FIM 2010 & MIM 2016
Security Baseline Configuration

Friday, 8 January 2016

Version 1.0 Draft

Prepared by

Peter Geelen

Sr. Premier Field Engineer - Security & Identity

Microsoft Services

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change reference
17/dec/2015	Peter Geelen	0.9	Draft for Review

Reviewers

Name	Version approved	Position	Date

Table of Contents

1 Purpose & Scope

1.1 Purpose

The purpose of this document to provide an overview of security best practices to secure your FIM and MIM infrastructure.

This document is not a detailed step by step guide but a security guideline.

It does not provide detailed hands-on guidance and screenshots to configure your environment.

1.2 In scope

This document is focused on the implementing the security best practices of the FIM server components.

1.2.1 SharePoint

FIM requires SharePoint Foundation to support the FIM Portal. This document is scoped to an infrastructure with a single server running SharePoint Foundation.

1.3 Out of scope

This document excludes a setup with a SharePoint Foundation farm.

But in the additional references section (See page: paragraph 57, paragraph 12.4 SharePoint) you will find links to plan for a SharePoint farm configuration.

This security configuration baseline does not cover detailed description on configuring secondary services, a.k.a the FIM backend, like

- IIS
- SharePoint
- SQL
- …

It’s essential to secure these platforms, work with technical platform experts.

As far as possible, the document provides pointers to detailed documentation.

2 Document & Naming Conventions

2.1 References

All references used in the documents are in the format **[<reference nr.>]**.
The complete collection of references is listed in paragraph 12, References & Authoritative resources on page 54.

2.2 FIM vs MIM

In general, the current document applies to both FIM 2010, FIM 2010 R2 as MIM 2016.
If a configuration item is particular for a version, it will be mentioned explicitly.

2.2.1 FIM components

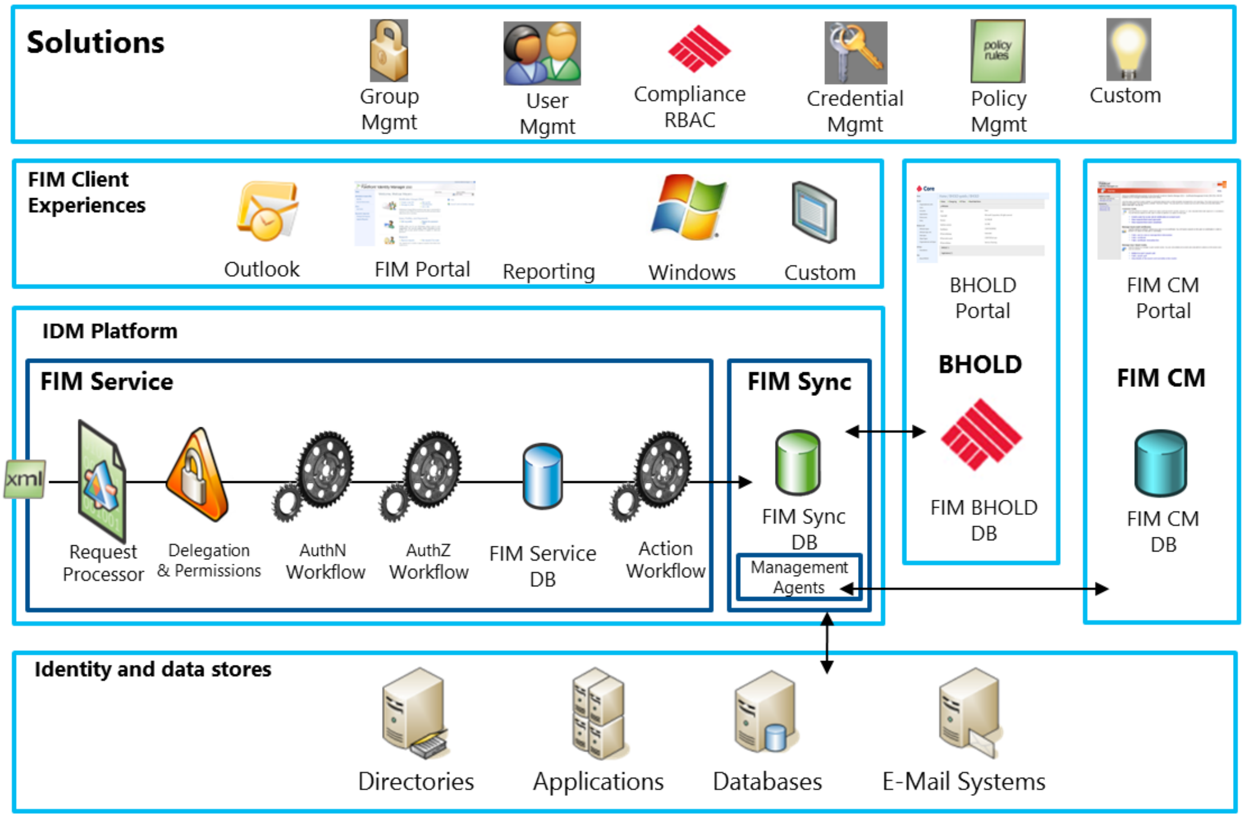


Figure 1: FIM components overview

Source: [9.] FIM 2010 Technical Overview

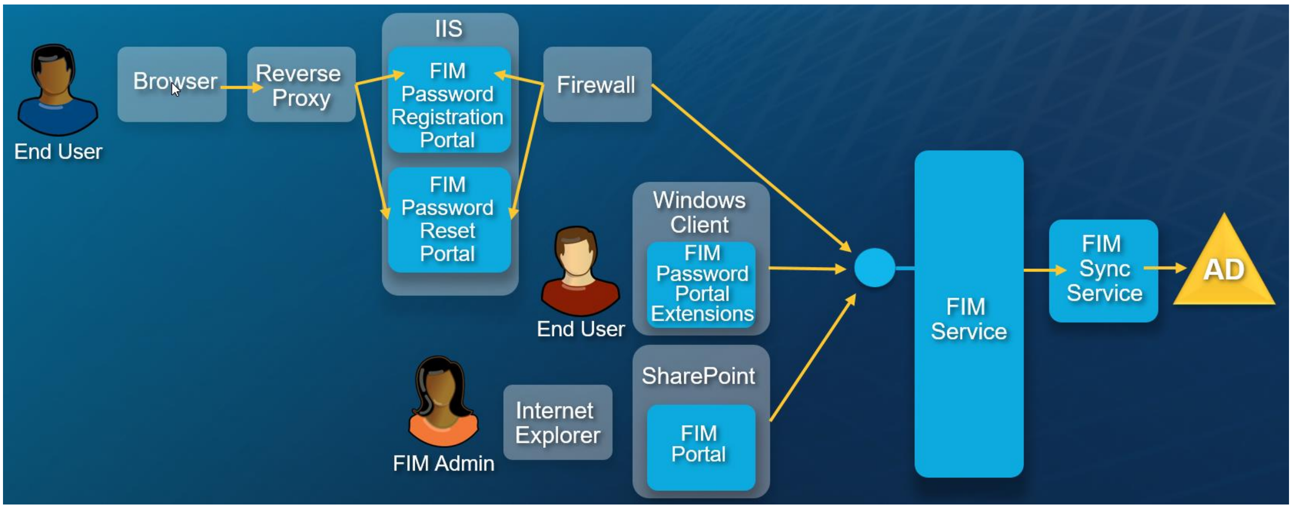


Figure 2: Typical FIM Infrastructure view

2.2.1.1 FIM Synchronization

> *"/../ As the central component necessary to* ***synchronize data across multiple connected data sources****, the synchronization service aggregates information about identities into the metaverse and provides an agentless method for connecting to each data source. The FIM Synchronization Service is the fulfillment mechanism, creating and maintaining identities in other systems /../*

2.2.1.2 FIM Service

> *"/../ The FIM Service presents the* ***Web service*** *request pipeline and is responsible for /../:*
>
> - *Request processing*
> - *All requests submitted to the Web service endpoint are processed by the FIM server and the built-in policy engine. /../"*

2.2.1.3 FIM Portal

The FIM Portal is mainly the user and administration interface with the FIM service:

> *"/../ In the earlier figure, several clients to the FIM Service are shown: The FIM Add-in for Outlook, the Password Reset Add-in, and the* ***FIM Portal*** *as well as custom clients. In addition, the FIM Synchronization Service and Exchange 2007 can be considered* ***clients of the FIM Service****.*
>
> */../*
>
> *Users are allowed to interact with the FIM Portal directly by using a Web browser and, depending upon permissions, allowed to make requests, respond to approval requests, or cancel existing pending requests./../"*

2.2.1.4 FIM SSPR Portals: Password registration and reset portals

As you noticed in the image above, there is an **essential difference** in functionality between the **FIM Portal** (as an administrative interface for the FIM Service), the **FIM Password Registration portal** and the **FIM Password reset portal**.

Essentially the FIM Portal must be hosted on SharePoint Foundation, while both FIM SSPR portals (Registration and Reset) only require IIS.

2.3 Naming conventions

The difference in behavior and the functionality of the FIM components, require a clear convention and understanding of the naming of the components to avoid any issues in the configuration.

2.3.1 Abbreviations Used

Following product abbreviations are frequently used.

For a detailed list see the at the end of the document, please refer to page 62, Chapter 14, Glossary, abbreviations & acronyms.

