

Forefront Identity Manager 2010 R2 Self-Service Password Reset Deployment Guide

Microsoft Corporation

Published: June 2012

Last Update:

Author: Bill Mathers

Version: 1.0

Acknowledgements

Special thanks to the following people for reviewing and providing invaluable feedback for this document:

Samer Fanek, Microsoft Corporation

Anthony Ho, Microsoft Corporation

Adrian Carutasu, Microsoft Corporation

Ram Babu Sattenapalli, Microsoft Corporation

Leon Dang, Microsoft Corporation

Abstract

This document will assist architects, consultants, system engineers, and system administrators in deploying Microsoft® Forefront® Identity Manager 2010 R2 SSPR.



Copyright

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred.

© 2012 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Forefront, MSDN, Outlook, SharePoint, SQL Server, Windows, Windows PowerShell, and Windows Server are trademarks of the Microsoft group of companies.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

[Deployment Guide for Forefront Identity Manager 2010 R2 - Self-Service Password Reset 9](#_Toc326301542)

[Deployment Guide for Forefront Identity Manager 2010 R2 – Self-Service Password Reset 9](#_Toc326301543)

[Planning for Forefront Identity Manager 2010 R2 - Self-Service Password Reset 9](#_Toc326301544)

[Planning for Forefront Identity Manager 2010 R2 - Self-Service Password Reset 9](#_Toc326301545)

[Considerations when Upgrading to FIM 2010 R2 SSPR 10](#_Toc326301546)

[Considerations when Upgrading to FIM 2010 R2 SSPR 10](#_Toc326301547)

[Upgrade Considerations 10](#_Toc326301548)

[Considerations for a Clean Installation of FIM 2010 R2 SSPR 11](#_Toc326301549)

[Considerations for a Clean Install of FIM 2010 R2 SSPR 11](#_Toc326301550)

[Environmental Considerations 11](#_Toc326301551)

[Supported Deployment Topologies 11](#_Toc326301552)

[Intranet / Extranet Consideration 11](#_Toc326301553)

[Single Server vs. Distributed 12](#_Toc326301554)

[Reverse Proxy in a DMZ 12](#_Toc326301555)

[Authentication Gate Considerations 13](#_Toc326301556)

[QA Gate Considerations 13](#_Toc326301557)

[OTP Email Gate Considerations 14](#_Toc326301558)

[OTP SMS Gate Considerations 14](#_Toc326301559)

[Application Pool Accounts 14](#_Toc326301560)

[Configuring the FIM Portal for Password Reset only 14](#_Toc326301561)

[Deploying Forefront Identity Manager 2010 R2 - Self-Service Password Reset 15](#_Toc326301562)

[Deploying Forefront Identity Manager 2010 R2 - Self-Service Password Reset 15](#_Toc326301563)

[Environmental Pre-requisites 15](#_Toc326301564)

[Environmental Pre-requisites 15](#_Toc326301565)

[Before You Begin 15](#_Toc326301566)

[Pre-requisite Tasks 16](#_Toc326301567)

[Associate the FIM Service with the Application Pool Accounts for Self-Service Password Reset 17](#_Toc326301568)

[Make the FIM Service account a member of the FIMSyncBrowse and FIMSyncPasswordSet groups 19](#_Toc326301569)

[Enable password management on the management agent for AD DS on the FIM Synchronization Server 19](#_Toc326301570)

[Enable FIM Service service account privileges in Windows Management Instrumentation on the FIM Synchronization Server 20](#_Toc326301571)

[Allow Windows Management Instrumentation traffic through the Windows Firewall on the FIM Synchronization Server 21](#_Toc326301572)

[Enable DCOM for the FIM service account 21](#_Toc326301573)

[Update the “Password Reset Users Set” in the FIM Portal to ensure it contains all the users you would like to participate in password reset 23](#_Toc326301574)

[Update the Password reset AuthN workflow in the FIM Portal 23](#_Toc326301575)

[Enable the Management Policy Rule named “Anonymous users can reset their password” 25](#_Toc326301576)

[Enable the Management Policy Rule named “Password reset users can read password reset objects” 26](#_Toc326301577)

[Enable the management policy rule named “Password reset users can update the lockout attribute of themselves” 26](#_Toc326301578)

[Enable the management policy rule named “User management: Users can read attributes of their own” 27](#_Toc326301579)

[Enable the management policy rule named “General: Users can read non-administrative configuration resources” 27](#_Toc326301580)

[Modify the management policy rule named “Administration: Administrators can read and update Users” to include new One Time Password attributes 27](#_Toc326301581)

[Password Registration and Reset Portal Deployment 28](#_Toc326301582)

[Password Registration and Reset Portal Deployment 28](#_Toc326301583)

[Installing the Password Registration and Reset Portal 28](#_Toc326301584)

[Post Installation Tasks 33](#_Toc326301585)

[Installing the Exchange 2007 and Exchange 2010 Web Service (EWS) Certificate 33](#_Toc326301586)

[Verifying the certificate and verify that the EWS can be reached 34](#_Toc326301587)

[Kiosk Scenario 34](#_Toc326301588)

[Change Mode Install – App Pool Account Change 35](#_Toc326301589)

[Add-ins and Extensions Deployment 36](#_Toc326301590)

[FIM 2010 R2 Add-ins and Extensions Deployment 36](#_Toc326301591)

[Manual Installation of Add-ins and Extensions 37](#_Toc326301592)

[Deploying Via Group Policy 39](#_Toc326301593)

[ForefrontIdentityManager.admx File 39](#_Toc326301594)

[ForefrontIdentityManager.adml File 46](#_Toc326301595)

[Unattended installation of FIM 2010 R2 Self-Service Password Reset 52](#_Toc326301596)

[Unattended installation of FIM 2010 R2 Self-Service Password Reset 52](#_Toc326301597)

[Pass-in parameters on the command line 52](#_Toc326301598)

[Create an MST file 53](#_Toc326301599)

[Troubleshoot an installation 53](#_Toc326301600)

[SSPR Features and properties 53](#_Toc326301601)

[Reset and Registration Portal Example 55](#_Toc326301602)

[Add-ins and Extensions Example 55](#_Toc326301603)

[Using the QuickStart Tool 55](#_Toc326301604)

[Using the QuickStart Tool 55](#_Toc326301605)

[Before you begin 56](#_Toc326301606)

[Setting up the QuickStart Package 56](#_Toc326301607)

[Invoke-QuickStart 59](#_Toc326301608)

[Syntax 59](#_Toc326301609)

[Detailed Description 59](#_Toc326301610)

[Parameters 60](#_Toc326301611)

[-Container <String> 60](#_Toc326301612)

[-DatabaseName <String> 60](#_Toc326301613)

[-DatabaseServer <String> 60](#_Toc326301614)

[-ForefrontIdentityManagerServiceBaseAddress <String> 61](#_Toc326301615)

[-Forest <String> 61](#_Toc326301616)

[-ActiveDirectoryManagementAgentCredential <PSCredential> 61](#_Toc326301617)

[-ForefrontIdentityManagerManagementAgentCredential <PSCredential> 61](#_Toc326301618)

[-RunInitialLoad [<Boolean>] 62](#_Toc326301619)

[<CommonParameters> 62](#_Toc326301620)

[Notes 62](#_Toc326301621)

[Example 1 63](#_Toc326301622)

[Testing the Deployment 63](#_Toc326301623)

[Test the Deployment 63](#_Toc326301624)

[Register for a self-service password reset 63](#_Toc326301625)

[Register from a client computer 63](#_Toc326301626)

[Register in the password registration portal 64](#_Toc326301627)

[Reset the password 64](#_Toc326301628)

[Reset the password from a client computer 64](#_Toc326301629)

[Reset the password in the password reset portal 65](#_Toc326301630)

[Maintaining Forefront Identity Manager 2010 R2 - Self-Service Password Reset 65](#_Toc326301631)

[Maintaining Forefront Identity Manager 2010 R2 - Self-Service Password Reset 65](#_Toc326301632)

[FIM 2010 R2 Password Registration Portal 66](#_Toc326301633)

[FIM 2010 R2 Password Registration Portal 66](#_Toc326301634)

[Home Page 66](#_Toc326301635)

[Completion Page 67](#_Toc326301636)

[FIM 2010 R2 Registration Portal Communication with the FIM Service 68](#_Toc326301637)

[FIM 2010 R2 SSPR Registration Portal Flow 69](#_Toc326301638)

[FIM 2010 R2 Password Reset Portal 71](#_Toc326301639)

[FIM 2010 R2 Password Reset Portal 71](#_Toc326301640)

[Home Page 71](#_Toc326301641)

[Choose New Password Page 73](#_Toc326301642)

[Success Page 73](#_Toc326301643)

[FIM 2010 R2 Reset Portal Communication with the FIM Service 74](#_Toc326301644)

[FIM 2010 R2 SSPR Reset Portal Flow 75](#_Toc326301645)

[FIM 2010 R2 Rich Client 77](#_Toc326301646)

[FIM 2010 R2 Rich Client 77](#_Toc326301647)

[How often registration is checked 77](#_Toc326301648)

[The Registration Portal URL 78](#_Toc326301649)

[The FIM Service Address 79](#_Toc326301650)

[Registration and Reset Portal Web.config settings 79](#_Toc326301651)

[Registration and Reset Portal Web.config settings 79](#_Toc326301652)

[FIM 2010 R2 Portal Customization 85](#_Toc326301653)

[FIM 2010 R2 Portal Customization 85](#_Toc326301654)

[Creating the Customizations folder 86](#_Toc326301655)

[Customizing strings 86](#_Toc326301656)

[Customizing the logo banner 100](#_Toc326301657)

[Customizing style sheets 101](#_Toc326301658)

[Common Customization Issues 105](#_Toc326301659)

[Programmatic User Registration 106](#_Toc326301660)

[Programmatic User Registration 106](#_Toc326301661)

[Required SNapIn 107](#_Toc326301662)

[Required Management Policy Rules 107](#_Toc326301663)

[Confirm-AuthenticationWorkflowRegistration 112](#_Toc326301664)

[Syntax 112](#_Toc326301665)

[Detailed Description 113](#_Toc326301666)

[Parameters 113](#_Toc326301667)

[-AuthenticationWorkflowName <String> 113](#_Toc326301668)

[-UserName <String> 113](#_Toc326301669)

[-Credential <PSCredential> 113](#_Toc326301670)

[-Uri <String> 114](#_Toc326301671)

[<CommonParameters> 114](#_Toc326301672)

[Notes 114](#_Toc326301673)

[Example 1 114](#_Toc326301674)

[Get-AuthenticationWorkflowRegistrationTemplate 114](#_Toc326301675)

[Syntax 115](#_Toc326301676)

[Detailed Description 115](#_Toc326301677)

[Parameters 115](#_Toc326301678)

[-AuthenticationWorkflowName <String> 115](#_Toc326301679)

[-Credential <PSCredential> 115](#_Toc326301680)

[-Uri <String> 116](#_Toc326301681)

[<CommonParameters> 116](#_Toc326301682)

[Notes 116](#_Toc326301683)

[Example 1 116](#_Toc326301684)

[Register-AuthenticationWorkflow 116](#_Toc326301685)

[Syntax 117](#_Toc326301686)

[Detailed Description 117](#_Toc326301687)

[Parameters 117](#_Toc326301688)

[-AuthenticationWorkflowRegistrationTemplate < AuthenticationWorkflowRegistrationTemplate > 117](#_Toc326301689)

[-UserName <String> 117](#_Toc326301690)

[-Credential <PSCredential> 118](#_Toc326301691)

[-Uri <String> 118](#_Toc326301692)

[<CommonParameters> 118](#_Toc326301693)

[Notes 118](#_Toc326301694)

[Example 1 118](#_Toc326301695)

[Unregister-AuthenticationWorkflow 119](#_Toc326301696)

[Syntax 119](#_Toc326301697)

[Detailed Description 119](#_Toc326301698)

[Parameters 119](#_Toc326301699)

[-AuthenticationWorkflowName <String> 119](#_Toc326301700)

[-UserName <String> 120](#_Toc326301701)

[-Credential <PSCredential> 120](#_Toc326301702)

[-Uri <String> 120](#_Toc326301703)

[<CommonParameters> 121](#_Toc326301704)

[Notes 121](#_Toc326301705)

[Example 1 121](#_Toc326301706)

[Kerberos and Self-Service Password Reset 121](#_Toc326301707)

[What is Kerberos? 121](#_Toc326301708)

[What are SPNs? 122](#_Toc326301709)

[How are tickets decrypted 123](#_Toc326301710)

[Kernel-Mode Authentication 123](#_Toc326301711)

[SPNs and Self-Service Password Reset 123](#_Toc326301712)

[Delegation and Self-Service Password Reset 126](#_Toc326301713)

[SSPR Authentication Gates 126](#_Toc326301714)

[SSPR Authentication Gates 126](#_Toc326301715)

[Security Context 127](#_Toc326301716)

[Password Gate 128](#_Toc326301717)

[QA Gate 128](#_Toc326301718)

[One-Time-Password Email Gate 136](#_Toc326301719)

[One-Time-Password SMS Gate 144](#_Toc326301720)

[Lockout Gates 153](#_Toc326301721)

[Gate Ordering 154](#_Toc326301722)

[Creating your own SSPR Workflow using the Authentication Gates 158](#_Toc326301723)

[Configuring password registration and reset for multiple languages 161](#_Toc326301724)

[SSPR Troubleshooting 163](#_Toc326301725)

[SSPR Troubleshooting 163](#_Toc326301726)

[Troubleshooting 163](#_Toc326301727)

# Deployment Guide for Forefront Identity Manager 2010 R2 - Self-Service Password Reset

## Deployment Guide for Forefront Identity Manager 2010 R2 – Self-Service Password Reset

The Deployment Guide for Forefront Identity Manager 2010 R2 – Self-Service Password Reset (FIM 2010 R2 SSPR) contains information to help you plan for and deploy FIM 2010 R2 SSPR, to help you upgrade from FIM 2010 Password Reset, and to help you maintain the FIM 2010 R2 SSPR infrastructure.

The following topics introduce the task areas covered in the Deployment Guide:

 [Planning for Forefront Identity Manager 2010 R2 - Self-Service Password Reset](#z14946f1ecb1b46119d8f8ed1220d8188)

 [Deploying Forefront Identity Manager 2010 R2 - Self-Service Password Reset](#zb232315cf7a143b59248172b5d5df9de)

 [Maintaining Forefront Identity Manager 2010 R2 - Self-Service Password Reset](#z68ea1bf8752d461f9ef0c1f30a192452)

You can download a copy of this technical documentation from the Microsoft Download Center.

# Planning for Forefront Identity Manager 2010 R2 - Self-Service Password Reset

## Planning for Forefront Identity Manager 2010 R2 - Self-Service Password Reset

This section provides major concepts to consider in the design and planning phase. This section provides things that should be considered if you are upgrading, doing a clean installation, and what the supported deployment topologies (i.e. Distributed, Extranet, DMZ) are.

The following topic areas are covered in this section:

 [Considerations when Upgrading to FIM 2010 R2 SSPR](#ze6bd028dc8fa4b70b6d9c9d1d5893879)

 [Considerations for a Clean Installation of FIM 2010 R2 SSPR](#z953324a557f74e69b23ee4ab108332d9)

# Considerations when Upgrading to FIM 2010 R2 SSPR

## Considerations when Upgrading to FIM 2010 R2 SSPR

The following are considerations that must be taken into account when upgrading to FIM 2010 R2 SSPR. These considerations deal strictly with upgrading. For additional Considerations such as security questions, service accounts see [Considerations for a Clean Installation of FIM 2010 R2 SSPR](#z953324a557f74e69b23ee4ab108332d9) later in this document.

### Upgrade Considerations

Always upgrade the FIM Service first before attempting to update the FIM 2010 native clients. The FIM 2010 native client will continue to work with a FIM 2010 R2 service with a little modification to the default QA gate, however the FIM 2010 R2 clients will not work with the FIM 2010 Service.

Upon upgrade to FIM 2010 R2, the new QA gate will by default use the new properties available to it. For a list of these see [SSPR Authentication Gates](#z5f47959d227e4adb91bf1ef442b5a87f) later in this document.

The FIM 2010 native client can register for a QA gate against an R2 server so long as the Allow radio button is selected under Compatibility of the QA Gate. By selecting Allow, the Allow duplicate answers and the Answer Constraint settings will not be enforced on registrations from these older clients. These selections are made in the AuthN workflow in the FIM portal. For an example of the QA gate see [QA Gate](#z1) later in this document.

Warning

Be aware that the FIM 2010 native client will not work with the OTP Email or OTP SMS gates, so if you have configured your workflow with either of these it will not work. The reason is, is that these were introduced with R2 and the FIM 2010 native client does not know about them.

# Considerations for a Clean Installation of FIM 2010 R2 SSPR

## Considerations for a Clean Install of FIM 2010 R2 SSPR

The following are considerations that must be taken into account when installing FIM 2010 R2 SSPR. These considerations deal strictly with a new install and not with upgrading. For Upgrade Considerations see [Considerations when Upgrading to FIM 2010 R2 SSPR](#ze6bd028dc8fa4b70b6d9c9d1d5893879) earlier in this document.

This section is comprised of the following:

 [Environmental Considerations](#z2)

 [Supported Deployment Topologies](#z3)

 [Authentication Gate Considerations](#z4)

 [Application Pool Accounts](#z5)

 [Configuring the FIM Portal for Password Reset only](#z6)

### Environmental Considerations

There are several pre-requisites required to implementing Self-Service Password Reset. These can be found here: [Environmental Pre-requisites](#z3d1ca293241845f8bef0e2c975d45aac). These pre-requisites should be considered prior to planning your deployment so you can assess your environment and see what other teams/divisions may need to be engaged to ensure a successful deployment.

### Supported Deployment Topologies

When planning a deployment of Forefront Identity Manager 2010 R2 Self-Service Password Reset you can design a topology that ranges from a single-server to a distributed deployment. Each of these, in turn, can be intranet-only or intranet/extranet. If a topology that has an extranet component is chosen, these may sit directly on an extranet or they can be published using a reverse-proxy such as Forefront Threat Management Gateway 2010.

#### Intranet / Extranet Consideration

One of the first things that need to be determined is whether or not any or all of the portals will be accessible via the intranet or via the intranet and extranet. If you choose to have both the registration and reset portals only available on the intranet, then users will not be able to reset their passwords externally. Users will have to be connected to your corporate environment to use the portals.

It is possible to specify that only one portal is accessible through an extranet while making the other one only available via the intranet. For instance, you can choose to deploy the portals in such a fashion as to have the registration portal be intranet facing and the reset portal be intranet/extranet facing. With this option, users must be logged on to the corporate network to register for password reset but once this is done they can reset their passwords from anywhere.

#### Single Server vs. Distributed

Depending on how much of Forefront Identity Manager 2010 R2 you plan to implement, you may choose a single-server option over a distributed one. With a single server option all of the features of Forefront Identity Manager 2010 R2 are installed on a single sever. This includes the FIM Service, the FIM Portal, the Synchronization Service, the Registration and Reset portals as well as SQL and SharePoint 2010. If you wish to deploy the FIM 2010 R2 Reporting Feature you will need to use minimum distributed deployment, as the SCSM pieces require two additional servers. The single-server option may be best suited for a very small deployment of FIM 2010 R2 or for a test environment. That is, for example, if you plan to only use SSPR and your AD environment is relatively small.

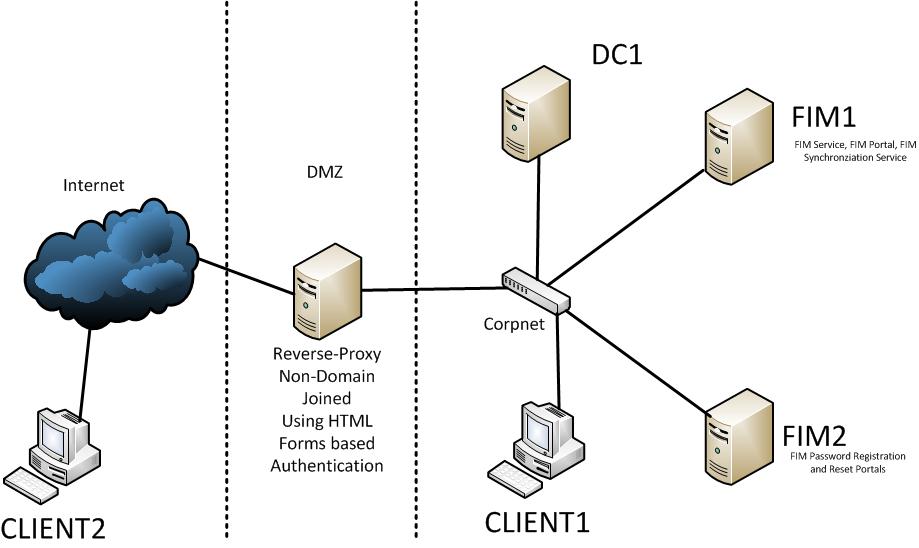
A distributed, scaled out deployment is the most common in the enterprise. The most common deployment of this type sees the FIM Service and the Synchronization Service residing on servers other than the SQL servers that house their databases. In fact, the FIM Service, the Synchronization Service and their two databases may actually all be on separate servers. From a security stand point this is a better solution in that, if you are going to have the password registration and password reset portals externally facing and sitting on the internet, you would not want to expose your FIM Service and Synchronization Service, or their databases to the internet.

#### Reverse Proxy in a DMZ

The Password Reset and Registration Portals are publishable to the internet using a reverse proxy such as Forefront Threat Management Gateway 2010 and other 3rd party reverse-proxy servers. A reverse proxy configuration is supported under the following conditions:

 The reverse proxy is domain joined and is publishing either or all of the password portals externally.

 The reverse proxy is not domain joined and is publishing either or all of the password portals externally.



### Authentication Gate Considerations

Forefront Identity Manager 2010 R2 includes several authentication gates that can be configured for use with Self-Service Password Reset. These gates can be setup as part of an Authentication workflow. There are a few considerations depending upon the type of Gate you select. For additional information on Authentication Gates see [SSPR Authentication Gates](#z5f47959d227e4adb91bf1ef442b5a87f) later in this document.

#### QA Gate Considerations

The QA gate provides a mechanism for users to authenticate to the FIM Service. During registration it accepts answers to various configurable questions and during reset it prompts for these answers. With regard to the QA Gate there are several considerations that need to be taken into account. The following is a list of these considerations:

 Easily Remembered – Are the security questions you are implementing easy for users to remember answer to?

 Relevant to everyone – Are the security questions you are implementing relevant to everyone? Not everyone has a cat or a dog or even a sibling.

 Not easy to guess – Are the answers to the security questions you are implementing difficult to guess? Do they have hundreds or thousands of possible answers?

 Not on Facebook – Are the answers to the security questions you are implementing things that you would not post on Facebook?

 Number of Questions – How many questions do you plan to implement? Are users required to register for all of these?

 Number of Answers – How many questions will users be required to answer correctly to change their password? Will you have them register for say 10 questions but then only randomly give them 3 that they need to answer correctly?

 Duplicate – Will you allow duplicates or not?

#### OTP Email Gate Considerations

The One-Time-Password (OTP) Email Gate is a new Authentication gate that is being introduced in FIM 2010 R2. This gate provides a way for a user’s identity to be verified by sending a one-time-password to the user’s email address. With regard to the OTP Email Gate there are a couple of considerations that need to be taken into account. The following is a list of these considerations:

 Valid E-mail Address – Does your environment have a mail attribute that is populated with a valid email address for your users or will the users need to specify this when registering.

 OTP Email and FIM 2010 R2 Client – If you are implementing an OTP Email gate and a user attempts to reset their password via the client because they are locked out of their laptop or desktop will they be able to access this email? Should the OTP Email gate be used for just extranet requests?

#### OTP SMS Gate Considerations

The One-Time-Password (OTP) SMS Gate is a new Authentication gate that is being introduced in FIM 2010 R2. This gate provides a way for a user’s identity to be verified by sending a one-time-password to the user’s mobile phone via an SMS provider. With regard to the OTP SMS Gate there are few considerations that need to be taken into account. The following is a list of these considerations:

 An SMS Provider – An SMS (Short Message System) provider is required to use the OTP SMS gate.

 Valid Mobile Phone number – Does your environment have an attribute that is populated with a valid mobile phone number for your users or will the users need to specify this when registering.

 Code Experience – In order to implement the SmsServiceProvider.dll a small amount of code will need to be written based on how you connect with your SMS service provider.

### Application Pool Accounts

You will need at least one account, possibly two if you want to run each site under a different application pool account. These accounts should be regular domain user accounts.

### Configuring the FIM Portal for Password Reset only

If you are using FIM only for password resets, you can remove the other elements from the FIM home page. For information about how to update the FIM home page, see [Introduction to Configuring the FIM Portal](http://go.microsoft.com/fwlink/?LinkID=165848) in the FIM 2010 documentation.

# Deploying Forefront Identity Manager 2010 R2 - Self-Service Password Reset

## Deploying Forefront Identity Manager 2010 R2 - Self-Service Password Reset

This section provides information and step-by-step instructions on installing the various components that make up a Forefront Identity Manager 2010 R2 – Self-Service Password Reset deployment.

The following topic areas are covered in this section:

 [Environmental Pre-requisites](#z3d1ca293241845f8bef0e2c975d45aac)

 [Password Registration and Reset Portal Deployment](#z69423d7caa8f45c48c8a76ea18ba2a2e)

 [Add-ins and Extensions Deployment](#z8cbbd557ee174aa28599d5f7c3c66e59)

 [Unattended installation of FIM 2010 R2 Self-Service Password Reset](#z4a4f26433d7141d482fc77fd0aa00fc1)

 [Using the QuickStart Tool](#z6987c7ce6bc0469ba002b35ca00c9a4d)

 [Testing the Deployment](#z4d772f66f55e46eeb697486bf79f3274)

# Environmental Pre-requisites

## Environmental Pre-requisites

The following information will guide you through the pre-requisites required to setup and configure FIM 2010 R2 Self-Service Password Reset. This section is composed of the following:

 [Before You Begin](#z7)

 [Pre-requisite Tasks](#z8)

### Before You Begin

Ensure that the following actions are taken before you begin the procedures for password reset:

 User resources are synchronized between AD DS and the FIM 2010 R2 database.

 If there is a firewall between the server running FIM and the server running AD DS, the following ports must be opened in the firewall between the FIM Synchronization Server and the Active Directory domain controller:

a. TCP/UDP 135 (RPC EPMapper)

b. TCP/UDP 389 (LDAP, LDAP Ping)

c. TCP 636 (LDAP over SSL)

d. TCP 3268 (GC)

e. TCP 3269 (GC SSL)

f. TCP/UDP 53 (DNS)

g. TCP/UDP 88 (Kerberos)

h. TCP Dynamic (RPC)

i. TCP/UDP 464 (Kerberos Change/Set Password)

j. TCP 445 – (CIFS/ MICROSOFT-DS)

 To facilitate WMI communication, you will also need to make sure the following ports are open between the server running the FIM Service and the server running the FIM Synchronization Service:

a. TCP/UDP 135 (RPC EPMapper)

b. TCP 135 (RPC EPMapper)

c. TCP 5725

d. TCP 5726

e. TCP 5000-5001 Dynamic RPC ports (PCNS)

f. TCP 57500-57520 Dynamic RPC ports (AD MA)

The following references can be helpful:

1. [Active Directory and Active Directory Domain Services Port Requirements](http://go.microsoft.com/fwlink/?LinkId=186040)

2. [Active Directory Replication over Firewalls](http://go.microsoft.com/fwlink/?LinkId=123775)

3. [Network Ports Used by Key Microsoft Server Products](http://technet.microsoft.com/en-us/library/cc875824.aspx)

4. [How to Use Portqry to Troubleshoot Active Directory Connectivity Issues](http://go.microsoft.com/fwlink/?LinkId=111883)

5. [Management Agent Communication Ports, Rights, and Permissions](http://go.microsoft.com/fwlink/?LinkId=187617)

### Pre-requisite Tasks

The following pre-requisite tasks must be completed prior to deploying the Self-Service Password Registration and Reset portals. This section will provide you with information on how to accomplish each of these tasks. It is recommended that these tasks be completed in order prior to installing the SSPR binaries. For a complete step-by-step example of implementing these steps see [Test Lab Guide: Demonstrating the FIM 2010 R2 Self-Service Password Reset with the Q/A Gate](http://technet.microsoft.com/en-us/library/hh826057(v=ws.10).aspx).

