

Extranet User Manager Deployment and Configuration Guide

Version 2.5

Saturday, November 26, 2011

Envision IT

7145 West Credit Avenue
Suite 100, Building 3
Mississauga, ON L5N 6J7



Contents

- WHAT'S NEW IN V 2.5..... 1**
 - WHAT'S NEW IN V2.5.0.0..... 1
- PREPARING FOR DEPLOYMENT 2**
 - SERVER ACCESS AND REQUIRED ACCOUNTS.....2
 - SHAREPOINT WEB APPLICATION2
 - EXCEL WORKBOOK2
 - CHOOSING A PROVIDER (AD OR SQL).....2
 - SHAREPOINT 2010 CONFIGURATION3
 - OTHER ITEMS3
- HYDRA LOGIN OR WINDOWS AUTHENTICATION INSTALLATION..... 4**
- HYDRA LOGIN INSTALLATION 5**
 - DEPLOYING THE EXTRANET USER MANAGER FILES TO THE SERVER.....5
 - 14Hive*5
 - GAC*5
 - SharepointWebRoot*.....5
 - CREATE THE LOG FOLDERS5
 - IIS – CONVERT FOLDERS TO APPLICATIONS6
 - IIS – SET THE AUTHENTICATION7
 - INSTALL THE DATABASES.....7
 - SQL ENTERPRISE MANAGER - SECURITY8
 - WEB APPLICATION CONFIGURATION9
 - WEB.CONFIG UPDATES11
 - Central Administration*.....11
 - Secure Token Service and SharePoint Web Application*.....11
 - EUM Landing and LandingAdmin*.....12
- WINDOWS AUTHENTICATION INSTALLATION 13**
 - DEPLOYING THE EXTRANET USER MANAGER FILES TO THE SERVER.....13
 - GAC*13
 - SharepointWebRoot*.....13
 - CREATE THE LOG FOLDERS13
 - IIS – CONVERT FOLDERS TO APPLICATIONS14
 - IIS – SET THE AUTHENTICATION15
 - INSTALL THE DATABASES.....15
 - SQL ENTERPRISE MANAGER - SECURITY15
 - WEB.CONFIG UPDATES16
 - SharePoint Web Application*16
 - EUM Landing and LandingAdmin*.....16
- COMPLETE THE EUM CONFIGURATION 17**
 - Mnaged Domains*.....17

<i>SharePoint Sites</i>	17
<i>Test the Email Functionality</i>	17
<i>Add a Group</i>	18
<i>Add a User</i>	18
<i>Add SharePoint Permissions</i>	18
<i>Set the Test Password</i>	18
<i>Test Login</i>	18
INSTALLATION TESTING	20
CONFIGURATION SETTINGS	21
SYSTEM/APPLICATION CONFIGURATION	21
ADDITIONAL HIDDEN SETTINGS	25
ADDITIONAL OBSOLETE SETTINGS.....	25
GENERAL EMAIL SETTINGS	26
EMAIL TEMPLATES AND SUBSTITUTION VARIABLES	28
PENDING APPROVAL	28
PENDING APPROVER	30
WELCOME	32
FORGOT PASSWORD	35
MANAGEUSERS DATABASE CONFIGURATION - DOMAIN TABLE	39
MANAGEUSERS DATABASE CONFIGURATION - SITE TABLE	40
APPENDIX A – CREATING THE SHAREPOINT WEB APPLICATION	41
CREATE A NEW DEFAULT ZONE WEB APPLICATION IF ONE DOESN'T EXIST:	41
APPENDIX B - CONVERT CLASSIC TO CLAIMS BASED AUTHENTICATION WITH POWERSHELL	45
APPENDIX C - CONFIGURING THE ASPNET DB FOR SQL PROVIDER	46
APPENDIX D – PROVIDING CONNECTION CREDENTIALS	47

What's new in V 2.5

This is the second release to target SharePoint 2010, as well as being constructed in Visual Studio 2010.

Forms mode login in 2010 uses a new "Claims" based security Token. The new login form (EZLogin) is only used for SharePoint 2010 Forms based authentication. There, is also an older one for use in 2007 in the Login2007 folder. More information about [Claims Authentication](#) from MSDN Blogs.

Multiple users with the same username can now be found and edited (only one may be Active, but the others can be Deactivated, or set to Pending Approval)

The [Pending Approver Email](#) is new. This is sent to the Administrators that are approving new user requests. It is sent at the same time, as the [Pending Approval Email](#) is sent to the registering user (e.g. when the account is saved in the Pending Approval state).

What's new in V2.5.0.0

???

Preparing for Deployment

Server Access and Required Accounts

In order to install and configure the EUM, you will need:

- 1) Access to the SharePoint server as a local administrator
- 2) Access to the SQL server as a SQL DB administrator
- 3) A domain account to be the first (“seed”) EUM administrator (for AD configurations)
- 4) An email server to relay emails from the EUM to end users. In some cases, an authorized account to send email is necessary as well.

SharePoint Web Application

A SharePoint web site must be configured with external access. The application can be in the default zone (for Windows integrated scenario) or in the Extranet zone (for the FBA scenario). SharePoint search requires that at least one zone be using Windows integrated authentication. Guidance on how to create a SharePoint 2010 web application is available in Appendix A.

Excel Workbook

Each Deployment should first fill out the specifics of the deployment in the Excel Workbook. This workbook will be referred to through out the installation.

Choosing a Provider (AD or SQL)

The two main choices for providers are AD and SQL. While they both can present the same user experience, there are distinct advantages to each.

Active Directory

- Can leverage an existing DMZ AD that is in place to manage the SharePoint farm
- Tighter account policy and auditing controls through AD
- Can still use email address as the login when using the Hydra provider

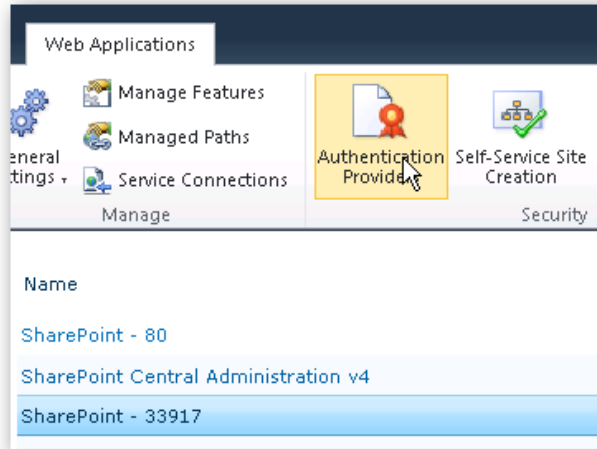
SQL ASPNETDB

- Doesn't require an additional DMZ AD. All user credentials are stored in an encrypted SQL database
- Email address can be the username

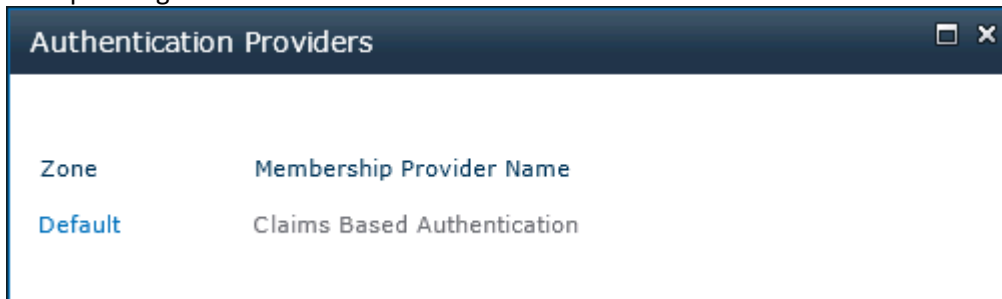
SharePoint 2010 Configuration

Before proceeding on the EUM install, the SharePoint web application setup needs to be confirmed. In order to use Forms-Based Authentication, the web application needs to be setup using Claims Based Authentication. This can be checked using the steps below.

- a. Select the web application and click the Authentication Providers button on the Ribbon Bar:



- b. You should now see a dialog similar to the following showing the zone(s) the web application is operating within.