Acronym (alphabetically)	Refers to
FIM	Forefront Identity Manager, a.k.a. FIM 2010, FIM 2010 R2
FIM Sync, FIMSync	FIM Synchronization engine, or FIM Synchronization Service Also applies to MIM Sync engine, ILM Sync Engine, MIIS Sync engine
ILM	ILM 2007 FP1
MIIS	MIIS 2013
MIM	Microsoft Identity Manager 2016, MIM 2016
Sync	FIM Sync

This also means that:

- “FIM Service” IS NOT “FIM Sync”
- “FIM Service” IS NOT “FIM Sync Service”
- The “FIM service - Service Account” is NOT the “FIM Sync Service – Service Account”

✦ IMPORTANT

It’s critical to use the proper terminology in your documentation and communication, as a mix up of the naming is a very common mistake which results in highly critical configuration issues in your FIM environment.
In most of the cases it’s nearly impossible to fix these issues without impact to your production environment.

2.4 Account types

To properly setup your environment, you’ll need to use different accounts.

According the use of these accounts we’ll define 4 account types

- Service account (SVCA)
- Technical account (TA)
- Functional account (FA)
- Personal account (PA)

2.4.1 Core account differentiators

	Account Type			
Task type	Service Account	Technical Account	Functional Account	Personal Account
Run Background Service	YES	NO	NO	NO
Only run Specific Program	YES	NO	NO	NO
Specific Task or script	NO	YES	NO	NO
Interact with desktop/Physical Logon	NO	NO	YES	YES
Highly Privileged Rights	NO	NO	YES	YES
Direct Link to physical person (link to HR)	NO	NO	NO	YES
Example of typical use	(1)	(2)	(3)	(4)

2.4.1.1 Examples of typical use

Example	Type of use
(1)	‘FIM Service’ service, ‘FIM Sync’ Service, ‘SQL Database server’ service, …
(2)	Task Scheduler account to run FIMSync scripts on an **automated** schedule
(3)	FIM Installer with admin access to Local Server & SQL, not used to manage daily operations
(4)	Personal Administrator account to manage daily operations

2.4.2 Detailed description & definition

2.4.2.1 Service account (SVCA)

A service account is

- **not linked** to a physical person.
- a user account that is created explicitly to provide a security **context for services** running on Microsoft® Windows® Server.

This service account typically runs the **services in the background**, with **no user interaction**.
Interaction with the **user desktop** is minimized, and should be **none**.

⚠ **CAUTION**

Until further notice, FIM and MIM (any version) DO NOT SUPPORT virtual or managed accounts.
You cannot even complete the installation if you try.

These service account run a specific service, not scheduled tasks. For scheduled tasks a technical account is used.

Security

Due to the fact that these accounts run in the background, the **rights & permissions** of these accounts must be reduced to the absolute **minimum**. Service account must not run as a Highly Privileged Account (HPA).

Although service accounts are usually exempted from the password policy for personal user accounts, it’s highly advised to change the password on a regular base (eg, 1-2 times a year).

Please consider, changing a service account password might break the application functionality.

Service account require **complex passwords**.

Audit & Monitoring

Due to the specific target of a service account, it does require monitoring for abnormal activity (outside the scope of the account).

Inappropriate use

Do NOT use the service account for any other purpose like

- Running scheduled task
- Installation of applications
- Administrative tasks
- HPA
- Daily administrative operational tasks
- …

2.4.2.2 Technical account (TA)

A technical account is

- **NOT linked to a physical person**.
- **NOT a service account** as it is not used to run services,
- Used to run a **specific task** (or a combination of tasks) on a regular, non-continuous base.

In the FIM context, for example technical accounts will be used for:

- Running scheduled tasks (using the account in the scheduled task configuration)
- Running PowerShell scripts
- MA (Management Agent) configuration
- …

Inappropriate use

Do NOT use the technical account for any other purpose like

- Running Windows services
- Installation of applications
- Administrative tasks
- HPA
- Daily administrative operational tasks
- …

2.4.2.3 Functional account (FA)

A functional account is **NOT directly linked** to a physical person. But it does require **physical logon**, it's linked to tasks a physical person must execute with **desktop interaction**.

In some cases, a functional account is required to **install programs** or to configure the **root application administrator** account.

An administrative functional account usually is a highly privileged account (HPA), with **elevated rights** on the IT infrastructure.

This type of account must never be used for normal, daily, operational tasks.

It's best practice to remove rights & permission when the account is not use, and only add the privileges when needed, removing them when the required task is completed.

For example:

- During installation of FIM Sync/FIM service, you need local admin rights on the Windows server and you need SA rights on SQL, which are highly sensitive.
- After installation of FIM you remove the privileges
- Before installing a hotfix, you elevate the account. Then you install the hotfix and after installation you remove the account form the elevated rights.

Security risk

Functional accounts are highly susceptible to hacks or security issues as these accounts are not linked to daily operations of a physical person.

The use of these account needs to be monitored closely.

Furthermore, the passwords of these account must be managed under the 4-eyes principle, and changed after use.

Advisory

- Apply the 4-eyes-principle,
- Split the password,
- Store the password components separately in a secured location guarded by 3rd person like CISO

Typical use

- Application installation
- Installation of hotfixes

2.4.2.4 Personal Account (PA)

Primarily a personal account is **directly linked** to a **physical person**.

As a consequence, it is directly linked to a person lifecycle.

This means it is created when a person joins the company and it gets (or must get) **deprovisioned** when a person leaves the company.

Also, it needs to comply to the **password management** rules, changing passwords on a regular basis.

An administrative personal account usually is a highly privileged account (HPA), with **elevated rights** on the IT infrastructure.

Security risk

Personal accounts are highly susceptible to hacks or security issues as these accounts can be easily found based on the social engineering.

Due to the link to the personal lifecycle, these personal accounts must not be used for automated operations, scheduled tasks or repeated installation tasks (ref. use of functional accounts).

3 Generic security principles

3.1 References

Following authoritative references are used in this section.

- **[1.]** Microsoft Security Intelligence Report
- **[19.]** SQL Server 2012 Security Best Practice Whitepaper

3.2 Threats

In the Microsoft Security Intelligence Report (SIR) you find a section on Managing Risk.

The report addresses a set of security threats and risks with related countermeasures.

This document has a particular focus on **prevention and limiting the impact of security breaches**.

From the SIR: section Protecting Your Organization, Prevent and Mitigate Security Breaches

> *"Enforce the idea of least privilege, wherein computer accounts are given only those permissions required to perform a job function.*
>
> */../*
>
> *Develop and implement plans to reduce the likelihood of common types of breaches to mitigate their impact should they occur and to respond if the mitiga-tions are not fully effective.*

3.3 Principle of least privilege (PoLP)

As explained in the "SQL Server 2012 Security Best Practices - Operational and Administrative Tasks":

> *"When choosing service accounts, consider the principle of least privilege.*
>
> *The service account should have exactly the privileges that it needs to do its job and no more privileges.*
>
> *You also need to consider account isolation; the service accounts should not only be different from one another, they should not be used by any other service on the same server. "*

And more:

> *Making the "service account an administrator, at either a server level or a domain level, or using Local System, bestows too many unneeded privileges. "*

As explained on WikiPedia:

> *"The principle means giving a user account only those privileges which are essential to that user's work.*
>
> *For example, a backup user does not need to install software: hence, the backup user has rights only to run backup and backup-related applications. Any other privileges, such as installing new software, are blocked.*
>
> *The principle applies also to a personal computer user who usually does work in a normal user account, and opens a privileged, password protected account (that is, a superuser) only when the situation absolutely demands it.*
>
> *When applied to users, the terms least user access or least-privileged user account (LUA) are also used, referring to the concept that all user accounts at all times should run with as few privileges as possible, and also launch applications with as few privileges as possible. Software bugs may be exposed when applications do not work correctly without elevated privileges.*

> *The principle of least privilege is widely recognized as an important design consideration in enhancing the protection of data and functionality from faults (fault tolerance) and malicious behavior (computer security)."*

Considering security, the principle of least privilege is applied to achieve following targets:

- Minimizing risk
- Better security
- Better system stability
- Ease of deployment

3.3.1 Rule of thumb

The service account should have exactly the privileges that it needs to do its job and no more privileges.

That also implies to use another account if different, unrelated tasks must be configured.

3.4 Privilege separation

Source: [7.] Privilege separation

> *"In computer programming and computer security, privilege separation is a technique in which a program is divided into parts which are limited to the specific privileges they require in order to perform a specific task. This is used to mitigate the potential damage of a computer security attack."*

To implement the PoLP or privilege separation, you can use SoD (Segregation of Duties a.k.a Separation of Duties).

3.4.1 Rule of thumb

The FIM documentation on TechNet clearly references to **use separate accounts** with **separate rights and permissions** to protect the various functional FIM components and platforms, related functional processes and data flows.

3.5 SoD (Segregation of duties) & Account Isolation

SoD (Segregation of duties) is also known as '**separation** of duties'.

SoD is tightly related to the principle of least privilege, explained in the previous chapters.

While privilege separation handles the split of **rights and permissions**, SoD rather handles the separation of duties and **tasks**.

Although SOD essentially is targeted at the tasks of physical persons, it should be applied to other account types too, for similar reasons.

In that case it's referenced as **account isolation**.

The focus on the task, is really helpful to define the required accounts and groups to execute specific task in your environment.