1. [Associate the FIM Service with the Application Pool Accounts for Self-Service Password Reset](#z9)

2. [Make the FIM Service account a member of the FIMSyncBrowse and FIMSyncPasswordSet groups](#z10)

3. [Enable password management on the management agent for AD DS on the FIM Synchronization Server](#z11)

4. [Enable FIM Service service account privileges in Windows Management Instrumentation on the FIM Synchronization Server](#z12)

5. [Allow Windows Management Instrumentation traffic through the Windows Firewall on the FIM Synchronization Server](#z13)

6. [Enable DCOM for the FIM service account](#z14)

7. [Update the “Password Reset Users Set” in the FIM Portal to ensure it contains all the users you would like to participate in password reset](#z15)

8. [Update the Password reset AuthN workflow in the FIM Portal](#z16)

9. [Enable the Management Policy Rule named “Anonymous users can reset their password”](#z17)

10. [Enable the Management Policy Rule named “Password reset users can read password reset objects”](#z18)

11. [Enable the management policy rule named “Password reset users can update the lockout attribute of themselves”](#z19)

12. [Enable the management policy rule named “User management: Users can read attributes of their own”](#z20)

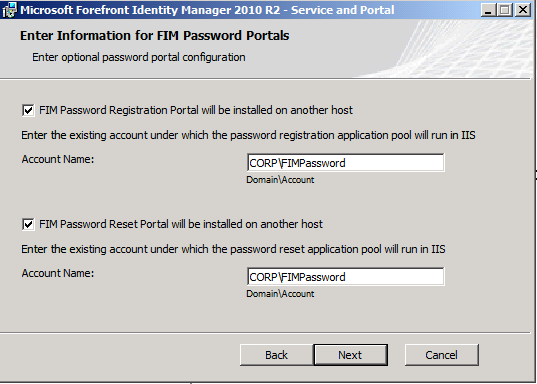
13. [Enable the management policy rule named “General: Users can read non-administrative configuration resources”](#z21)

14. [Modify the management policy rule named “Administration: Administrators can read and update Users” to include new One Time Password attributes](#z22)

#### Associate the FIM Service with the Application Pool Accounts for Self-Service Password Reset

One important thing that must be done in order for Self-Service Password Reset to work properly is that the FIM Service account must be aware of the application pool account or accounts that are running the Registration and Reset Portals. This is because these become well-known identities to the FIM Service. The FIM Service recognizes requests which originate from these identities and respond accordingly. If you plan to run the Registration and Reset portals on a server other than the one that is running the FIM Service, then these accounts need to be specified during the FIM Service setup. In other words, to associate the FIM Service with these accounts, you must specify these accounts at the end of installation wizard when setting up the FIM Service.

Enter information for FIM Password Portals



Warning

If you plan to run the Registration and Reset portals on the same server as the FIM Service, then these boxes can be left blank when you are installing the FIM Service. This is only if you plan to run the SSPR portals on the same server as the FIM Service.

If you are installing the registration and reset portals on the same server, you will not see the UI above.

For additional information on FIM Service communication with the Registration Portal and the Reset Portal see [FIM 2010 R2 Registration Portal Communication with the FIM Service](#z23) and [FIM 2010 R2 Reset Portal Communication with the FIM Service](#z24) later in this guide.

Also, be aware that if this account changes or you need to do a change mode install that you will need to ensure the FIM Service is associated with the app pool accounts by running a change mode install on the FIM Service server first, then on the servers that are hosting the Registration and Reset portasl. For more information on this see [Change Mode Install – App Pool Account Change](#z25).

#### Make the FIM Service account a member of the FIMSyncBrowse and FIMSyncPasswordSet groups

To make the FIM Service account a member of the FIMSyncBrowse and FIMSyncPasswordSet groups

|  |
| --- |
| 1. On the FIM 2010 R2 Synchronization Server click Start, then click Administrative Tools, then click Computer Management. Expand Local Users and Groups and click Groups.  2. Right click the FIMSyncBrowse group, and click Properties.  3. Click Add.  4. In Enter the object names to select, enter FIMService, and click Check Names.  5. Click OK twice.  6. Right click the FIMSyncPasswordSet group, and click Properties.  7. Click Add.  8. In Enter the object names to select, enter FIMService, and click Check Names.  9. Click OK twice.  10. Close Computer Management.  11. Restart the FIM Synchronization Service.  12. Restart the FIM Service. |

#### Enable password management on the management agent for AD DS on the FIM Synchronization Server

You must enable password management on the management agent for Active Directory Domain Services (AD DS). This makes it possible for AD DS to process the password reset requests that it receives.

To enable password management on the management agent for AD DS

|  |
| --- |
| 1. On the server running the FIM Synchronization Service, open the Synchronization Service Manager  2. Click the Management Agents tab.  3. Select the management agent for AD DS.  4. On the Actions menu, click Properties.  5. In the Properties window, click Configure Extensions.  6. Select the Enable password management check box.  7. Click OK. |

To assign rights in AD DS to allow the Active Directory management agent account to reset passwords and unlock accounts

|  |
| --- |
| 1. On the server running AD DS, open Active Directory Users and Computers.  2. Click View, and then click Advanced Features.  3. Right-click the organizational unit (OU) that contains the users for password reset, click Properties, and then click the Security tab.  Note  If you followed the naming in Common Configuration Guide, this will be the FIMObjects OU.  4. Click Add, the account name that is used by the AD DS management agent, and then click OK to return to the Security tab.  5. With the AD DS management agent account highlighted in the Group or user names window, click Advanced.  6. Select the AD DS management agent account, and then click Edit.  7. On the Object tab, in Apply to, select Descendant User objects and set the following permissions:   Reset password = Allow   Change password = Allow  8. On the Properties tab, in Apply to, select Descendant User objects and set the following permissions:   Read userAccountControl = Allow   Write userAccountControl=Allow   Read lockoutTime = Allow   Write lockoutTime = Allow  9. Click OK three times.  10. Grant Replicating Directory Changes permissions for the Active Directory Management service account. You can do that by following the steps in the following article: [How to grant the "Replicating Directory Changes" permission for the Microsoft Metadirectory Services ADMA service account](http://go.microsoft.com/fwlink/?LinkId=47854). |

#### Enable FIM Service service account privileges in Windows Management Instrumentation on the FIM Synchronization Server

The FIM Service service account must have security access to the namespace and subnamespaces on the FIM 2010 R2 server.

To enable Windows Management Instrumentation namespace and subnamespace privileges

|  |
| --- |
| 1. Log on to the server that is running the FIM Synchronization Service as an administrator.  2. Click Start, right-click Computer, and then click Manage.  3. In Server Manager, double-click Configuration, right-click WMI Control, and then click Properties.  4. Click the Security tab.  5. Double-click Root, click CIMV2, and then click Security.  6. On Security for ROOT\CIMV2, click Add.  7. On Select Users, Computers, and Groups, in the Enter the object names to select (examples) box, type the FIM Service service account name, and then click Check Name.  When the service account name resolves successfully, it appears underlined.  8. Click OK.  9. On Security for ROOT\CIMV2, ensure that Allow in the FIM Service service account is selected for Enable Account and Remote Enable.  10. On Security for ROOT\CIMV2, ensure that the FIM Service service account is selected, and then click Advanced.  11. On Advanced Security Settings for CIMV2, select the FIM Service service account, and then click Edit.  12. On Permission Entry for CIMV2, select This namespace and subnamespaces in the Apply To box.  13. Click OK.  14. On Advanced Security Settings for CIMV2, click Apply, and then click OK.  15. On Security for ROOT\CIMV2, click OK.  16. On WMI Control Properties, click OK.  17. Close Server Manager. |

#### Allow Windows Management Instrumentation traffic through the Windows Firewall on the FIM Synchronization Server

You must configure the firewall on the server running the FIM Synchronization Service to allow Windows Management Instrumentation (WMI) traffic to pass through.

To allow WMI traffic through the Windows Firewall

|  |
| --- |
| 1. Log on to the FIM 2010 R2 Server as an administrator.  2. Click Start, and then click Control Panel.  3. In Control Panel, click Windows Firewall.  4. On Windows Firewall, select Allow a program or feature through Windows Firewall.  5. On Allowed Programs, under Allowed programs and features, scroll down, and then select the Windows Management Instrumentation (WMI) check box.  6. Click OK.  7. Close Windows Firewall.  8. Close Control Panel. |

#### Enable DCOM for the FIM service account

WMI uses DCOM to communicate with the FIM 2010 R2 server. For this to occur, the FIM Service service account requires access to DCOM on the server running the FIM Synchronization Service. The following steps assume a single-server implementation. That is, the FIM Service and the FIM Synchronization Service are running on the same server. If your environment has the FIM Service and the FIM Synchronization Service running on separate servers, ensure that the permissions for the FIM Service service account are set on the server that is running the FIM Synchronization Service.

To enable DCOM for the FIM service account

|  |
| --- |
| 1. Log on to the server that is running the FIM Synchronization Service as an administrator.  2. Click Start, click Administrative Tools, and then click Component Services.  3. On Component Services, double-click Component Services, and then double-click Computers.  4. Right-click My Computer, and then click Properties.  5. On My Computer Properties, click COM Security.  6. On COM Security, under Access Permissions, click Edit Limits.  7. On Access Permissions, click Add.  8. On Select, Users, Computers, and Groups, in the Enter the object names to select (examples) box, type the FIM service account name, and then click Check Name.  When the service account name resolves successfully, it appears underlined.  9. Click OK.  10. On Access Permissions, select the FIM Service service account. Select the Allow check box for both Local Access and Remote Access.  11. Click OK.  12. On COM Security, under Access Permissions, click Edit Default.  13. On Access Permissions, click Add.  14. On Select, Users, Computers, and Groups, in the Enter the object names to select (examples) box, type the FIM service account name, and then click Check Name.  When the service account name resolves successfully, it appears underlined.  15. Click OK.  16. On Access Permissions, select the FIM Service service account. Select the Allow check box for both Local Access and Remote Access.  17. Click OK.  18. On COM Security, under Launch and Activation Permissions, click Edit Limits.  19. On Launch and Activation Permissions, click Add.  20. On Select, Users, Computers, and Groups, in the Enter the object names to select (examples) box, type the FIM Service service account name, and then click Check Name.  When the service account name resolves successfully, it appears underlined.  21. Click OK.  22. On Launch and Activation Permissions, select the FIM Service service account. Select the Allow check boxes for Local Launch, Remote Launch, Local Activation, and Remote Activation.  23. Click OK.  24. On COM Security, under Launch and Activation Permissions, click Edit Default.  25. On Access Permissions, click Add.  26. On Select, Users, Computers, and Groups, in the Enter the object names to select (examples) box, type the FIM service account name, and then click Check Name.  When the service account name resolves successfully, it appears as underlined.  27. Click OK.  28. On Launch and Activation Permissions, select the FIM Service service account. Select the Allow check boxes for Local Launch, Remote Launch, Local Activation, and Remote Activation.  29. Click OK.  30. On My Computer Properties, click Apply, and then click OK.  31. Close Component Services. |

#### Update the “Password Reset Users Set” in the FIM Portal to ensure it contains all the users you would like to participate in password reset

FIM 2010 R2 contains default sets for password reset. Open the Password Reset Users Set in the FIM portal to make sure it contains the users that you would like to participate in password reset.

To update the Password Reset Users Set in the FIM Portal to ensure it contains all the users you want to participate in password reset

|  |
| --- |
| 1. Log on to the FIM Portal as Administrator.  2. From the FIM Portal home page, under Administration, click Sets.  3. On the Sets page, locate the set named Password Reset Users Sets by searching or paging through the list of sets, and then click on the name.  4. By default, all users are included in the Password Reset Users Set. Click View Members to see the users that are currently in the set.  5. If you want to limit the set membership, change the criteria filter to limit the set to the users you would like to have to participate in password reset.  Note  Click More information on the Password Reset Users Set page for steps to modify the criteria filter. |

#### Update the Password reset AuthN workflow in the FIM Portal

There is a default workflow in the FIM Portal for password reset that defines the challenges a user must pass before resetting his or her password. In this step, you will modify the default Question and Answer gate, and add an additional One-Time Password gate for extranet users.

Tips

An attacker might launch a denial-of-service attack on password reset by purposely failing password reset challenges for multiple users, causing many users to be locked out of password reset. To mitigate this type of attack, you should place the lockout gate after a Question and Answer gate. By configuring the activities in this way, the attacker would need to pass at least one gate before they could try and lock out other users. You could then place an additional Question and Answer gate after the lockout gate for additional security. The sequence would then be as follows:

1. Password gate

2. Question and Answer gate

3. Lockout gate

4. Question and Answer gate

 To update the questions in the Question and Answer activity based on your organization’s preferences and ensure that the lockout gate settings (if applicable) match your organization’s requirements

|  |
| --- |
| 1. Log on to the FIM Portal as an administrator.  2. From the FIM home page, under Administration, click Workflows.  3. On the Workflows page, search or browse the list of workflows, and then click Password Reset AuthN Workflow.  4. Click Activities, and then expand QA Gate.  5. Under QAGate, scroll down and click Edit, configure the following steps in the order shown, and then click Save.  a. Security Context  Ensure that All is selected. This option will display this QA gate to users accessing the password portals from the Windows logon and from the Web.  b. Step 1 Question Settings  Specify the total number of questions asked and the number of questions that are displayed during the password registrations. Also, configure the number of questions that are required for registration, the number of questions that are randomly presented to the user, and the number of questions that the user must answer correctly.  c. Step 2 Enter Questions  Specify the questions that users must answer to register for self-service password reset.  d. Step 3 Compatibility  Select Disallow. This requires that you have the FIM 2010 R2 Password Reset Extensions installed on the client computer, and will let you test the constraint settings.  6. Click Save.  7. Select Add Activity, select One-Time Password Email Gate, and click Select.  8. Configure the following steps in the order shown, and then click Save.  a. Security Context  Ensure that Extranet is selected. This option will display this gate only to requests that originate from the extranet. This includes only requests from a FIM Password Reset Portal which is configured as being accessible to users on the extranet.  b. Registration Mode  Select Read/Write. This allows the user to enter or modify their One-Time Password Email Address during registration.  c. Length of one-time password  Enter a value between 6 and 12.  d. Email Template for sending one-time password to user:  Use the Default completed approval email template.  9. Click Save.  10. Expand Lockout Gate, scroll down and click Edit, confirm that the following options match your organization’s preferences, and then click Save.  Lockout duration after Lockout Threshold is reached (minutes) – Specify the number of minutes that users are locked out of password reset before they are allowed to attempt password reset again.  Lockout Threshold – number of times the user can fail to complete the workflow – Specify the number of times a user can enter an incorrect answer to the challenge questions before they must wait the specified amount of time as defined in the Lockout duration after Lockout Threshold is reached (minutes) setting.  Number of times the user can reach the Lockout Threshold before permanent lockout – Specify the number of additional attempts to answer the challenge questions—each separated by the lockout duration time—before the user is permanently locked out of the password reset feature.  11. Click OK, and then click Submit. |

#### Enable the Management Policy Rule named “Anonymous users can reset their password”

So that users can register for password reset, a Management Policy Rule (MPR) must exist that gives users the permissions to read the attributes necessary to register for password reset. This MPR is created by default for FIM 2010 R2, but it is also disabled by default.

Note

Some of these MPRs may already be enabled from testing other FIM 2010 R2 scenarios.

To enable the “Anonymous users can reset their password” MPR

|  |
| --- |
| 1. Log on to the FIM Portal as an administrator.  2. On the FIM home page, under Administration, click Management Policy Rules.  3. On the Management Policy Rules page, search or browse the list of MPRs to locate Anonymous users can reset their password.  4. Click the display name of the MPR, and on the General Information tab, ensure that the Policy is disabled check box is cleared.  5. Click OK, and then click Submit. |

#### Enable the Management Policy Rule named “Password reset users can read password reset objects”

For users to reset their passwords, the client server that requests the password reset must be able to locate and read the MPR that is associated with the user they are claiming to be.

To enable the “Password reset users set can read password reset objects” MPR

|  |
| --- |
| 1. Log on to the FIM Portal as an administrator.  2. From the FIM home page, under Administration, click Management Policy Rules.  3. On the Management Policy Rules page, search or browse the list of MPRs to find Password reset users can read password reset objects.  4. Open the MPR, and, on the General Information tab, ensure that the Policy is disabled check box is cleared.  5. Click OK, and then click Submit. |

#### Enable the management policy rule named “Password reset users can update the lockout attribute of themselves”

When a user successfully registers or resets his or her password, the lockout count is reset. For that update to happen to the lockout count, the user must have permissions to update it. This MPR grants those permissions.

To enable the “Password Reset Users can update the lockout attribute of themselves” MPR

|  |
| --- |
| 1. Log on to the FIM Portal as an administrator.  2. On the FIM home page, under Administration, click Management Policy Rules.  3. On the Management Policy Rules page, search or browse the list of MPRs to locate Password Reset Users can update the lockout attribute of themselves.  4. Open the MPR, and on the General Information tab, ensure that Policy is disabled is cleared.  5. Click OK, and then click Submit. |

#### Enable the management policy rule named “User management: Users can read attributes of their own”

To enable the “User management: Users can read attributes of their own” MPR

|  |
| --- |
| 1. Log on to the FIM Portal as an administrator.  2. On the FIM home page, under Administration, click Management Policy Rules.  3. On the Management Policy Rules page, search or browse the list of MPRs to locate User Management: Users can read attributes of their own.  4. Open the MPR, and on the General Information tab, ensure that Policy is disabled is cleared.  5. Click OK, and then click Submit. |

#### Enable the management policy rule named “General: Users can read non-administrative configuration resources”

To enable the “General: Users can read non-administrative configuration resources” MPR

|  |
| --- |
| 1. Log on to the FIM Portal as an administrator.  2. On the FIM home page, under Administration, click Management Policy Rules.  3. On the Management Policy Rules page, search or browse the list of MPRs to locate General: Users can read non-administrative configuration resources.  4. Open the MPR, and, on the General Information tab, ensure that the Policy is disabled check box is cleared.  5. Click OK, and then click Submit. |

#### Modify the management policy rule named “Administration: Administrators can read and update Users” to include new One Time Password attributes

To modify the “Administration: Administrators can read and update Users” MPR

|  |
| --- |
| 1. Log on to the FIM Portal as an administrator.  2. On the FIM home page, under Administration, click Management Policy Rules.  3. On the Management Policy Rules page, search or browse the list of MPRs to locate Administration: Administrators can read and update Users.  4. Open the MPR, and on the Target Resources tab, add the following attributes to Select specific attributes:  One-Time Password Email Address  One-Time Password Mobile Phone  5. Click OK, and then click Submit. |

# Password Registration and Reset Portal Deployment

## Password Registration and Reset Portal Deployment

This section includes information on installing the FIM 2010 R2 Password Registration and Reset Portals. This section is composed of the following:

 [Installing the Password Registration and Reset Portal](#z26)

 [Post Installation Tasks](#z27)

 [Kiosk Scenario](#z28)

 [Change Mode Install – App Pool Account Change](#z25)

The following section includes information on installing the FIM 2010 R2 Rich Client. This section does not discuss unattended installation of the Add-ins and Extensions. For information on this see [Unattended installation of FIM 2010 R2 Self-Service Password Reset](#z4a4f26433d7141d482fc77fd0aa00fc1) later in this document.

### Installing the Password Registration and Reset Portal

The screenshots below assumes that the password registration and password reset portal will be deployed on a server other than the one that is running the FIM Service and Synchronization Service. The reason is that the password registration and reset portals are often extranet facing. This allows users the ability to reset their passwords from non-domain joined machines. However, from a security stand point, it would not be recommended to have the FIM Service and the FIM Synchronization Service sitting on the internet.

If you are not going to have the password registration and password reset portals extranet facing and wish to install everything on one server, this is supported but there are some things that need to be considered. The first is that SharePoint for the FIM Portal will be using port 80 on IIS, so additional ports will be required for the password registration and password reset portals. Also, if you are installing everything on one machine and are using Kerberos then useAppPoolCRedentials=true will be set because SharePoint runs as a “farm”. If this is true, then the Application Pool account that runs the FIM Password Registration Site and the FIM Password Reset Site will need to have the appropriate SPNs and delegation configured.

To install the Password Registration and Reset Portals, do the following:

To install Password Registration and Password Reset Portal

|  |
| --- |
| 1. Log on to the server that will host the portals as CORP\Administrator.  2. Navigate to the directory that contains the binaries for Forefront Identity Manager 2010 R2 and double-click FIMSplash.htm. This will bring up the Forefront Identity Manager 2010 R2 splash screen.  3. On the splash screen, click Install Service and Portal. You will see a pop-up that says Do you want to run or save this file? Click Run. This will take a minute. Then you will see another pop-up asking Do you want to run this software? Click Run. This will start the Forefront Identity Manager 2010 Service and Portal Setup Wizard.  4. On the Welcome page, click Next.  5. On the End User License Agreement page, read the License Agreement, select I accept the terms in the License Agreement, and then click Next.  6. On the FIM Customer Experience Improvement Program page, select I don’t want to join the program at this time, and then click Next.  7. On the Custom Setup page, click the drop-down list next to FIM Service, select Entire feature will be unavailable.  8. On the Custom Setup page, click the drop-down list next to FIM Portal, select Entire feature will be unavailable.  9. Click Next.  Custom Setup    10. On the Configure FIM Password Registration Portal page, next to Account Name, enter your service account.  11. On the Configure FIM Password Registration Portal page, next to Password, enter your service account password.  12. On the Configure FIM Password Registration Portal page, next to Host Name, enter the appropriate host name.  13. On the Configure FIM Password Registration Portal page, next to Port, type the following text:  80. Place a check in the box next to Open port in firewall.  Configure FIM Password Registration Portal    14. Click Next.  Important  This will bring up a box that says Your deployment is not secure in its current configuration. This is because we have not setup SSL yet. Click Next.  15. On the Configure FIM Password Registration Portal page, next to FIM Server Service Address, enter the FIM Server Service Address.  Configure FIM Password Registration Portal    16. Click Next.  17. On the Configure FIM Password Reset Portal page, next to Account Name, enter your service account.  18. On the Configure FIM Password Reset Portal page, next to Password, enter your service account password.  19. On the Configure FIM Password Reset Portal page, next to Host Name, enter the appropriate host name.  20. On the Configure FIM Password Reset Portal page, next to Port, type the following text:  80. Place a check in the box next to Open port in firewall.  Configure FIM Password Reset Portal    21. Click Next.  Important  This will bring up a box that says Your deployment is not secure in its current configuration. This is because we have not setup SSL yet. This will be done in the steps that follow. Click Next.  22. On the Configure FIM Password Reset Portal page, next to FIM Server Service Address, enter the FIM Server Service Address.  Configure FIM Password Reset Portal    23. Click Next.  24. Click Install. This will begin the installation.  25. Once the installation completes, click Finish.  26. Close the Splash screen. |

### Post Installation Tasks

The following are a couple of post installation tasks that should be verified prior to using SSPR.

#### Installing the Exchange 2007 and Exchange 2010 Web Service (EWS) Certificate

Note

This is an optional task that is used to ensure the FIM Service can use Exchange with the SSPR OTP Email gate.

If your server running Exchange is using a certificate that is untrusted by the FIM Service, the certificate used by the Exchange server must be added to the local certificate store.

You can verify if you have an untrusted certificate by opening Internet Explorer and navigating to https://mailserver/ews/exchange.asmx. If you receive a certificate error, you must complete the all the steps in this section. Mailserver is the server running Exchange that you specified when you installed the FIM 2010 R2 component.

If you have several FIM Service servers, this task must be completed on every server.

Note

You must run the installation of the Exchange certificate with elevated rights. If User Account Control (UAC) is turned on, installing the Exchange certificate without elevated rights causes the installation to fail.

To install the Exchange certificate on the FIM Service server

|  |
| --- |
| 1. Open Internet Explorer.  2. In the address bar, type https://mailserver/EWS/exchange.asmx.  Mailserver is the server running Exchange that you specified when you installed the FIM 2010 R2 component.  Select Continue to this Web site.  3. In the Security Alert dialog box (where it reads Certificate Error), click View Certificate.  4. In the Certificate dialog box, click Install Certificate.  5. On the Welcome to the Certificate Import Wizard page, click Next.  6. On the Certificate Store page, select Place all certificates in the following store, and then click Browse.  7. Select the Show physical stores check box, navigate to Trusted People\Local Computer, and select this store. Click OK.  8. Click Next.  9. Click Finish to import the certificate. |

#### Verifying the certificate and verify that the EWS can be reached

In this procedure, you will ensure that the Exchange 2007 or Exchange 2010 Web Service (EWS) is running and can be accessed as the FIM service account. This is an optional task that is used to ensure the FIM Service can use Exchange for Self-Service Password Reset.

To ensure that the Exchange 2007 or Exchange 2010 Web service (EWS) is running and is accessible as the FIM service account

|  |
| --- |
| 1. Open Internet Explorer as the FIM 2010 administrator.  2. In the address bar, type https://<mail server>/EWS/Exchange.asmx. This ensures that you can access EWS by using the FIM service account. |

### Kiosk Scenario

If you want to enable a scenario in which the users cannot log on to the computer but have to reset their password, you can set up a password reset kiosk. To do that, you create and use a local machine account to log on to the computer. The user will then be able to access the browser without having to log on to the computer.

### Change Mode Install – App Pool Account Change

The following is a note on doing a change mode install. If you do a change mode install to change the account that runs the FIM Password Registration and Password Reset portals you must also run a change mode install on the server that is running the FIM Service and specify the application pool account or accounts. This should be done first. That is, prior to running the change mode install on the Registration and Reset portal server, run a change mode install on the server that is running the FIM Service and associate it with the new application pool account or accounts.