- c. If it is not Claims based you should convert it to Claims based using Powershell (see Appendix A)

Other Items

Other items you may need

- DNS settings
- SSL certificate
- Alternate Access Mappings

Hydra Login or Windows Authentication Installation

At this point there are two different paths that can be followed for the installation. The decision is whether forms-based authentication or Windows Authentication is going to be used on the site.

Generally forms-based authentication is used when setting up an Extranet. The scenario where you would use Windows Authentication is where you have a gateway device such as Forefront Threat Management Gateway or Forefront Unified Access Gateway in front of the Extranet. In these cases, these devices provide a rich HTML single sign-on experience. To leverage that the Extranet should be configured for Windows Authentication so that the credentials entered in the gateway are passed through.

Depending on the path chosen, follow either the Hydra Login Installation or Windows Authentication Installation in the following sections.

Hydra Login Installation

Deploying the Extranet User Manager Files to the Server

There are three folders of files that need to be distributed to various locations on the SharePoint web front end. These are all contained in the installation zip file, and they are:

- 14Hive
- GAC
- SharepointWebRoot

14Hive

This contains the concierge.aspx page that needs to be installed in the C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\TEMPLATE\IDENTITYMODEL\WINDOWS folder on the server. This page is used to do the automatic authentication of internal users using their Windows credentials.

GAC

The three DLLs in the GAC folder all need to be installed in the GAC on the server. By opening a Windows Explorer window to C:\Windows\assembly, these files can be dragged and dropped into the GAC. If there are earlier versions of these files present, they should be deleted.

SharepointWebRoot

In the SharepointWebRoot folder are three folders that need to be copied to the IIS root of the SharePoint web application. These are the _forms folder with the EZLogin form which provides the rich login page for EUM, and the Landing and LandingAdmin folders that contain the EUM applications.

Create the Log Folders

Envision IT Applications log to the C:\Logs folder by default.

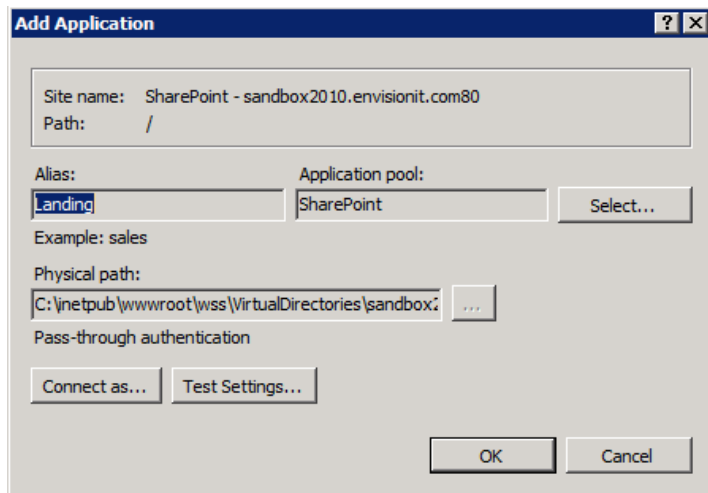
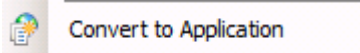
Ensure that this folder exists, and Grant Write Permissions to the App Pool account so the application can log exceptions and other details

If Email Logging is turned on the Emails are configured by default to go to C:\Logs\Emails. The folder must exist if logging is enabled.

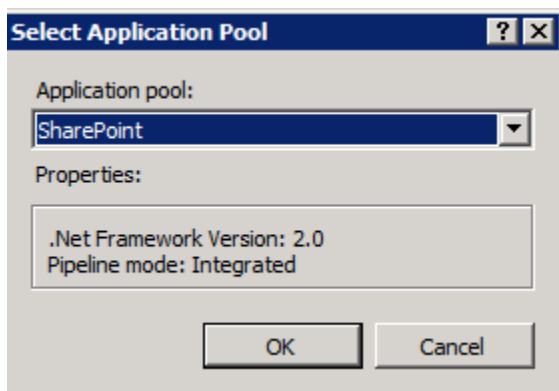
IIS – Convert Folders to Applications

Applications must be created in IIS for /Landing and /LandingAdmin. Open the IIS Manager, and go to the SharePoint web application.

Switch the IIS Manager to Content View,, right click on the folder, and select Convert to Application



Make sure that the Application Pool selected is that the same one used for SharePoint.



Repeat the above process for /LandingAdmin.

IIS – Set the Authentication

Both the /Landing and /LandingAdmin applications need to have their anonymous access turned off. This may or may not be the case depending on whether anonymous access was enabled for the SharePoint web application when it was created.

To validate this, go to the IIS Manager, select the Landing application, and double-click the Authentication icon. Confirm that only the Forms Authentication option is enabled.

Repeat the above process for /LandingAdmin.

The following /Landing sub-folders need to have their anonymous access turned on.

- Common
- ForgotPass
- Images
- Register (if used)

Install the Databases

To create an EUM Manage Users database follow these steps.

1. In SQL Server Management Studio create the ManageUsers database as named in the Excel workbook's EUM tab
2. In the context of the new ManageUsers database, run the 1 - Create EUM Objects in Database.sql database script from the SQL folder of the install package to create the tables and other database objects
3. Run the 2 - Populate EUM System Tables.sql database script to populate the system tables
4. Run the 3 - PCCError System Tables.sql database script to populate the system tables
5. Copy the SQL from the SQL tab of the Excel planning workbook into a new SQL query window. Due to Excel re-formatting when pasting, the following changes need to be done before running the SQL
 - a. Remove the extra double quotes at the start of the sixth line
 - b. Do a search and replace all of "" with "
 - c. Remove the extra double quotes at the end of the script

If an ASPNETDB database is needed to store the user credentials in, please see Appendix B - Configuring the ASPNET DB for SQL Provider.

SQL Enterprise Manager - Security

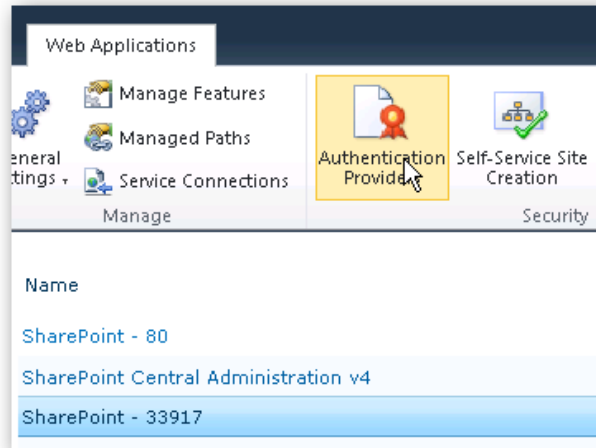
Both Databases (if using SQL Provider) need to allow access by the application. This is done by granting access to the Account that runs the SharePoint app pool in IIS.

- 1) Open SQL Server Management Studio,
Open Security-Logins and select the Sharepoint App Pool Account.
If the account does not already appear in the Logins list Right-Click Logins and select New Login... - fill in the Login name and Save
- 2) Right-Click the account and Select Properties
- 3) Select User Mapping and find the database in the list
- 4) Check the Map checkbox for the EUM Manage Users database and check the db_datareader and db_datawriter roles.
- 5) Click OK to save your changes
- 6) If appropriate, repeat for the ASPNETDB database, selecting all of the aspnet roles
- 7) Repeat for the ASPNETDB database for the Central Admin app pool account

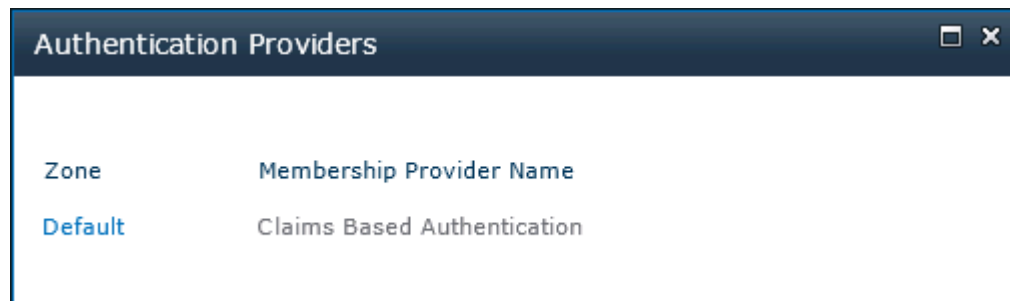
Web Application Configuration

In Central Admin, the web application now needs to be configured for forms-based authentication.