3.5.1 Rule of thumb

When focusing on FIM functionality, the **different FIM components** serve a **different purpose**, executing **different tasks** thus you need **different accounts**.

As mentioned before, the FIM documentation on TechNet clearly references to **separate accounts** and **separate groups** with separate rights and permissions to protect the various FIM components, related processes and data flows.

3.5.2 More info

Reference:

- [5.] Segregation of duties/ Separation of duties

3.6 4-eyes principle

Reference: [8.] http://whatis.techtarget.com/definition/four-eyes-principle

> *"The four eyes principle is a requirement that two individuals approve some action before it can be taken. The four eyes principle is sometimes called the two-man rule or the two-person rule."*

3.7 Number of accounts vs. security risk

Only configure the required accounts related to the FIM feature you need to implement. Not more, but also not less.

The more you install, the more attack surface you expose.

For example, if you only implement FIM Sync, there is not need to implement the FIM Service required accounts.

But IF you implement a certain component, like FIM sync, you MUST implement ALL required accounts to guarantee security best practices like account isolation, SoD, PoLP.

Violation of security best practices also increases the attack surface to your environment.

For example, if you implement FIM Sync and FIM Service, it's very a bad practice to use one single account for multiple services, management agents, technical and functional accounts and/or administrative accounts.

You don't need a lot of imagination to estimate the impact of breaching a single account, compared to the effort of managing multiple accounts or the effort required to breach multiple isolated accounts.

3.8 Additional reading

More information is available in paragraph 13.1, Security Best practices at page 59.

4 FIM security principles

4.1 References

Authoritative references:

- **[10.]** Forefront Identity Manager 2010 R2 Best Practices General
- **[19.]** Forefront Identity Manager 2010 R2 Best Practices for Security

4.2 Best practices

4.2.1 Required settings

Items	**Ref.**	**Description**
Infrastructure Security	**[10.]**	Proper setup of FIM 2010 R2 in your test lab and careful planning of your migration from test lab to production is essential to minimizing deployment problems.
Back up	**[10.]**	After installing FIM, make a backup copy of the encryption keys. You need a copy of the encryption keys to restore from a backup, or to change the Microsoft Forefront Identity Manager 2010 R2 service account. For more information, see MIISkmu: Encryption Key Management Tool.
Backup	**[10.]**	Test your backup and restore procedures for Microsoft Forefront Identity Manager.
DRP	**[10.]**	Set a deletion threshold in your run profile steps to limit the number of accidental deletions.

4.3 Best practices for security

4.3.1 Required settings

Items	**Ref.**	**Description**
Account Security	**[19.]**	Control access with Microsoft Forefront Identity Manager security groups.
Physical Access	**[19.]**	Restrict physical access to computers to trusted personnel.
Least Privilege	**[19.]**	Implement user rights and permissions to restrict software access to trusted accounts.
Account Security	**[19.]**	Enforce strong password policies for **all user accounts**.
Account Security	**[19.]**	Lock down the Microsoft Forefront Identity Manager service account
Account Security	**[19.]**	Periodically change the Microsoft Forefront Identity Manager service account password.

5 Compact Check list

5.1 Legend

5.1.1 Check boxes

Icon	Explanation
☐	Open configuration item
☑	Checked, fixed, installed, action applied
☒ **(+ Reason)**	Declined, blocked, not applicable (N/A), not used, excluded from configuration

5.1.2 Account types

See paragraph 2.4 Account types for detailed explanation.

According the use of these accounts we'll use 4 account types

- Service account (SVCA)
- Technical account (TA)
- Functional account (FA)
- Personal account (PA)

5.1.3 Location (LOC)

Code	Explanation
D	Domain
L	Local, on server

5.1.4 Important (SEV)

The indication of importance is related to the risk profile of the account.

This setting provides a basic assessment of the impact & risk of not-installing or using this account.

SEV	Countermeasure	Impact & risk	Explanation (examples)
HIGH **(RED)**	Configuration Required	Direct, high Impact Critical risk on FIM systems, linked systems & general infrastructure Real & proven danger High impact on recovery Impact of risk is critically higher than operational burden	High business impact Risk of setting up a configuration that cannot be recovered using a normal DRP planning. Critical impact on security, violation of common security best practices Critical impact on linked systems like HR, AD, O365
MEDIUM **(ORANGE)**	Strongly advised to follow best practice	Possible, Realistic danger Significant impact on FIM systems, linked systems & general infrastructure Impact of risk is significantly higher than operational burden	Important recovery needed, exceeding normal operational mode or SLA agreements
LOW **(YELLOW)**	Advised to follow best practice	Indirect impact Low risk Theoretical, low frequency Easy to recover Impact of risk is higher or equal than operational burden	Important recovery needed but within normal operational mode or SLA agreement
OPTIONAL **(GREEN)**	Suggestion to follow best practice	Optimization, additional security layer. Impact of risk is equal or lower than operational burden	Limited to no business impact

5.2 Pre-installation: Backend configuration

5.2.1 SPN

	Importance	LOC	Acct. Type	Account Reference	Name (to fill)
□	HIGH	D	SPN	MSSQLsvc/<SQLDatabase Server>	SQL Database Account
□	HIGH	D	SPN	FIMService/<FIM Service Server>	FIM Service Account
□	HIGH	D	SPN	HTTP/<FIM Portal Alias>	SharePoint Service Account
□	HIGH	D	SPN	HTTP/<pwd registration portal server>	Pwd Registration Server Account
□	HIGH	D	SPN	HTTP/<passwordreset portal server>	Password Reset Server Account
□	HIGH	D	SPN	HTTP/<FIM CM Server>	FIM CM Web Pool Agent Account

5.3 Pre-installation: Account creation

5.3.1 Back End

5.3.1.1 SQL

Reference:

- [19.] Server Configuration - Service Accounts

This section only has informational purposes, but has been added as a reminder to secure the FIM Back end services.

From: Server Configuration - Service Accounts:

> *"If you configure services to use domain accounts, Microsoft recommends that you configure service accounts individually to provide least privileges for each service, where SQL Server services are granted the minimum permissions they need to complete their tasks."*

	Importance	LOC	Acct. Type	Account Reference	Name (to fill)
□	HIGH	D	Service	SQL Server Database engine acct.	<domain>\<account>
□	HIGH	D	Service	SQL Server Agent service* acct.	<domain>\<account>
□	HIGH	D	Service	SQL Server Analysis Services acct.	<domain>\<account>
□	HIGH	D	Service	SQL Server Reporting Services acct.	<domain>\<account>
□	HIGH	D	Service	SQL Server Browser acct.	<domain>\<account>

There are 4 more accounts for the core SQL services, but this is outside the scope of this document.

Full details are available in the SQL Server whitepaper: SQL Server 2012 Security Best Practices - Operational and Administrative Tasks.

From the white paper:

> *"The SQL Server Agent service account requires **sysadmin** privilege in the SQL Server instance that it is associated with. In SQL Server 2005 and above, SQL Server Agent job steps can be configured to use proxies that encapsulate alternate credentials."*

5.3.1.2 SharePoint

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Functional	SharePoint Setup administrator acct*	<domain>\<account>
□	HIGH	D	Service	Farm service account	<domain>\<account>
□	LOW	D	Service	search service account	<domain>\<account>
□	LOW	D	Service	search content access account	<domain>\<account>
□	LOW	D	Service	SharePoint Application pool account	<domain>\<account>

5.3.2 All FIM Platforms

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Functional	FIM installer administrator account*	<domain>\<account>

5.3.3 FIM Synchronization

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Service	FIM Sync service SVCA	<domain>\<account>
□	HIGH	D	Security Group	FIMSyncAdmins	<domain>\<account>
□	HIGH	D	Security Group	FIMSyncOperators	<domain>\<account>
□	HIGH	D	Security Group	FIMSyncJoiners	<domain>\<account>
□	HIGH	D	Security Group	FIMSyncBrowse	<domain>\<account>
□	HIGH	D	Security Group	FIMSyncPasswordSet	<domain>\<account>
□	HIGH	D	Technical	FIM Task scheduler	<domain>\<account>

5.3.3.1 FIM Sync Management agents

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Technical	ADMA Account	<domain>\<account>
□	HIGH	D	Technical	FIMMA Account	<domain>\<account>
□	HIGH	D	Technical	SQL MA Account	<domain>\<account>
□	HIGH	D	Technical	Other Management agents: - 1 account per type of MA And by preference 1 account per MA.	<domain>\<account>

5.3.4 FIM Service

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Service	FIM service SVCA	<domain>\<account>
□	HIGH	D	Technical	FIMMA Account	<domain>\<account>

5.3.5 FIM Portal

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	MEDIUM	D	Functional	Backup Portal Administrator	<domain>\<account>
□	HIGH	D	Service	FIM Portal - Application Pool Account	<domain>\<account>

5.3.6 FIM SSPR Registration Portal

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Service	FIM SSPR Registration Portal - Application Pool Account	<domain>\<account>

5.3.7 FIM SSPR Reset Portal

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Service	FIM SSPR Reset Portal - Application Pool Account	<domain>\<account>

5.3.8 FIM CM

Source: [36.] Create an OU and User Accounts for FIM CM Agents

> *"The following table summarizes the accounts and permissions required by FIM CM. You can allow the FIM CM create the following accounts automatically, or you can create them prior to installation. The actual account names can be changed. If you do create the accounts yourself, consider naming the user accounts in such a way that it is easy to match the user account name to its function."*

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Technical	FIM CM Agent	<domain>\<account>
□	HIGH	D	Technical	FIM CM Authorization Agent	
□	HIGH	D	Technical	FIM CM CA Manager Agent	
□	HIGH	D	Technical	FIM CM Enrollment Agent	
□	HIGH	D	Technical	FIM CM Key Recovery Agent	
□	HIGH	D	Technical	FIM CM Web Pool Agent	

5.4 Pre-installation: Account lock down

5.4.1 All FIM Platforms

	Importance	LOC	Account Type	Account Reference	Procedure
□	HIGH	D	Functional	FIM Installer account	Just before installation[1] - Grant local admin rights - Grand SQL SysAdmin

[1] This applies both to fresh installation of FIM component or implementation of an hotfix or service pack. Only during implementation of a service pack, the installation account that runs the installation needs the elevated rights. Only DURING installation, not before, not after.

