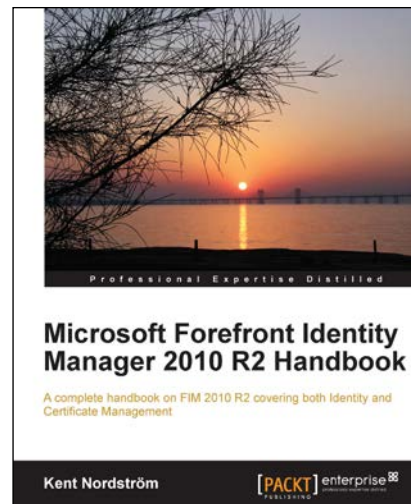


# Microsoft Forefront Identity Manager 2010 R2 Handbook

Kent Nordström



## Chapter No. 7 "Self-service Password Reset"

## In this package, you will find:

A Biography of the author of the book

A preview chapter from the book, Chapter NO.7 "Self-service Password Reset"

A synopsis of the book's content

Information on where to buy this book

## About the Author

**Kent Nordström** wrote his first lines of code in the late 70s, so he's been working with IT for quite some time now. When Microsoft released its Windows 2000 operating system, he started a close relationship with them, which has continued ever since.

For many years now, Kent has been working part-time as a Sub-contractor to Microsoft Consulting Services, and has been doing many of the implementations of FIM and its predecessors for multinational companies and large organizations in Sweden. Apart from FIM, Kent is also well known within the community for his knowledge about Forefront TMG, Forefront UAG, and PKI. Find out more by visiting his blog at <http://konab.com>.

---

I would like to thank my family for their patience during the many evenings and weekends I have spent writing this book.

I would also like to thank Peter Geelen and Henrik Nilsson for taking the time to review my writing. Your feedback has been invaluable!

---

### For More Information:

[www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book](http://www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book)

# Microsoft Forefront Identity Manager 2010 R2 Handbook

Microsoft's Forefront Identity Manager simplifies enterprise Identity Management for end users by automating admin tasks and integrating the infrastructure of an enterprise with strong authentication systems.

The Microsoft Forefront Identity Manager 2010 R2 Handbook is an in-depth guide to Identity Management. You will learn how to manage users and groups, and implement self-service parts. This book also covers basic Certificate Management and troubleshooting.

Throughout the book we will follow a fictional case study. You will see how to implement IM and also set up Smart Card logon for strong administrative accounts within Active Directory. You will learn to implement all the features of FIM 2010 R2. You will see how to install a complete FIM 2010 R2 infrastructure, including both test and production environments. You will be introduced to Self-Service management of both users and groups. FIM Reports to audit the identity management lifecycle are also discussed in detail.

With the Microsoft Forefront Identity Manager 2010 R2 Handbook you will be able to implement and manage FIM 2010 R2 almost effortlessly.

## What This Book Covers

*Chapter 1, The Story in this Book:* In this chapter, the author gives a short description of a fictive company, which he uses throughout the book as an example.

He also discusses some of the Identity Management-related challenges faced by the fictive company, solutions to these challenges, and the company's IT system infrastructure.

*Chapter 2, Overview of FIM 2010 R2:* In this chapter, the author gives an overview of the history of FIM 2010 R2, FIM Synchronization Service, FIM Service, FIM Portal, FIM Reporting, FIM Certificate Management, and licensing.

*Chapter 3, Installation:* In this chapter, we discuss the prerequisites for installing different components of FIM 2010 R2, see how to actually install the components, and look at a few post-installation steps to get it working.

**For More Information:**

[www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book](http://www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book)

*Chapter 4, Basic Configuration:* In this chapter, we discuss some of the basic configurations we need to look at, no matter how our environment looks or how we plan to use FIM 2010 R2. We focus on the initial configuration of FIM Synchronization Service and FIM Service, specifically topics such as creating Management Agents, schema management, FIM Service Management Agents, initial load versus scheduled runs, and moving configurations from the development to the production environment.

If you have an environment already set up, this chapter can act as a guide for you to verify that you have not missed any important steps that will cause your FIM environment to not work properly.

*Chapter 5, User Management:* User management is the primary goal for most FIM deployments. Synchronizing user information between different Management Agents, and managing user provisioning/deprovisioning is often the first thing we focus on in our FIM deployment.

In this chapter, we discuss how user management is set up in FIM Service and FIM Synchronization Service. We also discuss how to manage users in Active Directory, Microsoft Exchange, a fictive phone system, and how to enable users to do some self-service.

*Chapter 6, Group Management:* Once you have User Management in place, it is usually time to start looking at Group Management. In this chapter, we will look at the different group scopes and types in AD and FIM, how to manage groups using the Outlook add-in, and synchronizing groups between HR, AD, and FIM.

*Chapter 7, Self-service Password Reset:* In this chapter, we look at the Self-service Password Reset (SSPR) feature, which allows users to reset their own passwords if they have forgotten them.

We discuss how to enable password management in AD, allow FIM Service to set a password, and configure FIM Service. We also discuss the user experience of the Self-service Password Reset feature.

*Chapter 8, Using FIM to Manage Office 365 and Other Cloud Identities:* In this chapter, we see how FIM 2010 R2 might fit into the puzzle of managing Office 365 identities and also how FIM might play a role in Identity Federation scenarios.

*Chapter 9, Reporting:* One of the new features in FIM 2010 R2 is built-in Reporting support. In this chapter, we discuss how to verify the System Center Service Manager 2010 (SCSM) setup, the default reports that are automatically installed, and the SCSM ETL process. We look at the methods to check/verify and modify reports.

*Chapter 10, FIM Portal Customization:* In this chapter, we take a quick look at the components of the FIM Portal UI. We discuss how to modify the basic FIM Portal UI, and how to customize search scopes and forms.

**For More Information:**

[www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book](http://www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book)

*Chapter 11, Customizing Data Transformations:* In this chapter, we will discuss the overall need and options for data transformation and selective deprovisioning. We also look at an example of managing Microsoft Lync, and a case with strange roles.

*Chapter 12, Issuing Smart Cards:* In this chapter, we will take a look at how we can use FIM CM to issue Smart Cards. You will see how FIM CM adds a lot of functionality and security to the process of managing the complete lifecycle of your Smart Cards.

*Chapter 13, Troubleshooting:* In this chapter, we discuss how to go about troubleshooting issues, depending on where we see the failure and the type of failure. We also see how to perform backup and restore the various parts of FIM.

**For More Information:**

[www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book](http://www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book)

# 7

## Self-service Password Reset

By now, we have a functional FIM 2010 R2 able to manage our users and groups, and maybe also some self service. It is now time to look at one of the features of FIM that many customers believe is the most cost saving one.

The feature is **Self-service Password Reset (SSPR)**, which will allow users to reset their own passwords if they have forgotten them, so they will not have to contact a help desk. Through that, we not only save ourselves a help desk call, but also allow the user to be productive again, quicker. This saves money!