1. Select the web application and click the Authentication Providers button on the Ribbon Bar:



2. You should now see a dialog similar to the following showing the zone(s) the web application is operating within.



3. Enter names for the ASP.NET Membership Provider and Role Provider as shown below

- HydraMembershipProvider
- HydraRoleProvider

<p>Claims Authentication Types</p> <p>Choose the type of authentication you want to use for this zone.</p> <p>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.</p>	<p><input checked="" type="checkbox"/> Enable Windows Authentication</p> <p><input checked="" type="checkbox"/> Integrated Windows authentication</p> <p>NTLM</p> <p><input type="checkbox"/> Basic authentication (credentials are sent in clear text)</p> <p><input checked="" type="checkbox"/> Enable Forms Based Authentication (FBA)</p> <p>ASP.NET Membership provider name</p> <p>HydraMembershipProvider</p> <p>ASP.NET Role manager name</p> <p>HydraRoleProvider</p> <p><input type="checkbox"/> Trusted Identity provider</p>
---	---

4. Specify the path to the custom Login form in the **Sign In Page URL** section

- /_Forms/EZLogin.aspx

<p>Sign In Page URL</p> <p>When Claims Based Authentication types are enabled, a URL for redirecting the user to the Sign In page is required.</p>	<p><input type="radio"/> Default Sign In Page</p> <p><input checked="" type="radio"/> Custom Sign In Page</p> <p>/_forms/ezlogin.aspx</p>
---	---

Web.Config Updates

In order for the Extranet User Manager to function properly, changes need to be made to the following web.configs in SharePoint.

- Central Administration
- Secure Token Service
- SharePoint Web Application
- EUM Landing
- EUM LandingAdmin

Prior to making any changes to any of the SharePoint web.config files, backups of the files should be stored in a safe location. Incorrectly modifying any of these config files can render SharePoint (including Central Admin) non-functional.

Central Administration

Central Admin needs to be updated so that a EUM Hydra user can be added as a site collection administrator to the SharePoint site. This is done so that that user can log into the SharePoint site and grant further permissions from there.

In order to modify the Central Admin web.config file, refer to the Excel planning workbook for the sections to be added/edited.

Once the edits have been completed, open Central Admin and confirm that the people picker is functioning properly and finding Hydra users as follows:

1. Open Central Admin
2. Choose Application Management from the left hand navigation
3. Choose Change site collection administrators from the Site Collections section
4. Ensure that you have selected the correct web application and site collection
5. Click the book beside the primary site collection administrator to open the people picker
6. Enter the EditConfigurationUser from the EUM tab on the spreadsheet and perform a find. You may get both Windows users and Forms Auth users. Be sure to choose the Forms Auth user
7. Hover over the selected user, and confirm that the tooltip indicates HydraMembershipProvider as part of the username
8. Click OK to save the change

Secure Token Service and SharePoint Web Application

Similar edits need to be made to the Security Token Service and the SharePoint web application. Refer to the Excel planning workbook for the sections to be added/edited.

EUM Landing and LandingAdmin

For EUM Landing and LandingAdmin, the complete web.config file is generated in the Excel planning workbook. Simply copy the workbook contents into Notepad and save as the web.config in the appropriate folders.

Windows Authentication Installation

Deploying the Extranet User Manager Files to the Server

There are two folders of files that need to be distributed to various locations on the SharePoint web front end. These are all contained in the installation zip file, and they are:

- GAC
- SharepointWebRoot

GAC

The three DLLs in the GAC folder all need to be installed in the GAC on the server. By opening a Windows Explorer window to C:\Windows\assembly, these files can be dragged and dropped into the GAC. If there are earlier versions of these files present, they should be deleted.

SharepointWebRoot

In the SharepointWebRoot folder are two folders that need to be copied to the IIS root of the SharePoint web application. These are the Landing and LandingAdmin folders that contain the EUM applications.

Create the Log Folders

Envision IT Applications log to the C:\Logs folder by default.

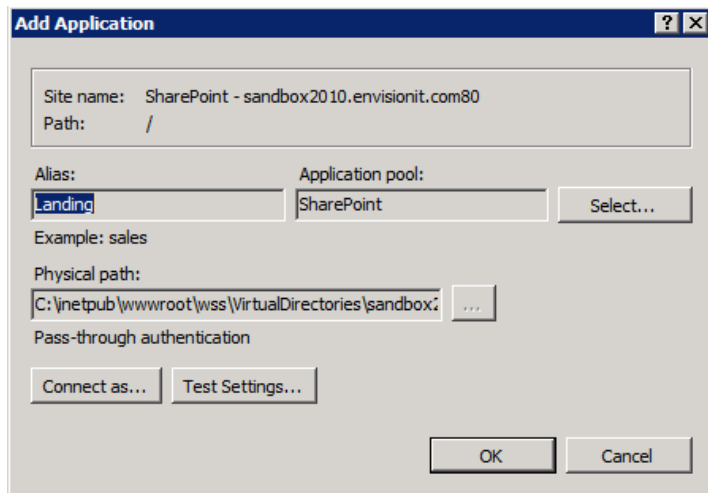
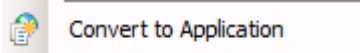
Ensure that this folder exists, and Grant Write Permissions to the App Pool account so the application can log exceptions and other details

If Email Logging is turned on the Emails are configured by default to go to C:\Logs\Emails. The folder must exist if logging is enabled.

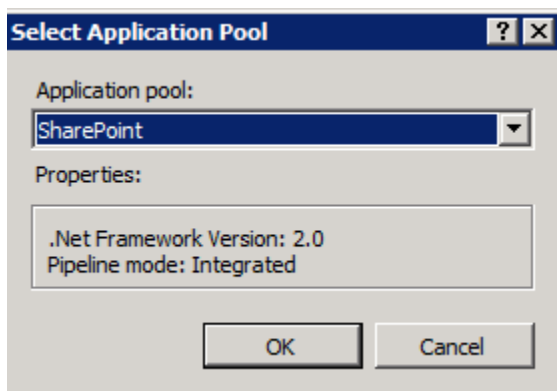
IIS – Convert Folders to Applications

Applications must be created in IIS for /Landing and /LandingAdmin. Open the IIS Manager, and go to the SharePoint web application.

Switch the IIS Manager to Content View,, right click on the folder, and select Convert to Application



Make sure that the Application Pool selected is that the same one used for SharePoint.



Repeat the above process for /LandingAdmin.

IIS – Set the Authentication

Both the /Landing and /LandingAdmin applications need to have their anonymous access turned off. This may or may not be the case depending on whether anonymous access was enabled for the SharePoint web application when it was created.

To validate this, go to the IIS Manager, select the Landing application, and double-click the Authentication icon. Confirm that only the Windows Authentication option is enabled.

Repeat the above process for /LandingAdmin.

The following /Landing sub-folders need to have their anonymous access turned on.

- Common
- ForgotPass
- Images
- Register (if used)

Install the Databases

To create an EUM Manage Users database follow these steps.

1. In SQL Server Management Studio create the ManageUsers database as named in the Excel workbook's EUM tab
2. In the context of the new ManageUsers database, run the 1 - Create EUM Objects in Database.sql database script from the SQL folder of the install package to create the tables and other database objects
3. Run the 2 - Populate EUM System Tables.sql database script to populate the system tables
4. Run the 3 - PCCError System Tables.sql database script to populate the system tables
5. Copy the SQL from the SQL tab of the Excel planning workbook into a new SQL query window. Due to Excel re-formatting when pasting, the following changes need to be done before running the SQL
 - a. Remove the extra double quotes at the start of the sixth line
 - b. Do a search and replace all of "" with "
 - c. Remove the extra double quotes at the end of the script

SQL Enterprise Manager - Security

The EUM Manage Users database needs to allow access by the application. This is done by granting access to the Account that runs the SharePoint app pool in IIS.

