terms and conditions acceptance; and captcha support for forms.

Here are some examples of these features in use:

Security Policies



Security Definition

Defines the permissions applied to this activity. Valid selections include the Site Collection's SharePoint Groups and/or Extranet Roles.

Security Definition:

xyz corp users

Field Type

Specify the type of field.

Field Type:

● Site Collection
○ Site
○ Domain Name

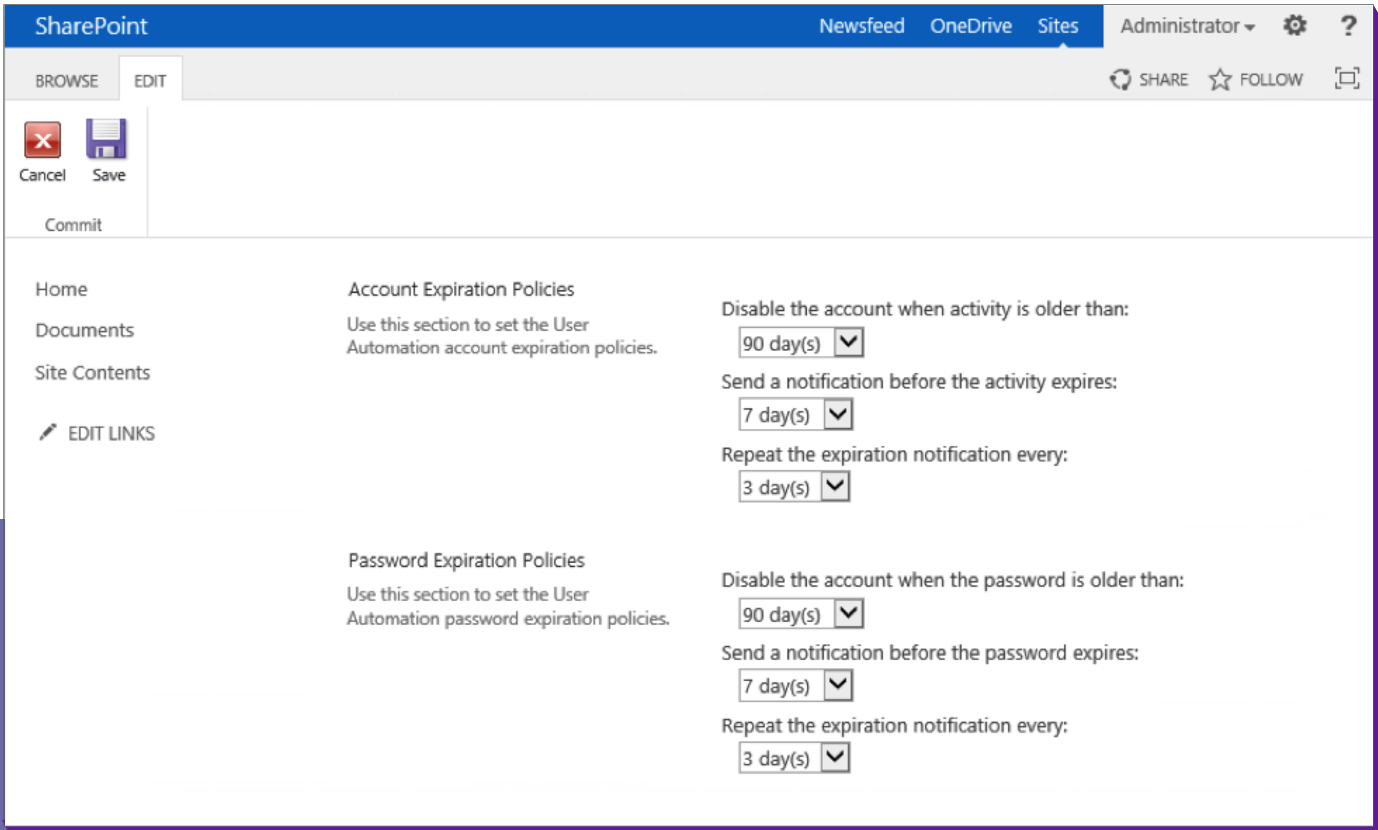
Security Policy Settings

Use this section to define the settings specific to this policy type.