5.4.2 FIM Sync

	Importance	LOC	Account Type	Account Reference	Procedure
□	HIGH	D	Service	FIM Sync Svc SVCA	Lock down FIM Sync Service SVCA
□	HIGH	D	Technical	FIM ADMA	Lock down AD MA Technical Account
□	HIGH	D	Security Groups	Security Groups	Minimize memberships to FIM Sync security groups
□	HIGH	D	Security Groups	Security Groups	Minimize administrative memberships to the FIM Servers

5.4.2.1 FIM Sync Management agents

	Importance	LOC	Account Type	Account Reference	Procedure
□	HIGH	D	Technical	FIM MA	Lock down the FIM MA technical account
□	HIGH	D	Technical	FIM MA	Block/Filter the administrative accounts from the FIM Service connector space
□	HIGH	D	Technical	FIM ADMA	Replicating Directory Changes
□	HIGH	D	Technical	FIM ADMA	Lock down the account to the minimum required permissions to the minimum required containers
□	HIGH	D	Technical	SQL MA	Lock down the account to the minimum required permissions to the minimum required tables
□	HIGH	D	Technical	Other MA	<TBD>

5.5 Post-Installation: Set operational admins

5.5.1 FIM Portal

	Importance	LOC	Account Type	Account Reference	Procedure
□	HIGH	D	Functional	FIM Portal Backup Account	Add a functional account as backup root account to the FIM Potal

5.6 Hotfix installation

5.6.1 All FIM Platforms

	Importance	LOC	Account Type	Account Reference	Procedure
□	HIGH	D	Functional	FIM Installer account	Just before hotfix installation[2] Grant local admin rights Grand SQL SysAdmin

[2] This applies both to fresh installation of FIM component or implementation of an hotfix or service pack. Only during implementation of a service pack, the installation account that runs the installation needs the elevated rights. Only DURING installation, not before, not after.

6 Pre-installation: Securing the FIM backend infrastructure

6.1 SQL Server

Although FIM heavily relies on SQL Server, SQL security configuration is out of scope for FIM configuration. Nevertheless, proper configuration of these accounts is key and it should be handled in cooperation with an SQL expert.

6.1.1 References

Please check the reference below to properly secure your SQL infrastructure you use to support FIM.

- **[42.]** Guidelines on choosing Service Accounts for SQL Server Services.
- **[46.]** SQL Server 2012 Security Best Practice Whitepaper

The Section "Service Account selection and management", says:

> *"/../**The Local System account** is not only an account with **too many privileges**, but it is a **shared account** and might be used by other services on the same server. Any other service that uses this account has the same set up privileges as the SQL Server service that uses the account.*
>
> *Although **Network Service** has network access and is not a Windows superuser account, it is a shareable account. This account is useable as a SQL Server service account only if you can ensure that no other services that use this account are installed on the server.*
>
> ***Using a local user or domain user that is not a Windows administrator is the best choice.***
>
> *If the server that is running SQL Server is part of a domain and must access domain resources such as file shares or uses linked server connections to other computers running SQL Server, a domain account is the best choice.*
>
> *If the server is not part of a domain (for example, a server running in the perimeter network (also known as the DMZ) in a Web application) or does not need to access domain resources, a local user that is not a Windows administrator is preferred.*
>
> *Creating the user account that will be used as a SQL Server service account is easier in SQL Server 2005 than in previous versions. When SQL Server 2005 is installed, a Windows group is created for each SQL Server service, and the service account is placed in the appropriate group. To create a user that will serve as a SQL Server service account, simply create an "ordinary" account that is either a member of the Users group (non-domain user) or Domain Users group (domain user). During installation, the user is automatically placed in the SQL Server service group and the group is granted exactly the privileges that are needed.*
>
> *If the service account needs additional privileges, the privilege should be granted to the appropriate Windows group, rather than granted directly to the service user account. This is consistent with the way access control lists are best managed in Windows in general. /../"*

The FIM 2010 deployment guide also discusses the SQL security requirements.

Source: **[12.]** Before You Begin

Before you install the FIM Service, certain tasks should be completed and verified on the server that is running SQL Server.

If you are using FIM Reporting, you will need to create two additional service accounts:

- SQL Reporting Service Account
- SQL Analysis Service Account

Ensure that the service accounts used by SQL Server Database and SQL Server Agent are either domain accounts or built-in service accounts (for example, Network Service). You cannot use local computer accounts.

When you configure the service accounts for SQL Server, consult the following articles:

- **[47.]** Service Account Types Supported for SQL Server Agent:
- **[48.]** Selecting an Account for the SQL Server Agent Service

Important

The SQL Server service account should not be a local computer account. A local account cannot impersonate domain accounts and the FIM Service will not behave as expected.

6.2 IIS

6.2.1 References

Please check full details in the reference below to properly secure your IIS infrastructure you use to support FIM.

- **[54.]** Security Best Practices for IIS 8

6.2.2 Action items

Please find below a list of configuration items relevant to FIM, but do remember the complete list has more actions to achieve an IIS lock down.

Items	Action
Installation and Configuration	Install only the IIS modules you need.
Web Application Isolation	Isolate web applications. Separate different applications into different sites with different application pools.
Web Application Isolation	Implement the principle of least privilege. Run your worker process as a low privileged identity (virtual application pool identity) that is unique per site.
Authentication	Disable anonymous access to server directories and resources.
Application Pool Identities	Don't use the built-in service identities (such as Network Service, Local Service, or Local System). For maximum security, application pools should run under the application pool identity that is generated when the application pool is created. The accounts that are built in to IIS are ApplicationPoolIdentity, NetworkService, LocalService, and LocalSystem. The default (recommended) and most secure is ApplicationPoolIdentity.
Application Pool Identities	Using a custom identity account is acceptable, but be sure to use a **different account** for each application pool.

6.2.3 Exception

Reference:

- **[32.]** To allow SSPR for users that forgot their password you must allow anonymous access to the password reset portal.

6.3 SharePoint

Essentially the SharePoint configuration is out-of-scope for this document, but proper configuration of the SharePoint environment is essential. Please work with a SharePoint expert to secure your environment.

This section only has informational purposes, but has been added as a reminder to secure the FIM Portal back-end services.

6.3.1 References

Please check the reference below to properly secure your SQL infrastructure you use to support FIM.[7]

- **[51.]** Initial deployment administrative and service accounts (SharePoint Server 2010

❖Important

We recommend that you install SharePoint Server 2010 by using least-privilege administration.

6.3.2 Accounts

Account	Purpose	Requirements
SQL Server service account	The SQL Server service account is used to run SQL Server. It is the service account for the following SQL Server services: - MSSQLSERVER - SQLSERVERAGENT If you do not use the default SQL Server instance, in the Windows Services console, these services will be shown as the following: - MSSQL$InstanceName - SQLAgent$InstanceName	Use either a Local System account or a domain user account. If you plan to back up to or restore from an external resource, permissions to the external resource must be granted to the appropriate account. If you use a domain user account for the SQL Server service account, grant permissions to that domain user account. However, if you use the Network Service or the Local System account, grant permissions to the external resource to the machine account (domain_name\SQL_hostname$). The instance name is arbitrary and was created when Microsoft SQL Server was installed.
(Sharepoint) **Setup user account**	The Setup user account is used to run the following: - Setup - SharePoint Products Configuration Wizard	- Domain user account. - Member of the Administrators group on each server on which Setup is run. - SQL Server login on the computer that runs SQL Server. - Member of the following SQL Server security roles: - securityadmin fixed server role - dbcreator fixed server role If you run Windows PowerShell cmdlets that affect a database, this account must be a member of the **db_owner** fixed database role for the database.

Account	Purpose	Requirements
Server farm account or database access account	The server farm account is used to perform the following tasks: - Configure and manage the server farm. - Act as the application pool identity for the SharePoint Central Administration Web site. - Run the Microsoft SharePoint Foundation Workflow Timer Service.	- **Domain** user account. Additional permissions are automatically granted for the server farm account on Web servers and application servers that are joined to a server farm. The server farm account is automatically added as a SQL Server login on the computer that runs SQL Server. The account is added to the following SQL Server security roles: - **dbcreator** fixed server role - **securityadmin** fixed server role - **db_owner** fixed database role for all SharePoint databases in the server farm

7 Pre-installation: Securing FIM Components

7.1 FIM general

7.1.1 SPN

7.1.1.1 References

Please check the reference below to properly secure the require SPN entries.