In this chapter we will cover:

- Enabling password management in AD
- Allowing FIM Service to set passwords
- Configuring FIM Service
- The user experience

### Anonymous request

What we need to keep in mind when looking at this feature is that the user, as he has forgotten his password, is unable to authenticate properly to FIM. So, the key problem with SSPR is how to authenticate the user.

Let's take an example.

Kent, our contractor, has forgotten his password. He then makes a request anonymously to FIM to reset the password of the user account *Kent*. Well, FIM won't just do that! So, we tell FIM to try to figure out who the *requestor* is. We add an Authentication (AuthN) workflow, which gives Kent a chance to prove his identity. If the AuthN workflow proves to FIM that the requestor is indeed the user *Kent*, it will allow Kent to reset his password.

**For More Information:**

[www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book](http://www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book)

In FIM 2010 R2, there are two built-in ways for FIM to find out who the user is – we can use either a **Question and Answer (QA)** gate or a **One Time Password (OTP)** gate.

## QA versus OTP

There are two different ways of doing SSPR in the R2 release – QA (Question and Answer) and OTP (One Time Password).

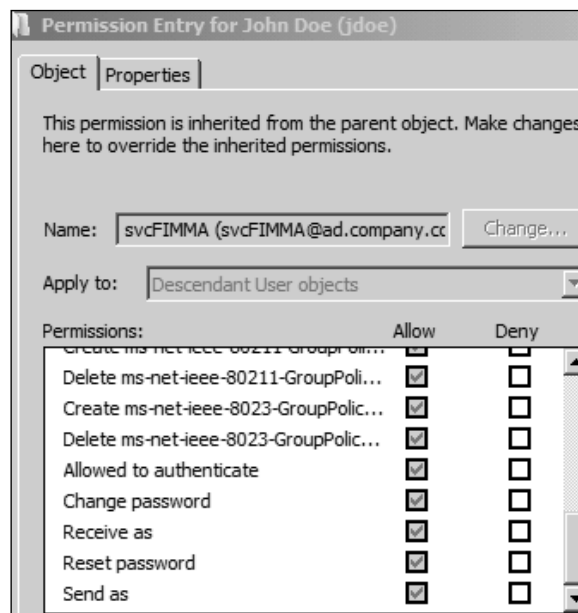
QA basically means that a user can reset his password by giving the correct (the same) answers to a couple of questions the user was presented with during registration of this service.

OTP is a solution where we distribute a one-time code to the users by SMS or e-mail. The user then uses that code to reset his password.

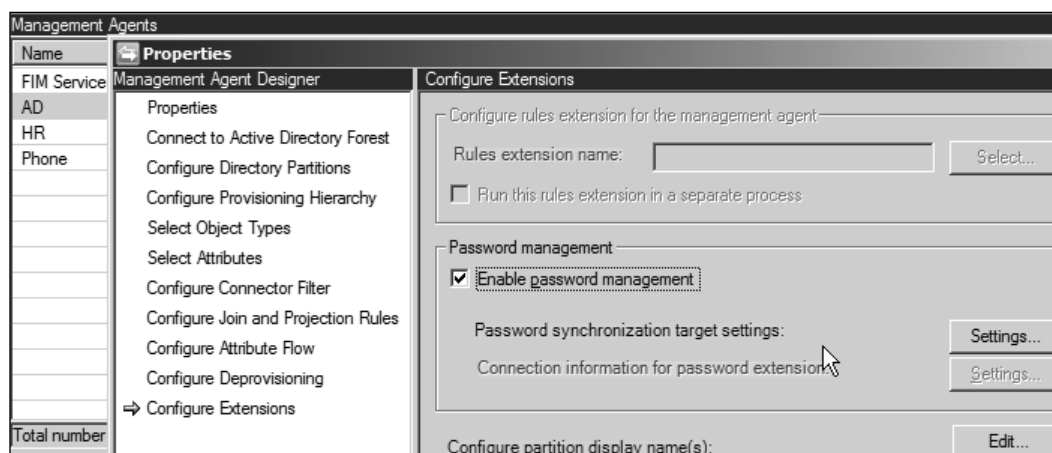
## Enabling password management in AD

The goal for SSPR is, usually, to reset the password of users' account in Active Directory, but the SSPR feature in FIM is not limited to that. It can be used to reset passwords in other CDSs as well.

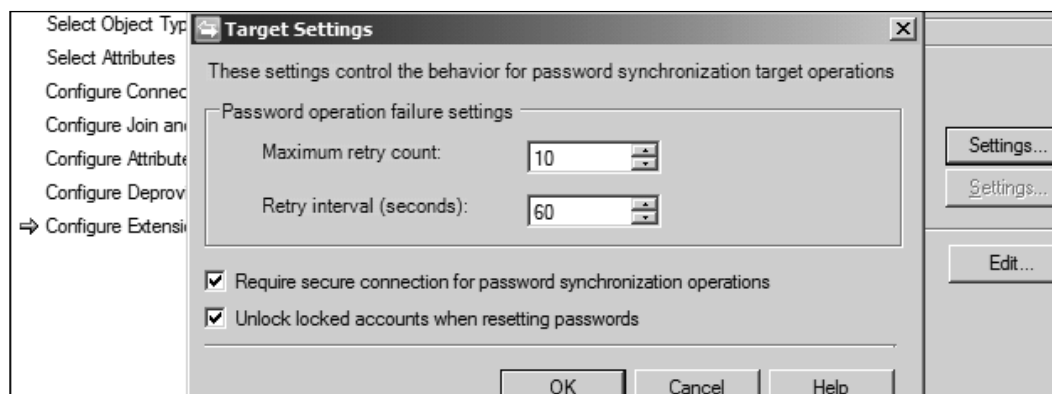
In order for FIM to change the password of a user in AD (or any other CDS), the account used by FIM needs to have the **Reset password** permission in AD, or a similar permission in another CDS:



In **Management Agents** for the target CDS, in this case the AD, we need to check the **Enable password management** checkbox:



If we then look at the settings, we can make some adjustments, as shown in the following screenshot:



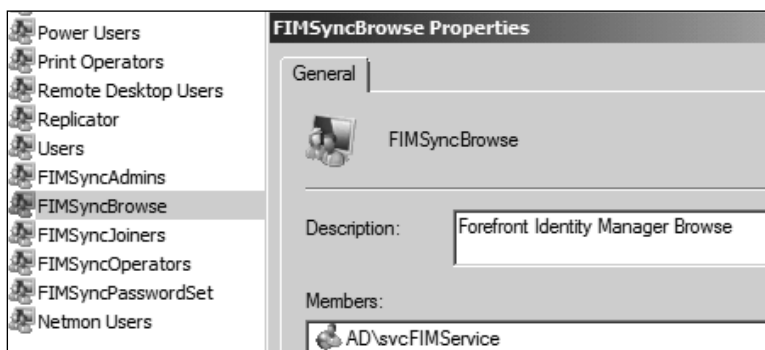
The **Unlock locked accounts when resetting passwords** option is not enabled by default, but I would think that most implementations of SSPR will use that setting. It might be that the user actually locked his own account before realizing he forgot his password.