To run a change mode install and associate the FIM Service account with the FIM Password Registration and Password Reset Portal Service account do the following:



|  |
| --- |
| 1. Begin a change mode install.  2. On the Enter optional password portal configuration page, place a check in FIM Password Registration Portal will be installed on another host and under Enter the existing account under which the password registration application pool will run in IIS, next to Account Name, type the new password registration service account.  3. On the Enter optional password portal configuration page, place a check in FIM Password Reset Portal will be installed on another host and under Enter the existing account under which the application pool will run in IIS, next to Account Name, type the new password reset service account.  Enter information for FIM Password Portals    4. Finish the change mode install. |

# Add-ins and Extensions Deployment

## FIM 2010 R2 Add-ins and Extensions Deployment

Forefront Identity Manager 2010 R2 includes a rich client that can be used for password registration, password reset and the FIM Add-in for Outlook. FIM 2010 R2 has a 32-bit and 64-bit version of the client. These are located on the installation media under Add-ins and Extensions. This section is composed of the following:

 [Manual Installation of Add-ins and Extensions](#z30)

 [Deploying Via Group Policy](#z31)

The following section includes information on installing the FIM 2010 R2 Rich Client. This section does not discuss unattended installation of the Add-ins and Extensions. For information on this see [Unattended installation of FIM 2010 R2 Self-Service Password Reset](#z4a4f26433d7141d482fc77fd0aa00fc1) later in this document.

### Manual Installation of Add-ins and Extensions

To manually install the Add-ins and Extensions.msi file, do the following:

Manually installing Add-ins and Extensions

|  |
| --- |
| 1. On the FIM Splash screen from a client select either Install Add-ins and Extensions, 64-bit or Install Add-ins and Extensions, 32-bit depending on the client. This will start the installation wizard.  2. On the Welcome screen, click Next.  3. On the End-User License Agreement screen, read the agreement, place a check in I accept the terms in the License Agreement and then click Next.  4. On the FIM Customer Experience Improvement Program screen, choose whether or not to join the Customer Experience Improvement Program and click Next.  5. On the Custom Setup screen, you can choose whether or not to install the FIM Add-in for Outlook. For SSPR, ensure that FIM Password and Authentication Extensions is selected and click Next.    6. On the Configure FIM Add-ins and Extensions screen, enter the name of the FIM Service Server address and then click Next.    7. On the Configure FIM Add-ins and Extensions screen, enter the Intranet Registration Portal URL and click Next.    8. On the Ready to Install Forefront Identity Manager Add-ins and Extensions click Install.  9. Once the installation completes, click Finish. |

### Deploying Via Group Policy

In very large FIM 2010 R2 deployments with a lot of clients, it may not be feasible to manually install the clients to every user machine in the organization. For this reason, the Add-ins and Extensions.msi file can be deployed via a group policy object. Depolying msi packages via group policy is outside the scope of this documentation, but you can refer to [Editing Domain-Based GPOs Using ADMX Files](http://technet.microsoft.com/en-us/library/cc748955(v=ws.10).aspx) using the ADMX and ADML files provided below. For detailed explanations of the registry settings see [FIM 2010 R2 Rich Client](#z6f114bfe1da744668dd407a92def4d52) later in this document.

#### ForefrontIdentityManager.admx File

The ADMX file for deploying via group policy.

<?xml version="1.0" encoding="utf-8"?>

<policyDefinitions

xmlns:xsd="http://www.w3.org/2001/XMLSchema"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

revision="1.0"

schemaVersion="1.0"

xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions">

<policyNamespaces>

<target prefix="fim" namespace="Microsoft.Policies.IdentityManagement" />

<using prefix="Windows" namespace="Microsoft.Policies.Windows" />

</policyNamespaces>

<resources minRequiredRevision="1.0" />

<categories>

<category name="FIMROOT" displayName="$(string.FIMROOT\_NAME)" explainText="$(string.FIMROOT\_EXPLAIN)" />

<category name="ADDINS" displayName="$(string.ADDINS\_NAME)" explainText="$(string.ADDINS\_EXPLAIN)">

<parentCategory ref="FIMROOT"/>

</category>

<category name="CMCLIENT" displayName="$(string.CMCLIENT\_NAME)" explainText="$(string.CMCLIENT\_EXPLAIN)" >

<parentCategory ref="FIMROOT"/>

</category>

</categories>

<policies>

<policy

name="MONACCTNAME"

displayName="$(string.MONACCTNAME\_NAME)"

explainText="$(string.MONACCTNAME\_EXPLAIN)"

presentation="$(presentation.MONACCTNAME)"

key="Software\Policies\Microsoft\Forefront Identity Manager\2010\Add-ins"

class="User">

<parentCategory ref="ADDINS"/>

<supportedOn ref="Windows:SUPPORTED\_ProductOnly"/>

<elements>

<text id="MONACCTNAME\_TEXT" valueName="MonitoredAccountName" required="false"/>

</elements>

</policy>

<policy

name="VALIDSENDERS"

displayName="$(string.VALIDSENDERS\_NAME)"

explainText="$(string.VALIDSENDERS\_EXPLAIN)"

presentation="$(presentation.VALIDSENDERS)"

key="Software\Policies\Microsoft\Forefront Identity Manager\2010\Add-ins"

class="User">

<parentCategory ref="ADDINS"/>

<supportedOn ref="Windows:SUPPORTED\_ProductOnly"/>

<elements>

<text id="VALIDSENDERS\_TEXT" valueName="ValidApprovalRequestSenders" required="false"/>

</elements>

</policy>

<policy

name="SHOWMGMTUI"

displayName="$(string.SHOWMGMTUI\_NAME)"

explainText="$(string.SHOWMGMTUI\_EXPLAIN)"

presentation="$(presentation.SHOWMGMTUI)"

key="Software\Policies\Microsoft\Forefront Identity Manager\2010\Add-ins"

class="User">

<parentCategory ref="ADDINS"/>

<supportedOn ref="Windows:SUPPORTED\_ProductOnly"/>

<elements>

<enum id="SHOWMGMTUI\_ENUM" valueName="ShowGroupManagementUi" required="false">

<item displayName="$(string.SHOWMGMTUI\_DISABLE)">

<value>

<decimal value="0"/>

</value>

</item>

<item displayName="$(string.SHOWMGMTUI\_ENABLE)">

<value>

<decimal value="1"/>

</value>

</item>

</enum>

</elements>

</policy>

<policy

name="PORTALURL"

displayName="$(string.PORTALURL\_NAME)"

explainText="$(string.PORTALURL\_EXPLAIN)"

presentation="$(presentation.PORTALURL)"

key="Software\Policies\Microsoft\Forefront Identity Manager\2010\Add-ins"

class="User">

<parentCategory ref="ADDINS"/>

<supportedOn ref="Windows:SUPPORTED\_ProductOnly"/>

<elements>

<text id="PORTALURL\_TEXT" valueName="PortalUrl" required="false"/>

</elements>

</policy>

<policy

name="ADDRBOOKGRP"

displayName="$(string.ADDRBOOKGRP\_NAME)"

explainText="$(string.ADDRBOOKGRP\_EXPLAIN)"

presentation="$(presentation.ADDRBOOKGRP)"

key="Software\Policies\Microsoft\Forefront Identity Manager\2010\Add-ins"

class="User">

<parentCategory ref="ADDINS"/>

<supportedOn ref="Windows:SUPPORTED\_ProductOnly"/>

<elements>

<text id="ADDRBOOKGRP\_TEXT" valueName="AllGroupsAddressBookName" required="false"/>

</elements>

</policy>

<policy

name="ADDRBOOKMBRS"

displayName="$(string.ADDRBOOKMBRS\_NAME)"

explainText="$(string.ADDRBOOKMBRS\_EXPLAIN)"

presentation="$(presentation.ADDRBOOKMBRS)"

key="Software\Policies\Microsoft\Forefront Identity Manager\2010\Add-ins"

class="User">

<parentCategory ref="ADDINS"/>

<supportedOn ref="Windows:SUPPORTED\_ProductOnly"/>

<elements>

<text id="ADDRBOOKMBRS\_TEXT" valueName="AllMembersAddressBookName" required="false"/>

</elements>

</policy>

<policy

name="DELETEAPPROVAL"

displayName="$(string.DELETEAPPROVAL\_NAME)"

explainText="$(string.DELETEAPPROVAL\_EXPLAIN)"

presentation="$(presentation.DELETEAPPROVAL)"

key="Software\Policies\Microsoft\Forefront Identity Manager\2010\Add-ins"

class="User">

<parentCategory ref="ADDINS"/>

<supportedOn ref="Windows:SUPPORTED\_ProductOnly"/>

<elements>

<enum id="DELETEAPPROVAL\_ENUM" valueName="DeleteApprovalRequest" required="false">

<item displayName="$(string.DELETEAPPROVAL\_DISABLE)">

<value>

<decimal value="0"/>

</value>

</item>

<item displayName="$(string.DELETEAPPROVAL\_ENABLE)">

<value>

<decimal value="1"/>

</value>

</item>

</enum>

</elements>

</policy>

<policy

name="SERVICEADDRESS"

displayName="$(string.SERVICEADDRESS\_NAME)"

explainText="$(string.SERVICEADDRESS\_EXPLAIN)"

presentation="$(presentation.SERVICEADDRESS)"

key="Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions\Intranet"

class="Machine">

<parentCategory ref="ADDINS"/>

<supportedOn ref="Windows:SUPPORTED\_ProductOnly"/>

<elements>

<text id="SERVICEADDRESS\_TEXT" valueName="Address" required="false"/>

</elements>

</policy>

<policy

name="CACHEINTERVAL"

displayName="$(string.CACHEINTERVAL\_NAME)"

explainText="$(string.CACHEINTERVAL\_EXPLAIN)"

presentation="$(presentation.CACHEINTERVAL)"

key="Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions"

class="User">

<parentCategory ref="ADDINS"/>

<supportedOn ref="Windows:SUPPORTED\_ProductOnly"/>

<elements>

<decimal id="CACHEINTERVAL\_TEXT" valueName="CacheInterval" minValue="0" maxValue="2147483647" required="false"/>

</elements>

</policy>

<policy

name="MAXOFFSET"

displayName="$(string.MAXOFFSET\_NAME)"

explainText="$(string.MAXOFFSET\_EXPLAIN)"

presentation="$(presentation.MAXOFFSET)"

key="Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions"

class="User">

<parentCategory ref="ADDINS"/>

<supportedOn ref="Windows:SUPPORTED\_ProductOnly"/>

<elements>

<decimal id="MAXOFFSET\_TEXT" valueName="MaxOffset" minValue="0" maxValue="2147483647" required="false"/>

</elements>

</policy>

<policy

name="SITELOCKCLM"

displayName="$(string.SITELOCK\_NAME)"

explainText="$(string.SITELOCK\_EXPLAIN)"

presentation="$(presentation.SITELOCK)"

key="Software\Policies\Microsoft\Clm\v1.0\SmartCardClient"

class="User">

<parentCategory ref="CMCLIENT"/>

<supportedOn ref="Windows:SUPPORTED\_ProductOnly"/>

<elements>

<text id="SITELOCK\_TEXT" valueName="SiteLock" required="false"/>

</elements>

</policy>

<policy

name="REGPORTALURL"

displayName="$(string.REGPORTALURL\_NAME)"

explainText="$(string.REGPORTALURL\_EXPLAIN)"

presentation="$(presentation.REGPORTALURL)"

key="Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions\PasswordRegistrationPortal"

class="User">

<parentCategory ref="ADDINS"/>

<supportedOn ref="Windows:SUPPORTED\_ProductOnly"/>

<elements>

<text id="REGPORTALURL\_TEXT" valueName="PasswordRegistrationPortalUrl" required="false"/>

</elements>

</policy>

</policies>

</policyDefinitions>

#### ForefrontIdentityManager.adml File

The ADML file for deploying via group policy.

<?xml version="1.0" encoding="utf-8"?>

<policyDefinitionResources

xmlns:xsd="http://www.w3.org/2001/XMLSchema"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

revision="1.0"

schemaVersion="1.0"

xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">

<displayName>Forefront Identity Manager</displayName>

<description>Configuration for Forefront Identity Manager clients</description>

<resources>

<stringTable>

<string id="FIMROOT\_NAME">Forefront Identity Manager</string>

<string id="FIMROOT\_EXPLAIN">Configuration for Forefront Identity Manager</string>

<string id="ADDINS\_NAME">Add-ins and Extensions</string>

<string id="ADDINS\_EXPLAIN">Configuration for Add-ins and Extensions</string>

<string id="CMCLIENT\_NAME">Certificate Management</string>

<string id="CMCLIENT\_EXPLAIN">Configuration for Certificate Management</string>

<string id="MONACCTNAME\_NAME">Configure FIM Service mailbox address</string>

<string id="MONACCTNAME\_EXPLAIN">

With this policy setting, you can specify the mailbox address of the FIM Service service account that processes incoming requests sent by the FIM Add-in for Outlook.

If you do not configure this policy setting, the mailbox address specified during setup will be used.

</string>

<string id="VALIDSENDERS\_NAME">Configure valid senders of approval requests</string>

<string id="VALIDSENDERS\_EXPLAIN">

With this policy setting, you can specify the mailbox addresses of valid service accounts which can send approval requests that are being accepted by the FIM Add-in for Outlook. You need to configure this policy setting if you change the FIM Service service account, e.g. by using the policy setting “Configure FIM Service mailbox address”. This policy setting should contain both the new and old mailbox addresses to make sure all previously sent approval emails are still treated as valid. You can specify several mailbox addresses by separating them with semicolon.

If you do not configure this policy setting, only the mailbox address in “Configure FIM Service mailbox address” will be used.

</string>

<string id="SHOWMGMTUI\_NAME">Configure group management in the UI</string>

<string id="SHOWMGMTUI\_EXPLAIN">

With this policy setting, you can specify whether the FIM Add-in for Outlook should show the group management options in the UI.

If you do no configure this policy setting, the group management options in the UI will be enabled.

</string>

<string id="SHOWMGMTUI\_DISABLE">Disable Group Management UI</string>

<string id="SHOWMGMTUI\_ENABLE">Enable Group Management UI</string>

<string id="PORTALURL\_NAME">Configure FIM Portal address</string>

<string id="PORTALURL\_EXPLAIN">

With this policy setting, you can specify the URL for the FIM Portal used in the FIM Add-in for Outlook when the user selects “Group Management Website”.

If you do not configure this policy setting, the URL specified during setup will be used.

</string>

<string id="ADDRBOOKGRP\_NAME">Configure the address book containing valid groups</string>

<string id="ADDRBOOKGRP\_EXPLAIN">

With this policy setting, you can specify the address book used by the FIM Add-in for Outlook when the user selects groups to add members to.

If you do not configure this policy setting, the address book All Groups will be used.

</string>

<string id="ADDRBOOKMBRS\_NAME">Configure the address book containing valid members</string>

<string id="ADDRBOOKMBRS\_EXPLAIN">

With this policy setting, you can specify the address book used by the FIM Add-in for Outlook when the user selects members to add to groups.

If you do not configure this policy setting, the address book Global Address Book will be used.

</string>

<string id="DELETEAPPROVAL\_NAME">Configure Approval Request deletion</string>

<string id="DELETEAPPROVAL\_EXPLAIN">

With this policy setting, you can specify whether the FIM Add-in for Outlook should delete the Approval Request email when the user has responded.

If you do not configure this policy setting, the user can configure this setting in the FIM Add-in for Outlook. The default is to delete those emails.

</string>

<string id="DELETEAPPROVAL\_DISABLE">Do Not Delete</string>

<string id="DELETEAPPROVAL\_ENABLE">Delete</string>

<string id="SITELOCK\_NAME">Configure valid ActiveX sites</string>

<string id="SITELOCK\_EXPLAIN">

With this policy setting, you can specify the sites used by the FIM CM Client component. The ActiveX control will only run from sites specified in this list. You can specify several sites by separating them with semicolon. Do not include a prefix (e.g. http://).

If you do not configure this policy setting, the sites specified during setup will be used.

</string>

<string id="SERVICEADDRESS\_NAME">Configure FIM Service address</string>

<string id="SERVICEADDRESS\_EXPLAIN">

With this policy setting, you can specify the address to the FIM Service used by password reset. The format is: http://serveraddress:5725

If you do not configure this policy setting, the address specified during setup will be used.

</string>

<string id="CACHEINTERVAL\_NAME">Configure cache duration for password reset registration</string>

<string id="CACHEINTERVAL\_EXPLAIN">

With this policy setting, you can configure how often the password reset registration status is checked for a user at logon.

If you do not configure this policy setting, the password reset registration status will be checked at every time the user logs on.

</string>

<string id="MAXOFFSET\_NAME">Configure max random offset for password reset registration</string>

<string id="MAXOFFSET\_EXPLAIN">

With this policy setting, you can configure the offset for the policy setting “Configure cache duration for password reset registration” in order to prevent all password reset registration checks for all users during the same day.

If you do not configure this policy setting but have configured “Configure cache duration for password reset registration” then password reset registration checks for all users will occur at the next login after the duration has been reached.

If you do not configure this policy setting and have not configured “Configure cache duration for password reset registration” then password reset registration checks will happen at every login for all users.

</string>

<string id="REGPORTALURL\_NAME">Configure FIM password registration portal URL for password reset registration</string>

<string id="REGPORTALURL\_EXPLAIN">

With this policy setting, you can configure the registration portal URL which the default browser will navigate to during password reset registration.

If you do not configure this policy setting, the registration portal URL specified during setup will be used.

</string>

</stringTable>

<presentationTable>

<presentation id="MONACCTNAME">

<textBox refId="MONACCTNAME\_TEXT">

<label>FIM Service mailbox address</label>

</textBox>

</presentation>

<presentation id="VALIDSENDERS">

<textBox refId="VALIDSENDERS\_TEXT">

<label>Valid senders of approval requests</label>

</textBox>

</presentation>

<presentation id="SHOWMGMTUI">

<dropdownList refId="SHOWMGMTUI\_ENUM" defaultItem="0">Show group management in the UI</dropdownList>

</presentation>

<presentation id="PORTALURL">

<textBox refId="PORTALURL\_TEXT">

<label>FIM Portal address</label>

</textBox>

</presentation>

<presentation id="ADDRBOOKGRP">

<textBox refId="ADDRBOOKGRP\_TEXT">

<label>Address Book</label>

</textBox>

</presentation>

<presentation id="ADDRBOOKMBRS">

<textBox refId="ADDRBOOKMBRS\_TEXT">

<label>Address Book</label>

</textBox>

</presentation>

<presentation id="DELETEAPPROVAL">

<dropdownList refId="DELETEAPPROVAL\_ENUM" defaultItem="0">Approval Request deletion</dropdownList>

</presentation>

<presentation id="SITELOCK">

<textBox refId="SITELOCK\_TEXT">

<label>Configure valid ActiveX sites</label>

</textBox>

</presentation>

<presentation id="SERVICEADDRESS">

<textBox refId="SERVICEADDRESS\_TEXT">

<label>FIM Portal address</label>

</textBox>

</presentation>

<presentation id="CACHEINTERVAL">

<decimalTextBox refId="CACHEINTERVAL\_TEXT" defaultValue="14">Registration status cache duration (in days)</decimalTextBox>

</presentation>

<presentation id="MAXOFFSET">

<decimalTextBox refId="MAXOFFSET\_TEXT" defaultValue="5">Maximum random offset (in days)</decimalTextBox>

</presentation>

<presentation id="REGPORTALURL">

<textBox refId="REGPORTALURL\_TEXT">

<label>Registration Portal URL</label>

</textBox>

</presentation>

</presentationTable>

</resources>

</policyDefinitionResources>

# Unattended installation of FIM 2010 R2 Self-Service Password Reset

## Unattended installation of FIM 2010 R2 Self-Service Password Reset

All components of the FIM 2010 R2 accept properties that allow unattended and silent installation. Those properties can either be set in a Windows Installer Transform (MST) file or specified at the command line during installation. The following section will provide information on how to do an unattended installation of the password reset and registration portals and the Add-ins and Extensions for clients.

The FIM 2010 R2 installation packages do not support advertisement (msiexec /j) or administrative (msiexec /a) installations.

There are several different ways to install FIM 2010 R2 SSPR silently (unattended). Two methods are described in this section: pass-in parameters in a command line and MST files. It is outside the scope of this document to describe unattended installations in general.

### Pass-in parameters on the command line

This can be used with Microsoft System Center Configuration Manager 2007. To install silently, use the command msiexec with an option, followed by properties, for example:

Msiexec /q /i NameofMSI.msi /Option ADDLOCAL=MSIFeatureName Property=Value /l\*v C:\mylogfile.txt

The possible values of MSIFeatureName and Property can be found in [SSPR Features and properties](#z32) later in this document. Note that all parameters are case sensitive. See the examples in [Reset and Registration Portal Example](#z33) and [Add-ins and Extensions Example](#z34)

Note

Windows Installer has a limit of 256 characters in the path when for installation of applications. Ensure that you do not place the root of the tree in a very deep structure, or the installation might fail.

### Create an MST file

Another solution is to use an MST file. MST files can be created with tools such as Orca (shipped with the Windows Software Development Kit (SDK)), and they contain the same settings as are passed in on the command line.

### Troubleshoot an installation

If an unattended installation fails, add the option /l\*v NameOfLogFile.txt to the command line. This option creates a log file that you can use for troubleshooting. You can identify an error in a Windows Installer log file by looking for the text Return Value 3.

### SSPR Features and properties

The tables in this section list the settings in the order that they appear during the user interface (UI) installation. Default values are in brackets. These only features and properties associated with Self-Service Password Reset and the Rich Client. For a full list of features and properties see the Forefront Identity Manager 2010 R2 Deployment Guide.

Table 1  Name of feature in Windows Installer file

The following table is listing the feature name in the UI and its feature name in the MSI. This can be used by the ADDLOCAL, REINSTALL, and REMOVE properties above.

|  |  |
| --- | --- |
| Name of the feature in the UI | Windows Installer feature name |
| FIM Password and Authentication Extensions | PasswordClient |
| FIM Password Registration Portal | RegistrationPortal |
| FIM Password Reset Portal | ResetPortal |

Table 2  SSPR properties

|  |  |
| --- | --- |
| Property name | Description |
| REGISTRATION\_ACCOUNT | Password Registration application pool account name in IIS. Must be in domain\username format. |
| REGISTRATION\_ACCOUNT\_PASSWORD | Password Registration application pool account password. |
| REGISTRATION\_HOSTNAME | HostName for the IIS site for password registration portal. |
| REGISTRATION\_PORT | Port number on which password registration portal IIS site is created. |
| REGISTRATION\_FIREWALL\_CONFIG | 1 – open port, 0 – do not open port |
| REGISTRATION\_SERVERNAME | This is the address the password registration portal will use to contact the FIM Service. |
| IS\_REGISTRATION\_EXTRANET {Extranet|None} | This value specifies if password registration site will be accessible by extranet users.  Extranet: can be accessed by extranet users  None: can be accessed only by internal users |
| RESET\_ACCOUNT | Password Reset application pool account name in IIS. Must be in domain\username format. |
| RESET\_ACCOUNT\_PASSWORD | Password Reset application pool account password |
| RESET\_HOSTNAME | HostName for the IIS site for password reset portal |
| RESET\_PORT | Port number on which password reset portal IIS site is created. |
| RESET\_FIREWALL\_CONFIG | 1 – open port, 0 – do not open port |
| RESET\_SERVERNAME | This is the address the password reset portal will use to contact the FIM Service. |
| IS\_RESET\_EXTRANET {Extranet|None} | This value specifies if password reset site will be accessible by extranet users.  Extranet: can be accessed by extranet users  None: can be accessed only by internal users |

Table 3  Add-ins and Extensions properties

|  |  |
| --- | --- |
| Property name | Description |
| RMS\_LOCATION | Address to the FIM Service. Used by Password Reset extensions |
| REGISTRATION\_PORTAL\_URL | The URL of the FIM 2010 R2 password registration portal that the rich client will navigate to by default. As part of the rich client password registration, the rich client will invoke the user's default browser to navigate to that URL if password registration be required. |

### Reset and Registration Portal Example

The following is an example of a command-line installation for the Password Reset and Registration Portal.

msiexec /q /i “D:\Service and Portal\Service and Portal.msi" ADDLOCAL=RegistrationPortal,ResetPortal REGISTRATION\_ACCOUNT=CORP\FIMPassword REGISTRATION\_ACCOUNT\_PASSWORD=Pass1word$ REGISTRATION\_HOSTNAME=passwordregistration.corp.contoso.com REGISTRATION\_PORT=80 REGISTRATION\_FIREWALL\_CONFIG=1 REGISTRATION\_SERVERNAME=FIM1 IS\_REGISTRATION\_EXTRANET=Extranet RESET\_ACCOUNT=CORP\FIMPassword RESET\_ACCOUNT\_PASSWORD=Pass1word$ RESET\_HOSTNAME=passwordreset.corp.contoso.com RESET\_PORT=81 RESET\_FIREWALL\_CONF=1 RESET\_SERVERNAME=FIM1 IS\_RESET\_EXTRANET=Extranet /L\*v C:\mylogfile.txt

### Add-ins and Extensions Example

The following is an example of a command-line installation for the Add-ins and Extensions.

msiexec /q /i “D:\Add-ins and extensions\x64\ Add-ins and extensions.msi" ADDLOCAL=PasswordClient RMS\_LOCATION=FIM1 REGISTRATION\_PORTAL\_URL=https://passwordregistration.corp.contoso.com /L\*v C:\mylogfile.txt

# Using the QuickStart Tool

## Using the QuickStart Tool

The QuickStart tool is new for FIM 2010 R2 and will allow you to quickly setup Self-Service Password Reset pre-requisites. Namely this cmdlet will do the following programmatically:

 Creates the FIM Management Agent

 Creates an Active Directory Management Agent

 Synchronizes an Active Directory OU that contains users into FIM.

Once these takes are complete, the Active Directory users that were in the OU specified, are able to use the Registration and Reset portals for SSPR.

### Before you begin

The following pre-requisites are required before using the QuickStart cmdlet.

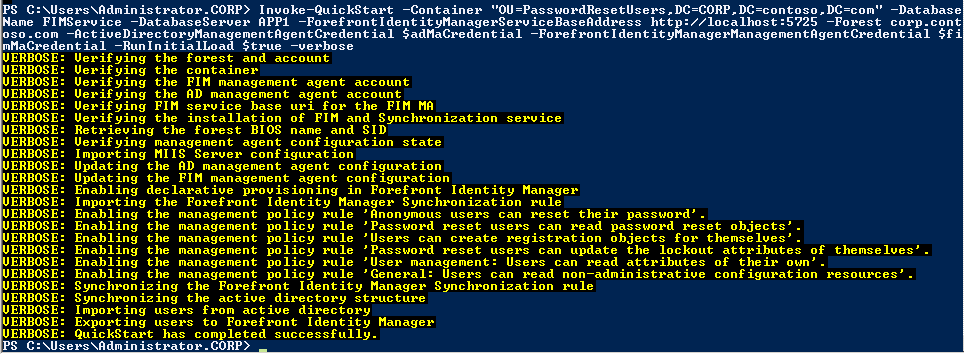
 PowerShell 2.0 must be installed on the server running the Synchronization Service.

 The “ActiveDirectoryManagementAgentCredential” account has DirSync permission on the domain that is specified.

 QuickStart package is installed by the Synchronization Service setup and can only be run where the Synchronization Service is installed.

 If the cmdlet is invoked with the “-verbose” parameter the status messages that is shown at the top of the command window in green will also be sent to the command line. This is useful if you are attempting to automate the process. With the status message on the command line you will be able to see which steps the cmdlet completed and which ones that may have failed.

Verbose output



### Setting up the QuickStart Package

Use the following steps to setup the QuickStart Package:

1. The QuickStart package will be located in \Program Files\Microsoft Identity Manager\2010\Synchronization Service\Tools\QuickStartPackage.zip. This zipped package must be extracted to PowerShell modules path. By default this is C:\Windows\System32\WindowsPowerShell\v1.0\Modules.