- **[16.]** FIM 2010 R2 Kerberos Settings (SPN Configuration)

Please refer to the references section at the end of the guide, for more details on Kerberos settings.

7.1.1.2 Description

From: [16.] FIM 2010 R2 Kerberos Settings (SPN Configuration):

> *”/../ 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).*

7.1.1.3 FIM SPN Configuration

From: [16.] FIM 2010 R2 Kerberos Settings (SPN Configuration):

Syntax configuration examples have been omitted in this guide.

SPN	Account	Description
MSSQLsvc/<SQLDatabase Server>	SQL Database Account	SPN required for the FIM Service database. Allows clients the ability to locate an instance of SQL.
FIMService/<FIM Service Server>	FIM Service Account	SPN required for the FIM Service. Allows clients the ability to locate an instance of the FIM Service.

SPN	Account	Description
HTTP/<FIM Portal Alias>	SharePoint Service Account	This is a requirement because SharePoint runs as a "farm" - even in single-server configurations - you have to run the site and authentication under the app pool account... AND still set up your SPN's.
HTTP/<passwordregistration portal server>	Password Registration Server Account	The SSPR portals use IIS 7.0/7.5. IIS 7.0/7.5 has an authentication feature - 'Enable Kernel Mode Authentication'. With this feature the Kerberos ticket for the requested service is decrypted using Machine account (Local system) of the IIS server. It no longer depends upon the application pool Identity for this purpose. The following assumes that the password registration and reset portals are being accessed through a custom host header. In this instance the SPN is required only for the IIS machine account and not for our FIM Password Service account.
HTTP/<passwordreset portal server>	Password Reset Server Account	The SSPR portals use IIS 7.0/7.5. IIS 7.0/7.5 has an authentication feature - 'Enable Kernel Mode Authentication'. With this feature the Kerberos ticket for the requested service is decrypted using Machine account (Local system) of the IIS server. It no longer depends upon the application pool Identity for this purpose. The following assumes that the password registration and reset portals are being accessed through a custom host header. In this instance the SPN is required only for the IIS machine account and not for our FIM Password Service account.
HTTP/<FIM CM Server>	FIM CM Web Pool Agent Account	This is a special case even though we are running on IIS 7.0/7.5. In this instance you must ensure that useAppPoolCredentials is set to true. This will force IIS to use the appPoolCredentials to decrypt the ticket. KernelModeAuthentication is still enabled in this instance.

7.1.1.4 SPN Delegation

> *"In a deployment with multiple FIMServices, ensure that each FIMService has constrained delegation configured so that each FIMService can successfully communicate to each other in order for Workflow Approvals to work properly. Approval Responses from users can come from any Portal or if Exchange is enabled from the FIMService that is polling. In all cases, the Approval Response will be directed to the FIMService machine that processed the original Request so cross-server communication: FIMPortal -> FIMService AND FIMService -> FIMService must work properly."*

7.1.2 Changing FIM Service account

7.1.2.1 References

Source: [11.] Change the Forefront Identity Manager 2010 R2 Synchronization Service Account

The procedure is described in detail in the reference TechNet page.

Before you change the account of any of the FIM Services, make sure you can roll-back, so you need to have a DRP plan in place (and a working backup-restore…)

7.1.2.2 Required settings

Items	Ref.	Description
Account Security	[11.]	To complete this procedure, you must be logged on as a member of the FIMSyncAdmins security group.
Account Security	[11.]	See the Account security requirement of the FIM Sync service account, section below.
Backup	[11.]	Back up the encryption key set by running MIISkmu.exe.
Installation	[11.]	Run Setup from the FIM installation CD in maintenance mode and change the Microsoft Forefront Identity Manager 2010 R2 service account credentials from the old account to the new one. During the setup process, you are prompted for the encryption key set

7.1.2.3 Risks

Items	Ref.	Description
Attacks	[11.]	To prevent attacks to the registry and system files by malicious users, it is strongly recommended that you do not add the Microsoft Forefront Identity Manager 2010 R2 service account to the local administrators group.
Account Lock down	[11.]	**Local Security Policy** - **Deny logon locally** - **Deny access to this computer from the network** - **Deny logon as a batch job** - **Deny log on through Terminal Services**. No additional lock-down procedures are needed to secure the Microsoft Forefront Identity Manager 2010 R2 service account in a domain. By default, you cannot log on locally with the Microsoft Forefront Identity Manager 2010 R2 service account.

7.2 FIM Setup

7.2.1 FIM setup account – functional account

7.2.1.1 References

- **[12.]** Before you begin
- **[17.]** Considerations for New Installation of FIM 2010 R2
- **[18.]** Installing the FIM 2010 R2 Server Components
- **[5.]** Segregation of duties

7.2.1.2 Required settings

Items	Ref.	Description
Account type: domain account	[18.]	You must create a user account to run installation of the FIM components. This installer account must be a **domain user** account. The most important reason is that the FIM installer account is assigned root administrator in the FIM service and portal, during the installation you need SQL sysadmin (SA) rights, which is by preference a domain joined SQL server with Windows authentication.

Items	Ref.	Description
Account Security: SQL	[18.]	**<u>ONLY DURING INSTALLATION</u>** To be able to install FIM Synchronization Service or FIM Service, the account must be a SQL sysadmin. The account that you use does not have to be a SQL sysadmin after the installation is complete. The user account used to install the FIM Service must be granted the sysadmin role in SQL Server. **By default, members of the Local Administrators group do not have the necessary permissions.** Unless the user account is either the built-in administrator account, or the user account used to install SQL Server, then the user account must be granted the sysadmin role in SQL Server.
Account Security: Sharepiont	[18.]	To be able to install the FIM Portal, the account must be a SharePoint administrator. To be able to install the FIM Portal, it is assumed that SharePoint is installed with the default settings, that the default SharePoint site can be reached using the address specified in the user interface, and that the user who is installing the FIM Portal is authorized as an administrator of that SharePoint site.
Account Security	[18.]	**<u>ONLY DURING INSTALLATION</u>** This account **should be** a local administrator account.
Account Security	[18.]	**<u>ONLY DURING INSTALLATION</u>** The FIM installer accounts should **be member of the local administrators** group.
Account Security	[18.]	The FIM installer account **should only be** a **member of the security group** FIMSyncAdmins.
Account security	[18.]	Use the following restrictions on the FIM installer account: • Deny logon as a batch job • Deny run as a service
Account separation	[5.]	Due to the fact that the FIM installer account is only used to install FIM component, during initial setup or during application of an hotfix, do not use this account for other purposes. DO NOT - use the FIM Installer account for operational, day-to-day management. - Use the FIM installer account as service account As other services require other privileges, the PoLP demands to use separate accounts.

7.2.1.3 Risks

Items	Ref.	Description
Same account	[18.]	The FIM Sync Service account has HPA access to the FIM Sync Service operations, using the same account bestows too many unneeded privileges to the FIM Sync service account

7.2.2 FIM Synchronization Service – service account

7.2.2.1 References

- **[22.]** FIM 2010 R2: Same Account being used for FIM Synchronization Service and FIM MA
- **[23.]** FIM 2010 R2: FIM Service or the FIM Synchronization Service Account does not have Deny Logon As Batch Job set
- **[12.]** Before you begin
- **[17.]** Considerations for New Installation of FIM 2010 R2

7.2.2.2 Required settings

Items	Ref.	Description
Account type: domain account	[12.]	You must create a service account to run the FIM Synchronization Service. This service account must be a domain service account.
Account Security	[12.]	This account should **not be a local administrator account**.
Account Security	[12.]	The service accounts should **not be members of the local administrators** group.
Account Security	[12.]	The FIM Synchronization Service SVCA should not be a **member of the security groups** that are used to control access to FIM Synchronization Service (groups starting with FIMSync, for example, FIMSyncAdmins).
Account security	[12.]	On the server running the **FIM Synchronization Service**, you must restrict only the **FIM Synchronization Service service account** and not the FIM Service service account. On the server running the **FIM Service**, you must only **restrict the FIM Service service account**, and not the FIM Synchronization Service service account. Use the following restrictions on the service accounts: • Deny logon as a batch job • Deny logon locally • Deny access to this computer from the network
Account separation	[12.], [17.]	Due to the fact that the FIM Synchronization account is only used to run the FIM Synchronization services, do not use this account for other purposes. As other services require other privileges, the PoLP demands to use separate accounts.
Account Separation	[12.], [17.]	The FIM Sync service SVCA must not be part of the FIM Sync Security Groups The FIM Service SVCA must be part of the FIM Sync Admins security group. (See Ref. 4) **This requirement excludes the use of 1 single account for both the FIM Service and the FIM Synchronization service.**

7.2.2.3 Exceptions

Items	Ref.	Description
Password reset	[12.]	If you are deploying password reset, do not use the **Deny access to this computer from the network restriction** option.

7.2.2.4 Risks

Items	Ref.	Description
Same account	[12.]	Due to the fact that the FIM Synchronization account is only used to run the FIM Synchronization services, do not use this account for other purposes. As other services require other privileges, the PoLP demands to use separate accounts.
Same account	[12.]	If you choose to use the same account for both service accounts and you separate the FIM Service and the FIM Synchronization Service, you cannot set **Deny access to this computer from the network** on the FIM Synchronization Service server. If access is denied, that action prohibits the FIM Service from contacting the FIM Synchronization Service to change configuration and manage passwords.
Same account	[12.]	The FIM Sync Service account has HPA access to the FIM Sync Service operations, using the same account bestows too many unneeded privileges to the FIM Sync service account

7.2.3 FIM Administrative Security Groups

7.2.3.1 References

- [13.] Using Security Groups

7.2.3.2 Purpose

During installation/reconfiguration FIM will need 5 groups to manage security in FIM Sync.