The Management Agent for AD is now ready for SSPR.

## Allowing FIM Service to set passwords

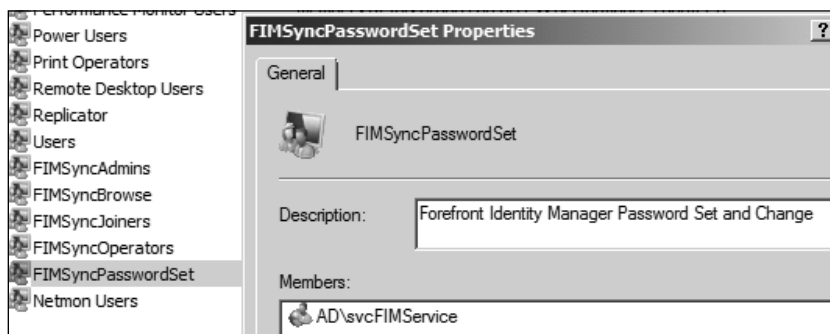
The FIM Service account will be the account that calls FIM Synchronization Service, and tells it to reset the password in AD. But in order for the FIM Service account to be able to do that, we need to assign it some permissions with the following steps:

1. We need to add the account to a couple of groups created during installation (see *Chapter 3, Installation*) of FIM Synchronization Service.
2. Add the FIM Service account to the **FIMSyncBrowse** group:



By default, this is a local group on the FIM Synchronization server; but you might have chosen to use groups in Active Directory instead. This will give FIM Service the ability to read information in FIM Synchronization Service.

3. To actually be allowed to initiate a password reset, we also need to add the FIM Service account to **FIMSyncPasswordSet**:



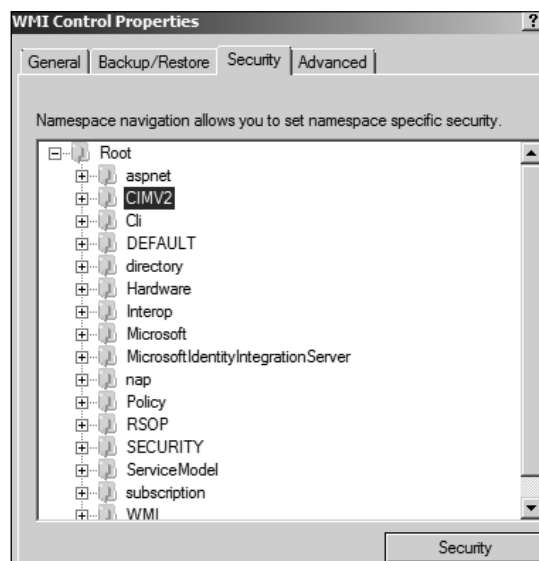
The call from FIM Service to FIM Synchronization Service to do a password reset is made using **Windows Management Instrumentation (WMI)**. This in turn means we need to give FIM Service the WMI permissions as well. This is not something we do on a daily basis and is somewhat tricky.

Because we have, in our example, separated FIM Service and the FIM Synchronization server, it will be remote WMI calls that demand a few extra steps. A few of these steps can be ignored if the services are running on the same server. You would then need to remember to make the changes when/if you separate the services:

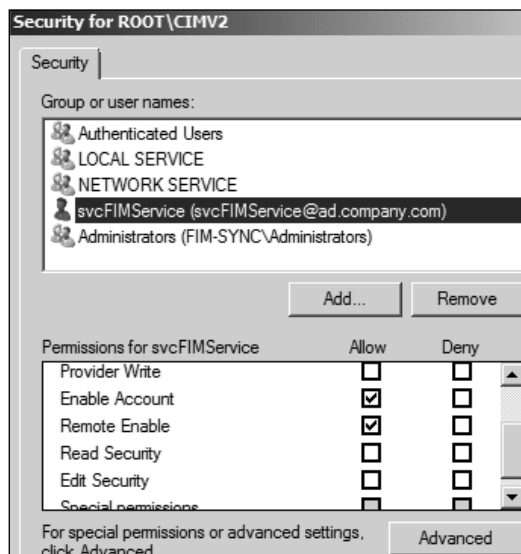
1. Open up the properties of **WMI Control** in **Server Manager (FIM-SYNC)**:



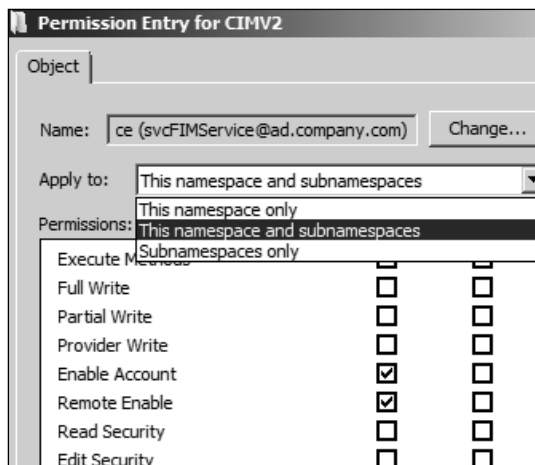
2. In the **Security** tab, expand the **Root** namespace and select the **CIMV2** namespace. Then click the **Security** button at the bottom:



3. Add the FIM Service account and assign the **Enable Account** and **Remote Enable** permissions. This will allow the FIM Service account to connect to this namespace:

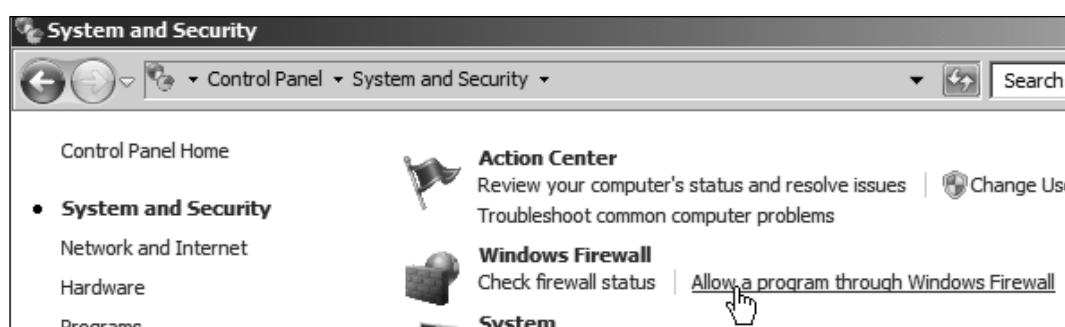


4. But we need to give access to sub namespaces as well. Click the **Advanced** button.
5. In the advanced security settings for CIMV2, select the entry with the FIM Service account and edit it. Change the **Apply to:** from **This namespace only** to **This namespace and subnamespaces**. Click **OK** a few times, to save your settings:

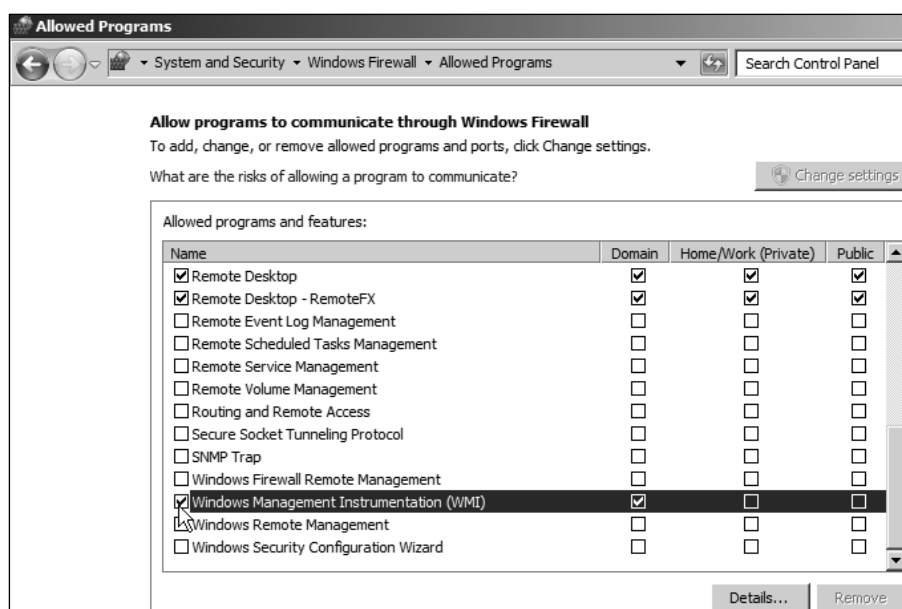


As we have separated the servers, we also need to allow WMI calls through the firewall in FIM Synchronization Server, with the following steps:

1. In the **Control Panel | System and Security** section, click the **Allow a program through Windows Firewall** link:



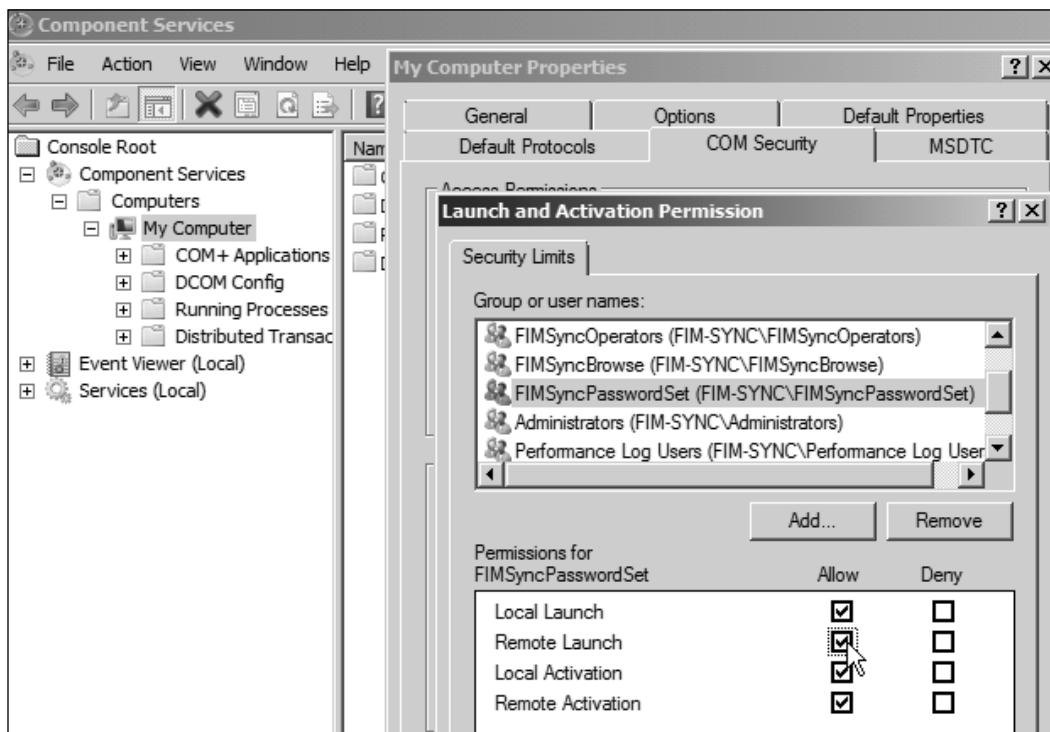
2. In the **Allowed Programs** setting, check the **Windows Management Instrumentation (WMI)** program:



This can be done using GPOs, if that is your preferred way of managing the local firewall on your servers. When allowing WMI to communicate through the firewall, it will create a firewall rule. If you would like to narrow down the IP addresses allowed to use the remote WMI, you can do so by modifying that rule.

The FIM Synchronization groups are assigned some DCOM permissions during setup, but we need to make some adjustments in order for SSPR to work. The following are steps for the same:

1. Under **Component Services** (in the FIM Synchronization server), in the **COM Security** tab of the properties of **My Computer**, click **Edit Limits...**
2. Assign the **Local Launch** and **Remote Launch** permissions to the **FIMSyncPasswordSet** group:



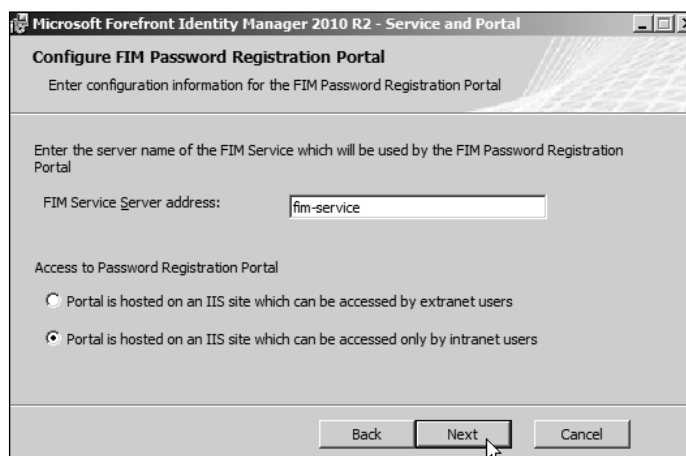
Now the FIM Service account has the permissions required to make the calls to FIM Synchronization Service, to tell FIM Synchronization Service to reset the password in the target CDS (AD).

## Configuring FIM Service

SSPR is not enabled by default in FIM Service, so we need to enable some MPRs and configure some *sets* and *workflows*.