Site Collection Policy:

The policy applies to all site collection activites.

Password and Account Expiration Policies



Account Expiration Policies

Use this section to set the User Automation account expiration policies.

Disable the account when activity is older than: 90 day(s)

Send a notification before the activity expires: 7 day(s)

Repeat the expiration notification every: 3 day(s)

Password Expiration Policies

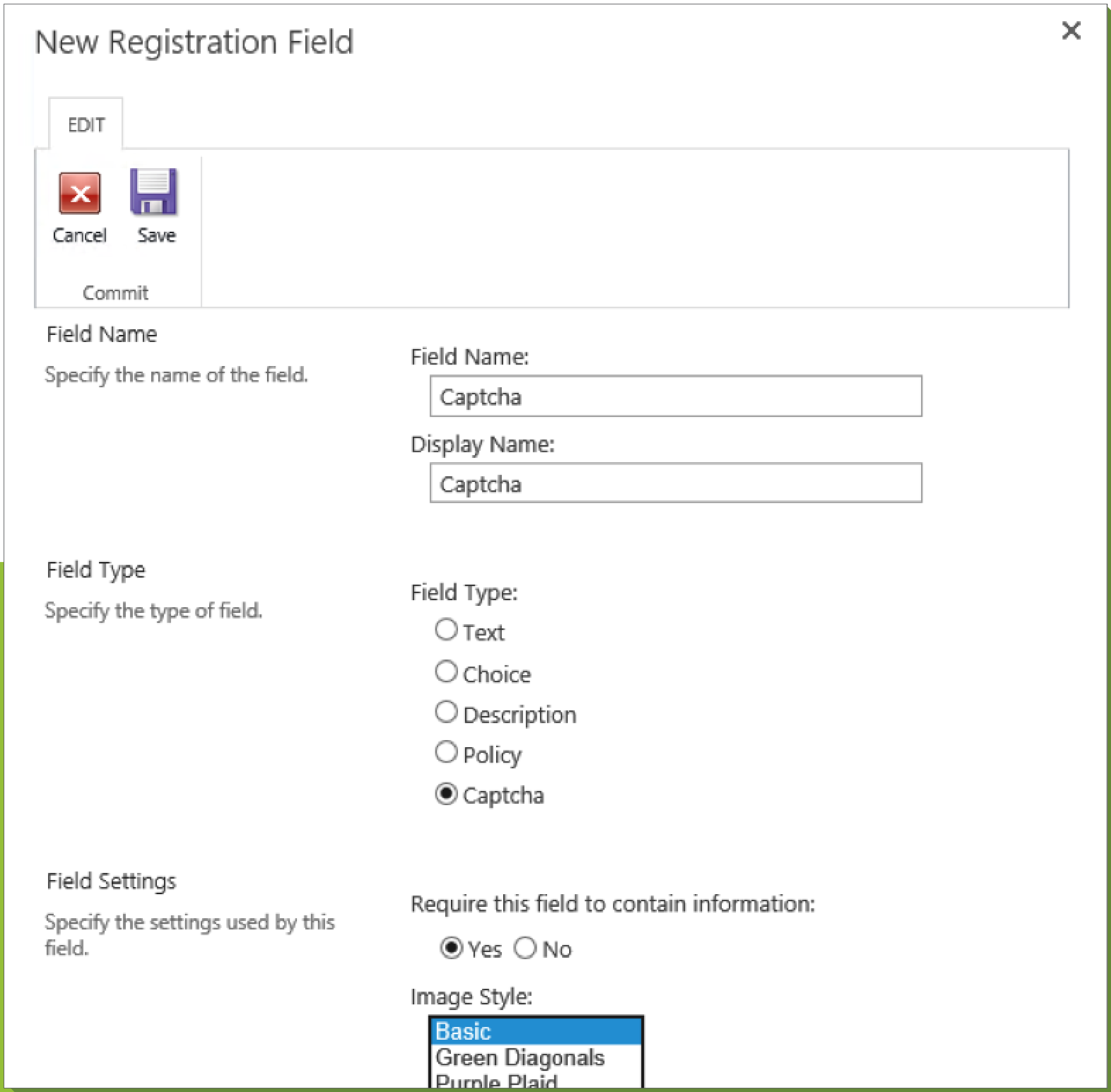
Use this section to set the User Automation password expiration policies.