Tip

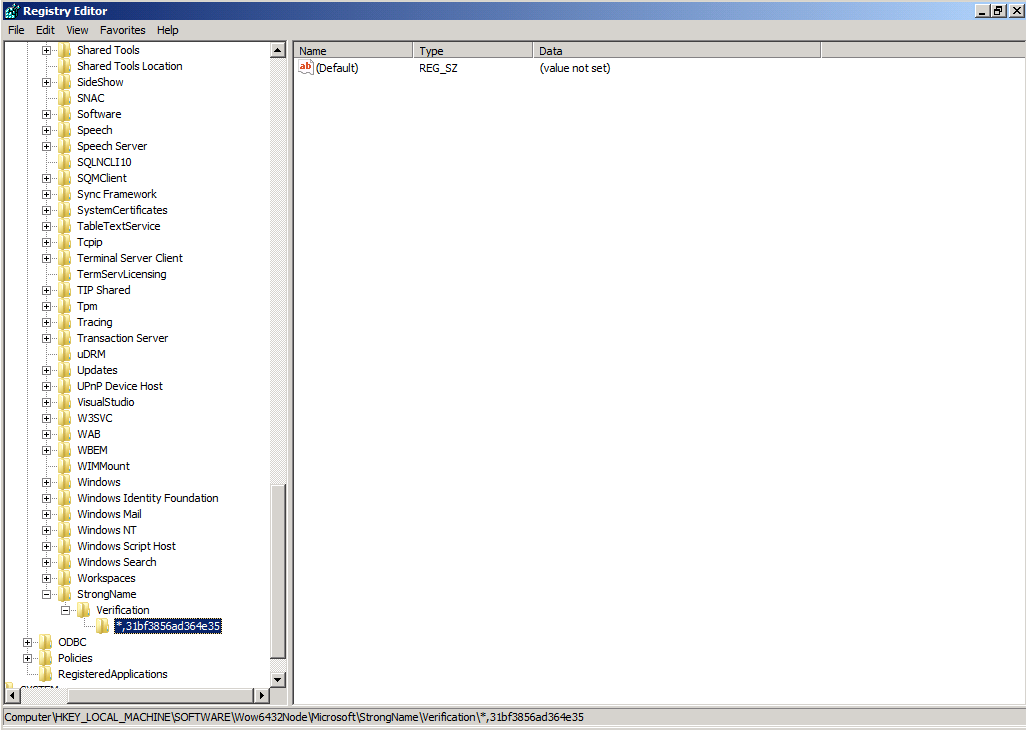
You can type the following in PowerShell to get the path: $env:PSModulePath

2. Once the package is extracted, open a Powershell Command prompt and enter: Import-Module QuickStart

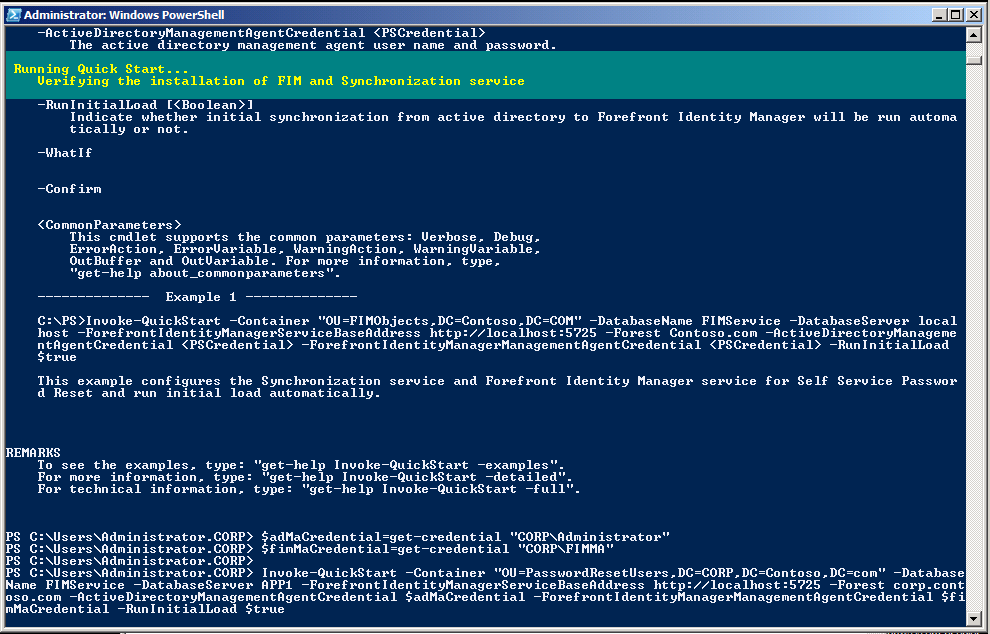
Warning

This may fail with a strong name validation error. If so, you can add the following registry keys to bypass it. [HKEY\_LOCAL\_MACHINE\Software\Microsoft\StrongName\Verification\\*,31bf3856ad364e35] and [HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\StrongName\Verification\\*,31bf3856ad364e35]

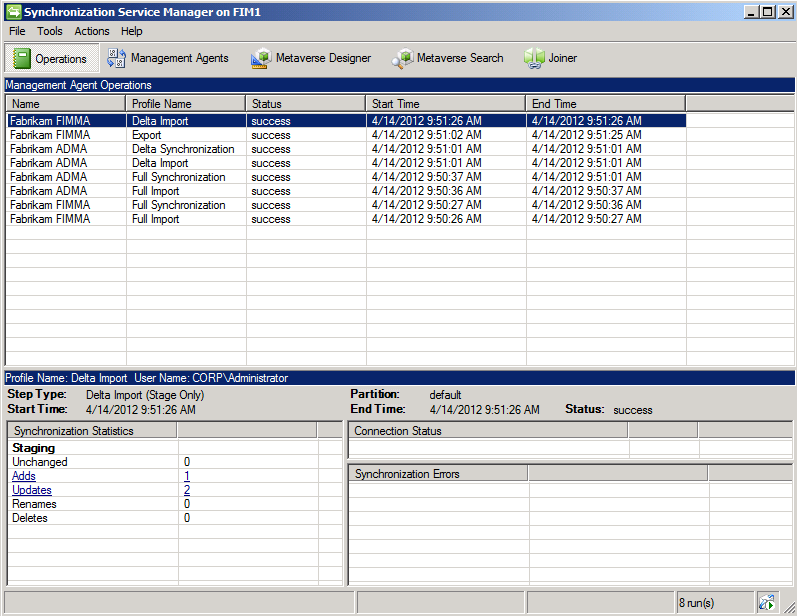
Registry Key



Once the module has been imported, the QuickStart tool is ready to use. When you use the Invoke-QuickStart cmdlet you will see the following while it runs.



Once it has completed, you can open the Synchronization Service and see that it has successfully run the management agents. They will be named Fabrikam ADMA and Fabrikam FIMMA by default. Likewise, if you check the FIM Portal you will see your users populated.



For a complete example and the Syntax see the [Invoke-QuickStart](#z148209835aa24d9e8e86db21a6d18e92) section of this guide.

# Invoke-QuickStart

Begins the QuickStart process.

## Syntax

Invoke-QuickStart –Container <String> -DatabaseName <String> -DatabaseServer <String> -ForefrontIdentityManagerServiceBaseAddress <String> -Forest <String> -ActiveDirectoryManagementAgentCredential <PSCredential> -ForefrontIdentityManagerManagementAgentCredential <PSCredential> [-RunInitialLoad [<Boolean>]] [-WhatIf] [-Confirm] [<CommonParameters>]

## Detailed Description

Begins the QuickStart process.

## Parameters

### -Container <String>

The organizational unit where users will be synchronized from Active Directory to Forefront Identity Manager 2010 R2.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -DatabaseName <String>

The Forefront Identity Manager 2010 R2 service database name.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -DatabaseServer <String>

The Forefront Identity Manager 2010 R2 Service database server.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -ForefrontIdentityManagerServiceBaseAddress <String>

The Forefront Identity Manager 2010 R2 service base URI.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -Forest <String>

The DNS name of the root domain of the forest that you want to connect to.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -ActiveDirectoryManagementAgentCredential <PSCredential>

The Active Directory management agent user name and password.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -ForefrontIdentityManagerManagementAgentCredential <PSCredential>

The Forefront Identity Manager 2010 R2 management agent user name and password.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -RunInitialLoad [<Boolean>]

Indicate whether initial synchronization from active directory to Forefront Identity Manager 2010 R2 will be run automatically or not.

|  |  |
| --- | --- |
| Required? | false |
| Position? | named |
| Default Value | Three possible values:  ****** $true – Runs the initial load (synchronization) at the end. Example: -RunInitialLoad:$true  ****** $false – The initial load run is skipped. Example: -RunInitialLoad:$false  ****** No value specified - The cmdlet will detect if there are any users in the specified ou. If there are user(s) then the cmdlet prompts to run the initial load. |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### <CommonParameters>

This cmdlet supports the common parameters: -Verbose, -Debug, -ErrorAction, -ErrorVariable, -OutBuffer, and -OutVariable. For more information, see [about\_CommonParameters](http://technet.microsoft.com/en-us/library/dd315352.aspx).

## Notes

## Example 1

This example configures the Synchronization service and Forefront Identity Manager 2010 R2 servcie for Self-Service Password Reset and runs the intial load automatically.

$adMaCredential = get-credential "CORP\Administrator"

$fimMaCredential = get-credential "CORP\FIMMA"

Invoke-QuickStart -ActiveDirectoryManagementAgentCredential $adMaCredential -ForefrontIdentityManagerManagementAgentCredential $fimMaCredential -Forest corp.contoso.com -DatabaseName FIMService -DatabaseServer APP1 -Container "OU=PasswordResetUsers,DC=CORP,DC=contoso,DC=COM" -ForefrontIdentityManagerServiceBaseAddress "http://localhost:5725" -RunInitialLoad:$true

.

# Testing the Deployment

The following section will provide you with steps on how to test your deployment once it is complete.

## Test the Deployment

After configuring the management agent for AD DS and then defining a password reset workflow, you will test your configuration. To test the configuration, you must perform the following steps in the order shown:

1. [Register for a self-service password reset](#z35)

2. [Reset the password](#z36)

### Register for a self-service password reset

After a user logs on to a client computer, the user must register for a self-service password reset. This enables that user to reset the password without contacting the helpdesk.

#### Register from a client computer

In this procedure, you will register for a self-service password reset from a client computer.

To register for a self-service password reset

|  |
| --- |
| 1. Log on to a client computer with a user account that resides in the set that you created to participate in password reset.  2. On the FIM Password Reset Registration page, click Next.  3. Answer the questions that you specified when you created the process for a self-service password reset, click Next, and then click OK. |

#### Register in the password registration portal

In this procedure, you will register for a self-service password reset using the password registration portal.

To register for self-service password reset in the password registration portal

|  |
| --- |
| 1. Log on to a client computer with a user account that resides in the set that you created to participate in password reset.  2. Open Internet Explorer, and then navigate to the FIM Password Registration Portal home page (http://<portal host name>/)  3. Click Next, and complete the registration wizard. |

Warning

Registration for password reset using the rich client has changed to launch the default browser and automatically navigate the user to the registration portal when they log on to a client machine.

### Reset the password

Now you can reset the user's password. After you have reset the password, the user can log on to the client computer and the AD DS domain with the new credentials.

#### Reset the password from a client computer

In this procedure, you will reset the user’s password from the logon screen on the client computer. This requires the rich client to be installed on the client machine.

To reset the password at the logon screen

|  |
| --- |
| 1. Log off the client computer.  2. On the Log On to Windows screen using one of the users that previously registered, and click Reset.  In the Windows Vista and Windows 7 operating system, the Reset Password command link is located under the box where you enter your password.  3. On the Authentication Required page, type the same answers to the questions that you entered when you registered for a self-service password reset, and then click Next.  4. On the Enter Your New Password page, type your new password in the New password and Confirm new password boxes, and then click Reset.  5. Click Finish.  6. In the Windows logon screen, log on using the new password. |

#### Reset the password in the password reset portal

In this procedure, you will reset the user’s password in the password reset portal.

To reset the password in the password reset portal

|  |
| --- |
| 1. Open Internet Explorer, and then navigate to the FIM Password Reset Portal home page (http://<portal host name>/).  2. Enter the username of one of the users that previously registered, and then complete the password reset wizard. |

# Maintaining Forefront Identity Manager 2010 R2 - Self-Service Password Reset

## Maintaining Forefront Identity Manager 2010 R2 - Self-Service Password Reset

This section provides technical information that is important for maintaining your installation of Forefront Identity Manager 2010 R2 – Self-Service Password Reset. This information will allow you to change and configure your deployment.

The following topic areas are covered in this section:

 [FIM 2010 R2 Password Registration Portal](#zdd5e9df8c70d45d781e3b4bc57738ba4)

 [FIM 2010 R2 Password Reset Portal](#z33be589601f4453ea9dfe08cca51725e)

 [FIM 2010 R2 Rich Client](#z6f114bfe1da744668dd407a92def4d52)

 [Registration and Reset Portal Web.config settings](#z96805728a47e488a8ca3360f47ed7d98)

 [FIM 2010 R2 Portal Customization](#zdade98571a20433b9c1f235685be39b0)

 [Programmatic User Registration](#z7a7cb73e2b82439abd8a7ef6b86a1ebb)

 [Kerberos and Self-Service Password Reset](#z8fccc10285d742f9a29665f171f5a0f1)

 [SSPR Authentication Gates](#z5f47959d227e4adb91bf1ef442b5a87f)

 [SSPR Troubleshooting](#z68b7a195387a42d7b661e4202a67d1db)

# FIM 2010 R2 Password Registration Portal

## FIM 2010 R2 Password Registration Portal

The FIM 2010 R2 Password Registration Portal page is the starting point for users to begin enrolling in self-service password reset. It consists of two logical pages which are specific to the reset experience:

 Home Page

 Completion Page

Additionally, depending on the Authentication Workflow and type of Authentication Gates that are specified in that workflow, you may see pages for any of the following:

 Password Gate

 QA Gate

 One-Time Password Email Gate

 One-Time Password SMS Gate

By default, the Password Reset AuthN Workflow has a Password Gate and a QA Gate. It also has a Lockout Gate but this gate does not have a user interface that is part of the registration experience. For additional information on Gates see the SSPR Authentication Gates section of this document.

### Home Page

The Password Registration home page provides a user interface that welcomes the end user, provides information that lets the user understand they’ve navigated to the place where they intended to begin the registration process, and initiate that process.

The only interactive element is the Next button. When clicked, the Next button initiates a request to the FIM Portal. That request is to register the user for any password registration workflows for which the user is eligible.

FIM 2010 R2 Password Registration Portal



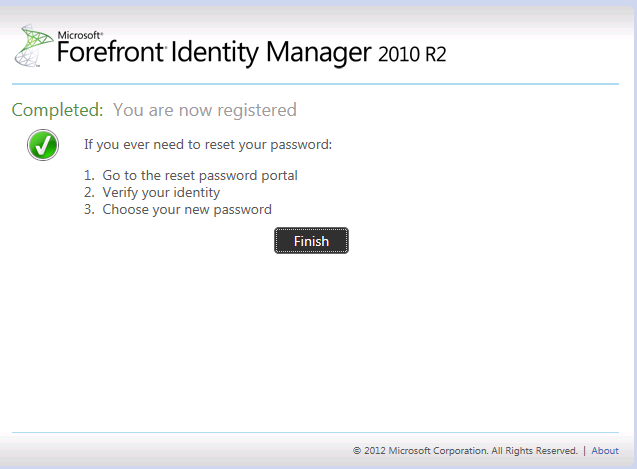
If the user is not eligible for any password registration workflows, the user is redirected to the error page.

If the user is eligible for one workflow, the registration portal will load the user interface corresponding to the first interactive gate in the workflow. If a user is eligible for multiple password workflows, the GUIDs for each workflow is submitted. The execution of each workflow is handled by the Security Token Service (STS) on the FIM Service. The Registration Portal will then handle the messages from the STS and present the appropriate gate to the user.

### Completion Page

The Password Registration completion page provides a user interface that informs the user that they’ve successfully completed the registration process.

There is one primary element of user interaction on the Success page a Finish button. Clicking the Finish button will re-direct the user to a custom Session Ended page. By default this button is not visible and will only appear if there is a value configured for FinishUrl in the registration/reset portal web.config file. If there is a value, a user will be re-directed to the custom page specified.



### FIM 2010 R2 Registration Portal Communication with the FIM Service

The Registration Portal communicates with the FIM Service using the FIM Service’s normal web services endpoint, via the WS-T protocol which is recognized by the FIM Service. The Registration Portal takes advantage of certain facilities which were added to the FIM Service to enable password registration from an internet user with a browser.

The Registration Portal makes requests to the FIM Service using the AD identity which was specified during the setup process for the registration portal. This identity is well-known to the FIM Service. The FIM Service recognizes request which originate from this identity, evaluates the “real” requestor based upon data in the message header described below, and changes the request to be from the “real” (human) requestor before it enters the request pipeline. This behavior enables the FIM Registration Portal to communicate with the FIM Service, even if the end user doesn’t have a Kerberos token.

When the FIM Registration Portal makes a request to the FIM Service, it includes a message header to identify the actual Windows user who is being served by the Registration Portal. This enables the FIM Service to evaluate and apply policy to the request, and to update the request. This allows an auditor the ability to see the request as originating from the user, rather than the identity of the registration portal.

<UserIdentitierProperty

xmlns="http://schemas.microsoft.com/2006/11/ResourceManagement">

{USERS-REAL-SID-HERE}

</UserIdentifierProperty>

When the FIM Registration Portal is configured during Setup as being on a host which is accessible to extranet users, it includes an additional message header when it submits requests to the FIM Service:

<SecurityContextAssertionProperty

xmlns="http://schemas.microsoft.com/2006/11/ResourceManagement">

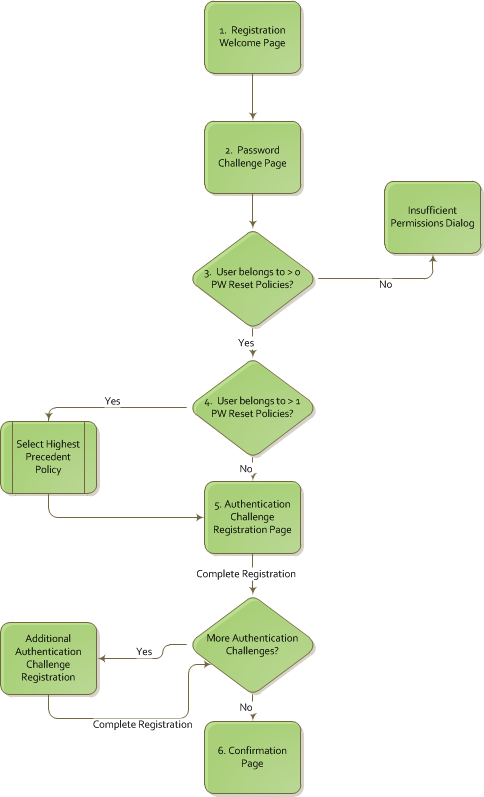
Extranet

</SecurityContextAssertionProperty>

This property is stamped on requests and enables auditors to determine requests that from an extranet-facing portal.

### FIM 2010 R2 SSPR Registration Portal Flow

The following flow chart shows the registration process.



# FIM 2010 R2 Password Reset Portal

## FIM 2010 R2 Password Reset Portal

The FIM 2010 R2 Password Reset Portal page is the starting point for users to begin resetting their password. It consists of three logical pages which are specific to the reset experience:

 Home Page

 Choose New Password Page

 Success Page

Additionally, depending on the Authentication Workflow and type of Authentication Gates that are specified in that workflow, you may see pages for any of the following:

 Password Gate

 QA Gate

 One-Time Password Email Gate

 One-Time Password SMS Gate

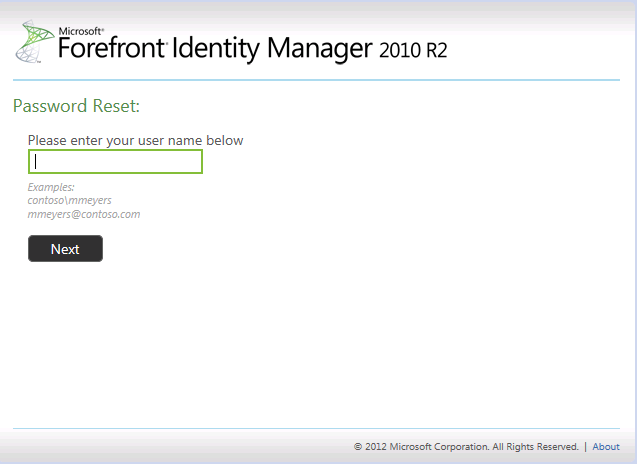
By default, the Password Reset AuthN Workflow has a Password Gate and a QA Gate. It also has a Lockout Gate but this gate does not have a user interface that is part of the reset experience. For additional information on Gates see the SSPR Authentication Gates section of this document.

### Home Page

The Password Reset home page provides a user interface for an end user to initiate the password reset process via a web browser.

The password reset home page has two primary interactive elements: a text box, and a next button. It also has all of the user interaction elements that are common across the Portals: help link, About link, Privacy Policy link.

FIM 2010 R2 Password Reset Portal



The text box takes input that specifies the user’s username and shows it unmasked. It supports pasting from the clipboard. Valid username formats are:

 Domain\account

 UPN

 Username (Provided DefaultDomainName has been specified in the web.config file)

When the user clicks the next button, the Portal verifies the user name is present and in a valid format, and then initiates a request to the FIM Service to reset the password for the user. In a default configuration of FIM, such a request would trigger the MPR which enables anonymous users to reset their password. This is the “Anonymous users can reset their password” MPR. This MPR has references to the authentication workflow Password Reset AuthN Workflow. As mentioned above this workflow has a default Password Gate, Lockout Gate, and a QA Gate. The Portal will then interact with the first interactive authentication gate and render the user experience specified for that gate. By default, this will be the Password Gate.

If the user name is in an invalid format, the portal displays the following error message:

 Invalid format. Enter your user name in a valid format.

Validation is performed on the Reset Portal based on Active Directory naming standards. The format of the username is configurable by a regex in the web.config file. Using ValidResetUsernameRegex in the web.config file you can specifiy the format that the password reset portal will accept.

### Choose New Password Page

The New Password page provides a user interface for an end user to choose a new Active Directory password.

There are three primary elements of user interaction on the New Password page: two text boxes for the user to enter the new password, and a Next button.

The text boxes take user input, including input pasted from the clipboard. It renders the user input as masked characters.

When the user clicks the Next button, the Portal verifies that both the new password and the re-entered password match one another. If they don’t match, including if one or the other fields is blank, the Portal displays an inline error.

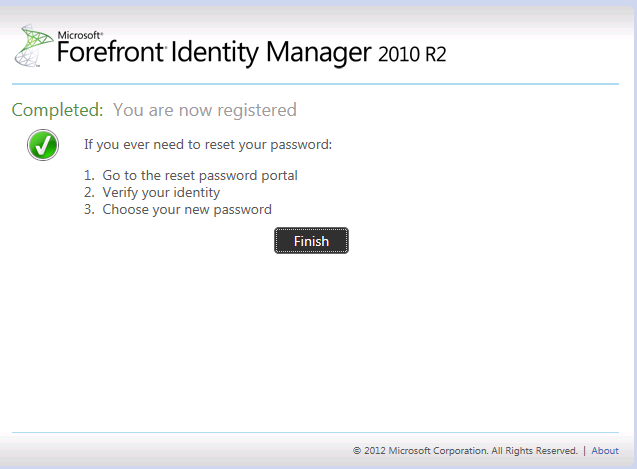
 Ensure both passwords match.

If both passwords match, then the Portal submits the user’s requested password to the Change Password activity which is running in an action workflow. If the request succeeds, then the user will be redirected to the Success page. If the request fails, then the portal will display an error message and allow the user to request some other password. The error message is contextual, for example “Requested password doesn’t comply with the password policy of your organization.”

### Success Page

The Success page provides a user interface that informs the user that they’ve successfully changed their password.

There is one primary element of user interaction on the Success page a Finish button. Clicking the Finish button will re-direct the user to a Session Ended page. By default this button is not visible and will only appear if there is a value configured for FinishUrl in the registration/reset portal web.config file. If there is a value, a user will be re-directed to the custom page specified.



### FIM 2010 R2 Reset Portal Communication with the FIM Service

The Reset Portal communicates with the FIM Service using the FIM Service’s normal web services endpoint, via the WS-T protocol which is recognized by the FIM Service. The Reset Portal takes advantage of certain facilities which were added to the FIM Service to enable password registration from an internet user with a browser.

The Reset Portal makes requests to the FIM Service using the AD identity which was specified during the setup process for the reset portal. This identity is well-known to the FIM Service. The FIM Service recognizes requests which originate from this identity and changes the requestor to be “Anonymous User”. This is the identity that the FIM Service uses for a user who has not authenticated to Windows and is making a request to the FIM Service. This behavior enables the FIM Reset Portal to communicate with the FIM Service, even though the end user doesn’t have a Kerberos token.

When the FIM Reset Portal is configured during Setup as being on a host which is accessible to extranet users, it includes an additional message header when it submits requests to the FIM Service. This property is stamped on requests and enables password reset to evaluate whether they should execute a particular gate for a particular request. If the SecurityContextAssertionProperty is marked with Extranet then, those gates that have been configured for only extranet requests will be run. This allows for additional Authentication gates to be added to extranet requests, while keeping requests from the intranet simpler. Also, it enables auditors to determine requests that came in from an extranet-facing portal.

<SecurityContextAssertionProperty

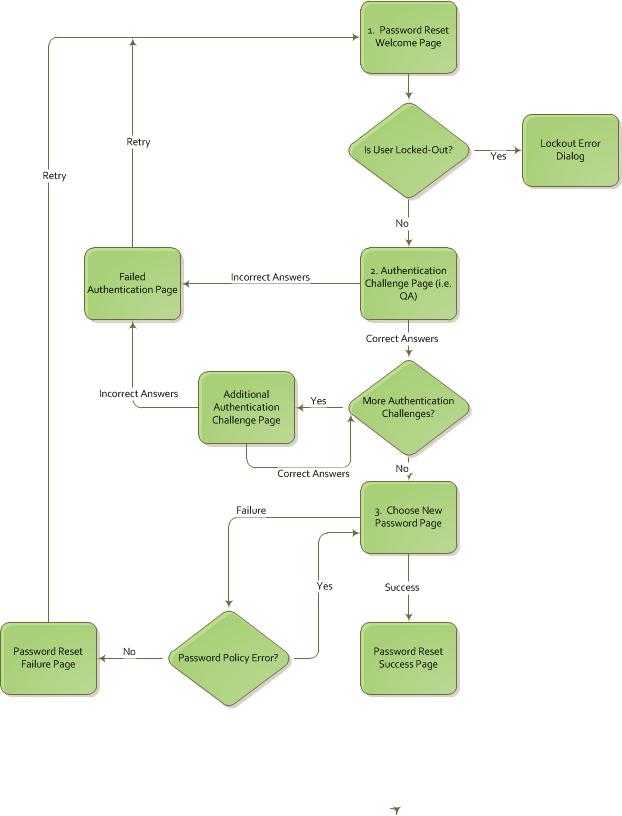
xmlns="http://schemas.microsoft.com/2006/11/ResourceManagement">

Extranet

</SecurityContextAssertionProperty>

### FIM 2010 R2 SSPR Reset Portal Flow

The following flow chart shows the reset process.