- 1) Open SQL Server Management Studio, Open Security-Logins and select the Sharepoint App Pool Account. If the account does not already appear in the Logins list Right-Click Logins and select New Login... - fill in the Login name and Save
- 2) Right-Click the account and Select Properties
- 3) Select User Mapping and find the database in the list
- 4) Check the Map checkbox for the EUM Manage Users database and check the db_datareader and db_datawriter roles.
- 5) Click OK to save your changes

Web.Config Updates

In order for the Extranet User Manager to function properly, changes need to be made to the following web.configs in SharePoint.

- SharePoint Web Application
- EUM Landing
- EUM LandingAdmin

Prior to making any changes to any of the SharePoint web.config files, backups of the files should be stored in a safe location. Incorrectly modifying any of these config files can render SharePoint (including Central Admin) non-functional.

SharePoint Web Application

The SharePoint web application needs the following lines modified in its web.config.

```
<pages enableSessionState="true"
<trust level="Full" originUrl="" />
<!-- remove name="Session" / -->
```

EUM Landing and LandingAdmin

For EUM Landing and LandingAdmin, the complete web.config file is generated in the Excel planning workbook. Simply copy the workbook contents into Notepad and save as the web.config in the appropriate folders.

Complete the EUM Configuration

The last configuration steps are done in the /LandingAdmin application itself. Open the browser and go to the *portal*/LandingAdmin URL logged in as the EditConfigurationUser specified in the spreadsheet.

Managed Domains

The first task is to setup the managed domains. There are typically two: the internal corporate domain and the extranet domain (which could be AD or SQL). Follow these steps:

1. From the /LandingAdmin home page, select Managed Domains
2. Choose Add New Domain
3. Enter the Domain Name, LDAP Connection String, and Username from the Domain Table tab in the spreadsheet
4. Enter the appropriate password twice
5. Submit
6. Repeat for the second row in the Domain Table spreadsheet, noting that the LDAP Connection String, Username, and Passwords are all blank if a SQL Provider is being used)
7. Ensure that the EditConfigurationUser is also a member of the EditConfigurationGroup group
8. Remove the EditConfigurationUser line in the web.configs for both Landing and landingAdmin
9. Confirm that you can still access /LandingAdmin with full configuration editor rights

SharePoint Sites

The next task is to setup the SharePoint sites that EUM should be aware of. This is typically just the one content database associated with the site, but there may be multiple content databases.

1. From the /LandingAdmin home page, select SharePoint Sites
2. Choose Add New SharePoint Site
3. Enter the SharePointRoot, ContentDBServer, and ContentDBName from the Site Table tab in the spreadsheet
4. Ensure that the app pool account has db_reader access to the content database. If this is not possible, enter the username and password for the account that does have rights
5. Submit

Test the Email Functionality

1. Select Welcome Email from the Configure menu
2. Enter your email address in the Test Email field

3. Click OK to save and send the test email
4. Confirm that the email is received correctly

Add a Group

1. Select Group from the Add menu
2. Enter a group name
3. Submit

Add a User

1. Select User from the Add menu
2. Enter a first name, last name, and the email address in the email and username fields
3. Leave the status as Active
4. Add the new group to the list of Assigned Groups
5. Click OK
6. Confirm that the welcome is received

Add SharePoint Permissions

1. Return to the top of the portal site
2. Select Site Permission from the Site Actions menu
3. Choose an appropriate SharePoint group to assign group membership to
4. Select New
5. Enter the full group name created, including the Extranet Domain Prefix from the Domains tab of the spreadsheet

Set the Test Password

1. Click the Set a Password link in the welcome email
2. Set the new password

Test Login

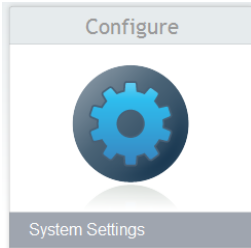
1. Select Home to return to the SharePoint home page
2. From the Welcome menu choose Sign in as a Different User
3. Log in using the email address (Hydra) or username (Windows Authentication) and password set


Installation Testing

Configuration Settings

The following provide details on the configuration of the Extranet User Manager.

System/Application Configuration





Home Search Add Configure

Application Configuration

This help text should describe the function of the application configuration page.

Application Name:	<input type="text" value="/EITWebDev"/>	Edit User Show Extra Info:	<input checked="" type="checkbox"/>
Home URL:	<input type="text" value="https://securedevsql.envisionit.com/"/>	Show Debug Info:	<input type="checkbox"/>
Extranet URL:	<input type="text" value="https://securedevsql.envisionit.com/"/>	Login Show Remember Me:	<input checked="" type="checkbox"/>
Edit User URL:	<input type="text" value="/LandingAdminSQL/EditUser.aspx"/>	Search Export To Excel:	<input checked="" type="checkbox"/>
Site List URL:	<input type="text" value="/LandingAdminSQL/SiteList.aspx"/>	Edit Provider Groups:	<input checked="" type="checkbox"/>
Forgot Password URL:	<input type="text" value="/LandingAdminSQL/forgotpass/default.aspx"/>	Edit Provider Unmanaged Groups:	<input checked="" type="checkbox"/>
Site Tree Provider Prefix:	<input type="text" value="i:0#.ffbamembershipprovider "/>	Edit Send Email:	<input checked="" type="checkbox"/>
Site Tree Provider Group Prefix:	<input type="text" value="c:0-.ffbaroleprovider "/>		
Edit Groups Group Domain:	<input type="text" value="/SecureDevSQL"/> ▼		
Edit Groups Group:	<input type="text" value="Group Editor Group"/>		

ApplicationName	Name of this specific configuration. When using ASPNET SQL providers this name must match with the Application name in the ASPNET DB
HomeURL	The url to the home directory of the site. Used in the two Emails; Welcome and Forgot Password
ExtranetURL	The url to the root of the Extranet_Enduser site. Used in the two Emails; Welcome and Forgot Password
EditUserURL	Used on the UserSearch page to provide EditUser hyperlinks. It can be used to take the administrator to the Standard Edituser.aspx, or to UserProfileChooser.aspx for access to customer registration fields. Beware that the correct Application must be selected from the dropdown
SiteListURL	Used on the UserSearch page to provide a hyperlink to the users site list tree. This was made a configuration item in case a customer wants to have a custom page.
ForgotPassURL	Used on the UserSearch page to provide a hyperlink to the forgot password page. This was made a configuration item in case a customer wants to have a custom page.
SiteTreeProviderPrefix	The domain prefix used to reference users in the domain. Used by SiteTree code when resolving the users group membership and associated site access rights.
SiteTreeProviderGroupPrefix	The domain prefix used to reference groups in the domain. Used by SiteTree code when resolving the users site access rights.
EditGroupsDomain_FK	The Domain of the EditGroupsGroup selected from a dropdown The Valid Domains are stored in the Domain Table of the EUM Database. Both Active Directory Domains, and ASPNET DB Applications are allowed.
EditGroupsGroup	The name of the group that a user must belong to in order to have GroupEdit rights. In our security model these users will have the ability to create/edit groups and users.
EditUserShowExtraInfo	This is a debugging value. When set to true the EditUser.aspx page will display several additional pieces of data about the user. This feature is not currently available