## Security context

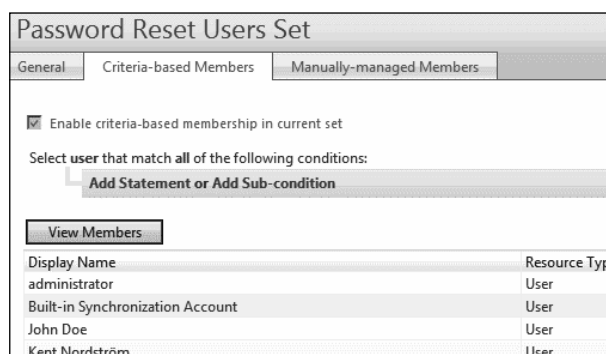
I am not sure if you remember the steps when we installed the FIM password registration and reset portals back in *Chapter 3*. But let me remind you of one critical part in that setup:



During the setup, we decided that the portal should be used for Intranet users. While configuring SSPR, we can configure some settings to only apply to Extranet users. At The Company, we only have one set of password registration and reset portals. But the idea is that you might also want to have a special set for Extranet users. Later, we will refer to this as *security context*. Security context can either be *All* or *Extranet*, where *All* means it applies to both Intranet and Extranet users.

## Password Reset Users Set

The default MPRs around SSPR use a predefined set called **Password Reset Users Set**. If you look at the criterion for that set, you will find it applies to all users:



**For More Information:**

[www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book](http://www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book)

Allowing SSPR for all users is likely not the case in reality. So, we need to modify the criterion in this set. We could also create a new one, but then we would also need to modify all MPRs to reflect the new set. Initially at The Company, this feature will be used by Employees:

**Password Reset Users Set**

General Criteria-based Members Manually-managed Members

☒ Enable criteria-based membership in current set

Select user that match all of the following conditions:

- Employee Type is Employee
- Add Statement or Add Sub-condition

View Members

Display Name	Resource Type
John Doe	User

We have now defined users for whom we would like to use the SSPR feature.

## Password Reset AuthN workflow

As we discussed earlier, we need to have at least one Authentication workflow in our SSPR implementation. The default one is called the **Password Reset AuthN** workflow. The default activity used in this workflow to authenticate the users is the QA gate:

**Password Reset AuthN Workflow**

General Activities

Use this page to design your workflow. The workflow depicted will execute in a top-down sequential order, with the first activity completing its execution before the workflow moves to the next activity.

Replace Workflow ☐ Replace existing Workflow Definition with a new XOML file

↓

Password Authentication Challenge

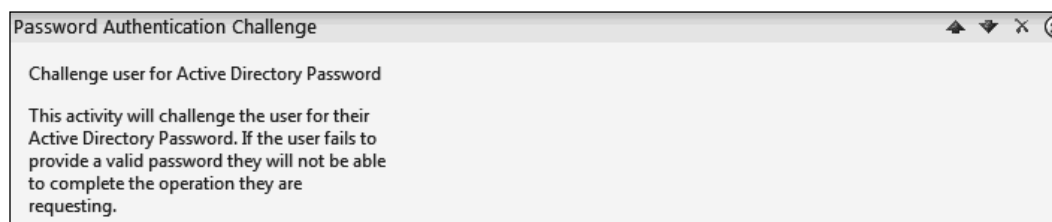
Logout Gate:

QA Gate:

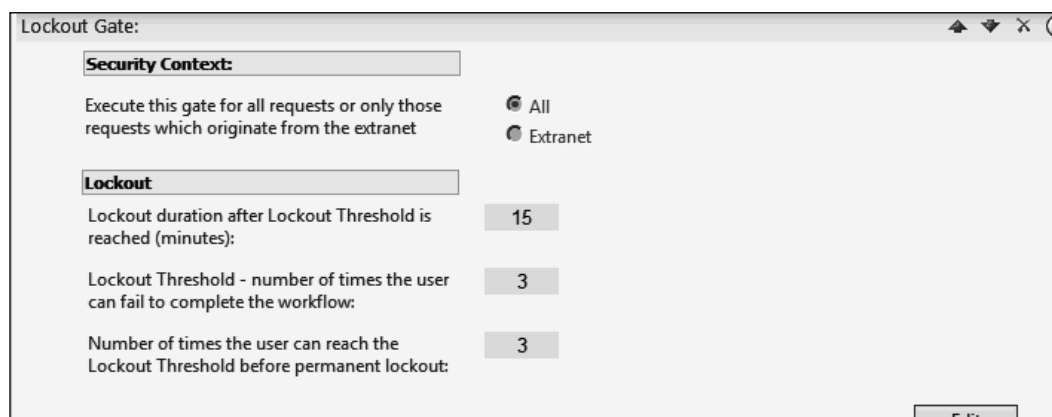
Add Activity

There are also some activities to support the SSPR feature; we will look at those now.

The **Password Authentication Challenge** activity is used during registration and will force the user to reenter their current password during the registration process:



The **Lockout Gate** activity decides how many tries a user will get, and how we should handle lockout if users fail to authenticate correctly:

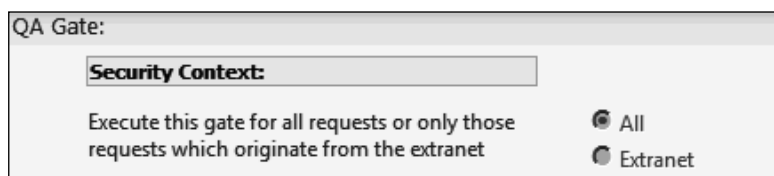


In the previous screenshot, note that the **Security Context:** in this activity is, by default, set to **All**.

## Configuring the QA gate

Finally, the QA gate activity needs to be configured with the following steps:

1. As with **Lockout Gate**, the **Security Context:** section is, by default, set to **All**:



2. We need to decide how many questions to ask and how many questions users are required to answer:

Step 1 - Question Settings	
Enter the total number of questions for this gate:	3
Number of questions displayed during registration:	3
Number of questions required for registration:	3
Number of questions randomly presented to the user:	3
Number of questions that must be answered correctly:	3
Allow duplicate answers:	<input type="checkbox"/>
Answer constraint:	^.{4,}\$
Message to user that describes uniqueness and answer text constraints:	Each answer must contain at least four characters, and no two answers may be the same.
Terse inline error message to user for answers that violate uniqueness or text constraints:	Answer is duplicated or has less than four characters.

Note that the default value of **Answer constraint** requires the answer to contain at least four characters. This you might need to change if you, for example, ask a question such as favorite car, as the answer *BMW* will not work. In the R2 release, the duplicate check and answer constraints were added to prevent users from answering, for example, *123* on all questions.

3. Then, we need to define the question pool to be used by the QA gate. This can be a very time consuming task, as there are many thoughts on what a good question is. You need to ask questions such that they prove a person's identity, but are not likely to be easily guessed by other people.

In many cases, the questions also need to be reviewed by the legal department to make sure that we do not violate any rules or laws. I mean, asking a person about sexual preferences, for example, might not be such a good idea.

There are no best practices in this case. But in my opinion, it is better to have a few good questions than many bad ones. One way is to have the users generate new information with a question, such as asking to "enter a personal PIN (4 digits)". But this kind of information is easier to forget, even though it is a good identifier. In the following example, I ask about Social Security number. This might seem like a good question, but we need to remember that it might be illegal to store this information in our database:

Step 2 - Enter Questions	
1.	Mothers maiden name?
2.	Favorite car?
3.	Social security number?