# FIM 2010 R2 Rich Client

## FIM 2010 R2 Rich Client

Forefront Identity Manager 2010 R2 includes a rich client that can be used for password registration, password reset and the FIM Add-in for Outlook.

One thing that is new for FIM 2010 R2 is that the rich client no longer allows interactive registration. Rather, it uses the default web browser and re-directs that user to the Password Registration Portal.

When the FIM client determines that the user is to be prompted for password registration the client:

1. Opens the user’s default browser, which may or may not be Internet Explorer, in its default size and position.

2. Passes a URL to the browser based upon a key in the client’s registry: RegistrationPortalURL.

3. If a value is present for RegistrationPortalURL in the policy node (HKCU\Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions\RegistrationPortal), then this takes highest precedence.

4. If no value is present in the policy node, then the value is read from the registry location which is written at setup time: HKLM\Software\Microsoft\Forefront Identity Manager\2010\Extensions\RegistrationPortal.

The FIM 2010 R2 client is not required to participate in Self-Service Password Reset. With FIM 2010 R2 SSPR everything can be done from a browser. However, the client does offer one benefit over the browser in that it allows users to reset their password from a domain-joined machine from the logon screen. So for example, if a user goes on vacation and then returns to work but cannot remember their password, they can still reset it from their workstation or laptop.

Several settings for the rich client can be configured via Group Policy. The following sections include information on Registry settings that pertain to self-service password rest that can be configured via Group Policy.

### How often registration is checked

By default, the FIM client checks the end user’s registration status every time he or she logs on to Windows. The frequency setting for how often registration is checked is located in the registry. If you are deploying password reset broadly in your organization, we recommend that you configure FIM 2010 to check periodically, not every time that the user logs on to Windows.

There are two potential locations for the registry key:

1. HKCU\Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions

2. HKCU\Software\Microsoft\Forefront Identity Manager\2010\Extensions

The location under Policies takes precedence. However, the second key, in the second listing above, must be created. It can be an empty key.

The settings are as indicated in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Data description | Registry location |
| CacheInterval | Int | Registration status cache duration in days | HKCU\Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions  HKCU\Software\Microsoft\Forefront Identity Manager\2010\Extensions |
| MaxOffset | Int | Maximum random offset in days to be added or subtracted to cache interval | HKCU\Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions  HKCU\Software\Microsoft\Forefront Identity Manager\2010\Extensions |

CacheInterval specifies the amount of time in days before the FIM client checks the user’s registration status again. MaxOffset adds or subtracts a random number of days to CacheInterval. The offset exists so that all FIM clients are not checking registration status on the same day. We recommend that you create these settings in the Policies folder.

### The Registration Portal URL

To specify the URL for the Password Registration Portal you can set the following registry key on the clients

 HKCU\Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions\RegistrationPortal

The settings are as indicated in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Data description | Registry location |
| RegistrationPortalURL | REG\_SZ | URL of the password registration portal | HKCU\Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions\RegistrationPortal |

RegistrationPortalURL - With this policy setting, you can configure the registration portal URL which the default browser will navigate to during password reset registration. If you do not configure this policy setting, the registration portal URL specified during setup will be used. This is located at HKLM\Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions\RegistrationPortal.

### The FIM Service Address

To specify the URL of the FIM Service used by password reset, you can set the following registry key on the clients

 HKCU\Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions\Intranet

The settings are as indicated in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Data description | Registry location |
| Address | REG\_SZ | URL of the FIM Service used by password reset. | HKCU\Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions\Intranet |

Address - With this policy setting, you can specify the address to the FIM Service used by password reset. The format is: http://serveraddress:5725. If you do not configure this policy setting, the address specified during setup will be used. This is located at HKLM\Software\Policies\Microsoft\Forefront Identity Manager\2010\Extensions\Intranet.

# Registration and Reset Portal Web.config settings

## Registration and Reset Portal Web.config settings

The following is a list of the web.config settings that can be configured on the Password Registration and Reset Portals.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Setting | Values | Relevance | Configuration element belongs to the following web.config section: | Description |
| SecurityContextAssertion | Contains one of the following:  **** Extranet  **** NotSpecified | The following setting is relevant to:  **** Registration Portal  **** Reset Portal | <settings> | SOAP property that identifies whether the portal is deployed on the extranet or not.  Example: <add key=”SecurityContextAssertion” value=”Extranet” /> |
| SessionTimeoutInMinutes | Numerical value | The following setting is relevant to:  **** Registration Portal  **** Reset Portal | <settings> | The number of minutes until the session will timeout from inactivity.  Example: <add key=”SessionTimeoutInMinutes” value=”20” /> |
| ShowTroubleshootingInfoOnErrorPage | Contains one of the following:  **** true  **** False | The following setting is relevant to:  **** Registration Portal  **** Reset Portal | <settings> | When this value is set to true then the following user intefaces are shown on the error page:  1. A Stack Trace  2. Copy to Clipboard  3. Send information by Email  Send information by Email will only be available if TroubleshootingEmailRecipient has a value assigned to it.  Example: <add key=” ShowTroubleshootingInfoOnErrorPage” value=”true” /> |
| TroubleshootingEmailRecipient | A Valid Email Address | The following setting is relevant to:  **** Registration Portal  **** Reset Portal | <settings> | Used with the Send information by Email link on an error page. This is the recipient of the email.  Example: <add key=” TroubleshootingEmailRecipient” value=”Administrator@corp.contoso.com” /> |
| TroubleshootingEmailSubject | A specific subject to denote a Troubleshooting email | The following setting is relevant to:  **** Registration Portal  **** Reset Portal | <settings> | Used with the Send information by Email link on an error page. This is the subject of the email.  Example: <add key="TroubleshootingEmailSubject" value="There was an error with the Web Portal"/> |
| PrivacyPolicyLink | A valid URL | The following setting is relevant to:  **** Registration Portal  **** Reset Portal | <customizationSettings> | The URL that the Privacy Statement link points to on the About page.  Example: <add key="PrivacyPolicyLink" value="http://go.microsoft.com/fwlink/?LinkId=233314"/> |
| HomepageLink | A valid URL | The following setting is relevant to:  **** Registration Portal  **** Reset Portal | <customizationSettings> | Used on the error page to provide a link to the home page of either the registration or reset portal. It is used to restart the process.  Example: <add key=" HomepageLink" value="https://passwordregistration.corp.contoso.com"/> |
| PasswordResetLink | A valid URL | The following setting is relevant to:  **** Registration Portal | <customizationSettings> | If this value is specified, the user will be provided with a hyperlink to the password reset portal on the password registration success page.  Example: <add key=" PasswordResetLink " value="https://passwordreset.corp.contoso.com"/> |
| DisplayUsernameInUPNFormat | Contains one of the following:  **** true  **** False | The following setting is relevant to:  **** Registration Portal | <customizationSettings> | It value can be used to ensure that during registration, the user only sees the UPN format.  Example: <add key=”DisplayUsernameInUPNFormat value=”true” /> |
| FinishURL | A valid URL | The following setting is relevant to:  **** Registration Portal  **** Reset Portal | <customizationSettings> | If this value is specified, the user will be provided with a Finish button once registration or reset has been completed. By clicking this Finish button, the user will be redirected to the URL provided.  If this value is not specified and clicking on the Finish button will take you to the “Session Ended” portal page.  Example: <add key=" FinishURL " value="https://passwordregistration.corp.contoso.com"/> |
| ValidResetUsernameRegex | A Regular expression. | The following setting is relevant to:  **** Reset Portal | <customizationSettings> | A Regular expression of acceptable characters for a username entered into the Reset portal.  Example: <add key="ValidResetUsernameRegex" value="^[^@\\]+((@|\\)[^@\\]+)?$" /> |
| DefaultDomainName | A valid domain. | The following setting is relevant to:  **** Reset Portal | <customizationSettings> | This value is the default domain that will be used for fallback if a user enters a username without a domain in the reset portal.  Example: <add key=” DefaultDomainName” value=”CONTOSO” /> |
| CancelURL | A valid URL | The following setting is relevant to:  **** Registration Portal  **** Reset Portal | <customizationSettings> | If this value is specified, the user will be redirected to the URL by clicking the Cancel button.  If this value is not specified and clicking on the Cancel button will take you to the “Session Ended” portal page.  Example: <add key=" CancelURL " value="https://passwordregistration.corp.contoso.com"/> |

# FIM 2010 R2 Portal Customization

## FIM 2010 R2 Portal Customization

Warning

Be sure to clear the browser cache when any CSS customizations are made.

In FIM 2010 R2 , you can customize selected elements of the password portals, including the banner logo, string resources, and cascading style sheets.

In order to do this, a few things are required depending on the level of customization. The following is a list of items that are involved in customizing the FIM 2010 R2 password registration and reset portals.

 Customizations Folder - This is the folder that FIM 2010 R2 will check prior to using the defaults. Each portal that will be customized requires a Customizations folder. Customizations should only be done in this folder because setup will not overwrite it on upgrades, change mode installs or repair mode installs.

 Strings.resources - This is an XML-based file that allows you to modify the strings that appear in the portal. This file needs to reside in the Customizations folder.

 Style.css – This is the cascading style sheet used by the portals for customization. This style sheet needs to be created and modified to change the logo or can be entirely replaced with your own customizations.

For detailed step-by-step instructions on customizing the password registration and password reset portals see [Test Lab Guide: Demonstrating FIM 2010 R2 Password Registration and Reset Portal Customization](http://technet.microsoft.com/en-us/library/hh877809(v=ws.10).aspx).

Warning

In order for FIM to recognize any customized changes, you must restart IIS by running iisreset.

### Creating the Customizations folder

On startup, FIM will look for the Strings.resources file in the Customizations folder before using the defaults. You must create a Customizations folder under the directory for the portal you wish to customize (i.e. Password Registration Portal or Password Reset Portal). If you want to customize both portals then you will need to create a Customizations folder under each of the following:

 C:\Program Files\Microsoft Forefront Identity Manager\2010\Password Registration Portal

 C:\Program Files\Microsoft Forefront Identity Manager\2010\Password Reset Portal

To create the customization folder

|  |
| --- |
| 1. Navigate to the C:\Program Files\Microsoft Forefront Identity Manager\2010\Password Registration Portal folder.  2. Create a folder named Customizations.  3. Navigate back one level to the Password Reset Portal folder, and create a folder named Customizations. |

### Customizing strings

Many of the strings in the portal UI can be customized by creating a Strings.resources file and adding this file to the Customizations folder. You will need to create a Strings.resources file for each portal that you wish to customize.

To customize strings

|  |
| --- |
| 1. Using notepad, copy the following code below into it and save it to the Customizations folder as Strings.resources  <?xml version="1.0" encoding="utf-8"?>  <root>    <resheader name="resmimetype">      <value>text/microsoft-resx</value>    </resheader>    <resheader name="version">      <value>2.0</value>    </resheader>    <resheader name="reader">      <value>System.Resources.ResXResourceReader, System.Windows.Forms, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089</value>   </resheader>    <resheader name="writer">      <value>System.Resources.ResXResourceWriter, System.Windows.Forms, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089</value>    </resheader>   <!-- Customizations begin here -->    <data name=" QAGateResetTitle " xml:space="preserve">      <value>Contoso Question and Answer Reset</value>    </data>    <data name="ResetPageTitle" xml:space="preserve">      <value>Contoso Self-Service Password Reset</value>    </data>  </root>  2. Under the <!-- Customizations begin here --> section change the data name to match the strings that you wish to customize and enter the value for that string between the <value></value> tags. See the list below for the strings that can be customized and their default values. |

Note

The Strings.resources file is language neutral. To create language specific customized strings, you must have that language pack installed, and save the file in the format Strings.<language>-<culture>.resources, for example Strings.en-us.resources.

The following is a list of portal strings that can be customized.

Portal Strings

|  |  |  |
| --- | --- | --- |
| Name | Default Value | Comment |
| AboutLinkText | About |  |
| ButtonCancel | Cancel |  |
| ButtonFinish | Finish |  |
| ButtonNext | Next |  |
| ButtonOk | OK |  |
| CancelFinishedMessage | Your session is no longer active. You can close the window, or you can restart by clicking the link below. |  |
| CancelFinishedTitle | Session Ended |  |
| ErrorDescription\_3000 | An error has occurred. Please try again, and if the problem persists, contact your help desk or system administrator. (Error 3000) |  |
| ErrorDescription\_3001 | Ensure you enter your user name correctly.If you still cannot reset your password, please contact your helpdesk for assistance. (Error 3001) |  |
| ErrorDescription\_3002 | Your session has ended. Return to the home page to start again. (Error 3002) |  |
| ErrorDescription\_3003 | The current user account is not recognized by Forefront Identity Manager.Please contact your help desk or system administrator. (Error 3003) |  |
| ErrorDescription\_3004 | You are not authorized to register for password reset.Please contact your help desk or system administrator. (Error 3004) |  |
| ErrorDescription\_3005 | One or more answers that you provided do not match the answers which you provided during Password Registration.In order to reset your password, the answers that you provide now must match the answers that you provided when you registered.You can start again from the home page, or contact your help desk or system administrator. (Error 3005) |  |
| ErrorDescription\_3006 | The password that you entered is incorrect.You must enter the correct password in order to register for Password Reset. (Error 3006) |  |
| ErrorDescription\_3007 | You are temporarily prohibited from resetting your password.Please try again later, or contact your help desk or system administrator for assistance. (Error 3007) |  |
| ErrorDescription\_3008 | An error has occurred. Please try again, and if the problem persists, contact your help desk or system administrator. (Error 3008) |  |
| ErrorDescription\_3009 | Your input contains text in a format that is not allowed. Try again with different input, or contact your help desk or system administrator. (Error 3009) |  |
| ErrorDescription\_3010\_Registration | Scripting is not enabled on your browser. Enable scripting and return to the Password Registration home page, or contact your help desk for assistance. |  |
| ErrorDescription\_3010\_Reset | Scripting is not enabled on your browser. Enable scripting and return to the Password Reset home page, or contact your help desk for assistance. |  |
| ErrorDescription\_3011 | This site uses cookies. Configure your browser to accept cookies and try again, or contact your help desk for assistance. |  |
| ErrorDescription\_3012 | The data you entered did not match the security code that was sent to you. You can try to reset your password again, or contact your help desk for assistance. |  |
| ErrorDescription\_3013 | Unable to send a security code. Please contact your help desk for assistance. |  |
| ErrorMessageDomainUsernameFormat | Enter your user name in the correct format. |  |
| ErrorMessageDomainUsernameRequired | Enter a user name to continue. |  |
| ErrorMessagePasswordRequired | Enter a password. |  |
| ErrorMessagePasswordsDoNotMatch | Ensure both passwords match. |  |
| ErrorPageDefaultHeading | Application Error |  |
| ErrorPageServerTime | Server time: {0:T} | {0} is the time at which the exception was caught. The 'T' causes the passed-in time to be formatted as a "long time." It will end up showing the hour, minute, and second, and possibly the AM/PM designation (depending on the current culture). |
| ErrorPageTitle | Forefront Identity Management - Password Error |  |
| ErrorTitle\_3000 | Error |  |
| ErrorTitle\_3001 | Access Denied |  |
| ErrorTitle\_3002 | Session Ended |  |
| ErrorTitle\_3003 | Unrecognized User |  |
| ErrorTitle\_3004 | Unauthorized User |  |
| ErrorTitle\_3005 | Answers Don't Match |  |
| ErrorTitle\_3006 | Incorrect Password |  |
| ErrorTitle\_3007 | Access Denied Temporarily |  |
| ErrorTitle\_3008 | Communication Error |  |
| ErrorTitle\_3009 | Prohibited Input |  |
| ErrorTitle\_3010 | Browser Configuration Error |  |
| ErrorTitle\_3011 | Browser Configuration Error |  |
| ErrorTitle\_3012 | Verification failed |  |
| ErrorTitle\_3013 | Unable to send security code |  |
| FinalizeRegistrationHeading1 | If you ever need to reset your password: |  |
| FinalizeRegistrationSubHeading1 | Go to the reset password portal |  |
| FinalizeRegistrationSubHeading2 | Verify your identity |  |
| FinalizeRegistrationSubHeading3 | Choose your new password |  |
| FinishingDescription | Choose Your New Password |  |
| FinishingTitle | Password Reset: |  |
| GotoPortalPrefix | Go to |  |
| GotoPortalSuffix | home page |  |
| LabelTroubleshootingLinkText | View Details |  |
| LoadingText | Loading ... |  |
| NoScriptTagErrorMessage | Scripting is not enabled on your browser. Enable scripting and return to the home page, or contact your help desk for assistance. |  |
| PasswordResetOperationGeneralErrorMessage | Error while attempting to reset password. |  |
| PasswordResetOperationPolicyViolationErrorMessage | The password does not comply with your organization's password policies. |  |
| PasswordResetOperationUserCantChangePasswordErrorMessage | Error while resetting password, the user cannot change the password. |  |
| PrivacyStatement | Privacy Statement |  |
| RegistrationDescription | Self-Service Password Registration |  |
| RegistrationMission | If you ever forget your password, you can reset it yourself without calling your help desk. |  |
| RegistrationPageTitle | Forefront Identity Management - Password Registration |  |
| RegistrationSteps | Click 'Next' to begin the registration process. |  |
| RegistrationSuccessDescription | You are now registered |  |
| RegistrationSuccessTitle | Completed: |  |
| RegistrationWelcomeTitle | Password Registration: |  |
| ResetDescription | Self-Service Password Reset |  |
| ResetEnterNamePrompt | Please enter your user name below |  |
| ResetEnterPassword | Enter a new password: |  |
| ResetExample1 | contoso\mmeyers |  |
| ResetExample2 | mmeyers@contoso.com |  |
| ResetExamples | Examples: |  |
| ResetPageTitle | Forefront Identity Management - Password Reset |  |
| ResetReenterPassword | Re-enter the password: |  |
| ResetSuccessDescription | Your password has been reset |  |
| ResetSuccessTitle | Success: |  |
| ResetUseNewPassword | You can now use your new password to log in. |  |
| ResetUsernameTextFormat | (Resetting password for {0}) | {0} is the user's logon name |
| ResetWelcomeTitle | Password Reset: |  |
| TroubleshootingEmailSubject | FIM request processing error details |  |
| TroubleshootingLabelAttributes | Attributes: |  |
| TroubleshootingLabelCloseButton | Close |  |
| TroubleshootingLabelCopyToClipboard | Copy to Clipboard |  |
| TroubleshootingLabelCorrelationId | Correlation Id: |  |
| TroubleshootingLabelDetails | Details: |  |
| TroubleshootingLabelPostCopyClipboardMessage | The information has been copied to the clipboard. |  |
| TroubleshootingLabelRequestId | Request Id: |  |
| TroubleshootingLabelSendEmail | Send Information by Email |  |
| TroubleshootingLabelSource | Reason: |  |
| TroubleshootingLabelViewRequestDetails | View Request Details |  |
| TroubleshootingLinkText | Troubleshooting Information |  |

The following is a list of Authentication Gate strings that can be customized.

Authentication Gate Strings

|  |  |  |
| --- | --- | --- |
| Name | Default Value | Commnent |
| OTPEmailRegistraionEmailTextboxLabel | Email address: |  |
| OTPEmailRegistrationEmailRequiredErrorMessage | The email address field cannot be empty. |  |
| OTPEmailRegistrationFooterReadOnly | To update your email address, follow the process defined by your organization or call your help desk. |  |
| OTPEmailRegistrationFooterReadWrite | The email address is stored by your organization in Forefront Identity Manager. |  |
| OTPEmailRegistrationGateTitle | Email Address Verification |  |
| OTPEmailRegistrationHeaderReadOnly | If you ever need to reset your password, a verification security code will be sent to your email. If the email address shown below is not correct, you will need to update this in order to use self-service password reset. |  |
| OTPEmailRegistrationHeaderReadWrite | Enter your email address below. If you ever need to reset your password, a verification code will be sent to your email. |  |
| OTPEmailResetGateTitle | Verify Your Identity: Email Verification |  |
| OTPEmailResetHeader | Enter your security code below. A security code was sent to the email address registered with this organization. |  |
| OTPRegularExpressionErrorMessage | The specified value does not match the expected format. |  |
| OTPResetOneTimePasswordRequiredErrorMessage | The security code field cannot be empty. |  |
| OTPResetVerificationLabel | Security Code: |  |
| OTPSmsRegistrationFooterReadOnly | To update your mobile phone number, follow the process defined by your organization or call your help desk. |  |
| OTPSmsRegistrationFooterReadWrite | The mobile phone number is stored by your organization in Forefront Identity Manager. |  |
| OTPSmsRegistrationGateTitle | Mobile Phone Verification |  |
| OTPSmsRegistrationHeaderReadOnly | If you ever need to reset your password, a verification security code will be sent to your mobile phone. If the mobile phone number shown below is not correct, you will need to update this in order to use self-service password reset. |  |
| OTPSmsRegistrationHeaderReadWrite | Enter your mobile phone number below. If you ever need to reset your password, a verification code will be sent to your mobile phone. |  |
| OTPSmsRegistrationMobilePhoneRequiredErrorMessage | The mobile phone number field cannot be empty. |  |
| OTPSmsRegistrationSMSTextBoxLabel | Mobile Phone: |  |
| OTPSmsResetGateTitle | Verify Your Identity: Mobile Phone Verification |  |
| OTPSmsResetHeader | Enter your security code below. A security code was sent to the mobile phone registered with this organization. |  |
| PasswordGateDescriptionText | Enter your current password below, then click 'Next'. |  |
| PasswordGateErrorMessagePasswordRequired | Enter your current password. |  |
| PasswordGateGateTitle | Your Current Password |  |
| PasswordGatePasswordLabelText | Password: |  |
| PasswordGateUsernameTextFormat | <i>(logged in as: <b>{0}</b>)</i> |  |
| QAGateErrorNotEnoughQuestionsAnswered | You must answer at least {0} questions. |  |
| QAGateIncorrectAnswer | Your answers are not correct. |  |
| QAGatePrivacyNotice | The responses you provide are stored by your organization in Forefront Identity Manager. |  |
| QAGateRegistrationNumberOfQuestionsExplanation\_Format | You must answer at least {0} questions to register. |  |
| QAGateRegistrationOneOrMoreAnswersFailedValidation | One or more answers do not comply with policy. |  |
| QAGateRegistrationThisAnswerValidationFailed | This answer does not comply with policy. |  |
| QAGateRegistrationTitle | Register Your Answers |  |
| QAGateResetNumberOfQuestionsExplanation\_Format | You must answer {0} of the following {1} questions. |  |
| QAGateResetTitle | Verify Your Identity: Submit Your Answers |  |

### Customizing the logo banner

The default banner on the portal pages can be customized for your organization.

To customize the logo banner

|  |
| --- |
| 1. Create your custom banners and save them as .png files. The files should meet the following recommendations:   Size: 490 X 50 pixels.   Bit depth: 32  2. Copy the files to the \Customizations folder in each portal that you want to customize.  3. Create a Style.css file in each folder. Have it point to the Customizations folder and the new logo.. You may change the logo name if applicable (i.e. /Customizations/contosologo.png). The code should look like the following:  Example 1:  .title-block { background:url(../Customizations/fimlogo.png) no-repeat scroll 0 0 transparent; }  4. If you are using Internet Explorer 6.0, you will need to provide an alternate non-transparent logo, and add the following code to Style.css:  .ie6 .title-block { background-image:url(../Customizations/fimlogo-ie6.png); }  Example 2:  .title-block { background:url(../Customizations/contosologo.png) no-repeat scroll 0 0 transparent; }  If you are using Internet Explorer 6.0, you will need to provide an alternate non-transparent logo, and add the following code to Style.css:  .ie6 .title-block { background-image:url(../Customizations/contosologo-ie6.png); } |

### Customizing style sheets

You can modify the layout and style of the password portals by using a customized cascading style sheet (CSS).

To use a customized CSS

|  |
| --- |
| 1. Create your customized CSS files and save them as Style.css.  2. Copy the files to the \Customizations folder in each portal that you want to customize. |

The following is a basic example of a Style.css file:

body

{

font: 15px Algerian;

color: #303030;

background: white;

}

.pad

{

padding: 30px;

padding-top: 50px;

background: white;

}

.backgroundWhite

{

border: #e9e9e9 2px solid;

}

.title-block

{

background:url(../Customizations/contosologo.png) no-repeat scroll 0 0 transparent;

}

Important

In order for FIM to recognize any customized changes, you must restart IIS by running iisreset.

The following is a more advanced example of a Style.css file. This file provides smartphone and ipad specific information for displaying the portals on these devices.