3 Groups are used to control which tasks that users can perform in Synchronization Service Manager.

Items	Ref.	Description
FIMSyncAdmins	[13.]	Members of this group have full access to everything in Synchronization Service Manager GUI.
FIMSyncOperators	[13.]	Members of this group have access to Operations in the Synchronization Service Manager only. FIMSyncOperators can run management agents, view synchronization statistics for each run, and save the run histories to a file. Members of the FIMSyncOperators group must also be members of the FIMSyncBrowse group to open links in synchronization statistics.
FIMSyncJoiners	[13.]	Members of this group have access to Joiner and Metaverse Search in Synchronization Service Manager. FIMSyncJoiners can join or project disconnectors by using Joiner, and they can use Metaverse Search to view object properties and disconnect objects from the metaverse.

FIM also needs 2 security groups for authentication during password management operations, these do not have access to Synchronization Service Manager:

Items	Ref.	Description
FIMSyncBrowse	[13.]	Can gather information about a user's lineage when resetting passwords by using Windows Management Instrumentation (WMI) queries.

FIMSyncPasswordSet	[13.]	Members of this group have permission to perform all operations by using the password management interfaces with WMI. Members in this group inherit all FIMSyncBrowse permissions. For more information about setting passwords by using WMI, see the FIM Developer Reference.

7.2.3.3 Required configuration

Items	Ref.	Description
Account type: domain local groups	[13.]	By default, FIM setup creates these groups as local computer groups, rather than domain local groups. But local computer groups are known **only to that server**, whereas domain local groups can be recognized throughout the domain. There might be cases where you need to use domain local groups for these roles. For example: - If the FIM configuration needs to be moved from one server to another, using domain local groups enables you manage access from a single location. - If you plan to have two servers running FIM share a database for the purposes of redundancy, it is recommended that the same users be members of the security groups that you create, and that they be recognized as such by FIM. You can accomplish this by using domain local groups. - … And also: - Disaster recovery - Server fail over - Server migration
Account creation	[13.]	If you plan to use domain local groups, create the groups **before** installing FIM.
Account creation	[13.]	Add the FIM setup account to the domain group FIM Sync admins

7.2.3.4 Risk

Items	Ref.	Description
Group creation by wizard	[13.]	During installation and setup, FIM adds the user account that is running the installation to the FIMSyncAdmins group, but **only if the FIMSyncAdmins group is also created during setup**. If you specify a preexisting group during setup, the user account that is running the installation will not be added to the preexisting group.
Local groups	[13.]	If you do not create the groups in advance, FIM setup will suggest to create these groups as local computer groups, rather than domain local groups. There might be cases where you need to use domain local groups for these roles. For example: - Two servers running FIM wiht a shared database for the purposes of redundancy - FIM management is distributed across the organization, using domain local groups grant access to the appropriate people within your organization. - When the FIM configuration must be moved from one server to another - Centralised or remote log management, you can use domain local groups to control access remote servers. - If you are enabling password synchronization on FIM, you must use a domain account for the FIM Synchronization Service service account.

7.2.3.5 Group type selection

Source: **[13.]** Using Security Groups

There might be cases where you need to use **domain local groups** for these roles. For example:

- Two servers running FIM wiht a shared database for the purposes of redundancy
- FIM management is distributed across the organization, using domain local groups grant access to the appropriate people within your organization.
- When the FIM configuration must be moved from one server to another
- Centralised or remote log management, you can use domain local groups to control access remote servers.
- If you are enabling password synchronization on FIM, you must use a domain account for the FIM Synchronization Service service account.

Important

If you plan to use domain local groups, create the groups **before** installing FIM.

7.2.3.6 FIM task scheduler – technical account

7.2.3.7 Required settings

Items	Ref.	Description
Account type: domain account		You must create a service account to execute the FIM Task scheduler jobs. Due to the fact the FIM Security groups should be hosted on AD, this service account must be a domain user account.
Account Security		This account should **not be a local administrator account**.
Account Security		The service accounts should **not be members of the local administrators** group.
Account Security		The FIM task scheduler account must be a **member of the security group** FIMSyncAdmins, to allow for cleaning the run history
Account security		On the server running the **FIM Synchronization Service**, you must allow the **FIM Task scheduler account** - Allow logon as a batch job Use the following restrictions on the FIM task scheduler account: - Deny Logon as a service - Deny access to this computer from the network - Deny logon on through Remote Desktop services
Account Security – Folder access		The FIM task scheduler account might need specific access on files and folders on the server to - Run scripts - Create log files - …
Account separation		Due to the fact that the FIM Task scheduler account is only used to execute the tasks, do not use this account for other purposes. As other services require other privileges, the PoLP demands to use separate accounts.

7.2.4 PCNS

7.3 FIM Service

7.3.1 FIM Service – service account

7.3.1.1 References

- **[23.]** FIM 2010 R2: FIM Service or the FIM Synchronization Service Account does not have Deny Logon As Batch Job set
- **[12.]** Before you begin
- **[17.]** Considerations for New Installation of FIM 2010 R2
- **[18.]** Installing the FIM 2010 R2 Server Components

7.3.1.2 Required settings

Items	Ref.	Description
Account type: domain account	[12.]	To run the FIM Service component, you must have a dedicated domain service account
Account type: mail enabled	[12.]	To be able to use the Office Outlook integration feature, an Exchange Server mailbox must also be created for this account. To use the FIM 2010 R2 Add-in for Outlook feature, you must set up the domain service e-mail account on a server that hosts Exchange Server 2007 or Exchange Server 2010. If you plan to use SMTP for notifications rather than Exchange Server, ensure that this service account has the required permissions on the SMTP gateway.
Account Security	[23.]	This account should **not be a local administrator account**.
Account Security	[12.]	The service accounts should **not be members of the local administrators** group.
Account Security	[17.]	The FIM Service Service SVCA must be **member of the security groups**: - FIMSyncAdmins For SSPR - FIMSyncBrowse and FIMSyncPasswordSet
Account security	[23.]	On the server running the **FIM Synchronization Service**, you must restrict only the **FIM Synchronization Service service account** and not the FIM Service service account. On the server running the **FIM Service**, you must only **restrict the FIM Service service account**, and not the FIM Synchronization Service service account. Use the following restrictions on the service accounts: - Deny logon as a batch job - Deny logon locally - Deny access to this computer from the network For SSPR - WMI and DCOM permissions for SSPR
Account separation	[12.], [17.]	Due to the fact that the FIM Service account is only used to run the FIM Service service, do not use this account for other purposes. As other services require other privileges, the PoLP demands to use separate accounts.
Account Separation	[12.], [17.]	The FIM Service SVCA must be part of the FIM Sync Admins security group. (See Ref. 4) The FIM Sync service SVCA must not be part of the FIM Sync Security Groups **This requirement excludes the use of 1 single account for both the FIM Service and the FIM Synchronization service.**
Account Separation	[12.]	You must reserve the domain service e-mail account for the exclusive use of the FIM Service. If e-mail messages are being processed by other applications, such as Office Outlook 2007, the functionality of FIM Service might be affected.

Account settings: mail	[18.]	See page 50, par. 9.1, post-installation FIM Service

7.3.1.3 Risks

Items	Ref.	Description
Same account	[17.]	Due to the fact that the FIM Synchronization account is only used to run the FIM Synchronization services, do not use this account for other purposes. As other services require other privileges, the PoLP demands to use separate accounts.
Same account	[17.]	If you choose to use the same account for both service accounts and you separate the FIM Service and the FIM Synchronization Service, you cannot set **Deny access to this computer from the network** on the FIM Synchronization Service server. If access is denied, that action prohibits the FIM Service from contacting the FIM Synchronization Service to change configuration and manage passwords.
Same account	[17.]	The FIM Service account has HPA access to the FIM Service operations, using the same account bestows too many unneeded privileges to the FIM Sync service account

IMPORTANT
You must reserve the domain service e-mail account for the exclusive use of the FIM Service. If e-mail messages are being processed by other applications, such as Office Outlook 2007, the functionality of FIM Service might be affected.

7.3.2 FIM MA account

7.3.2.1 References

- [12.] FIM 2010 Installation Guide > Before you begin [12.]

7.3.2.2 Required settings

Items	Ref.	Description
Configuring the Service Accounts Running the FIM 2010 R2 Server Components in a Secure Manner	[12.]	There are three service accounts that are used to run the FIM server components. They are called the FIM Service service account, the FIM Synchronization Service service account, and the FIM Password service account in this guide. The **FIM MA account is not considered a service account**, and it should be a regular user account. For the FIM Synchronization Service service account to be able to impersonate the FIM MA account, the FIM MA must be able to log on locally.

Items	Ref.	Description
Account type	[12.]	You must create a domain account that is reserved for the exclusive use of the FIM Service management agent (FIM MA) used by the FIM Synchronization Service to communicate with the FIM Service.
Account Security	[12.]	The FIM Service has to know the name of the account that the FIM MA is using so that during setup it can give the account the required permissions. This account should not be a local administrator account.