<p>ShowDebuginfo</p>	<p>This is a debugging value. When set to true the EditUser.aspx page will display several additional pieces of data about the user :</p> <p>Provider Details</p> <ul style="list-style-type: none"> • Provider Name = FBAMembershipProvider • Domain Name = SecureDev2010Sql (SQL membership provider.) • Application Name = SecureDev2010Sql • Description of Provider = SQL membership provider. • Users can reset Passwords • Password Retrieval at the Provider level is disabled • Password Must be this long: 7 • Password Requires This many NonAlphaNumeric characters: 1 • Password Strength RegEx = <code>^(?=[^d])(?=[a-z])(?=[A-Z]).{7,}\$</code> • Max Invalid Password Attempts Allowed: 5 • Minutes for Invalid attempts to occur: 10 • Q and A is NOT required • Accounts can Share an Email Address <p>Additional User Details</p> <ul style="list-style-type: none"> • Provider UserKey = c04ff4d-9673-47d4-8126-280fcc1e1536 • This user is Approved • This user is NOT Locked Out • This user is currently Online • Account was Created 10-Jun-2010 9:31 (12 days ago) • Last Activity for Account was on 22-Jun-2010 14:57 (0 days ago) • User was last lockedout on 31-Dec-1753 19:00 (93674 days ago) • Password was last changed on 10-Jun-2010 16:11 (11 days ago) • Disclaimer was read on (733944 days ago) <p>also the Provider Description is shown on the User Search.aspx Page</p> <p>e.g. SecureDev2010Sql (SQL membership provider.)</p>			
<p>LoginShowRememberMe</p>	<p>When set to true the login page will display and use a RememberMe checkbox that stores the username in a cookie.</p> <p>This does not work in the Claims Based Login2010 Form</p>			
<p>SearchExportToExcel</p>	<p>Check this box, to enable the Export to Excel button on the search pages.</p>			
<p>EditProviderGroups</p>	<p>Checking this box causes the EditUser page to display the Assigned Groups / Available Groups controls, allowing the Admin user to change the user's group membership.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Group Membership</p> <p><small>Add this user to the required group(s) by selecting the group on the left under Available Groups and clicking the right arrow to move the group name under Assigned Groups. Unmanaged groups displays other groups that this user may be assigned to that you cannot change. This is for informational purposes only.</small></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; vertical-align: top;"> <p><small>Available Groups:</small></p> <div style="border: 1px solid gray; padding: 2px; min-height: 100px;"> Configuration Editors Group Editor Group Peter Test Toms Test Group TomsGroupEditors </div> </td> <td style="width: 10%; text-align: center; vertical-align: middle;"> <div style="border: 1px solid gray; padding: 2px; width: 20px; margin: 0 auto;"> >> << </div> </td> <td style="width: 40%; vertical-align: top;"> <p><small>Assigned Groups:</small></p> <div style="border: 1px solid gray; padding: 2px; min-height: 100px;"> (Empty) </div> </td> </tr> </table> </div>	<p><small>Available Groups:</small></p> <div style="border: 1px solid gray; padding: 2px; min-height: 100px;"> Configuration Editors Group Editor Group Peter Test Toms Test Group TomsGroupEditors </div>	<div style="border: 1px solid gray; padding: 2px; width: 20px; margin: 0 auto;"> >> << </div>	<p><small>Assigned Groups:</small></p> <div style="border: 1px solid gray; padding: 2px; min-height: 100px;"> (Empty) </div>
<p><small>Available Groups:</small></p> <div style="border: 1px solid gray; padding: 2px; min-height: 100px;"> Configuration Editors Group Editor Group Peter Test Toms Test Group TomsGroupEditors </div>	<div style="border: 1px solid gray; padding: 2px; width: 20px; margin: 0 auto;"> >> << </div>	<p><small>Assigned Groups:</small></p> <div style="border: 1px solid gray; padding: 2px; min-height: 100px;"> (Empty) </div>		

<p>EditUnmanagedGroups</p>	<p>Checking this box causes the EditUser page to display the UnmanagedGroups list for the edited user. You might want to turn this off if your users are confused by this list of groups that they don't have the authority to change.</p> <p>Unmanaged Groups: none</p>
<p>EditSendEmail</p>	<p>Checking this box makes available the bottom section of the EditUser page which allows the current user to send a simple, brief email to the user whose account is being edited.</p> <p>Send Email Use this option to send an email to the user. For example you might do this to let the user know that they have been granted additional rights to the site.</p> <p><input type="checkbox"/> Send Email</p> <p>Subject : <input type="text"/></p> <p>Message : <input type="text"/></p>

Additional Hidden Settings

There is currently no GUI for these settings, they must be set directly in the DB, in the SystemConfiguration table.

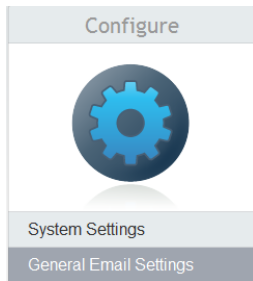
LoginShowDisclaimer	When set to true the login process will display a disclaimer page requiring the user to click a button acknowledging that they have read the disclaimer. This does not work in the Claims Based Login2010 Form
WelcomeMessage	Used on the home page of the Extranet module to greet the user. e.g. Welcome to the Envision IT (SQLFBA)
ChangePasswordDefaultSiteURL	Used to set the target for the "Click Here" to return to the site link that is displayed by the ChangePassword page when the user has completed the password change process.
EmailNewAccountSendToken	True means to use the time limited token method of setting a user's password. In the interest of security this value should always be True. However if security is not an issue and the client wants a simpler way of welcoming new users the tool can generate a random password and include in it PLAINTEXT in the welcome email.
SignoutLoginLinkURL	Displays on the Signout page, to allow the user to sign in again It can be left blank, and the URL will not show

Additional Obsolete Settings

These are in the DB, in the SystemConfiguration table, but are not used by the application

ForgotPassEmailURL	
--------------------	--

General Email Settings

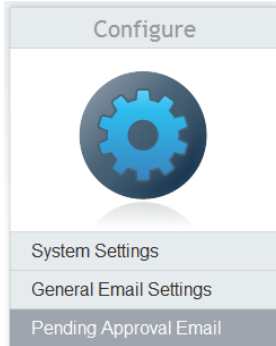


EmailSMTPServer	The server that will be used for outgoing emails. If it is in another domain you may need to specify the full domain name. Also some email servers need to be configured (more info) to accept and route emails coming from the server that is generating the emails. E.g. the web server or the server where AccountProvisioner is running.
EmailFromUser	The address used for the From tag in the emails. This should be a valid looking email address but the mailbox need not exist.
EmailReplyToUser	The address used for the Reply To tag in the emails. This should be a valid looking email address but the mailbox need not exist.
EmailDisableSend	Set this value to true while configuring and debugging and the email engine will not actually send out the generated emails. This can be used in conjunction with the EmailCopyFolder to allow you to take a look at the emails that would be sent. When you are sure that the emails are good you can set this value back to false and re-run the email generator process.

EmailCopyFolder	<p>A local folder where copies of all generated emails are stored. This is helpful when initially setting up the server to verify that the correct emails are being generated. It can be left on in production to keep a record of every email sent or it can be set to null to stop storing local copies.</p>
EmaillImagePath	<p>In an HTML formatted email we will want to embed images into the email rather than use the img src tags as found in the raw HTML template. These src tags could point to protected repositories or even to local files on the pc of the user who created the template. These paths would not work in an email so the code will replace any path information with references to embedded images. All images must appear in the EmaillImagePath folder on the server that is generating the emails. The code will strip off any path information and will use the filename to read the image from the EmaillImagePath folder.</p> <p>e.g. if I created an HTML template using Frontpage or some other tool it could contain tags like <code></code> The email engine will expect to find Welcome.gif in the EmaillImagePath folder on the server and will embed this image into the email so that it will be accessible to the recipient.</p>

Email Templates and Substitution variables

Pending Approval



Pending Approval Email Configuration

The optional "Pending Approval Email" is sent to the newly registered user, to allow acknowledgment of their registration, and remind them that the account has to be approved before it can be used.

Subject:

Body:

BCC:

Test Email:

Enable email:


EmailPendingApprovalSubject	The subject line for Pending Approval emails.
EmailPendingApproval Template	The template used to generate Pending Approval emails. It can be plain text or it can contain formatted html. HTML templates should start with <html> and end with </html>. There are no substitution variables allowed in this Email.
EmailPendingApproverBCC	One or more comma separated Email address, that should get a copy of the sent email, unbeknownst to the recipient.

EmailPendingApproverEnable	To enable this Email to be sent by the system, the Check box must be checked.
----------------------------	---

The Test Email, is not persisted, but can be used to see if the Email message can be received, and how the layout looks. The Email is sent to the entered Test Email account, when the OK button is clicked.

Pending Approver

Configure



System Settings

General Email Settings

Pending Approval Email

Pending Approver Email

Pending Approver Email Configuration

The optional "Pending Approver Email" is sent to the person(s) who are selected to approve new users. The template should include a link to the Edit User Page for easier approval.

To:	ExtraNet_Test@envisionit.com
Subject:	An Extranet account requires your approval
Body:	<pre><html><body style="background-color:white"> <div style="margin:0px">

</pre>
BCC:	ExtraNet_BCC@envisionit.com
Test Email:	
Enable email:	<input checked="" type="checkbox"/>

EmailPendingApproverTo	One or more comma separated Email Addresses for Approvers of new accounts. This field is merged with a virtual field at run time, if the Registration page wants to add context specific approvers. <i>(MembershipProvider_EmailAddressforPendingApprover)</i>
EmailPendingApproverSubject	The subject line for Pending Approver emails.
EmailPendingApproverTemplate	The template used to generate Pending Approver emails. It can be plain text or it can contain formatted html. HTML templates should start with <html> and end with </html>.