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

BASE

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

body {

font-size: 14px; /\*Customizeable- Body Font Size \*/

background-color: #ced5ec; /\*Customizeable- Backgound Color behind the product \*/

}

body, button, input, select, textarea {

font-family: Segoe UI, Arial, Verdana, Sans-Serif, Helvetica; /\*Customizeable- Body Font Family \*/

color: #595959; /\*Customizeable- Body Font Color \*/

}

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

LINKS

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

a { color: #396faf; text-decoration: none; } /\*Customizeable- Link Color and Underline \*/

a:visited { color: #396faf; text-decoration: none; } /\*Customizeable- After Link is clicked color and underline \*/

a:hover { color: #6486ae; text-decoration: none; } /\*Customizeable- Hover mouse over Link color and underline \*/

a:focus { outline: thin dotted; } /\*Customizeable- Keyboard event to Link and Link is in focus outline\*/

a:hover, a:active { outline: 0; } /\*Customizeable- Hover and Active Link outline \*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Typography

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

hr { border-top: 1px solid #acd9ec; } /\*Customizeable- Horizontal Rule Color Above the Footer \*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Layout

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

#wrapper {

background: url(../images/bg-top-slice.png) repeat-x 0 0; /\*Customizeable-remove this line to remove top gradient \*/

}

#container {

background: url(../images/bg-bottom-slice.png) repeat-x 100% 100% transparent; /\*Customizeable-remove this line to remove bottom gradient \*/

}

.title-block {

background: url("../images/fimlogo.png") no-repeat scroll 0 0 transparent; /\*Customizeable- Logo must be 600px or less in width. Logo must be 50px or less in height. \*/

border-bottom: 2px solid #acd9ec;/\*Customizeable- 2px border color under logo \*/

}

.ie6 .title-block {

background-image: url(../images/fimlogo-ie6.png); /\*Customizeable- Can make a non-transparent image for IE6 only \*/

}

h2 {

color: #578e4c; /\*Customizeable- h2 page header color \*/

}

h3 {

color: #999; /\*Customizeable- h3 page header color \*/

}

input[type=text]:focus, input[type=password]:focus {

border: #82bd3b 2px solid; /\*Customizeable- Highlight color around textbox when cursor is inside \*/

}

.chromeButton, .chromeButton:visited {

background-color: #333; /\*Customizeable- Color of button \*/

color: #fff; /\*Customizeable- Color of text on the button \*/

border: 1px solid #666; /\*Customizeable- Border color of button \*/

}

.chromeButton:hover {

background-color: #666; /\*Customizeable- Hover color of button \*/

border: 1px solid #999; /\*Customizeable- Hover border color of button \*/

}

.qcol /\*Style from QAgate.css \*/ {

color: #7a7a7a; /\*Customizeable- Font color of Q&A container \*/

background-color:#e6e7e9; /\*Customizeable- Background color of Q&A container \*/

}

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Media Queries

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

/\* Smartphones ----------- \*/

@media only screen and (max-width: 480px) {

body {

font-size:12px; /\*Customizeable- Body Font Size for devices \*/

}

.title-block {

background: url("../images/fim-logo-portrait.png") no-repeat scroll 0 0 transparent; /\*Customizeable- Logo must be 458px (landscape) or less in width. Logo must be 50px or less in height. \*/

}

h2, h3 {

font-size:14px; /\*Customizeable- H2 and H3 Heading Size for devices \*/

}

}

/\* iPads (landscape) ----------- \*/

@media only screen and (min-device-width : 768px) and

(max-device-width : 1024px) and

(orientation : landscape)

{

}

/\* iPads (portrait) ----------- \*/

@media only screen and (min-device-width : 768px) and

(max-device-width : 1024px) and

(orientation : portrait)

{

}

## Common Customization Issues

The following table is a list of known common issues that can occur with upgrading the FIM Service and Portal. This table also includes the resolutions for these issues.

|  |  |
| --- | --- |
| Issue | Resolution |
| I made a string customization but it wasn’t reflected in the UI | String customizations in strings.resources always require iisreset |
| After making a strings.resources change, I don’t see any of my string changes anymore | Strings.resources format is probably malformed and hence is ignored by the portal. Check the event log under Windows Logs – Application and Services Logs – Forefront Identity Manager |
| The first time I added Style.css, I did not see my style changes in the portal | The very first time you introduce a Style.css file, you need to do an iisreset |
| New styles are added/modified in Style.css but changes are not seen in the browser | Clear the browser cache and refresh the page  Check the CSS syntax |
| I directly changed the contents of the CSS folder in path\_to\_sspr\_portal\css\\*.css or the banner logo in path\_to\_sspr\_portal\images\fimlogo.png and lost these changes on upgrade | You should never change these files to begin with. Only use the Customization folder as a means to provide a banner logo and CSS style customizations in Style.css. Customizations folder is deliberately not overwritten by major upgrades  Do not try to use tools like ILSpy and Reflector to change strings in the portal assemblies. Use strings.resources to override default strings. The assemblies are replaced on upgrade |
| Banner logo is not displayed in the portals / I still see the FIM logo | The image name/path in Style.css is not valid or the browser cache was not cleared |
| Banner logo looks ugly in IE6 | You’ll need to provide a non-transparent image for IE6 and a special accompanying style in style.css |

# Programmatic User Registration

## Programmatic User Registration

FIM 2010 R2 Self-Service Password Reset provides a way for administrators to programmatically register users for password reset workflows. This is done with the use of PowerShell cmdlets. These cmdlets can be used to set required data for all the FIM 2010 R2 interactive authentication gates: QA gate, one-time-password Email gate, and the one-time-password SMS gate. These cmdlets will allow administrators to populate the QA gates and set user data for the OTP Email and OTP SMS gates

The following four new cmdlets have been added to accomplish these tasks.

 [Confirm-AuthenticationWorkflowRegistration](#z0b76060729e248138026a67e36086e03)

 [Get-AuthenticationWorkflowRegistrationTemplate](#z9dabcbe7561d4eefa71b9e4abaecf44a)

 [Register-AuthenticationWorkflow](#za2c8374f9447422f9763d66217adc6f2)

 [Unregister-AuthenticationWorkflow](#zff5a1dba440c483db475d8370f072d08)

### Required SNapIn

These new cmdlets have been added to the FIM Automation SNapIn. In order to use the cmdlets you must add the FIMAutomation SnapIn in PowerShell. This can be done by entering the following in PowerShell before using one of the cmdlets:

PS C:\> Add-PSSNapIn FIMAutomation

### Required Management Policy Rules

The following Management Policy Rules must be created before an administrator can use the programmatic user registration functionality that is provided by the PowerShell cmdlets. The first policy allows the creation and deletion of gate registration objects. The second policy allows modification of user attributes for the case of OTP gates:One-Time Password Email Address (msidmOneTimePasswordEmailAddress) and One-Time Password Mobile Phone (msidmOneTimePasswordMobilePhone). The settings for these MPRs are:

|  |  |
| --- | --- |
| Policy 1 | Create and Delete Gate Registration Objects |
| Type: | Request |
| Requestors: | Administrators |
| Operation: | ****** Delete resource  ****** Create resource |
| Permissions: | Grant |
| Target Resource Definition Before Request: | All Gate Registration |
| Target Resource Definition After Request: | All Gate Registration |
| Resource Attributes: | All Attributes |

|  |  |
| --- | --- |
| Policy 2 | Modify OTP Gate Attributes |
| Type: | Request |
| Requestors: | Administrators |
| Operation: | ****** Add a value to multivalue attribute  ****** Remove a value from a multivalue attribute  ****** Modify a single-valued attribute |
| Permissions: | Grant |
| Target Resource Definition Before Request: | All People |
| Target Resource Definition After Request: | All People |
| Resource Attributes: | ****** AuthN Workflow Locked Out  ****** AuthN Workflow Registered  ****** One-Time Password Email Address  ****** One-Time Password Mobile Phone |

The following example shows how one might use programmatic registration. It is code that creates a C# console application which pulls data from a fictional HR text file.

The following is a copy of the text file:

EmployeeId, SSN, DomainName, Department, AccountName, AlternateEmail, FirstName, LastName

10120, 123-20-5555, Contoso, Identity, bsimon, bsimon@corp.contoso.com, Britta, Simon

10121, 123-21-5555, Contoso, Identity, ljacobson, ljacobson@corp.contoso.com, Lola, Jacobson

This code is provided as an example of how one might programmatically register large numbers of users with data from authoritative data sources.

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

//\* \*

//\* Copyright (C) Microsoft. All rights reserved. \*

//\* \*

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

using System;

using System.Collections.Generic;

using System.Linq;

using System.Text;

namespace PowerShellAutomation

{

using System.Collections.ObjectModel;

using System.Data;

using System.IO;

using System.Management.Automation;

using System.Management.Automation.Runspaces;

class Program

{

static void Main(string[] args)

{

// Get Users Data

DataSet dataSource = Program.GetDataSource(@"C:\demo\datasource.txt");

// Create Runspace Configuration and add the FIMAutomation snapin

RunspaceConfiguration rc = RunspaceConfiguration.Create();

PSSnapInException warning;

PSSnapInInfo info = rc.AddPSSnapIn("FIMAutomation", out warning);

if (warning != null)

{

Console.WriteLine(warning.Message);

return;

}

using (Runspace runspace = RunspaceFactory.CreateRunspace(rc))

{

runspace.Open();

Console.WriteLine("Getting the registration template...");

Pipeline pipeline1 = runspace.CreatePipeline();

pipeline1.Commands.AddScript("$wftemplate = Get-AuthenticationWorkflowRegistrationTemplate -AuthenticationWorkflowName \"Password Reset AuthN Workflow\" ");

Collection<PSObject> results1 = pipeline1.Invoke();

foreach (DataRow userRow in dataSource.Tables["users"].Rows)

{

string registerScript = CreateRegistrationScript(userRow);

Console.WriteLine("Registering user... ");

RunPowrShellScript(runspace, registerScript);

}

runspace.Close();

}

}

private static string CreateRegistrationScript(DataRow userRow)

{

string domainName = userRow[2].ToString();

string accountName = userRow[4].ToString();

string lastName = userRow[7].ToString();

string employeeId = userRow[0].ToString();

string socialSecurityNumber = userRow[1].ToString();

string alternateEmail = userRow[5].ToString();

StringBuilder scriptText = new StringBuilder();

scriptText.AppendLine("$usertemplate = $wftemplate.Clone()");

scriptText.AppendLine("$usertemplate.GateRegistrationTemplates[0].Data[0].Value=\"" + lastName + "\"");

scriptText.AppendLine("$usertemplate.GateRegistrationTemplates[0].Data[1].Value=\"" + employeeId + "\"");

scriptText.AppendLine("$usertemplate.GateRegistrationTemplates[0].Data[2].Value=\"" + socialSecurityNumber + "\"");

scriptText.AppendLine("$usertemplate.GateRegistrationTemplates[1].Data[0].Value=\"" + alternateEmail + "\"");

scriptText.AppendLine("Register-AuthenticationWorkflow -UserName \"" + domainName + "\\" + accountName + "\" -AuthenticationWorkflowRegistrationTemplate $userTemplate");

return scriptText.ToString();

}

private static void RunPowrShellScript(Runspace runspace, string script)

{

try

{

Pipeline pipeline = runspace.CreatePipeline();

pipeline.Commands.AddScript(script);

Collection<PSObject> results = pipeline.Invoke();

Console.WriteLine("Operation Completed");

}

catch(Exception exception)

{

Console.WriteLine("Error Encountered");

File.AppendAllText("ErrorLog.txt", DateTime.Now.ToString() + exception.ToString());

}

}

private static DataSet GetDataSource(string csvFileName)

{

DataSet dataSource = new DataSet();

DataTable usersTable = new DataTable("users");

bool firstline = true;

foreach (string line in File.ReadAllLines(csvFileName))

{

if (firstline)

{

foreach (string columnName in line.Split(','))

{

usersTable.Columns.Add(columnName);

}

firstline = false;

}

else

{

DataRow row = usersTable.NewRow();

string[] dataItems = line.Split(',');

for (int i = 0; i <= dataItems.GetUpperBound(0); i++)

{

row[i] = dataItems[i].Trim();

}

if (row.ItemArray.Length > 0)

{

usersTable.Rows.Add(row);

}

}

}

dataSource.Tables.Add(usersTable);

return dataSource;

}

}

}

# Confirm-AuthenticationWorkflowRegistration

Use to determine if a user is a registered for a specific authentication workflow.

## Syntax

Parameter Set: Default

Confirm-AuthenticationWorkflowRegistration -AuthenticationWorkflowName <String> -UserName <String> [-Credential <PSCredential> ] [-Uri <String> ] [ <CommonParameters>]

## Detailed Description

Use to determine if a user is a registered for a specific authentication workflow.

## Parameters

### -AuthenticationWorkflowName <String>

The display name of the authentication workflow which you wish to return.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -UserName <String>

The username of the user for which you wish to register. Please provide the username in the format: domain\username.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -Credential <PSCredential>

The user credentials required to access the authentication workflows via the Forefront Identity Manager service.

|  |  |
| --- | --- |
| Required? | false |
| Position? | named |
| Default Value | none |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -Uri <String>

The uniform resource identifier for the Forefront Identity Manager service.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### <CommonParameters>

This cmdlet supports the common parameters: -Verbose, -Debug, -ErrorAction, -ErrorVariable, -OutBuffer, and -OutVariable. For more information, see [about\_CommonParameters](http://technet.microsoft.com/en-us/library/dd315352.aspx).

## Notes

## Example 1

Check to see if a user is registered for a specific authentication workflow.

C:\PS> Add-PSSnapin FIMAutomation

C:\PS> Confirm-AuthenticationWorkflowRegistration -username "domain\user1" -AuthenticationWorkflowName "Password Reset AuthN Workflow"

.

# Get-AuthenticationWorkflowRegistrationTemplate

Returns an object of type AuthenticationWorkflowRegistrationTemplate that corresponds to an authentication workflow defined within the target Forefront Identity Manager service instance. The workflow is specified by passing the name of the workflow as parameter.

## Syntax

Parameter Set: Default

Get-AuthenticationWorkflowRegistrationTemplate -AuthenticationWorkflowName <String> [-Credential <PSCredential> ] [-Uri <String> ] [ <CommonParameters>]

## Detailed Description

Returns an object of type AuthenticationWorkflowRegistrationTemplate that corresponds to an authentication workflow defined within the target Forefront Identity Manager service instance. The workflow is specified by passing the name of the workflow as parameter. The registration workflow templates contain a collection of gate registration templates which correspond to the interactive gates (authentication activities) contained within the authentication workflow. Each registration gate in turn contains a Data property which is hashtable containing the name/value pairs of data required to register for the gate.

Use the returned template objects to register a user for an authentication workflow using the Register-AuthenticationWorkflow cmdlet.

## Parameters

### -AuthenticationWorkflowName <String>

The display name of the authentication workflow which you wish to return.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -Credential <PSCredential>

The user credentials required to access the authentication workflows via the Forefront Identity Manager service.

|  |  |
| --- | --- |
| Required? | false |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -Uri <String>

The uniform resource identifier for the Forefront Identity Manager service.

|  |  |
| --- | --- |
| Required? | false |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### <CommonParameters>

This cmdlet supports the common parameters: -Verbose, -Debug, -ErrorAction, -ErrorVariable, -OutBuffer, and -OutVariable. For more information, see [about\_CommonParameters](http://technet.microsoft.com/en-us/library/dd315352.aspx).

## Notes

## Example 1

Returns information on a specific Authentication Workflow Registration Template.

C:\PS> Add-PSSnapin FIMAutomation

C:\PS> Get-AuthenticationWorkflowRegistrationTemplate –AuthenticationWorkflowName “Password Reset AuthN Workflow”

.

# Register-AuthenticationWorkflow

Registers a user for a Forefront Identity Manager service authentication workflow.

## Syntax

Parameter Set: Default

Register-AuthenticationWorkflow -AuthenticationWorkflowRegistrationTemplate <AuthenticationWorkflowRegistrationTemplate> -UserName <String> [-Credential <PSCredential> ] [-Uri <String> ] [ <CommonParameters>]

## Detailed Description

Registers a user for a Forefront Identity Manager service authentication workflow. In order to register a user, an authentication workflow registration template that contains that users registration data must be created and supplied to this cmdlet.

## Parameters

### -AuthenticationWorkflowRegistrationTemplate < AuthenticationWorkflowRegistrationTemplate >

An authentication workflow registration template that has been filled in with the gate registration data for the specified user.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -UserName <String>

The username of the user for which you wish to register. Please provide the username in the format: domain\username.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -Credential <PSCredential>

The user credentials required to access the Forefront Identity Manager service.

|  |  |
| --- | --- |
| Required? | false |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -Uri <String>

The uniform resource identifier for the Forefront Identity Manager service.

|  |  |
| --- | --- |
| Required? | false |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### <CommonParameters>

This cmdlet supports the common parameters: -Verbose, -Debug, -ErrorAction, -ErrorVariable, -OutBuffer, and -OutVariable. For more information, see [about\_CommonParameters](http://technet.microsoft.com/en-us/library/dd315352.aspx).

## Notes

## Example 1

In this example, the cmdlet is called to register user “domain\user1” using the specified template.

C:\PS> Add-PSSnapin FIMAutomation

C:\PS> $template = Get-AuthenticationWorkflowRegistrationTemplate –AuthenticationWorkflowName “Password Reset AuthN Workflow”

$usertemplate = $template.Clone()

$userTemplate.GateRegistrationTemplates[0].Data[0].Value="answer1"

$userTemplate.GateRegistrationTemplates[0].Data[1].Value="answer2"

$userTemplate.GateRegistrationTemplates[0].Data[2].Value="answer3"

Register-AuthenticationWorkflow -UserName "domain\user1" -AuthenticationWorkflowRegistrationTemplate $userTemplate

.

# Unregister-AuthenticationWorkflow

Unregisters a user for a Forefront Identity Manager service authentication workflow.

## Syntax

Parameter Set: Default

Unregister-AuthenticationWorkflow -AuthenticationWorkflowName <String> -UserName <String> [-Credential <PSCredential> ] [-Uri <String> ] [ <CommonParameters>]

## Detailed Description

Unregisters a user for a Forefront Identity Manager service authentication workflow.

## Parameters

### -AuthenticationWorkflowName <String>

The display name of the authentication workflow which you wish to unregister the user from.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -UserName <String>

The username of the user for which you wish to unregister. Please provide the username in the format: domain\username.

|  |  |
| --- | --- |
| Required? | true |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -Credential <PSCredential>

The user credentials required to access the Forefront Identity Manager service.

|  |  |
| --- | --- |
| Required? | false |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### -Uri <String>

The uniform resource identifier for the Forefront Identity Manager service.

|  |  |
| --- | --- |
| Required? | false |
| Position? | named |
| Default Value | No default |
| Accept Pipeline Input? | false |
| Accept Wildcard Characters? | false |

### <CommonParameters>

This cmdlet supports the common parameters: -Verbose, -Debug, -ErrorAction, -ErrorVariable, -OutBuffer, and -OutVariable. For more information, see [about\_CommonParameters](http://technet.microsoft.com/en-us/library/dd315352.aspx).

## Notes

## Example 1

Unregister a user for a Forefront Identity Manager service authentication workflow.

C:\PS> Add-PSSnapin FIMAutomation

C:\PS> Unregister-AuthenticationWorkflow -UserName "domain\user1" -AuthenticationWorkflowName “Password Reset AuthN Workflow”

.

# Kerberos and Self-Service Password Reset

The following section is presented to explain Kerberos and how it pertains to Self-Service Password Reset.

## What is Kerberos?

The Kerberos authentication protocol provides a mechanism for authentication — and mutual authentication — between a client and a server, or between one server and another server. The Kerberos authentication protocol originated at MIT more than a decade ago, where it was developed by engineers working on Project Athena. The Kerberos protocol is more secure, more flexible, and more efficient than NTLM. The benefits gained by using Kerberos authentication are:

 Delegated Authentication

 Interoperability

 More efficient authentication to servers.

 Mutual authentication

Kerberos authentication has the following authentication dependencies:

1. Operating System - client must be XP or later and server must be 2000

2. TCP/IP connectivity - network connectivity must exist between client, domain controller and target server

3. DNS - DNS must be functioning for the client to obtain the FQDN. The FQDN is used to access the domain controller.

4. Active Directory

5. Time Service

6. SPN - Service principal names (SPNs) are unique identifiers for services running on servers.

### What are SPNs?

Service principal names (SPNs) are unique identifiers for services running on servers. Every service that uses Kerberos authentication needs to have an SPN set for it so that clients can identify the service on the network. If an SPN is not set for a service, clients have no way of locating that service. Without correctly set SPNs, Kerberos authentication is not possible.

An SPN is registered in Active Directory under a user account as an attribute called Service-Principal-Name. The SPN is assigned to the account under which the service the SPN identifies is running. Any service can look up the SPN for another service. When a service wants to authenticate to another service, it uses that service's SPN to differentiate it from all of the other services running on that computer.

Because multiple services can run simultaneously under the same account, setting an SPN requires four unique pieces of information. These four pieces of information uniquely identify any service running on a network and can be used to mutually authenticate to any service.

For each SPN that is set, the following information is required:

1. The type of service, formally called a service class. This enables you to differentiate between multiple services running under the same account.

2. The account under which the service is running.

3. The computer on which the service is running, including any aliases that point to that computer.

4. The port on which the service is running (optional if the default port for the service of that type is used such as port 80 for HTTP).

The syntax of an SPN itself is service/hostname:port, where:

1. Service is the service class of the SPN.

2. Hostname is the computer to which the SPN belongs.

3. Port is the port on which the service that the SPN is registered to runs.

### How are tickets decrypted

A client makes a HTTP Request to an IIS server running SharePoint. The IIS server denies the request with a 401 Authorization Required and indicates to the client that it supports Kerberos authentication. The client then requests a Service Ticket from the KDC on a Domain Controller. This is done by sending the SPN for that service to the DC. The DC finds the domain account that matches the SPN and creates a ticket for the client. The ticket is encrypted with the password for the domain account of the receiving application, for example the SharePoint service account. The DC returns the Service ticket to the client. The client, then sends the ticket to IIS, in the authentication header to prove the identity of the client. To decrypt the ticket IIS must know the password of the domain account, in this case, the SharePoint service account. The password for this account is encrypted and stored in the applicationHost.config file. IIS will then decrypt the ticket.

### Kernel-Mode Authentication

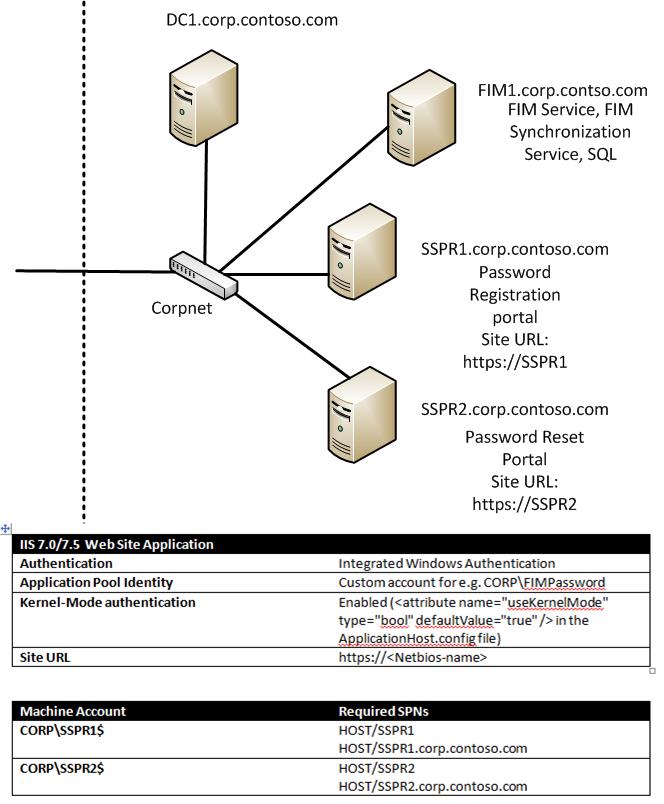
With the release of IIS 7.0 on Windows Server 2008 and IIS 7.5 on Windows Server 2008 R2 a new mode kernel-mode authentication was introduced. This means that the ticket for the responding service is decrypted using the Machine account (Local System) of the IIS Server. It no longer depends on the application pool Identity for this purpose by default. You no longer need to worry about the correlation between HTTP SPNs and the Application pool Identity that was required in the earlier versions of IIS.

By default, UseKernelMode Authentication is set to true automatically on the applicationHost file after the password registration and password reset portals have been installed.

### SPNs and Self-Service Password Reset

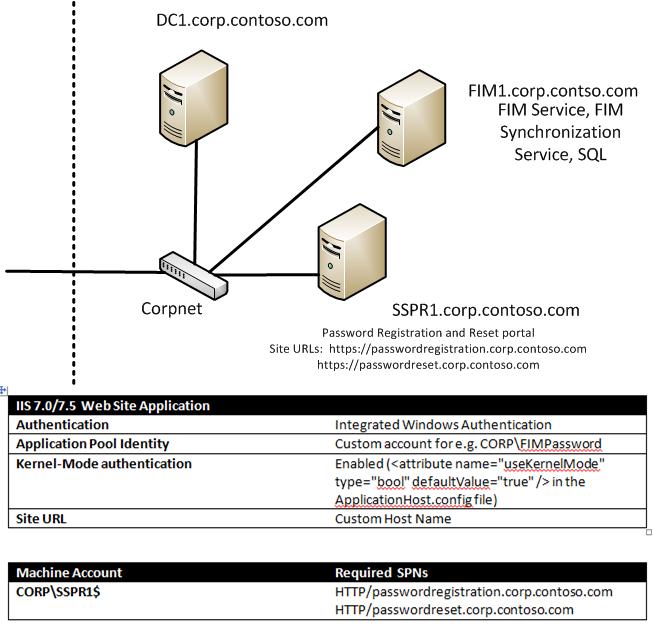
Self-Service Password Reset requires either the use of IIS 7.0 or IIS 7.5. This means that we can take advantage of Kernel-Mode and use the machine account to decrypt tickets. This does not mean however that we can forget entirely about SPNs. Depending on how you have SSPR setup is going to depend on whether or not additional SPNs are required.

Scenario 1



Under this scenario, it is assumed that the password registration and password portal sites are split and being hosted by two dedicated IIS servers. The site URLs used by both are https:<netbios-name>. In this case https://SSPR1 and https://SSPR2 are the site URLs. To access the Password Registration Portal we simply open Internet Explorer and enter https://SSPR1. Likewise, to access the Password Reset Portal we would enter https://SSPR2. In this scenario, the only SPNs that would be required would be on the SSPR1 machine account and the SSPR2 machine account. For instance, on SSPR1, the SPNs would be HOST/SSPR1 and HOST/SSPR1.corp.contoso.com. On SSPR2 they would be HOST/SSPR2 and HOST/SSPR2.corp.contoso.com. In this case, you would not have to set any SPNs because the HOST SPNs are set automatically when the machine is joined to the domain. This however, is not the most likely scenario.

Scenario 2



Under this scenario, the password registration and password portal sites are being hosted on the same IIS server. They have been configured with custom host headers. The site url for the Password Registration site is https://passwordregistration.corp.contoso.com. The site url for the Password Reset site is https://passwordreset.corp.contoso.com. Now because we are using custom host names, SPNs will be required but only for the IIS machine and in the following format:

 HTTP/<custom-site-name>

The SPNs can be set on the IIS machine account from a command prompt using SetSPN.exe. The following are examples:

Setspn -S HTTP/passwordregistration.corp.contoso.com corp\SSPR1$

Setspn -S HTTP/passwordreset.corp.contoso.com corp\SSPR1$

At this point no other SPNs are required. There are no SPNs required on the web application pool account that runs the password registration and the password reset portals. However, you will need to add related DNS A (IPV4) and/or AAAA (IPV6) records for each of the host headers. For a step-by-step example of adding a DNS A record see [Test Lab Guide: Demonstrating the FIM 2010 R2 Self-Service Password Reset with the Q/A Gate](http://technet.microsoft.com/en-us/library/hh826057(v=ws.10).aspx).

## Delegation and Self-Service Password Reset

A client might need to let an application or a service connect to other servers or services on its behalf. A client might use a front-end server, for example, that then needs to authenticate with a back-end server. The front-end server needs to authenticate to the back-end server with the client's credentials, because if it authenticated under its own service account, it would have different authorization than the user.

Delegation of authentication allows the client to send its identity in the form of a Kerberos ticket to the front-end server. The front-end server can then impersonate the client and authenticate with the back-end server as if the front-end server were the client.

Delegation is not limited to a single pair of a front-end and a back-end server. A client can delegate its identity to a service that can then authenticate with any number of back-end services. It is also possible for the client to delegate its identity to Service A, and for Service A to in turn delegate the client's identity to Service B, for Service B to delegate the client's identity to Service C, and so on.Delegation is possible only with the Kerberos protocol. Thus, all parties involved in delegation scenarios must use the Kerberos protocol.

In order to make a Forefront Identity Manager 2010 R2 deployment more secure, certain service accounts, namely the FIM Service account and the SharePoint Service account should be setup to use constrained delegation. However, with regard to the FIM Password Service account, this is not the case. As mentioned above, the web application pool account, or the FIM Password Service account does not need any SPNs set on it. Likewise, it does not need to be setup for delegation. This is because the FIM Service account is already aware of the FIM Password Service account. For more information on the FIM Service and portal communication see the [FIM 2010 R2 Password Registration Portal](#zdd5e9df8c70d45d781e3b4bc57738ba4) and [FIM 2010 R2 Password Reset Portal](#z33be589601f4453ea9dfe08cca51725e) topics.

# SSPR Authentication Gates

## SSPR Authentication Gates

Forefront Identity Manager 2010 R2 includes several authentication gates that can be configured for use with Self-Service Password Reset. These gates can be setup as part of an Authentication workflow. By default, FIM 2010 R2 includes the Password Reset AuthN Workflow which is configured with a password gate, a lockout gate and a QA gate. Each gate can be interactive (requires user interaction) or non-interactive; and regardless of which type of gate it is, gates are executed in sequential order one after each other.