- Finally, we need to set the compatibility level. If you have an existing pre-R2 implementation of FIM, and have installed the earlier (pre-R2) add-ins and extensions for Windows, you might need to allow them to use the SSPR feature without the duplicate and regular expression check. If you are upgrading from an earlier version of FIM 2010, please read <http://aka.ms/FIMR2Upgrade>.

Step 3 - Compatibility	
Allow registration from FIM2010 Password Reset Extensions for Windows.	<input checked="" type="radio"/> <b>Disallow</b> Disallow registration from these older clients. The Allow duplicate answers and Answer constraint settings will be enforced for all registrations.
	<input type="radio"/> <b>Allow</b> Allow registrations from these older clients. The Allow duplicate answers and Answer constraint settings will not be enforced for registrations from these older clients.

## The OTP gate

If we do not want the QA gate, or we need to support more ways (two-factor authentication) of resetting passwords, we can use the OTP gate included in FIM 2010 R2.

If you click **Add Activity** in the workflow, you will get the following page:

The screenshot shows the 'Password Reset AuthN Workflow' configuration page. It has two tabs: 'General' and 'Activities'. The 'Activities' tab is selected. Below the tabs, there is a text box with instructions: 'Use this page to design your workflow. The workflow depicted will execute in a top-down sequential order, with the first activity completing its execution before the workflow moves to the next activity.' To the right of this text is a 'More info' link. In the center of the page is a large 'Add Activity' button. Below this button is a modal dialog box titled 'Activity Picker'. The dialog lists several activity options, each with a radio button and a description:

- Lockout Gate**  
☐ This is a Lockout gate for Authentication workflows.
- One-Time Password Email Gate**  
☒ This is a one-time password email gate for authentication workflows used during password registration and reset.
- One-Time Password SMS Gate**  
☐ This is a one-time password SMS gate for authentication workflows used during password registration and reset.
- Password Gate**  
☐ This is a Password Gate for Authentication workflows at registration.
- QA Gate**  
☐ This is a Question and Answer gate for Authentication workflows.

At the bottom of the 'Activity Picker' dialog are two buttons: 'Select' and 'Cancel'.

As you can see, there are two OTP gates — one is **One-Time Password Email Gate** and the other is **One-Time Password SMS Gate**.

The e-mail gate can be used pretty much out of the box, as long as FIM Service is allowed to send e-mails to external e-mail addresses. Just remember that it might not be useful for internal users, whose only e-mail address is the internal one. For external users, such as consultants or partners, this might be an easy way of implementing SSPR. During the registration, the users will provide the email address they want to use for SSPR. As you can see, there is an option to have the e-mail address as read-only. This is used when FIM will get the e-mail address to be used, from some other source:

**One-Time Password Email Gate**

**Security Context:**

Execute this gate for all requests or only those requests which originate from the extranet

☐ All  
☒ Extranet

**Registration mode:**

☒ Read/Write  
User can enter or update their One-Time Password Email Address during registration.

☐ Read-Only  
User's One-Time Password Email Address must be stored in the FIM Service by another process.

**Length of one-time password:** \* 6 Digits

**Email Template for sending one-time password to user:** \* Default one-time password notification email template

**Edit**

If you look in the schema of FIM Service, you will find that there is a special set of attributes that are used by the OTP gates. If you are providing the e-mail address used for the e-mail gate, or the mobile phone number used by the SMS gate, you need to make sure the values are stored in the attributes **One-Time Password Email Address** and **One-Time Password Mobile Phone**, respectively:

**Schema Management - All Attributes**

Search for: password

Display Name	Name	Description
AD User Cannot Change Password	AD_UserCannotChangePassword	Will sync from AD to track whether the user is locked out from changing AD password
One-Time Password Email Address	msidmOneTimePasswordEmailAddress	Email address used to deliver a one-time password to the user.
One-Time Password Mobile Phone	msidmOneTimePasswordMobilePhone	Mobile phone number used to deliver a one-time password to the user.
Reset Password	ResetPassword	This attribute is used to trigger a password reset process.

The OTP attributes are **not**, by default, allowed to be managed by the synchronization engine or by users, if that is what you want. Changes in the MPRs are required for this to be possible.

The SMS gate has almost the same settings as the e-mail gate, but requires some additional coding to take place, as we need to compile the DLL files that FIM should use to send the SMS. If you go to <http://aka.ms/SSPRconfigureSMSOTP>, you will find an example of how to create the `SmsServiceProvider.dll` file. You would, of course, also need a provider to send the SMS:

The screenshot shows the 'One-Time Password SMS Gate' configuration window. It has a 'Security Context' section with two radio buttons: 'All' (selected) and 'Extranet'. Below this is the 'Registration mode' section with two radio buttons: 'Read/Write' (selected) and 'Read-Only'. The 'Read/Write' option has a description: 'User can enter or update their One-Time Password Mobile Phone during registration.' The 'Read-Only' option has a description: 'User's One-Time Password Mobile Phone must be stored in the FIM Service by another process.' At the bottom, there are two fields: 'Length of one-time password:' with a value of '6' and 'Digits', and 'SMS text message to user:' with a value of 'Your security code is {0}'.

The reason I do not have an example of this in my book is that the solution varies a lot, depending on how you are calling your SMS provider. I would guess your SMS provider will be a good source of information on how to programmatically call their endpoint using .NET code.

## Require re-registration

If for some reason, you would like users to re-register to the SSPR—the reason could, for example, be that you have redesigned all your questions in the QA gate—you need to check the little **Require Re-Registration** box in the **Password Reset AuthN Workflow** page. This will prompt the users to register again:

The screenshot shows the 'Password Reset AuthN Workflow' configuration page. It has two tabs: 'General' (selected) and 'Activities'. The 'General' tab contains the following fields: 'Workflow Name' (required, value: 'Password Reset AuthN'), 'Description' (empty text area), 'Workflow Type' (value: 'Authentication'), and 'Registration Settings' (checkbox: 'Require Re-Registration' is unchecked). The 'Registration Settings' section has a description: 'Require re-registration for this workflow'.


## SSPR MPRs


Now that we have decided the set and the gate we want to use, we need to enable and configure the relevant MPRs to get the SSPR started.


There are three MPRs that we need to enable; they are as follows:


- **Anonymous users can reset their password**
- **Password reset users can read password reset objects**
- **Password Reset Users can update the lockout attributes of themselves**

Management Policy Rules










Search for:

password



Search within:

All Policies

Advance

<input type="checkbox"/> Display Name ^	Action Type	Disabled	Grant Right	Authentication Workflows	Authorization Workflows	Action
<input type="checkbox"/> Anonymous users can reset their password	Modify	No	Yes	Yes	No	Yes
<input type="checkbox"/> Password reset users can read password reset objects	Read	No	Yes	No	No	No
<input type="checkbox"/> Password Reset Users can update the lockout attributes of themselves	Add, Remove, Read	No	Yes	No	No	No

The first one, **Anonymous users can reset their password**, is the one that does the trick. It will fire off the Password Reset AuthN workflow we talked about earlier and the Password Reset Action workflow that will do the actual reset.