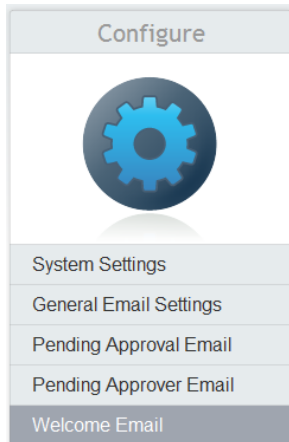
EmailPendingApproverBCC	One or more comma separated Email address, that should get a copy of the sent email, unbeknownst to the recipient.
EmailPendingApproverEnable	To enable this Email to be sent by the system, the Check box must be checked.

The Test Email, is not persisted, but can be used to see if the Email message can be received, and how the layout looks. The Email is sent to the entered Test Email account, when the OK button is clicked.

Substitution variables allowed in this Email:

~email~	Email address of the registering user.
~displayname~	Display name for the registering user (typically first and last name)
~username~	The Username of the registering user.
~userkey~	The key in the User Table for the registering user. (integer)

Welcome



Welcome Email Configuration

The "Welcome Email" is sent when a user is approved.

Subject:	<input type="text" value="Your New Account is ready at EnvisionIT SQLFBA"/>
Token Expiry:	<input type="text" value="20"/>
Body:	<pre><html><body style="background-color:white"> <div style="margin:0px">

</pre>
BCC:	<input type="text"/>
Test Email:	<input type="text"/>
Enable email:	<input checked="" type="checkbox"/>

EmailNewAccountSubject	The subject line for New account welcome emails.
NewAccountTokenExpiryMinutes	Users who receive a Welcome email will have this many minutes to use the ChangePassword link that is provided in the email.
EmailNewAccountTemplate	The template used to generate NewAccount welcome emails. It can be plain text or it can contain formatted html. HTML templates should start with <html> and end with </html>.

EmailNewAccountBCC	One or more comma separated Email address, that should get a copy of the sent email, unbeknownst to the recipient.
EmailNewAccountEnable	To enable this Email to be sent by the system, the Check box must be checked.

The Test Email, is not persisted, but can be used to see if the Email message can be received, and how the layout looks. The Email is sent to the entered Test Email account, when the OK button is clicked.

Substitution variables allowed in this Email:

~username~	The Username of the new account
~displayname~	Display name for the registering user (typically first and last name)
~homeurl~	HomeUrl from Application Configuration
~language~	The Language of the user (e.g. EN, FR, ES, NL). Can be used on urls to trigger the alternate language display of the page.

If EmailNewAccountSendToken = 0

~password~	The password of the new account
------------	---------------------------------

If EmailNewAccountSendToken = 1

~token~	Guid of the assigned token for password retrieval
~tokenexpiry~	When does the token expire. (see Token Expiry setting)
~updatepasswordurl~	The url to the UpdatePassword.aspx page in the landing project Comes from the ExtranetUrl in the Application Configuration with “/ForgotPass/UpdatePassword.aspx” on the end, with the Query String fully populated.
~forgotpasswordurl~	The url to the ForgotPassword page. Used to offer a link to the password reset functionality. Comes from the ExtranetUrl in the Application Configuration with

“/ForgotPass/default.aspx” on the end

The Following Multilingual options are also available:

The tokenexpiry can be displayed in

English (~tokenexpiry~),
French (~tokenexpiryfr~),
Spanish (~tokenexpiryes~),
Dutch (~tokenexpirynl~)

The Token expiry date is a long date format including the day of the week, and the time.


Also each of the URLs can have an &lang= added to the query String

English (~updatepasswordurl~,~ forgotpasswordurl~)
French (~updatepasswordurlfr~,~ forgotpasswordurlfr~)
Spanish (~updatepasswordurles~,~ forgotpasswordurles~)
Dutch (~updatepasswordurlnl~,~ forgotpasswordurlnl~)

There is only one Email Template, not one per language, so to support multilingual emails, all the variables could be used at the same time, in different sections, or a single unilingual template can be used in any of the languages.

Forgot Password

Configure



- System Settings
- General Email Settings
- Pending Approval Email
- Pending Approver Email
- Welcome Email
- Forgot Password Email

Forgot Password Email Configuration

A User can request the "Forgot Password Email" at any time, if they have forgotten their password.

Subject:

Token Expiry:

Body:

```
<html><body style="background-color:white">
<div style="margin:0px">

<br/>
<br/>
<br/>
<br/>
<br/>
<br/>
```

BCC:

Test Email:

Enable email:

EmailForgotPasswordSubject	The subject line for Forgot Password emails.
LostPasswordTokenExpiryMinutes	Users who use the ForgotPassword link will have this many minutes to use the ChangePassword link that is provided to them via email.
EmailForgotPasswordTemplate	<p>The template used to generate Change password emails. It can be plain text or it can contain formatted html.</p> <p>Refer to the documentation of the EIT_Email engine for details about the substitution variables that can be used in the template.</p>

EmailForgotPasswordBCC	One or more comma separated Email address, that should get a copy of the sent email, unbeknownst to the recipient.
EmailForgotPasswordEnable	To enable this Email to be sent by the system, the Check box must be checked.

The Test Email, is not persisted, but can be used to see if the Email message can be received, and how the layout looks. The Email is sent to the entered Test Email account, when the OK button is clicked.

Substitution variables allowed in this Email:

~homeurl~	HomeUrl from Application Configuration
~language~	The Language of the user (e.g. EN, FR, ES, NL). Can be used on urls to trigger the alternate language display of the page.
~tokenexpiry~	When does the token expire. (see Token Expiry setting)
~forgotpasswordurl~	The url to the ForgotPassword page. Used to offer a link to the password reset functionality. Comes from the ExtranetUrl in the Application Configuration with “/ForgotPass/default.aspx” on the end
~updatepasswordurl~	The url to the UpdatePassword.aspx page in the landing project Comes from the ExtranetUrl in the Application Configuration with “/ForgotPass/UpdatePassword.aspx” on the end You must construct your own QueryString, if using this one (see also ~updatepasswordlist~ and ~updatepasswordlink~ below)
~username~	Used when constructing your own Query String with ~updatepasswordurl~. Only the first username that matches the entered email can be returned. If there are multiple usernames for the same email address, then use ~updatepasswordlist~
~token~	Guid of the assigned token for password retrieval Used when constructing your own Query String with ~updatepasswordurl~.

e.g.	<p>This is an example of the 3 substitution variables being used to construct a single URL (spaces added for readability – URL should not contain spaces)</p> <pre>Reset your Password</pre>
~updatepasswordlist~	<p>The Forgot password request is based on an Email address. It is possible for more than one account to have the same email. This provides for a bulleted list of accounts with a separate reset for each one. Only one link per email can be used to reset a password.</p> <p>Comes from the ExtranetUrl in the Application Configuration with “/ForgotPass/ UpdatePassword.aspx” on the end, as well as the customized QueryString.</p>
~updatepasswordlink~	<p>*NEW * This one shows the EMAIL address as the link, and only includes the first username from the updatepasswordlist. Otherwise the link is the same as above. This is meant as a direct replacement for ~updatepasswordlist~ if you are generally using email addresses as if they were usernames.</p> <p>Note that you can not log on with an Email address, if there is more than one in the database that matches.</p> <p>Comes from the ExtranetUrl in the Application Configuration with “/ForgotPass/ UpdatePassword.aspx” on the end, as well as the customized QueryString.</p>
~emailaddress~	<p>The email address used to request the forgotten password. Email will be sent to this user, so it is not always necessary to include it in the body as well.</p>

The Following Multilingual options are also available:

The tokenexpiry can be displayed in

English (~tokenexpiry~),
French (~tokenexpiryfr~),
Spanish (~tokenexpiryes~),
Dutch (~tokenexpirynl~)

The Token expiry date is a long date format including the day of the week, and the time.