7.3.3 Understanding the Purpose of the FIM Service Management Agent Account

The purpose of this account is to make it possible for the FIM Service to be able to identify the FIM Synchronization Service when it is exporting to the FIM Service through the Web services. When the FIM Synchronization Service engine is exporting, all authentication (AuthN) and authorization (AuthZ) workflows are ignored and only action workflows run.

7.3.4 Risk

Items	Ref.	Description
Portal logon with trusted account	[12.]	The account that you use for the FIM MA should be considered a trusted account. You should not use it to access the FIM Portal. If you do, all requests that are made through the FIM Portal with this account will skip AuthN and AuthZ.
Account Change	[12.]	If you later change this account in the FIM Synchronization Service, you must also run a change install on the FIM Service to update the service with the new account information.

7.4 FIM SSPR – Registration & Reset portals

Due to the fact that the SSPR portals for the Password registration and Password Reset are hosted on IIS, the security mainly focusses on IIS.

The FIM configuration part is rather applying on the installation or reconfiguration.

7.4.1 IIS

Reference: [54.]: Security Best Practices for IIS 8

7.5 Management agents

7.5.1 General

General: http://aka.ms/FIM_PortsRightsPersmissions

7.5.2 FIM MA

FIM MA Acocunt security

7.5.3 ADMA

How to grant the"Replicating Directory Changes" permission for the Microsoft Metadirectory Services ADMA service account: hhttp://support.microsoft.com/kb/303972

- For Exchange permission, incl. executing remote Exchange PowerShell, see below.

- FIM Reference: How to set more granular permissions than "replicating directory changes" on a source AD read by the ADMA
- FIM Reference: FIM 2010 - Installation Companion - Accounts
-

7.5.3.1 Exchange 2010 / 2013

See:

7.5.4 GALSync

- Permissions for GALSync User MA User Account

7.5.5 SQL MA

7.5.6 Other MAs

7.6 FIM Certificate Management

7.6.1 References

- [36.] Create an OU and User Accounts for FIM CM Agents

> *“The following table summarizes the accounts and permissions required by FIM CM. You can allow the FIM CM create the following accounts automatically, or you can create them prior to installation. The actual account names can be changed. If you do create the accounts yourself, consider naming the user accounts in such a way that it is easy to match the user account name to its function.”*

7.6.2 FIM CM Agent

Provides the following services:

- Retrieves encrypted private keys from the CA.
- Protects smart card PIN information in the FIM CM database.
- Protects communication between FIM CM and the CA.

Items	Ref.	Description
Account Type	[36.]	Domain account
Account Security	[36.]	- Allow logon locally user right. - Issue and Manage Certificates user right. - Read and Write permission on the system Temp folder at the following location: %WINDIR%\Temp. - A digital signature and encryption certificate issued and installed in the user store.

7.6.3 FIM CM Key Recovery Agent

Provides the following services:

- Recovers archived private keys from the CA.

Items	Ref.	Description
Account Type	[36.]	Domain account
Account Security: Local permissions	[36.]	- Allow logon locally user right. - Membership in the local Administrators group.
Account Security: Certificates	[36.]	- Key Recovery Agent certificate is issued and installed in the user store. The certificate must be added to the list of the key recovery agents on the CA.
Account Security: Folder Security	[36.]	- Read permission and Write permission on the system Temp folder at the following location: %WINDIR%\Temp.

7.6.4 FIM CM Authorization Agent

Provides the following services:

- Determines user rights and permissions for users and groups.

Items	Ref.	Description
Account Type	[36.]	Domain account
Account Security:	[36.]	- Membership in the Pre-Windows 2000 Compatible Access domain group. - Granted the Generate security audits user right.

7.6.5 FIM CM CA Manager Agent

Provides the following services:

- Performs CA management activities.

Items	Ref.	Description
Account Type	[36.]	Domain account
Account Security: PKI	[36.]	- This user must be assigned the Manage CA permission.

7.6.6 FIM CM Web Pool Agent

Provides the following services:

- Provides the identity for the IIS application pool. FIM CM runs within a Microsoft Win32® application programming interface process that uses this user's credentials.

Items	Ref.	Description
Account Type	[36.]	Domain account
Account Security: Local permissions	[36.]	- Membership in the local IIS_WPG group. - Membership in the local Administrators group.
Account Security: Audit	[36.]	- Granted the Generate security audits user right.
Account Security: Special Rights		- Granted the Act as part of the operating system user right. - Granted the Replace process level token user right. -
Account Security: IIS	[36.]	- Assigned as the identity of the IIS application pool, CLMAppPool.
Account Security: Registry	[36.]	- Granted Read permission on the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CLM\v1.0\Server\WebUser registry key.
Account Security: AD Special Rights	[36.]	- This account must also be trusted for delegation.

7.6.7 FIM CM Enrollment Agent

Provides the following services:

- Performs enrollment on behalf of a user.

Items	Ref.	Description
Account Type	[36.]	Domain account
Account Security: PKI	[36.]	- An Enrollment Agent certificate that is issued and installed in the user store. - Enroll permission on the Enrollment Agent certificate template (or the custom template, if one is used).
Account Security: Special Rights	[36.]	- Allow logon locally user right.

7.7 FIM Reporting (SCSM)

7.7.1 Reference

- [37.] FIM 2010 R2 Reporting Permissions

7.7.2 SCSM Installer Account

Items	Ref.	Description
Account Type	[36.]	Domain account
Account Security: Local Rights	[36.]	- Local admin on the SCSM and SCSMDW server. - member of the local Administrators group on the SQL Server.
Account Security: SQL Rights	[36.]	rights in SQL to create databases and assign security roles.

◆Important

After installation, the account access can be lowered or the account can be disabled and re-enabled if updates need to be installed.

7.7.3 SCSM Administrators Group

Items	Ref.	Description
Account Type	[36.]	Security group in AD
Account Security: Rights	[36.]	The Installer account is added automatically.
Account Security: Rights	[36.]	• The group is added to the Service Manager Administrators role automatically. • The group is added to the Data Warehouse Administrators role automatically.

7.7.4 Service Manager Service Account

Items	Ref.	Description
Account Type	[36.]	Domain account
Account Security: Local Rights	[36.]	Local admin on the SCSM and SCSMDW server.
Account Security	[36.]	After installation becomes the Operational System Account, is assigned to logon account for both System Center Data Access Service and System Center Management Configuration Service After installation, becomes the data warehouse run as account, is assigned to the Service Manager SDK account and Service Manager Config account.
Account Security: SQL		In SQL, it is added to the sdk_users and configsvc_users database roles on the SCSM and SCSMDW databases becomes a member of the db_datareader role for the DWRepository database.

7.7.5 Workflow Account

Items	Ref.	Description
Account Type	[36.]	Domain account
Account Security: Local Rights	[36.]	Member of the local Users security group.

Items	Ref.	Description
Account Security: Local Rights	[36.]	If email notifications are required, this account must be mail enabled.

7.7.6 Reporting Account

Items	Ref.	Description
Account Type	[36.]	Domain account
Account Security: SQL	[36.]	- Used by SSRS to access the DWDataMart data - In SQL, it is added to the db_datareader and reportuser roles on the DWDataMart database.

7.8 BHOLD

7.8.1 References

See: [38.] FIM 2010: Quick Guide to installing BHOLD Core

7.8.2 BHOLDApplicationGroup

Items	Ref.	Description
Account Type	[38.]	Domain group

7.8.3 BHOLD Core Service Account

Items	Ref.	Description
Account Type	[38.]	Domain user
Account Security	[38.]	Log on as a Service
Account Security	[38.]	Password never expires
Account Security	[38.]	Add this user to the following groups: - IIS_IUSRS - II. ii. BHOLDApplicationGroup

8 Security during Installation

8.1 FIM setup account – functional account

8.1.1.1 References

- **[12.]** Before you begin
- **[17.]** Considerations for New Installation of FIM 2010 R2
- **[18.]** Installing the FIM 2010 R2 Server Components
- **[5.]** Segregation of duties

8.1.1.2 Required settings

Items	Ref.	Description
Account type: domain account	[18.]	You must create a user account to run installation of the FIM components. This installer account must be a **domain user** account. The most important reason is that the FIM installer account is assigned root administrator in the FIM service and portal, during the installation you need SQL sysadmin (SA) rights, which is by preference a domain joined SQL server with Windows authentication.
Account Security: SQL	[18.]	**ONLY DURING INSTALLATION** To be able to install FIM Synchronization Service or FIM Service, the account must be a SQL sysadmin. The account that you use does not have to be a SQL sysadmin after the installation is complete. The user account used to install the FIM Service must be granted the sysadmin role in SQL Server. **By default, members of the Local Administrators group do not have the necessary permissions.** Unless the user account is either the built-in administrator account, or the user account used to install SQL Server, then the user account must be granted the sysadmin role in SQL Server.
Account Security: Sharepiont	[18.]	To be able to install the FIM Portal, the account must be a SharePoint administrator. To be able to install the FIM Portal, it is assumed that SharePoint is installed with the default settings, that the default SharePoint site can be reached using the address specified in the user interface, and that the user who is installing the FIM Portal is authorized as an administrator of that SharePoint site.
Account Security	[18.]	**ONLY DURING INSTALLATION** This account **should be** a local administrator account.
Account Security	[18.]	**ONLY DURING INSTALLATION** The FIM installer accounts should **be member of the local administrators** group.
Account Security	[18.]	The FIM installer account **should only be** a **member of the security group** FIMSyncAdmins.