Disable the account when the password is older than: 90 day(s)

Send a notification before the password expires: 7 day(s)

Repeat the expiration notification every: 3 day(s)

Requiring a Captcha Field to "Prove You're Not a Robot"



New Registration Field

Field Name

Specify the name of the field.

Field Name: Captcha

Display Name: Captcha

Field Type

Specify the type of field.

Field Type:

○ Text

○ Choice

○ Description

○ Policy

● Captcha

Field Settings

Specify the settings used by this field.

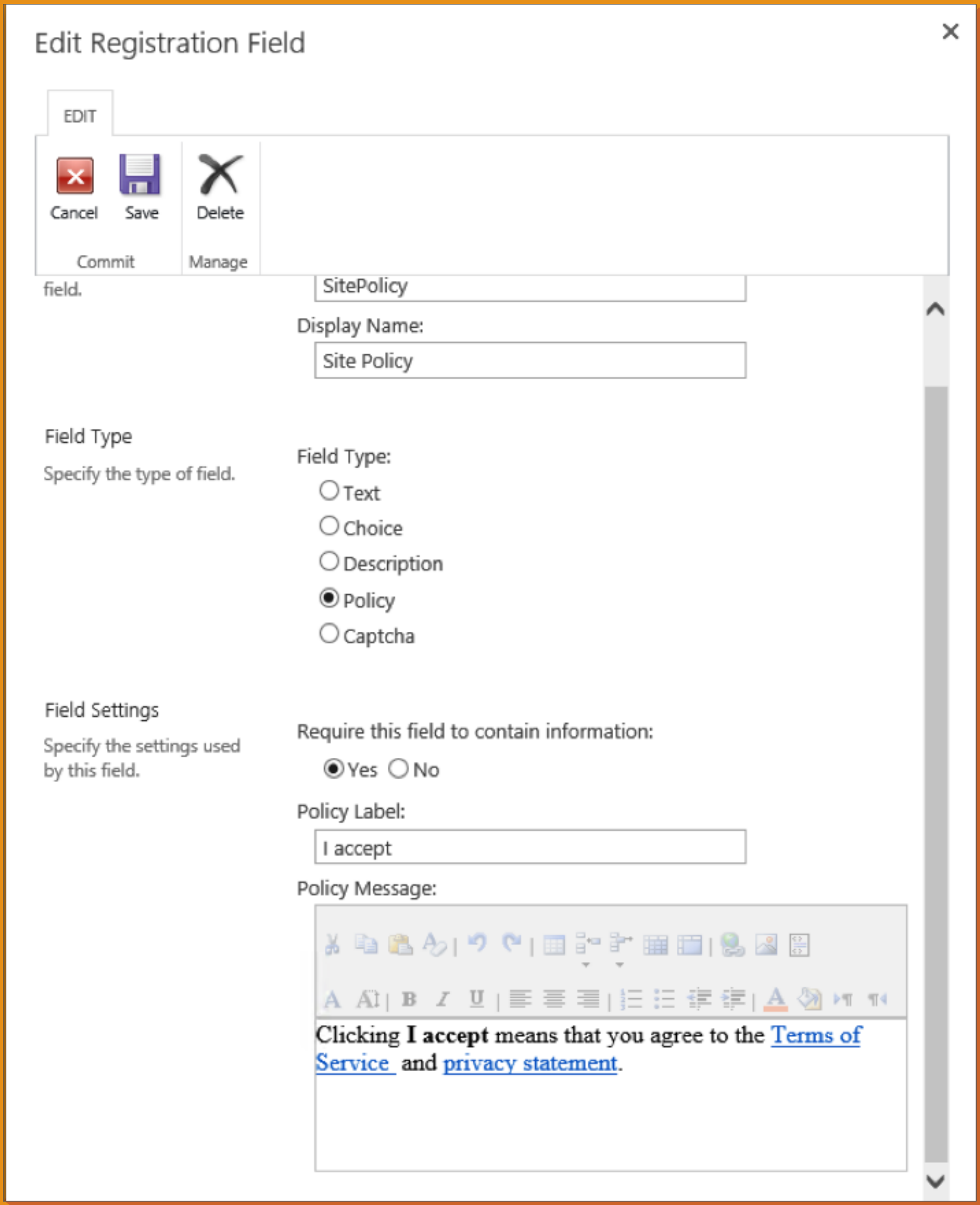
Require this field to contain information:

● Yes ○ No

Image Style:

Basic
Green Diagonals
Purple Plaid

Requiring the Acceptance of Terms and Conditions in Registration Process



field.