Also each of the URLs can have an &lang= added to the query String

English (~updatepasswordlist~, ~ forgotpasswordurl~)
French (~updatepasswordlistfr~, ~ forgotpasswordurlfr~)
Spanish (~updatepasswordlistes~, ~ forgotpasswordurles~)
Dutch (~updatepasswordlistnl~, ~ forgotpasswordurlnl~)

There is only one Email Template, not one per language, so to support multilingual emails, all the variables could be used at the same time, in different sections, or a single unilingual template can be used in any of the languages.

ManageUsers Database Configuration - Domain Table

This table has 1 row for each domain that needs to be queried when building the Site Tree list for a user in the Extranet module. For each domain we build a query looking for groups that the user belongs to within that domain. We need this set of groups when we are looking to find all the sites that the user has access to. This is because the user may have access to a site directly because the username was granted access, or indirectly because a group was granted access and the user belongs to the group. Typically there are one or two domains defined in this table.

DomainName	The domain that the users and roles will exist in.
Username	The username to be used when doing LDAP queries in this domain. Doesn't need to be the Domain Admin but does need to have rights to query and modify users and roles.
Password	The encrypted password for the Username above. Use the Envision IT command-line utility StoreEncryptedDataInDB tool to populate this field.
PasswordSalt	The salt value used to encrypt and decrypt the password value above. Will also be populated by the StoreEncryptedDataInDB tool.
LDAPConnectionString	The full LDAP path to the Users unit in the LDAP structure. This could be an OU=Users or a CN=Users (the default Microsoft schema). Someone familiar with the LDAP structure at the client needs to supply this value.

If the account that is running the IIS app pool can read from the domain, the username, password, and password Salt values can be left as NULL.

ManageUsers Database Configuration - Site Table

This table has one row for each sharepoint site collection that the users might have access to. This is used when building the Site Tree in the Extranet module. For each site (row in this table) we query for any sites the specified user (and any groups they belong to) has access to. For most installations there will be only 1 row that describes the Extranet sharepoint site.

SharePointRoot	The root of the sharepoint site to be queried.
ContentDBServer	The database server hosting the content database for the sharepoint site above.
ContentDBName	The name of the content database for the sharpeoint site above.
UserName	The SQL username to be used to access the database. Make sure this account has at minimum read access to the content database.
Password	The encrypted password for the Username above. Use the Envision IT command-line utility StoreEncryptedDataInDB tool to populate this field.
PasswordSalt	The salt value used to encrypt and decrypt the password value above. Will also be populated by the StoreEncryptedDataInDB tool.

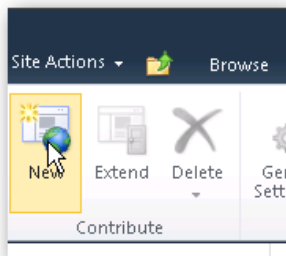
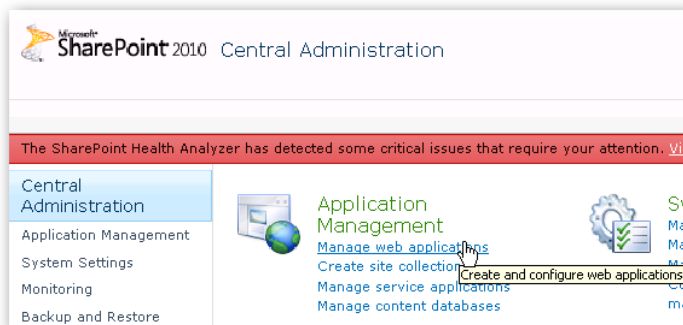
If the account that is running the IIS app pool can read from the specified content database, the username, password, and password Salt values can be left as NULL.

Appendix A – Creating the SharePoint Web Application

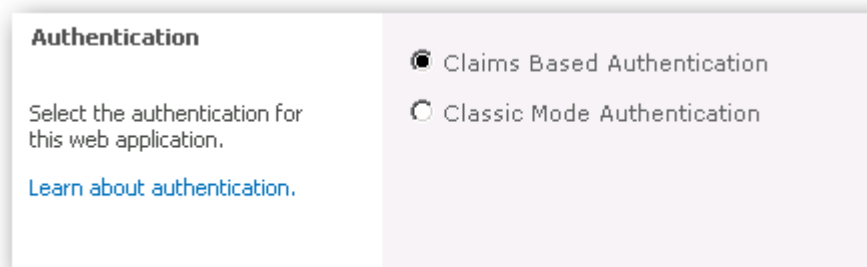
A SharePoint web site must be configured with external access. The application can be in the default zone (for Windows integrated scenario) or in the Extranet zone (for the FBA scenario). SharePoint search requires that at least one zone be using Windows integrated authentication.

Create a new Default Zone web application if one doesn't exist:

- a. Open SharePoint 2010 Central Administration on the host Web Front End Server.
- b. Navigate to Manage Web Applications, and select “New” on the ribbon bar:



- c. Fill out the web application dialog, beginning with selecting **Claims Based Authentication**:



- d. Define a name for the web application - defaults used in EIT are "SharePoint_{domain name of web app}{port}", eg. "SharePoint_SecureDev2010.envisionit.com443"
- e. Provide a **host header** name for the web app, eg. **securedev2010.envisionit.com** - this helps to auto-configure the the Alternate Access Mappings for the extranet zone later on.

- f. Set **Allow Anonymous** to Yes if anonymous access requests to the **Default Zone** web application is required.
- g. If using SSL set "Use Secure Sockets Layer (SSL)" to Yes

Security Configuration

If you choose to use Secure Sockets Layer (SSL), you must add the certificate on each server using the IIS administration tools. Until this is done, the web application will be inaccessible from this IIS web site.

Allow Anonymous

Yes

No

Use Secure Sockets Layer (SSL)

Yes

No

- h. Under **Claims Authentication Types**, leave the default settings checked, ie. Enable Windows Authentication, Integrated Windows Authentication (NTLM)

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.

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

- i. Under Sign In Page Url, leave the default settings.
- j. Under the Public Url section, ensure the URL for the **Default Zone** is correct, eg. fully qualified and has a corresponding DNS entry in the the domain:

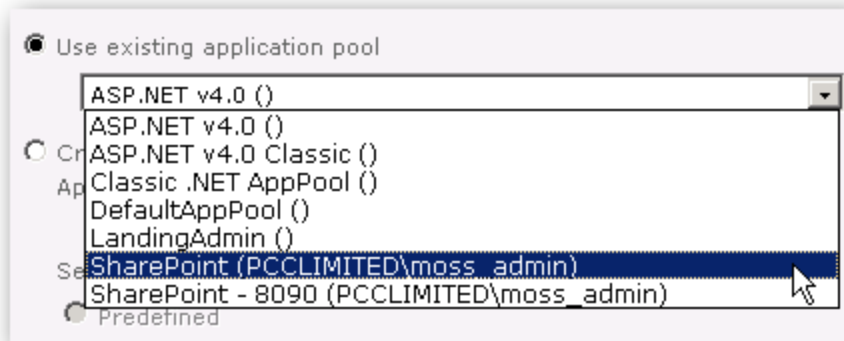
URL

http://sharepoint.envisionit.com:8081

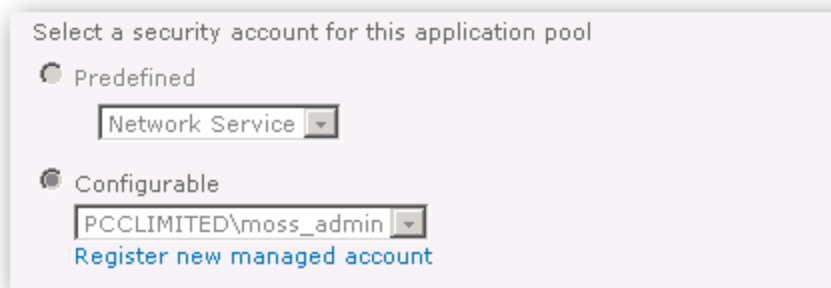
Zone

Default

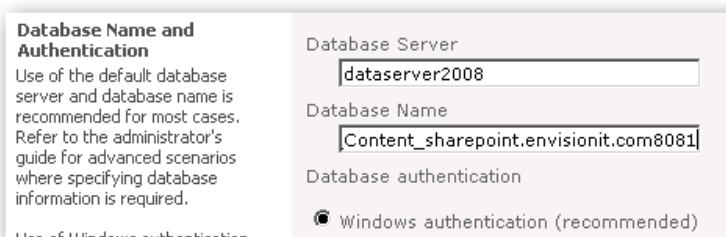
- k. Under Application Pool either create a new app pool for the web site, or optionally re-use a pre-existing Application Pool that is appropriate for your environment.