The contents of this section are as follows:

1. [Security Context](#z42)

2. [Password Gate](#z43)

3. [QA Gate](#z1)

4. [One-Time-Password Email Gate](#z44)

5. [One-Time-Password SMS Gate](#z45)

6. [Lockout Gates](#z46)

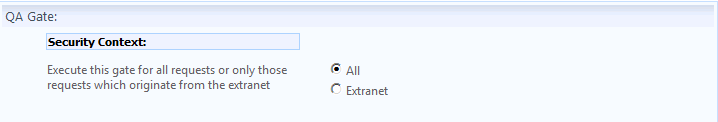
7. [Gate Ordering](#z47)

8. [Creating your own SSPR Workflow using the Authentication Gates](#z48)

### Security Context

Security context is an attribute that was added for FIM 2010 R2. It is an extended attribute on requests. It is used in conjunction with Authentication gates to specify whether or not a request originates from the extranet. The Security Context property is set when a gate is created and can have a value of All or Extranet.

QA Gate Security Context



The following is an example of a message header that has the Security Context of Extranet:

<SecurityContextAssertionProperty

xmlns="http://schemas.microsoft.com/2006/11/ResourceManagement">

Extranet

</SecurityContextAssertionProperty>

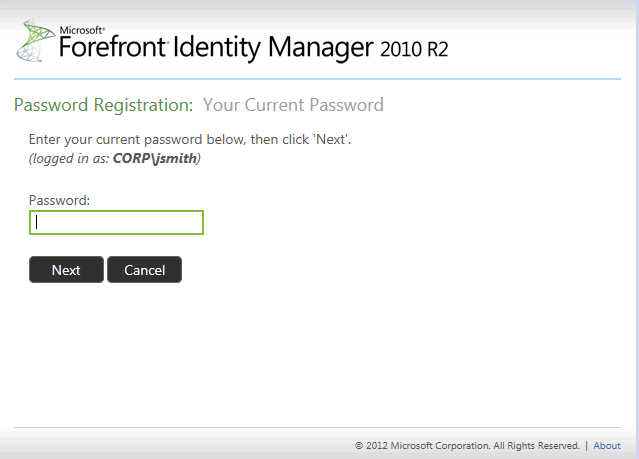
If the Security Context is set to Extranet, the activity/gate will only be run if the request comes from the extranet.

Authentication gates will ignore the Security Context property during registration. During registration, a user has the opportunity to register for all gates which have an interactive registration experience, regardless of whether the user registers from the intranet or the extranet. This ensures that regardless of where the user registers from, they have the opportunity to register for all gates that they may need to reset their password.

### Password Gate

The goal of the password gate is to ensure that the user who is registering for self-service password reset is the user who is actually logged into the Windows session. By default, it is the first gate in the password registration process. This gate is not used in the reset process. The Password Gate does not use Security Context.

Password Gate – Registration Portal



### QA Gate

The QA gate provides a mechanism for users to authenticate to the FIM Service. This is typically used as part of the authentication workflow for an anonymous user to authenticate to FIM, as part of the password reset process, when the user has forgotten their Active Directory password.

The QA gate was implemented in FIM 2010, and provides a mechanism for:

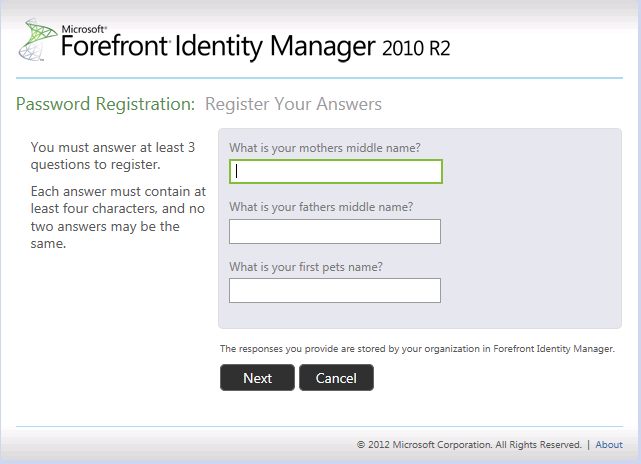
 An administrator to define policies related to the QA gate, including the questions used in the gate.

 An end user to register their answers to the questions which are presented to them in the gate UX.

 An end user to authenticate to the FIM Service, by providing answers to questions which match the answers that they provided during the registration process.

The Password Registration Portal provides user experience to interact with the QA gate during registration. The Password Reset Portal provides user experience to interact with the QA gate during the reset process.

During Registration, the user is presented with a number of questions. The number of questions displayed depends on how the gate is configured. The gate may also be configured to require a user to answer some or all of the questions and to not allow duplicate answers. It can also be configured so that answers much match a particular regular expression. For example, a length requirement can be imposed on users so that their answers must be a certain number of characters long.



During Reset, the user is presented with a number of questions to answer. The number of questions displayed depends on how the gate is configured. This may be all of the questions the user registered answers for or it may be a subset. If for example, the user registered for 5 questions but the gate is configured to only present 3 questions randomly, then only those questions would appear. Likewise, the gate can be configured to only require the user to answer a specific number of questions correctly. When the user clicks the ‘Next’ button, the Reset Portal validates that the user has answered a sufficient number of questions, validates that the answers comply with uniqueness policy and text constraints defined in the QA gate, and sends the data to the QA activity which is executing on the FIM Service.

.



The QA gate is configured in the business process management designer in the FIM portal. FIM 2010 R2 has several new properties in the QA gate that an administrator can configure. These are as follows:

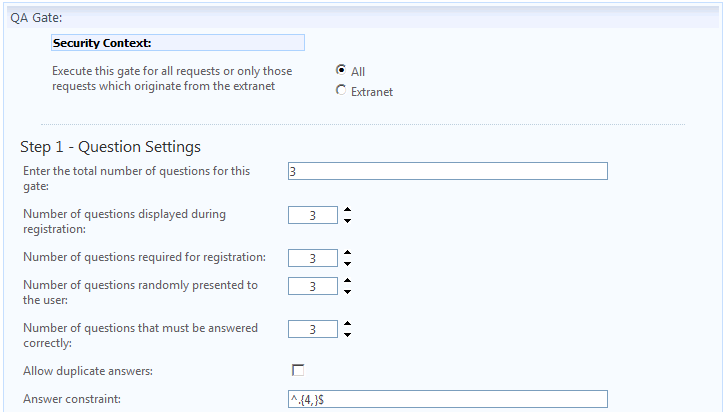
 Allow Duplicates

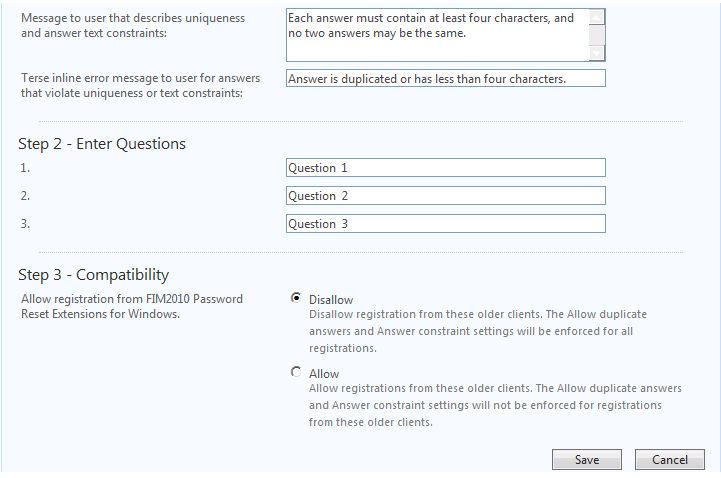
 Answer Constraint

 Answer Constraint User Description

 Answer Constraint Violation Error Message

 Allow registration from FIM 2010 Password Reset Extensions for Windows





Allow Duplicates - This is a checkbox that, when checked, will allow users to provide the same answer to more than one question.

Answer Constraint – This is a textbox that allows administrators to specify what text is allowed in the text box. This is expressed as a regular expression. The default value is ^.{4,}$. This means that the answers must contain at least 4 characters. Be aware that the regular expression is applied to the answer after the answer is normalized as follows:

 The white spaces characters are removed

 The characters with accents are replaced for the character with no accent

 The characters are converted to lowercase.

For additional information on regular expressions, see [Regular Expression Language - Quick Reference](http://msdn.microsoft.com/en-us/library/az24scfc.aspx).

Answer Constraint User Description – This is the text box for a message that is used to describe to the end user, what is an acceptable answer based on what is defined in the Answer Constraint. This text box is located next to Message to user that describes uniqueness and answer text constraints:

Answer Constraint Violation Error Message – This is the text box for an error message that will be shown to end users when they violate the Answer Constraint. It is located next to Terse inline error message to user for answers that violate uniqueness or text constraints:

Allow registration from FIM 2010 Password Reset Extensions for Windows – This is a radio button that can be marked Allow or Disallow and specifies whether an end user, who has the FIM 2010 rich client installed can register for the QA gate with the client. The default value is Disallow.

When answers are submitted to a QA gate activity, the answers are evaluated for compliance with the policy defined in the gate configuration. If the answers comply with policy, the registration process proceeds. If the answers do not comply with policy then the registration request fails with no opportunity to retry, without resubmitting the request.

Note

During registration, if the user violates the QA gate policy, they will be allowed to re-enter answers without the session being terminated.

In R2, it is the responsibility of the server to communicate to the client sufficient information so that the client (PW Registration Portal) can guide the user to input data which can enable successful registration, or stated differently, prevent the user from submitting data during registration which would cause the registration request to fail.

The QA gate enforces that the user’s registration complies with policy by failing registration if:

 The user responses have less than the minimum number of answers specified in the gate configuration.

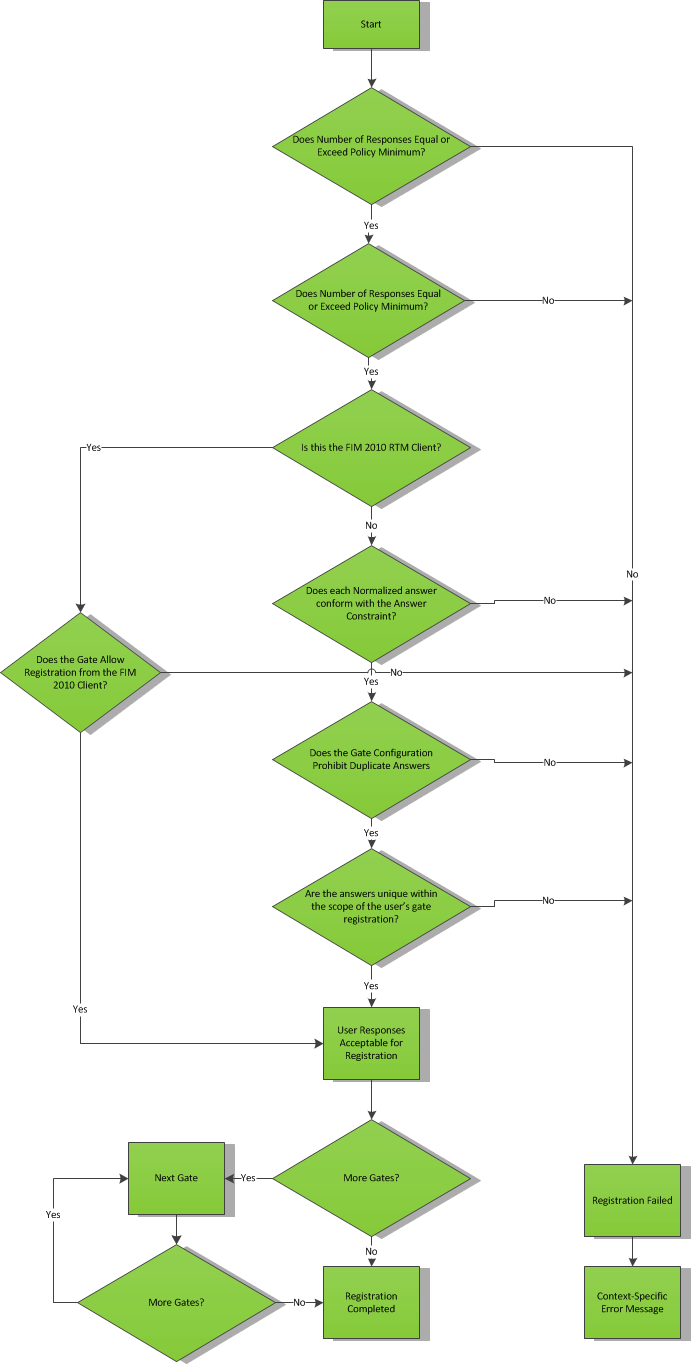
 The user responses include more answers than the number of questions that are specified to be shown to the user during registration.

 Any normalized answer does not conform to the regex specified in Answer Constraint. If no regex is specified in the gate configuration, then this criterion is always evaluated as ‘pass’.

 Any two normalized answers are duplicated. (Except, if the gate is configured to allow duplicate answers, in which case this criterion is always evaluated as ‘pass’).

The business logic for validation of user answers is summarized in the diagram below:

Business Logic for User Answer Validation



During the password reset process, the Password Reset portal renders a user experience to allow the user to interact with the QA gate which is executing on the FIM Service. Specifically, the user can see some or all of the questions for which they registered, and can input their answers to the questions; by successfully providing answers that match the answers from the registration process, the user will be able to proceed with the password reset process.

None of the answer policies which are enforced during registration are evaluated during reset. It would constitute information disclosure for the reset experience to tell an unauthenticated user who may not be affiliated with the organization, what are the requirements for answers to questions in the QA gate.

As during the Registration process, there are two primary types of controls which enable user interaction with the QA gate during reset, text entry boxes,the ‘Next’ button, and the Cancel button which ends the session. Additionally, the page contains the interactive controls which are shared on other portal pages: About link, Privacy Policy link, Help link.



When the user clicks the ‘Next’ button, the Portal validates that the user has answered a sufficient number of questions, and sends the data to the QA activity which is executing on the FIM Service.

If the user has answered fewer questions than specified by policy, then the Portal displays the text : You must answer [n] questions in order to reset your password. Where [n] is the number specified in the gate configuration.

In the normal case where the user’s answers are successfully received by the QA activity, the user experience is as follows:

 If the answers provided during reset match the answers stored on the gate registration object, for at least the number of questions defined in the QA gate configuration, then the user has passed the QA gate, and the user experience depends upon whether there are other gates remaining in the workflow, or other AuthN workflows to which apply to password reset for the user.

 If there are additional gates defined in the workflow which require user interaction, or additional workflows which require authentication, then the Portal loads the user experience for the next gate in workflow which requires user interaction.

 If there are no additional gates which require user interaction, and no other AuthN workflows, then the Portal redirects the user to the Change Password page.

 If the user does not answer a sufficient number of questions correctly, then the user is directed to the error page, where they see the error specified in that section.

 If the user’s answers aren’t successfully received by the QA activity, then the user is directed to the error page, with the error message defined in that section. For example, if the session times out or the Reset Portal is unable to contact the FIM Service for some reason.

### One-Time-Password Email Gate

The One-Time-Password (OTP) Email Gate is a new Authentication gate that is being introduced in FIM 2010 R2. This gate provides a way for a user’s identity to be verified by sending a one-time-password to the user’s email address. This password is then retrieved from their email and presented to the Password Reset portal to continue the reset experience.

The OTP Email Gate uses the e-mail address that is populated in the One-Time Email address attribute of a user. This is a new extended attribute on User in the FIM Portal. If you are using Read-Only as the registration mode you must ensure that the One-Time Password Email Address attribute is populated.

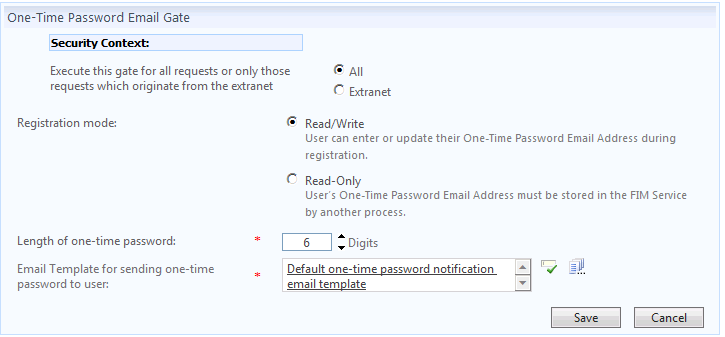
The OTP Email gate is configured in the business process management designer and has the following configurable options:

 Security Context

 Registration mode:

 Length of one-time password

 Email Template for sending one-time password to user

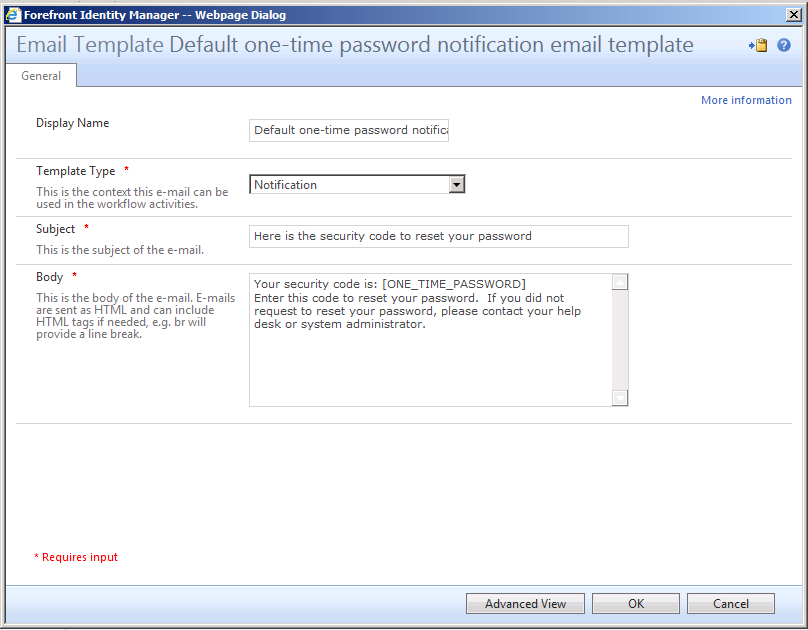


Security Context – As described above this can be set to either All or Extranet.

Registration mode – This is a radio button that allows Administrators to specify whether or not the user should specify an email address during registration. If this is set to Read/Write, then the user will be prompted for an email address when they register. If this is set to Read-Only then the user will not be allowed to enter an email during registration.

Length of one-time password – This specifies the length of the one-time-password that is sent to the user’s email. It can be between 6 and 12 digits long. The default value is 6.

Email Template for sending one-time password to user – This is the template that is used for sending the one-time-password. By default the OTP Email gate uses the Default one-time password notification email template. This is an email template in FIM 2010 R2. This template can be edited with your own message or an entirely new email template can be created and used. This template will contain the one time password. The ONE\_TIME\_PASSWORD variable, which gets auto-populated with the one time password when the email is sent to the user’s email address is responsible for this.



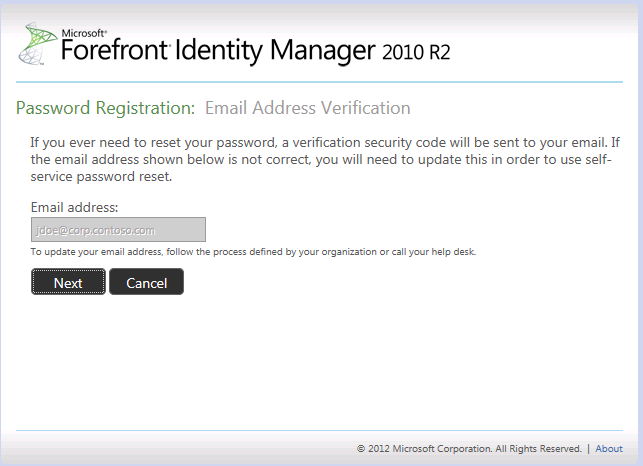
During user registration, depending on how the OTP Email Gate is configured, the end user may or may not be asked to provide an email address. If the Registration mode is set to Read/Write, then the user will be presented with the screen below



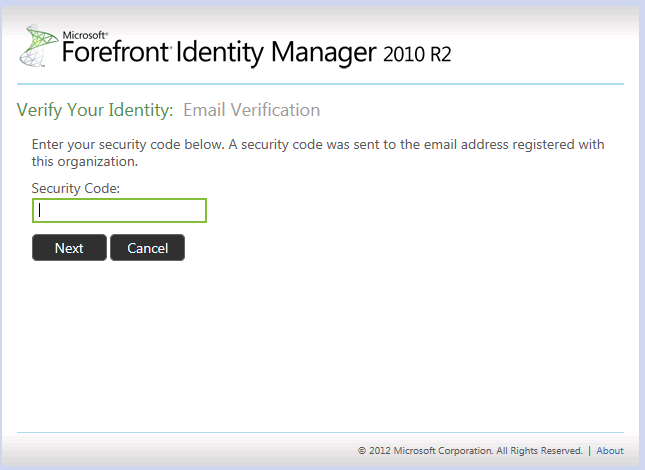
Note

Administrators can bulk-register the user info such as email address through programmatic registration.

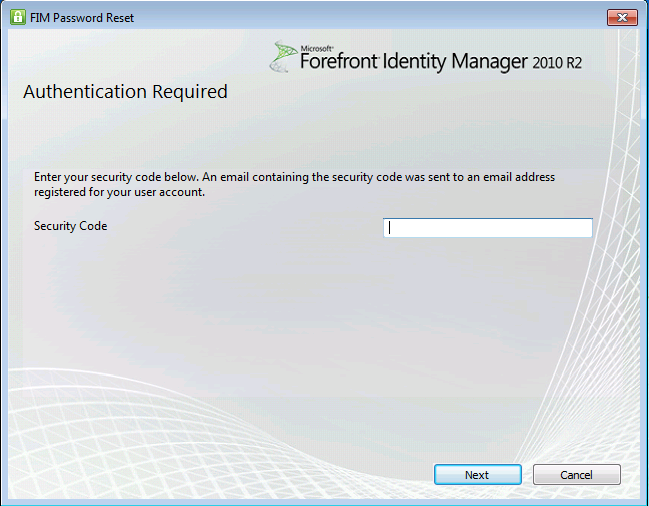
If the Registration mode is set to Read-Only then the user will be presented with the screen shown below. This is to make the user aware that during the reset experience they will receive a security code in their email and what their current email address is in the organization. The grayed out value that is shown in the box is pulled from the One-Time Password Email Address attribute of the user. This is a new extended attribute on User in the FIM Portal. If you are using Read-Only as the registration mode you must ensure that the One-Time Password Email Address attribute is populated. This can be done through synchronization with AD, manually, or by some other process.



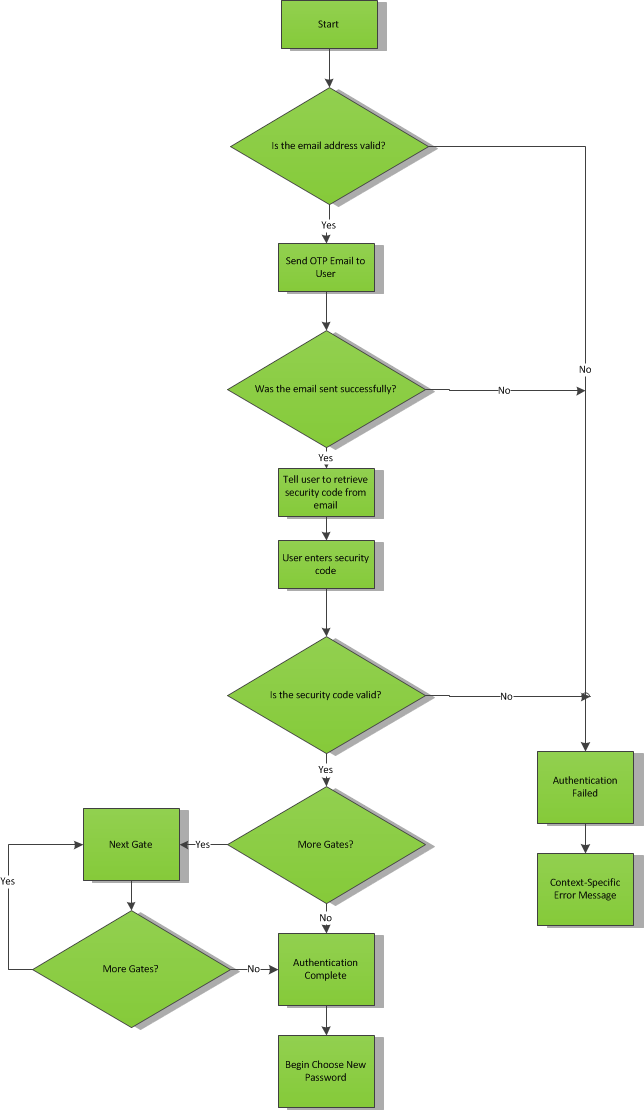
During reset the user is presented with a text box for entering in the security code that has been sent to the users email. The security code must match exactly or reset will fail. This means if any leading or trailing spaces are added in the text box, the reset will fail.



It is also possible to use the rich client to enter a OTP Email security code. It is important to remember that if this is going to be used in your organization then the email address used to send the OTP Email security code should be an email that is accessible by the end-user and doesn’t require the password for the organization.



The business logic for user Authentication is summarized in the diagram below:



### One-Time-Password SMS Gate

The One-Time-Password (OTP) SMS Gate is a new Authentication gate that is being introduced in FIM 2010 R2. This gate provides a way for a user’s identity to be verified by sending a one-time-password to the user’s mobile phone via an SMS provider. This password is then retrieved from their mobile phone and presented to the Password Reset portal to continue the reset experience.

The OTP SMS Gate uses the mobile phone number that is populated in the One-Time Password Mobile Phone attribute of the user. This is a new extended attribute on User in the FIM Portal. If you are using Read-Only as the registration mode you must ensure that the One-Time Password Mobile Phone attribute is populated.

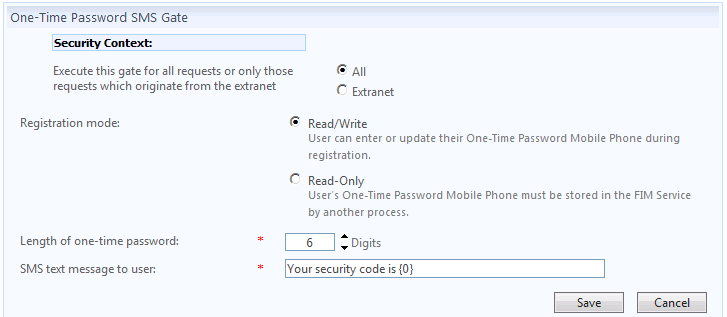
The OTP SMS gate is configured in the business process management designer and has the following configurable options:

 Security Context

 Registration mode:

 Length of one-time password

 SMS text message to user



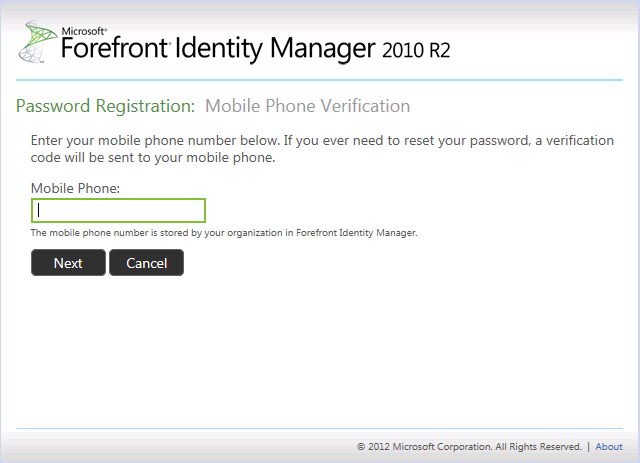
Security Context – As described above this can be set to either All or Extranet.