SitePolicy

Display Name:

Site Policy

Field Type

Specify the type of field.

Field Type:

○ Text
○ Choice
○ Description
● Policy
○ Captcha

Field Settings

Specify the settings used by this field.

Require this field to contain information:

● Yes ○ No

Policy Label:

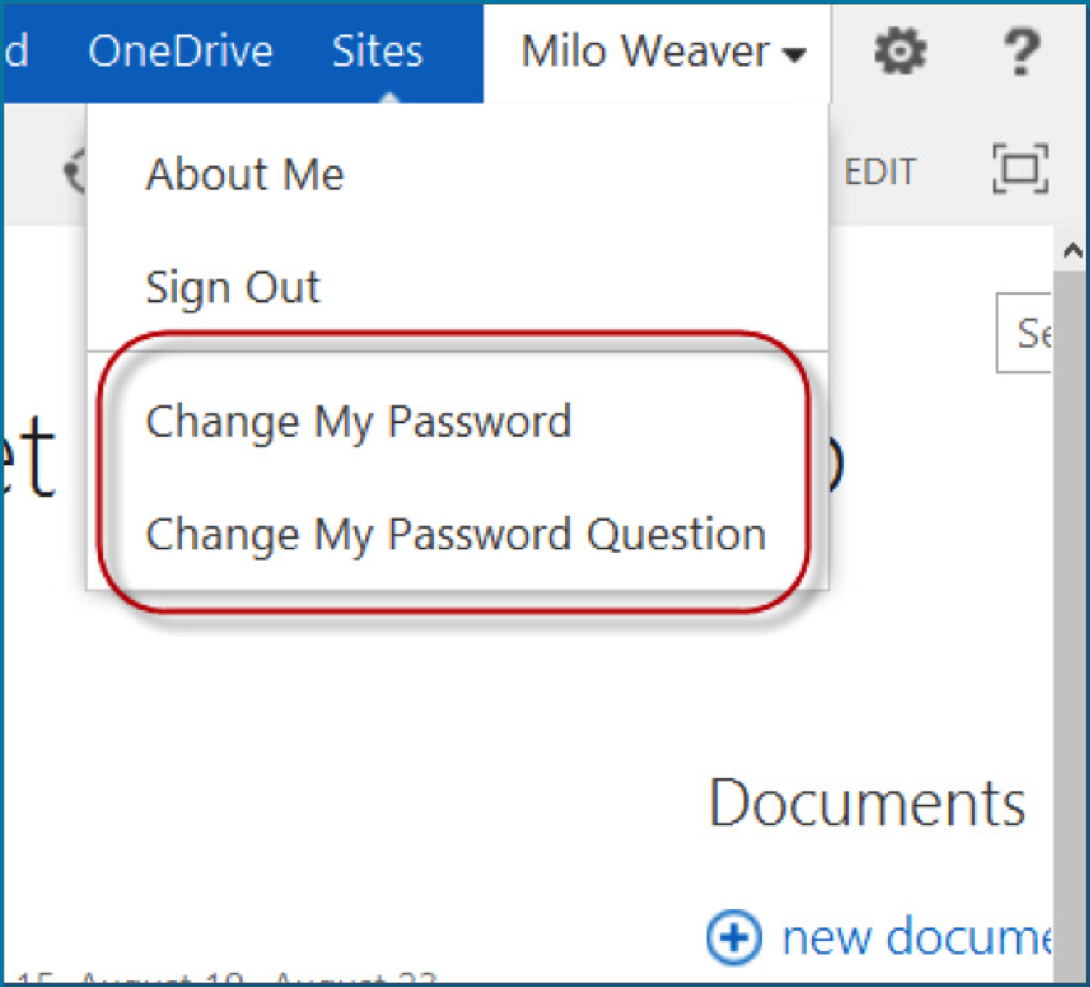
I accept

Policy Message:

Clicking **I accept** means that you agree to the Terms of Service and privacy statement.