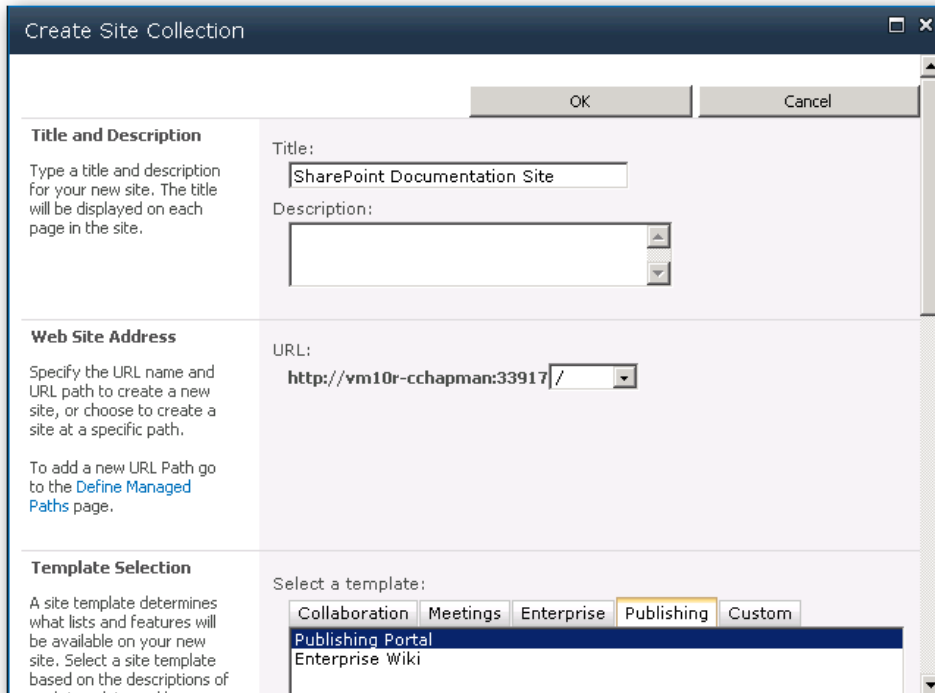
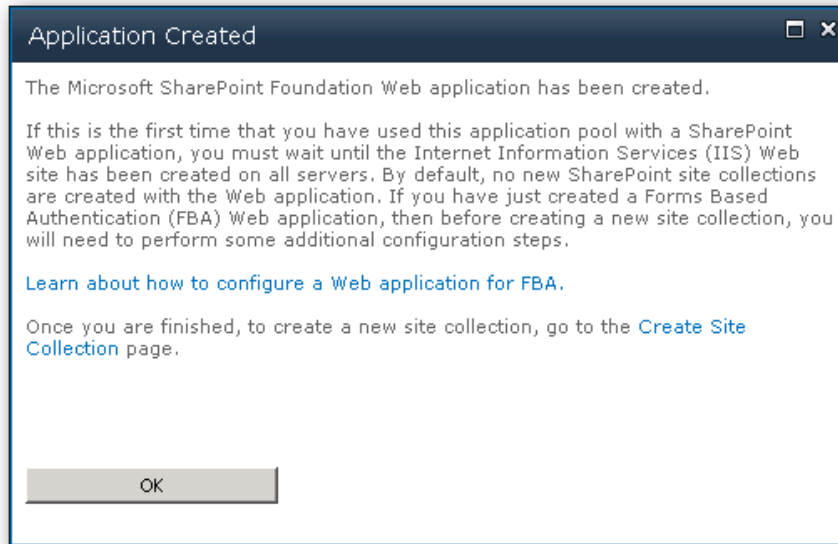
- l. Select the Security Account for the Application Pool via the drop-down - this may already be pre-populated for you.



- m. Under Database Name and Authentication, enter the name of the database server and provide a Database name. Usually this will correspond to {server name}_WSS_Content_{web app domain}{port number}, eg. SecureDev2010_WSS_Content_secureddev2010.envisionit.com443



- n. If you have a failover SQL Database, enter it in the Failover Database Server textbox.
- o. Leave all other settings unchanged and click OK at the bottom of the form to start the site creation process - this can take a few minutes.
- p. Once complete, you will be prompted with a dialog to create a new Site Collection - click the link to do so and follow the steps in the dialog screen, entering a name, URL, site collection template, and primary and secondary owner AD accounts.



Appendix B - Convert Classic to Claims Based Authentication with PowerShell

Once a SharePoint 2010 Web Application has been created using “Classic” authentication, the Central Administration GUI prevents changing this to “Claims Based” by greying-out the options. By using the SharePoint 2010 Management Shell on the Web Front End server, changing authentication can be easily accomplished using the following commands:

```
$webapp = Get-SPWebApplication("http://urlToWebApplication:Port")
$webapp.UseClaimsAuthentication = $True
$webapp.Update()
$webapp.ProvisionGlobally()
```

The change can be verified by opening Central Administration on the Web Front End server, selecting Manage Web Applications, choosing the desired web app and clicking the Authentication Providers button on the ribbon bar.

Note that this is a one-way conversion that cannot be reversed. Once authentication has been converted from Classic to Claims, the site cannot be reverted to Classic.

Security permissions will need to be re-applied once the site has been converted to Claims. EUM Hydra users appear as different users to SharePoint, even if they are the same AD account.

Appendix C - Configuring the ASPNET DB for SQL Provider

Microsoft provides a command line utility that is used to setup the ASPNETDB database. For further information about this utility please refer to <http://msdn2.microsoft.com/en-us/library/x28wfk74.aspx>. Note that if no parameters are provided on the command line then the tool will run in wizard mode, but it will not prompt for or setup the role support needed.

Location

`C:\windows\Microsoft.NET\Framework64\v2.0.50727\aspnet_regsql.exe`

Example

```
C:\windows\Microsoft.NET\Framework64\v2.0.50727\aspnet_regsql.exe -E -S
SQLServer -d EUM_ManageUsers_ASPNETDB -A all
```

In this example a database called “EUM_ManageUsers_ASPNETDB” will be created on the server “SQLServer” and support for all features will be installed.

`-A all` is very important to get the role support into the db, if you omit this you will get “Roles have been disabled” when configuring EUM.

Instead of specifying `-E` (use your credentials on the db server) `-U username -P password` can be specified to provide a specific username/password pair.

If command line parameters are not provided, `aspnet_regsql` will run in Wizard mode, but it will not run with `-A all`, so you will end up without the role support.

To enable the role support after the initial DB has been created, use `-A all`

Respecify the name of the server and the database to update an existing one

```
aspnet_regsql -E -A all -S dataserer2008 -d EIT_ManageUsers_V25_ASPNETDB
```

`-S` can be omitted if you are running this on the database server rather than the webserver.

Appendix D – Providing Connection Credentials

In some cases the application pool identity cannot be given rights into Active Directory. This is typically the case when SharePoint is running in the DMZ with its own AD, and there is no trust of the internal AD. If internal users are still intended to access the site with their internal credentials, an account with rights to the internal AD is needed.

It is not necessary to run the application pool with this account. What is needed is to modify the provider definitions in the various web.configs to provide a username and password combination.

```
<add name="InternalMP" connectionStringName="InternalCS"
type="EIT_ADProviders.ADMembershipDescendant,EIT_ADProviders, Version=2.5.4346.4,
Culture=neutral, PublicKeyToken=4fd2c7bc0e383e0a"
attributeMapUsername="SAMAccountName" enableSearchMethods="true"
connectionUsername="XXXX" connectionPassword="XXXX" />
```

This needs to be done for the membership, role, and profile definitions in each config file.

It is not generally best practice to leave privileged account information in plain text in the config files. In order to prevent this, the config files should be encrypted. This is done with the following steps.