Registration mode – This is a radio button that allows Administrators to specify whether or not the user should specify a mobile phone number during registration. If this is set to Read/Write, then the user will be prompted for a mobile phone number when they register. If this is set to Read-Only then the user will not be allowed to enter a mobile phone number during registration.

Length of one-time password – This specifies the length of the one-time-password that is sent to the user’s mobile phone. It can be between 6 and 12 digits long. The default value is 6.

SMS text message to user – This is the message that will be sent to the user’s mobile phone along with the security code. By default the OTP SMS gate uses Your security code is {0}. Where {0} is replaced with the security code.

During user registration, depending on how the OTP SMS Gate is configured, the end user may or may not be asked to provide a mobile phone number. If the Registration mode is set to Read/Write, then the user will be presented with the screen below



If the Registration mode is set to Read-Only then the user will be presented with the screen shown below. This is to make the user aware that during the reset experience they will receive a security code on their mobile phone and what their current phone number is in the organization. The grayed out value that is shown in the box is pulled from the One-Time Password Mobile Phone attribute of the user. This is a new extended attribute on User in the FIM Portal. If you are using Read-Only as the registration mode you must ensure that the One-Time Password Mobile Phone attribute is populated. This can be done through synchronization with AD, manually, or by some other process.

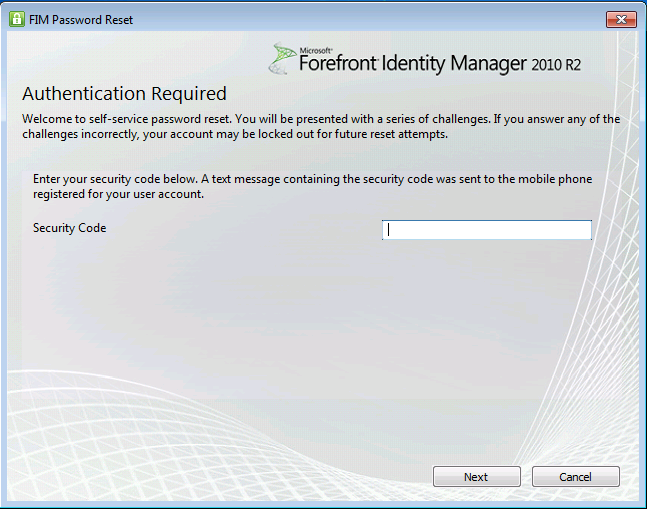
Note

Administrators can pre-populate this field by bulk-registering users through programmatic registration.

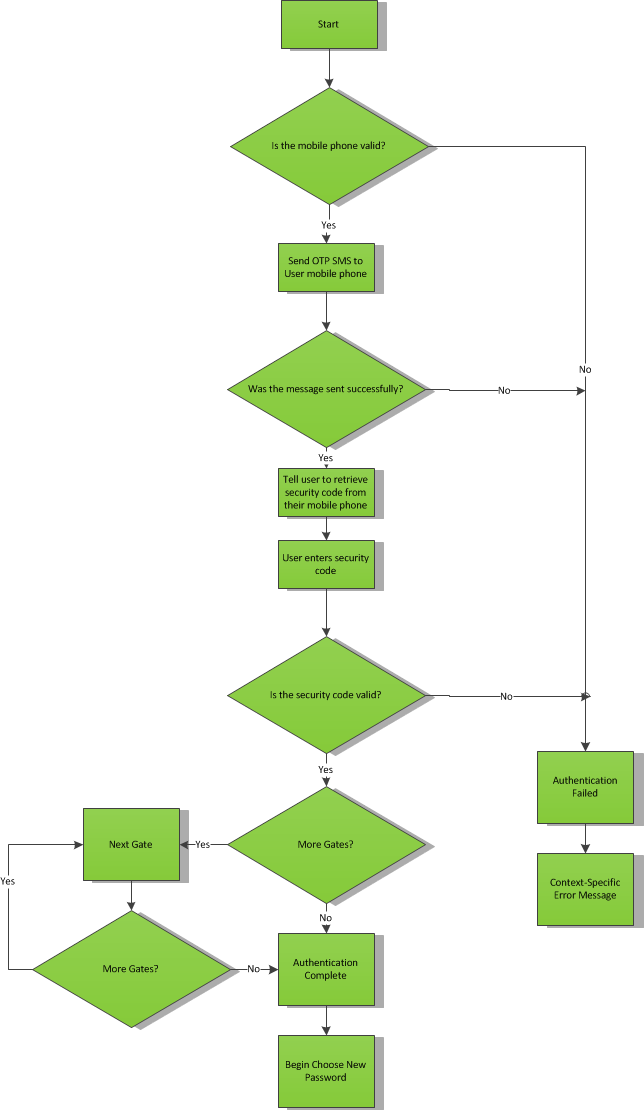


During reset the user is presented with a text box for entering in the security code that has been sent to the user’s mobile phone. The security code must match exactly or reset will fail. This means if any leading or trailing spaces are added in the text box, the reset will fail.

It is also possible to use the rich client to enter a OTP SMS security code.



The business logic for user Authentication is summarized in the diagram below:



Be aware that in order to implement a OTP SMS gate, there are two things that are required. They are:

 A valid SMS (Short Message Service) provider - You need to sign up with an SMS Service Provider.

 SmsServiceProvider.dll – This is code that is written the enables FIM 2010 R2 to send an SMS message to your provider. This file must be named SmsServiceProvider.dll and must be located in Program Files\Microsoft Forefront Identity Manager\2010\Service.

The following is a code example of the SmsServiceProvider.dll

//------------------------------------------------------------

// Copyright (c) Microsoft Corporation. All rights reserved.

//------------------------------------------------------------

namespace Microsoft.IdentityManagement.Samples

{

using System;

using System.Collections.Generic;

using System.Globalization;

using System.Net;

using System.Text;

using Microsoft.IdentityManagement.SmsServiceProvider;

using System.Web;

using System.Security.Cryptography;

using System.IO;

public class SmsServiceProvider : ISmsServiceProvider

{

public void SendSms(string mobileNumber,

string message,

Guid requestId,

Dictionary<string, object> deliveryAttributes)

{

mySMSProvider.SendSms(mobileNumber, message);

}

}

class mySMSProvider

{

static string RequestURL = "http://www.mySMSProvider.contoso.com/sms.dll?Action=SendSMS";

static string adminAccount;

static string adminEmail;

static string adminPassword;

mySMSProvider()

{

}

public static int SendSms(string userMobileNumber, string message)

{

WebClient wc = new WebClient();

string requestData;

requestData = Microsoft.IdentityManagement.Samples.mySMSProvider.GetRequestData(userMobileNumber, message);

byte[] postData = Encoding.ASCII.GetBytes(requestData);

byte[] response = wc.UploadData(mySMSProvider.RequestURL, postData);

string result = Encoding.ASCII.GetString(response); // result contains the error text

int returnValue = System.Convert.ToInt32(result.Substring(0, 4), NumberFormatInfo.InvariantInfo);

return returnValue;

}

public static string GetRequestData(string mobile, string message)

{

string myrequestData;

myrequestData = "AccountId=" + adminAccount

+ "&Email=" + System.Web.HttpUtility.UrlEncode(adminEmail)

+ "&Password=" + System.Web.HttpUtility.UrlEncode(adminPassword)

+ "&Recipient=" + System.Web.HttpUtility.UrlEncode(mobile)

+ "&Message=" + System.Web.HttpUtility.UrlEncode(message);

return myrequestData;

}

public void GetCredentials()

{

string mypwordFile = (@"C:\Program Files\Microsoft Forefront Identity Manager\2010\Service\SmsEncryptedCredentials.txt");

FileInfo info;

int len;

byte[] buffin;

byte[] buffout;

byte[] Entropy = { 9, 8, 7, 6, 5 };

info = new FileInfo(mypwordFile);

len = (int)info.Length;

buffin = File.ReadAllBytes(mypwordFile);

buffout = ProtectedData.Unprotect(buffin, Entropy, DataProtectionScope.CurrentUser);

File.WriteAllBytes(mypwordFile, buffout);

StreamReader sr = new StreamReader(mypwordFile);

adminAccount = sr.ReadLine();

adminEmail = sr.ReadLine();

adminPassword = sr.ReadLine();

sr.Close();

buffin = File.ReadAllBytes(mypwordFile);

buffout = ProtectedData.Protect(buffin, Entropy, DataProtectionScope.CurrentUser);

File.WriteAllBytes(mypwordFile, buffout);

}

};

}

For additional information on creating the SmsServiceProvider.dll see [Test Lab Guide: Demonstrating the FIM 2010 R2 Password Reset SMSProvider with the OTP SMS Gate](http://technet.microsoft.com/en-us/library/hh826055(v=ws.10)) and MSDN.

## Lockout Gates

Lockout Gate is a non-interactive gate and it does the following:

1. It checks if the user is temporarily locked out. If yes, the authentication will fail and the user would receive an error message. Notice if the user is permanently locked out, the request processor will kick the user out in earlier stages and will never hit the Lockout Gate.

2. Increments the lockout counter for the specific user.

3. Temporarily or permanently lockout the user if necessary based on the updated counter.

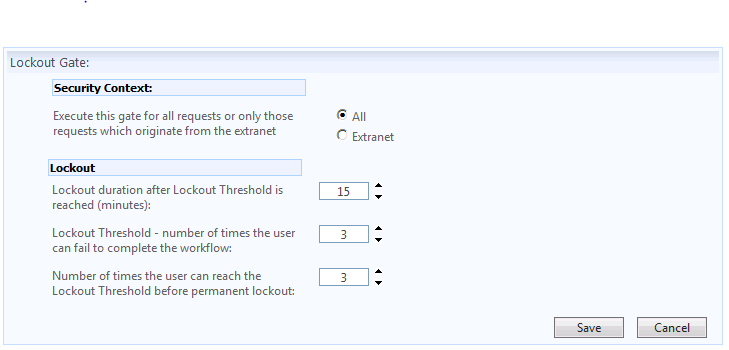
It also registers itself to the workflow's Completed event, when signaled, will unlock the user.

The Lockout gate is configured in the business process management designer and has the following configurable options:

 Security Context

 Lockout

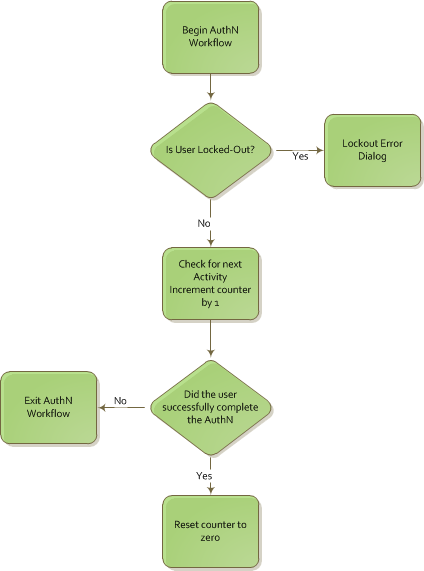
Lockout Gate



Security Context – As described above this can be set to either All or Extranet.

Lockout – This allows for three items to be configured. The first is the lockout duration in minutes. This is how long a user will be locked out of the reset portal if the lockout threshold is reached. The second, is the lockout threshold. This is the number of times the user can fail to complete the workflow before they are locked out. And finally the number of times a user can be locked out of the reset portal before becoming permanently locked out of the portal.

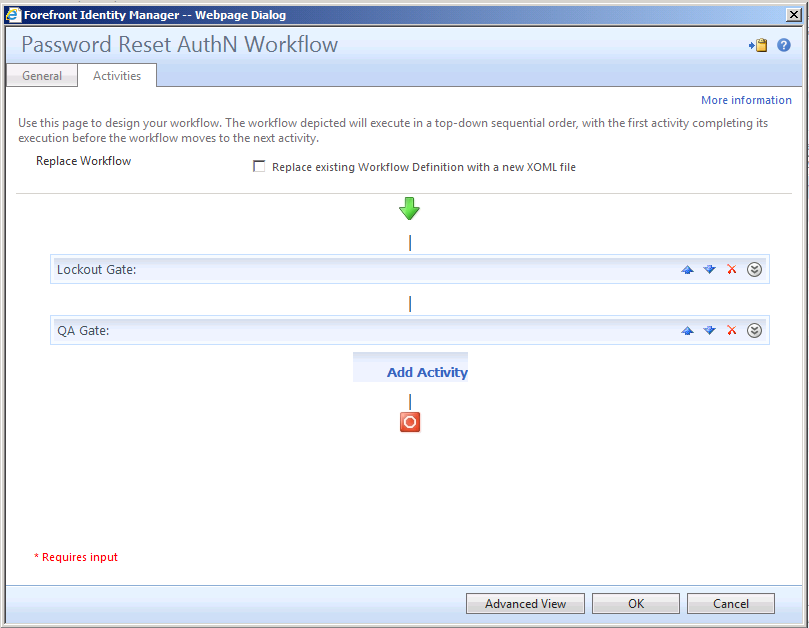
The business logic for the Lockout gate is summarized in the diagram below:



## Gate Ordering

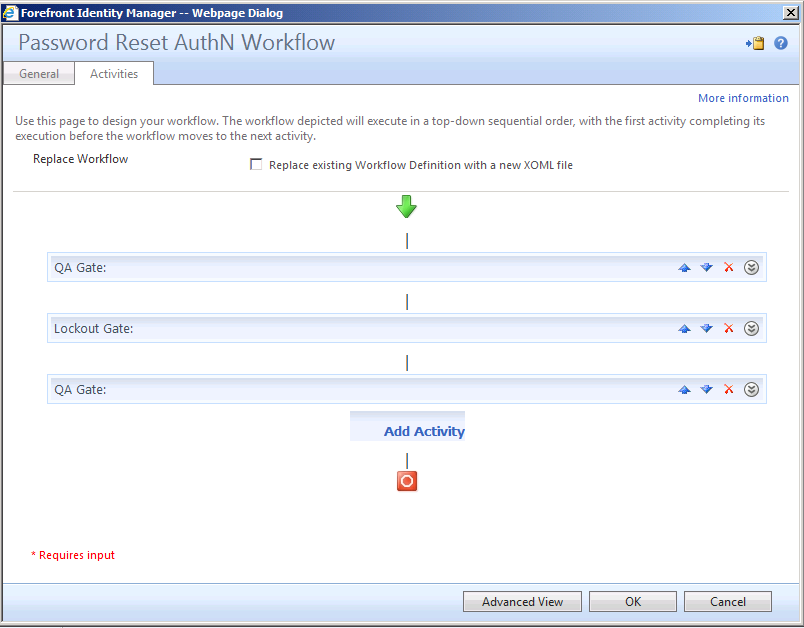
Suppose you have an Authentication Workflow (AuthN WF) that has a Lockout gate followed by a QA gate. A malicious user could initiate SSPR for EmployeeA and intentionally fail the QA gate to permanently lockout EmployeeA.

AuthN Workflow



By changing the AuthN WF to QA -> Lockout -> QA, the Lockout Gate will not be hit unless the malicious user passes the first QA Gate.

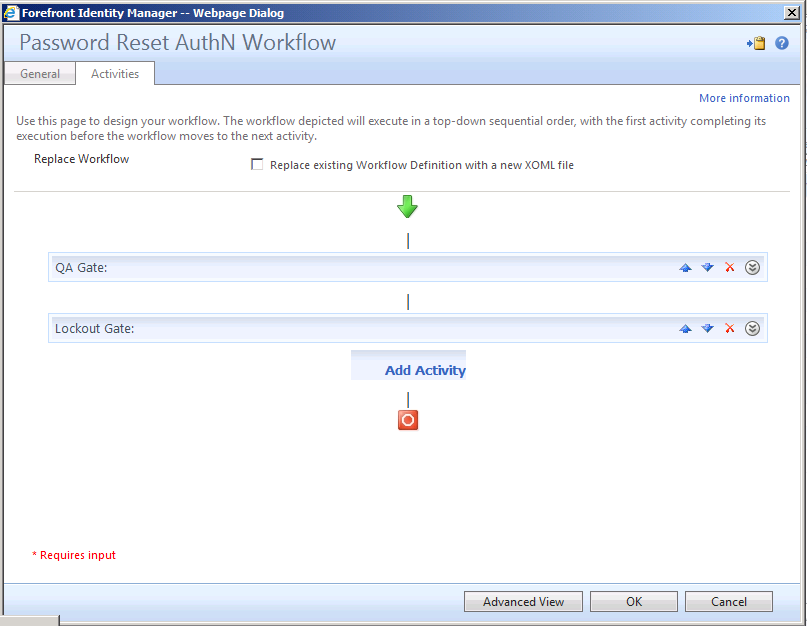
AuthN Workflow



Please note that in this case, the first QA Gate is not protected by the Lockout Gate and is subjected to a brute force attack. That is the price you have to pay to prevent Denial of Service using the Lockout Gate. You should work with your security compliance team in your organization to decide what is right for your organization.

A common mistake in gate ordering is to have only a lockout gate after a QA gate.

AuthN Workflow



In this instance you can attempt to answer questions several times and you will never get locked out. The reason is you will only hit the lockout gate if the QA gate is passed successfully. Because the lockout gate is non-interactive, it will increment the lockout counter but then subsequently reset it to zero because the workflow is over and has been successful. The QA gate does not hold the lockout counter. Only the lockout gate does.

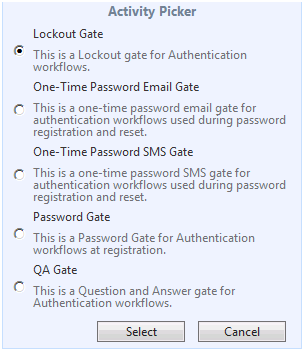
So to resolve this you can place either a password authentication gate (for the registration page) or a QA gate before the lockout gate and then have an additional QA gate after the lockout gate. This way, once the user has either successfully passed the first gate, the lockout gate is hit and the counter incremented then the next gate is hit. If the user fails this gate, the counter is still incremented and additional attempts will ultimately hit the lockout threshold and lock the user out. Keep in mind that if a user cancels out of the QA gate, say by just exiting their browser, the lockout counter will still be incremented and will not be set back to zero. Only successfully completing the workflow will achieve this.

Also, as mentioned above, you don’t want to have just a Lockout gate followed by a QA gate as this could allow a malicious user the ability to lock accounts out.

## Creating your own SSPR Workflow using the Authentication Gates

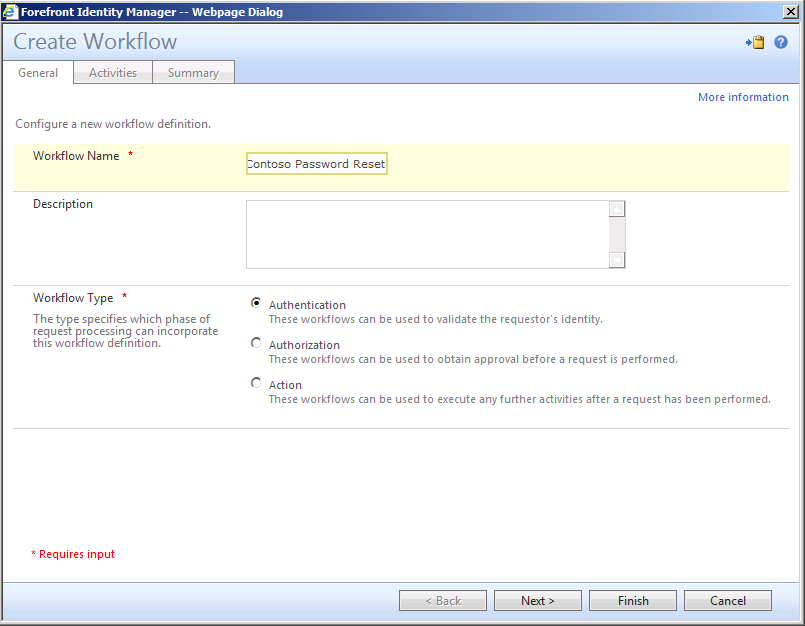
By default, FIM 2010 R2 provides the Password Reset AuthN Workflow. This workflow can be modified to suite your organizations needs by adding or removing additional Authentication gates. This can be done from the Activity Picker in the business process management designer.

Activity Picker

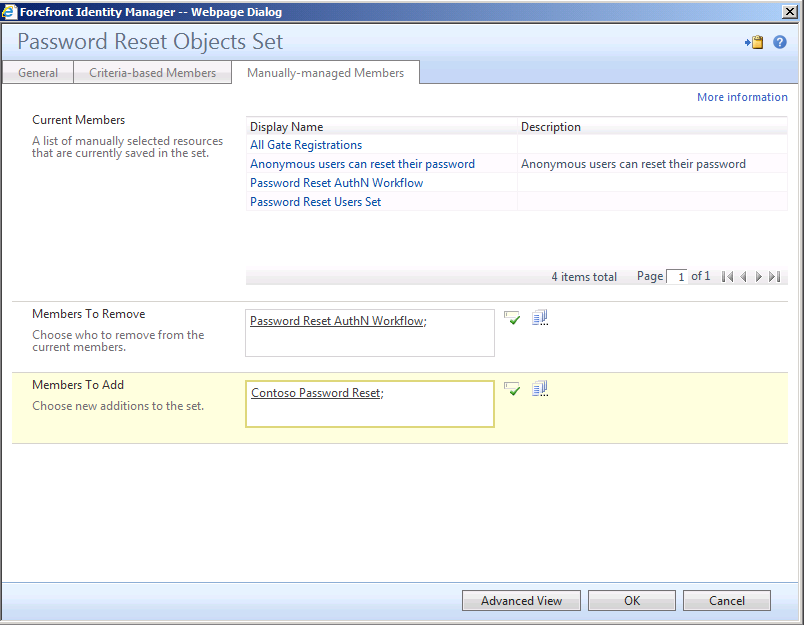


In some cases, it may be desirable to create your own workflow and use that instead of the default one provided. This can be done with the following steps.

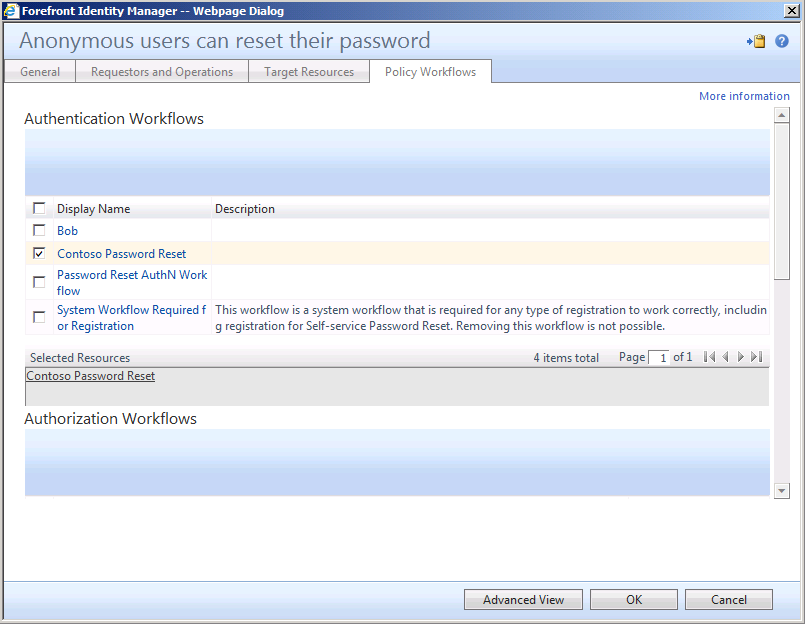
1. Create an Authentication Workflow



2. Modify the Password Reset Objects set



3. Modify the Anonymous Users can reset their password Management Policy



### Configuring password registration and reset for multiple languages

Use the following steps to configure environments where users may need to access the password portals in different languages. This example will use English, French, German, and Italian.

Note

Refer to the online help in the FIM Portal for details on these steps.

To configure password registration and reset for multiple languages

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. For each language, do the following:   Create a set for the related language – For example: EnglishUsersSet, FrenchUsersSet, GermanUsersSet, ItalianUsersSet   Create a duplicate of the Password Reset AuthN Workflow for the related language – For example: EnglishAuthNWorkFlow, FrenchAuthNWorkflow, GermanAuthNWorkFlow, ItalianAuthNWorkflow   Create a duplicate of the MPR ‘Anonymous Users Can Reset Password’ for all of the related languages  The following is the structure for English users:   |  |  | | --- | --- | | Policy | English Anonymous Users Can Reset Password | | Type: | Request | | Requestors: | Anonymous Users | | Operation: | Modify a single-valued attribute | | Permissions: | Grant | | Target Resource Definition Before Request: | EnglishUsersSet | | Target Resource Definition After Request: | EnglishUsersSet | | Resource Attributes: | Select specific attributes   Reset Password | | Policy Workflows | Authentication Workflows   EnglishAuthNWorkFlow  Action Workflows   Password Reset Action Workflow |   2. Add the following to the Password Reset Objects set:   All newly created sets – For example: EnglishUsersSet, FrenchUsersSet, GermanUsersSet, ItalianUsersSet   All newly created AuthN workflows – For example: EnglishAuthNWorkFlow, FrenchAuthNWorkflow, GermanAuthNWorkFlow, ItalianAuthNWorkflow   All newly created MPRs – For example: English Anonymous Users Can Reset Password, French Anonymous Users Can Reset Password, German Anonymous Users Can Reset Password, Italian Anonymous Users Can Reset Password  3. Disable the default MPR “Anonymous Users can Reset Password”  Warning  Be aware that once Anonymous Users can Reset Password is disabled, any user outside of the sets we created above will not be able to reset the password. |

# SSPR Troubleshooting

## SSPR Troubleshooting

The following section will assist with troubleshooting issues that may arise with your SSPR deployment.

### Troubleshooting

If you have issues when you set up the self-service password reset, look for the issues in the following list for information about how to resolve the issues.

###### Password reset configuration

 If the firewall on the FIM 2010 R2 RC server is enabled, you must open a range of ports to allow remote procedure call (RPC) communication between the domain controller and the server with FIM 2010. For more information, see the [Microsoft Identity Integration Server 2003 Technical Reference](http://go.microsoft.com/fwlink/?LinkId=38680) (http://go.microsoft.com/fwlink/?LinkId=38680).

 If the firewall on the server running FIM 2010 R2 RC is on, the password reset does not work unless you manually unblock TCP ports 5725 and 5726. If necessary, manually unblock TCP ports 5725 and 5726.

 In the Question and Answer activity settings, the following condition exists:

 A question should not exceed 100 characters.

###### Password reset use case

 Answers to questions should not exceed 255 characters.

###### Password reset client deployment

 If a user does not register for a password reset during the initial logon, he or she will be prompted to register during each subsequent logon.

 If a user wants to reregister for a self-service password reset, follow the procedures in the [Register for a self-service password reset](#z35) section of this document.