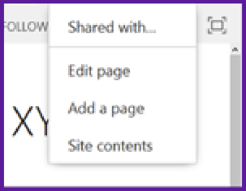
Utilizing the SQL Membership Provider in conjunction with ExCM allows self-service account options, such as security questions and self-password resets if a password is forgotten or expired.

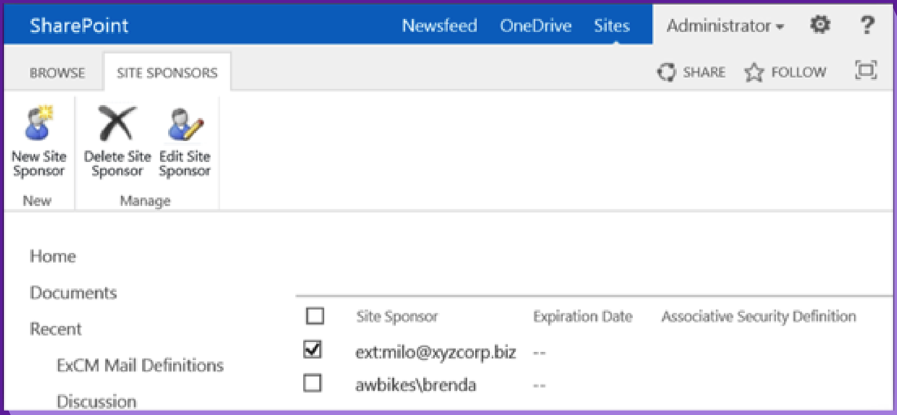
Enabling these self-service features **decreases administrative overhead.** If such information were maintained in Active Directory, users would need to call the help desk or the IT Department to have someone reset these items for them.



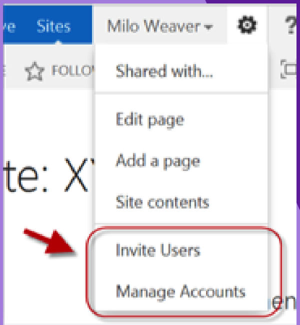
Simple extranet administrative tasks can be delegated to power users designated “Site Sponsors.”

ExCM allows the delegation of simple administrative tasks to power users who are designated “Site Sponsors.” They can be given granular permission to change passwords, unlock accounts, assign permissions, etc. And because ExCM utilizes FBA and SQL Membership Provider, delegation of administrative tasks can be done at a very granular level, even to people outside the organization, without compromising security. So an organization could conceivably have one or more Site Sponsors at each of its partner organizations handling basic extranet membership administration for that organization’s users.





☐	Site Sponsor	Expiration Date	Associative Security Definition
☑	ext:milo@xyzcorp.biz	--	
☐	awbikes\brenda	--	