If we haven't done it before, we also need to enable the following MPRs:

- **User management:** Users can read attributes of their own
- **General:** Users can read non-administrative configuration resources

## The user experience

So what does this look like for the user? In my little example, the employees are the ones that will be using the SSPR to begin with.

In order to get the best user experience, requirement number one is that the client computer has the FIM client add-ins and extensions installed, as we talked about in *Chapter 6, Group Management*.

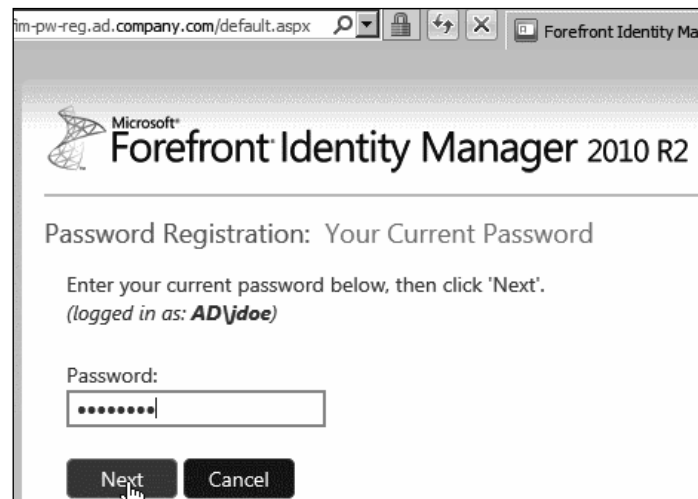
As soon as we enable the MPRs and John (a member of the Password Reset Users set) logs on to his computer, which has the FIM add-ins and extensions installed, it will start up a browser window connecting to the Password Registration portal, which we defined during the installation of the add-ins in *Chapter 6*.

He could also access the Password Registration portal manually; the experience is similar, but using the add-ins and extensions will likely increase the number of users actually taking time to register, as they will be automatically prompted to do so.

If we used FQDN for the Password Registration portal URL, we should make sure that the URL is in the local Intranet zone of the client, so that IE can use Integrated Authentication. To get a good experience with FIM, I recommend adding \*.ad.company.com to the local Intranet zone:



1. First the user has to prove he knows the current password. This is the Password Authentication Challenge activity we have in our workflow kicking in:



- The user is then asked to answer the questions we configured in the **QA Gate** activity. If the QA gate is configured with five questions, but is only supposed to ask three, the three questions asked are randomly picked among the five:

The screenshot shows a web browser window with the address bar displaying "pw-reg.ad.company.com/default.aspx". The page title is "Forefront Identity Manager 2010 R2". The main heading is "Password Registration: Register Your Answers". Below the heading, there is a message: "You must answer at least 3 questions to register. Each answer must contain at least four characters, and no two answers may be the same." To the right of this message, there are three input fields with labels: "Mothers maiden name?", "Favorite car?", and "Social security number?". Each field contains a series of asterisks. Below the input fields, there is a small text: "The responses you provide are stored by your organization". At the bottom, there are two buttons: "Next" and "Cancel".

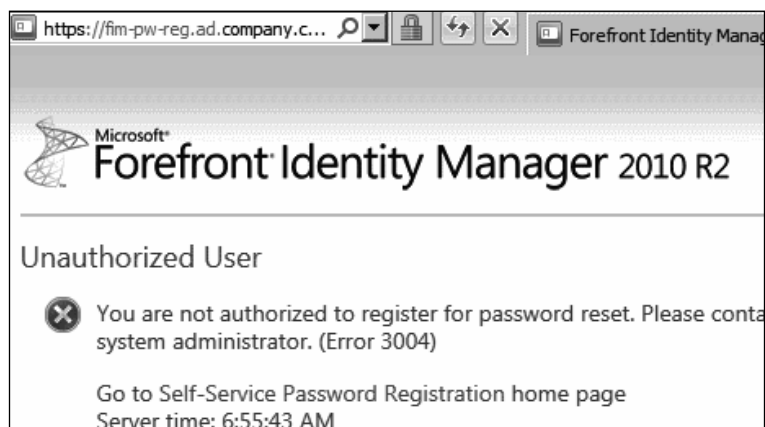
- If we also used the OTP e-mail gate, the user might be asked to also register the e-mail address to be used for the OTP:

The screenshot shows a web browser window with the address bar displaying "pw-reg.ad.company.com/default.aspx". The page title is "Forefront Identity Manager 2010 R2". The main heading is "Password Registration: Email Address Verification". Below the heading, there is a message: "Enter your email address below. If you ever need to reset your password be sent to your email." Below this message, there is a label "Email address:" followed by an input field containing the text "john.doe@msn.com". Below the input field, there is a small text: "The email address is stored by your organization in Forefront Identity Manager." At the bottom, there are two buttons: "Next" and "Cancel".

- When the user has completed the guide, he is informed that he might use the Password Reset portal to reset the password. This is, however, not the only way for the user to reset his password. If he has the add-ins and extensions installed, he can also use the Windows logon screen:



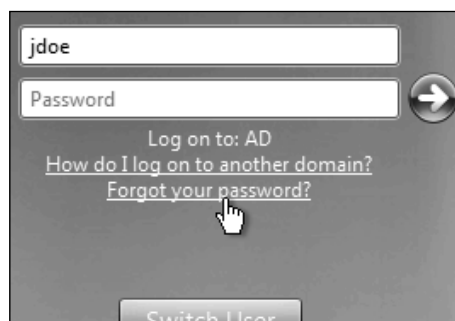
- If a user who is not a part of the Password Reset Users set tries to manually access the Password Reset Registration portal, he will be duly notified that he is not authorized to register:



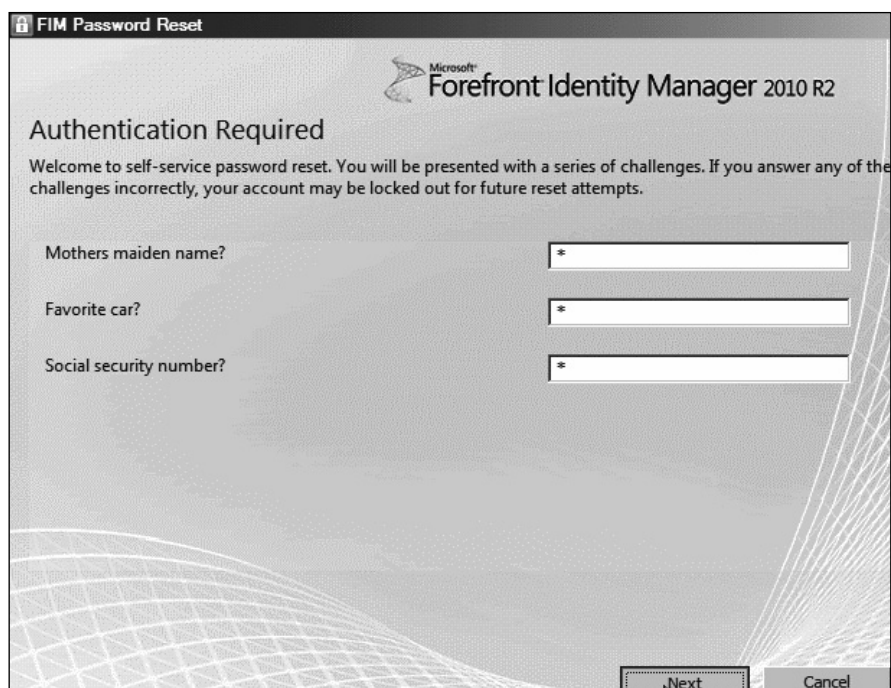
So, what happens when the user finds himself forgetting his password?

Well, there are two options here – he can either access the Password Reset portal from some internal kiosk computer, or maybe we could have the Password Reset portal published to the Internet, using, for example, Microsoft Forefront UAG. But, as we have also installed the add-ins and extensions on his computer, he can use that as well:

1. At the Windows logon screen, the user can just click the **Forgot your password?** link:



2. To authenticate himself, he answers the QA gate questions:

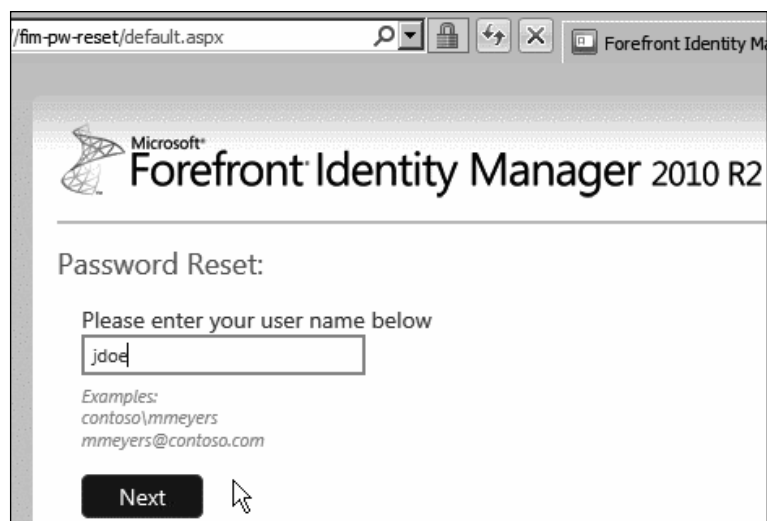


3. If he answers the gate correctly, he is given the chance to enter a new password. He then clicks **Reset**. Normally, the user can then log on using the new password immediately:



The screenshot shows a window titled "FIM Password Reset" with the Microsoft Forefront Identity Manager 2010 R2 logo. The main heading is "Enter Your New Password". Below this, there are three input fields: "Domain\Username:" with the value "AD\jdoe", "New password:" with masked characters, and "Confirm new password:" with masked characters. A note states: "Note: The user name above may display in a different format than you are accustomed to logging in with. An example of another logon format is user@example.com." At the bottom right, there are "Reset" and "Cancel" buttons.

4. As an option, the user can also go to the Password Reset portal and do the following:
  - a. Enter his username:



The screenshot shows a web browser window with the address bar displaying "/fim-pw-reset/default.aspx". The page features the Microsoft Forefront Identity Manager 2010 R2 logo and the heading "Password Reset:". Below the heading, it says "Please enter your user name below" followed by a text input field containing "jdoe". Below the input field, there are examples: "Examples: contoso\mmeyers" and "mmeyers@contoso.com". At the bottom, there is a "Next" button with a mouse cursor hovering over it.

b. Answer the questions:

Microsoft®  
**Forefront Identity Manager 2010 R2**

Verify Your Identity: Submit Your Answers

You must answer 3 of the following 3 questions.

Mothers maiden name?  
\*\*\*\*\*

Favorite car?  
\*\*\*\*

Social security number?  
\*\*\*\*\*

Next Cancel

c. Enter a new password:

Microsoft®  
**Forefront Identity Manager 2010 R2**

Password Reset: Choose Your New Password

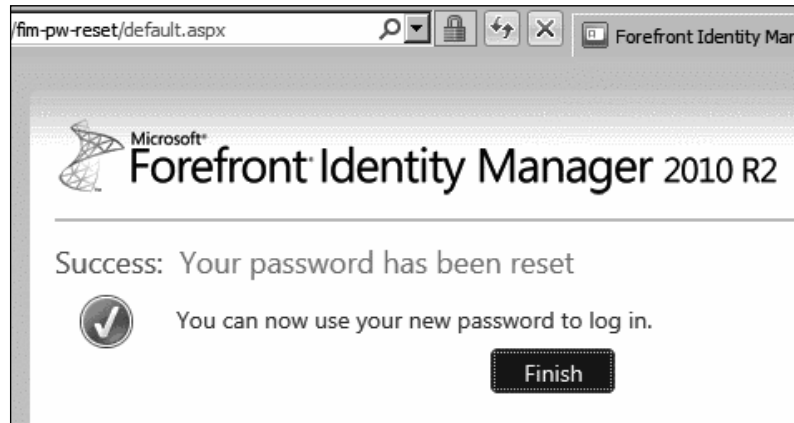
(Resetting password for **jdoe**)

Enter a new password:  
\*\*\*\*\*

Re-enter the password:  
\*\*\*\*\*

Next Cancel

- d. Finally, start using his new password:



As you can see, the user experience is quite friendly; especially the fact that it integrates with the Windows logon screen, if we install the add-ins and extensions.

## Summary

The SSPR feature is a very nice one, which can save companies that are using passwords a lot of money. In this chapter, we have seen how easy it is to enable and configure the Self-Service Password Reset feature. If you look at <http://aka.ms/FIMR2QuickStart>, you will see that there is a **QuickStart** tool to get started with SSPR even quicker.

We need to decide early on whether we want the same solution for both internal and external access to the SSPR feature. If we would like to separate them, we need to install a separate set of SSPR registration and reset portals and modify the FIM Service MPRs and workflows, accordingly.

Talking about external, *what if the identities we manage are in the cloud?* The next chapter will discuss how FIM can be used when managing *cloud* identities.

## Where to buy this book

You can buy Microsoft Forefront Identity Manager 2010 R2 Handbook from the Packt Publishing website: <http://www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book>.

Free shipping to the US, UK, Europe and selected Asian countries. For more information, please read our [shipping policy](#).

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.



[www.PacktPub.com](http://www.PacktPub.com)

**For More Information:**

[www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book](http://www.packtpub.com/microsoft-forefront-identity-manager-2010-r2-handbook/book)