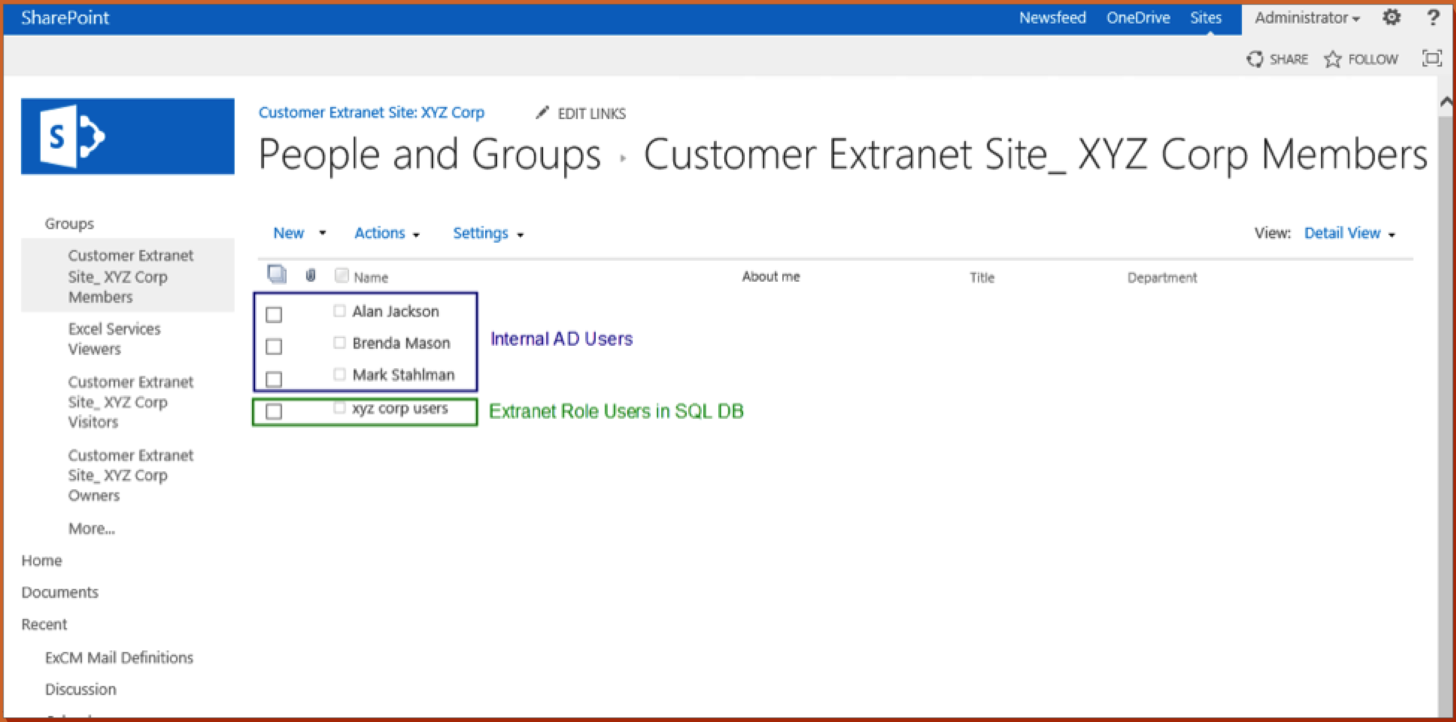
FBA users can still be part of SharePoint groups for security access to the sites.

The FBA user can be granted direct permission, added to a SharePoint group, or added to an FBA role. (FBA roles are in many ways similar to SharePoint groups.)

For example, suppose a SharePoint site utilizes the default Members SharePoint group. Let's say this is VendorA.com's site, and the default members group is called VendorA Members. A company can add the FBA users to the VendorA SharePoint Group and have them in that group alongside its internal (Active Directory) users.

Or, it can create an FBA role called VendorA Member Role and give it the same access as the VendorA Members Group. This would allow for separation of groups between internal users and external users if desired. One other advantage of using FBA roles is that while SharePoint groups are limited to a single site collection, FBA roles can span multiple site collections.

Here's an example showing some of the possibilities:



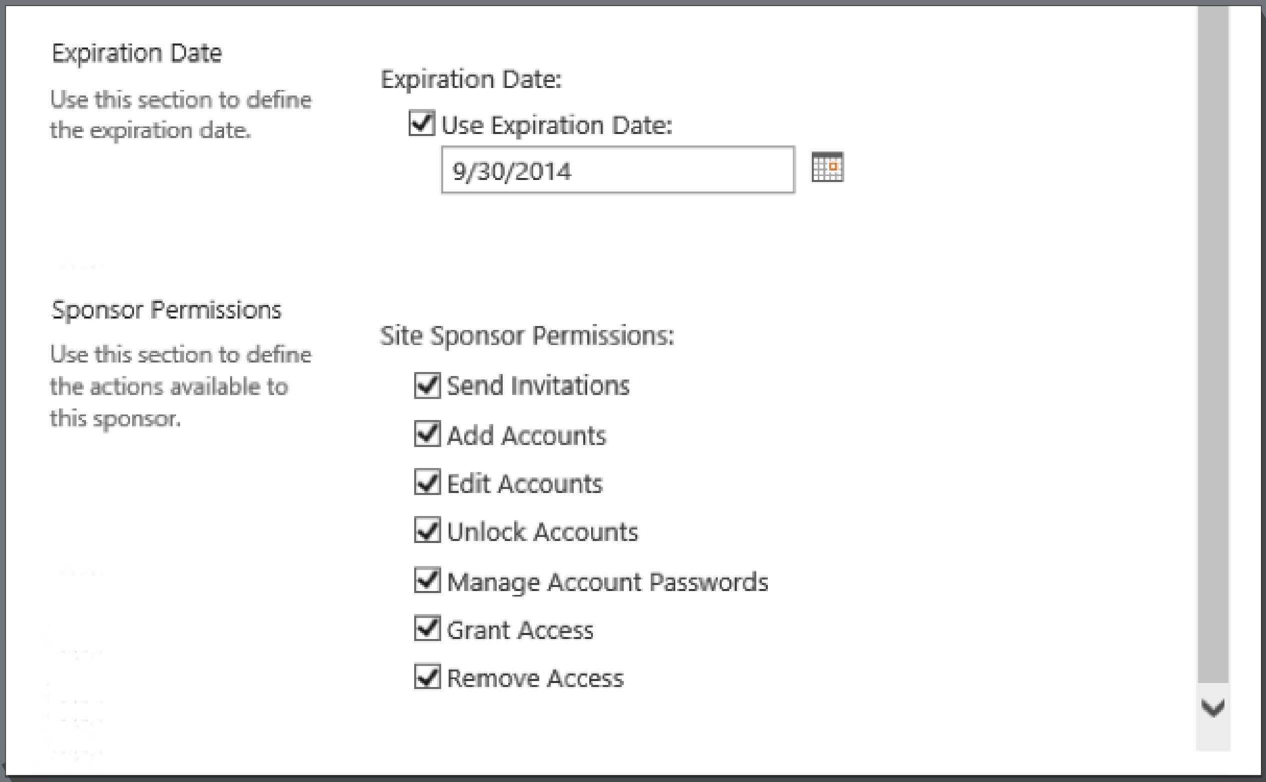
People and Groups › Customer Extranet Site_ XYZ Corp Members

	Name	About me	Title	Department
□	□ Alan Jackson			
□	□ Brenda Mason			
□	□ Mark Stahlman			
□	□ xyz corp users			

Internal AD Users

Extranet Role Users in SQL DB

Utilizing FBA and SQL Membership Provider for external users enables a company to store pertinent information about the user (collected at registration time and completed by the user) that otherwise wouldn't be available in Active Directory.



Expiration Date

Use this section to define the expiration date.

Expiration Date:

☑ Use Expiration Date:

9/30/2014

Sponsor Permissions

Use this section to define the actions available to this sponsor.

Site Sponsor Permissions:

☑ Send Invitations

☑ Add Accounts

☑ Edit Accounts

☑ Unlock Accounts

☑ Manage Account Passwords

☑ Grant Access

☑ Remove Access

Passwords are salted and hashed in the SQL database so no one can gain access to them. Since SQL Membership Provider is a standard, there is a lot of information available to do any custom coding that might be deemed necessary against the database.

For extranet management, it is very possible that there is more information a company would want to know about each user than would be needed for internal employee users. It’s also possible to specify a specific role that contains the users who are allowed to edit, and specify exactly what they can do (e.g. unlock accounts, reset passwords, grant permission, remove permission, etc.) This cannot be done with Active Directory.

Finally, FBA and SQL Membership Provider are proven and have stood the test of time.

While new methods come and go, FBA and SQL Membership Provider have been a reliable constant.

About

PremierPoint Solutions (formerly SharePoint Solutions) is a Microsoft Certified Partner and a nationwide leader in expert-led, in-person and online public classes on SharePoint products and technologies. The company's software division professionally develops high-quality commercial add-ons for SharePoint, including ExCM. Many of the company's courses and services are also applicable to Office 365.

PremierPoint Solutions, P.O. Box 1588, Brentwood, TN 37024-1588
(615) 515-0210, option 1 / http://premierpointsolutions.com