Items	Ref.	Description
Account security	[18.]	Use the following restrictions on the FIM installer account: • Deny logon as a batch job • Deny run as a service
Account separation	[5.]	Due to the fact that the FIM installer account is only used to install FIM component, during initial setup or during application of an hotfix, do not use this account for other purposes. DO NOT - use the FIM Installer account for operational, day-to-day management. - Use the FIM installer account as service account As other services require other privileges, the PoLP demands to use separate accounts.

8.1.1.3 Risks

Items	Ref.	Description
Same account	[18.]	The FIM Sync Service account has HPA access to the FIM Sync Service operations, using the same account bestows too many unneeded privileges to the FIM Sync service account

8.2 FIM SSPR – Registration & Reset portals

Due to the fact that the SSPR portals for the Password registration and Password Reset are hosted on IIS, the security mainly focusses on IIS.

The FIM configuration part is rather applying on the installation or reconfiguration of the FIM SSPR portals for asword registration or password reset.

8.2.1 Change mode install

8.2.1.1 Reference

From: [34.] Password Registration and Reset Portal Deployment

8.2.1.2 Procedure

> *"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."*

9 Post-installation: Securing FIM

9.1 FIM Service

9.1.1.1 References

- [18.] Installing the FIM 2010 R2 Server Components
- [29.] Configure Message Delivery Restrictions
- [30.] Configure Message Size Limits for a Mailbox or a Mail-enabled Public Folder
- [31.] Configure Storage Quotas for a Mailbox

9.1.1.2 Required settings

Items	Ref.	Description
Account type: domain account	[18.]	Configuring the FIM Service Service Exchange mailbox 1. Configure the service account so that it can accept mail only from internal e-mail addresses 2. Configure the service account so that it rejects mail messages with sizes greater 3. Configure the service account so that it has a mailbox storage quota of 5 gigabytes (GB). than 1 MB.

9.2 FIM Portal (SharePoint)

9.2.1 Reference

- [15.] Step 7: Perform FIM 2010 R2 Prerequisite Tasks

Items	Ref.	Description
Account type	[15.]	Change the SharePoint Application Pool Account to Use CORP\SPService

9.2.2 SharePoint in depth

See, page 57, paragraph 12.4, SharePoint .

9.3 Portal Security

9.3.1 User Account login

Items	Ref.	Description
User Account mapping		To logon to the portal these administrators must have an account in the portal, with the following attributes matched to an AD user account - logon name = corresponding AD sAMAccountName - Domain = logondomain (NetBIOS) of domain user is logging on to - objecSid = objectSid of user account

There are different ways of creating accounts in the FIM portal:

- synchronizing the accounts into the portal from AD, via the FIM Sync engine
- creating the accounts in the portal and setting the objectSID attribute by PowerShell script
    - For more information see: How to Use PowerShell to Fix an ObjectSID on an FIM Portal Object

9.3.2 Administrator account / installation account

The account that installs the FIM Service / FIM portal will be assigned as **primary portal administrator**, as it will be added to the Administrators set in the FIM Portal.

Items	Ref.	Description
Additional administrators		Additional administrators must be added to the 'Administrators' set

10 Post-installation: Securing FIM Backend

10.1 Portal Security

10.1.1 User Account login

- To logon to the portal these administrators must have an account in the portal, with the following attributes matched to an AD user account
- logon name = corresponding AD sAMAccountName
- Domain = logondomain (NetBIOS) of domain user is logging on to
- objecSid = objectSid of user account

There are different ways of creating accounts in the FIM portal:

- synchronizing the accounts into the portal from AD, via the FIM Sync engine
- creating the accounts in the portal and setting the objectSID attribute by PowerShell script

For more information see: How to Use PowerShell to Fix an ObjectSID on an FIM Portal Object

10.1.2 Primary Administrator account / setup account

The account that installs the FIM Service / FIM portal will be assigned as primary portal administrator, as it will be added to the Administrators set in the FIM Portal

10.1.3 Secondary / personal administrator accounts

Additional administrators must be added to the 'Administrators' set

11 Operational best practices

11.1 References

- [13.] Using Security Groups

11.2 FIM Default folders

	Importance	Items	Ref.	Description
□	MEDIUM	Default File and folder permissions	[12.]	Do not change permissions on the default files and folders When reinstalling FIM component or applying a FIM hotfix, these permissions will be reset.

11.3 Source code location

	Importance	Items	Ref.	Description
□	MEDIUM	Source code location		Do not store your source code on the production server.
□	MEDIUM	Source code location		Do not store your source code on the C-drive
□	MEDIUM	Source code location		Store your source code in a source control tool like Visual Studio Team Foundation Server…

12 References & Authoritative resources

The following documents and authors were used as core reference in this guide.

12.1 Security (General)

Ref. no.	Document	Description
[1.]	Microsoft Security Intelligence Report	http://www.microsoft.com/security/sir/default.aspx
[2.]	Security Risk Management Guide	https://technet.microsoft.com/library/cc163143.aspx
[3.]	IT Infrastructure Threat Modeling Guide	http://www.microsoft.com/en-us/download/details.aspx?id=2220 To download a copy of the IT Infrastructure Threat Modeling Guide, click here.
[4.]	The Administrator Accounts Security Planning Guide	https://technet.microsoft.com/en-us/library/cc162797.aspx Click here to download The Administrator Accounts Security Planning Guide from the Microsoft Download Center.
[5.]	Segregation of duties aka. Separation of duties	https://en.wikipedia.org/wiki/Separation_of_duties
[6.]	Principle of least privilege	https://en.wikipedia.org/wiki/Principle_of_least_privilege
[7.]	Privilege separation	https://en.wikipedia.org/wiki/Privilege_separation
[8.]	4-eyes principle	http://whatis.techtarget.com/definition/four-eyes-principle

12.2 FIM

12.2.1 Overview

Ref. no.	Document	Description
[9.]	FIM 2010 Technical Overview	https://technet.microsoft.com/en-us/library/ff621362(v=ws.10).aspx

12.2.2 FIM Best practices

Ref. no.	Document	Description
[10.]	Forefront Identity Manager 2010 R2 Best Practices General	http://aka.ms/fimbeforeyoubegin
[11.]	Change the Forefront Identity Manager 2010 R2 Synchronization Service Account	https://technet.microsoft.com/en-us/library/jj590224(v=ws.10).aspx

12.2.3 FIM Security

Ref. no.	Document	Description
[12.]	FIM 2010 Installation Guide > Before you begin	http://aka.ms/fimbeforeyoubegin
[13.]	Using Security Groups	http://aka.ms/fimsecuritygroups http://technet.microsoft.com/en-us/library/jj590183(v=ws.10).aspx

Ref. no.	Document	Description
[14.]	Test Lab Guide: Installing Forefront Identity Manager 2010 R2	http://technet.microsoft.com/en-us/library/hh322905(v=ws.10).aspx
[15.]	Step 7: Perform FIM 2010 R2 Prerequisite Tasks	http://technet.microsoft.com/en-us/library/hh322882(v=ws.10)
[16.]	FIM 2010 R2 Kerberos Settings (SPN Configuration)	http://technet.microsoft.com/en-us/library/jj134299(v=ws.10).aspx
[17.]	Considerations for New Installation of FIM 2010 R2	http://technet.microsoft.com/en-us/library/jj134293(v=ws.10).aspx
[18.]	Installing the FIM 2010 R2 Server Components	https://technet.microsoft.com/en-us/library/hh332711(v=ws.10).aspx

12.2.4 FIM Best practices for security

Ref. no.	Title (alphabetically)	URL
[19.]	Forefront Identity Manager 2010 R2 Best Practices for Security	http://aka.ms/fim2010r2bestpracticessecurity
[20.]	FIM 2010 (R2): Well-known GUIDS	http://aka.ms/FIMGuids
[21.]	Best practices for the FIM Portal Administrator account	http://www.wapshere.com/missmiis/best-practices-for-the-fim-portal-administrator-account

12.2.5 FIM Best practice analyzer

Ref. no.	Title (alphabetically)	URL
[22.]	FIM 2010 R2: Same Account being used for FIM Synchronization Service and FIM MA	https://technet.microsoft.com/en-us/library/jj204553(v=ws.10).aspx
[23.]	FIM 2010 R2: FIM Service or the FIM Synchronization Service Account does not have Deny Logon As Batch Job set	https://technet.microsoft.com/en-us/library/jj204563(v=ws.10).aspx

12.2.6 FIM Sync

Ref. no.	Title (alphabetically)	URL
[24.]	Forefront Identity Manager Password Management	https://technet.microsoft.com/en-us/library/jj590203(v=ws.10).aspx
[25.]	Management Agent Communication Ports, Rights, and Permissions	http://aka.ms/fim_portsrightspermissions

12.2.7 FIM PCNS

Ref. no.	Title (alphabetically)	URL
[26.]	Forefront Identity Manager Password Management	https://technet.microsoft.com/en-us/library/jj590203(v=ws.10).aspx
[27.]	Pcnscfg: Password Change Notification Service (PCNS) Configuration Utility	https://technet.microsoft.com/en-us/library/jj590227(v=ws.10).aspx
[28.]	Using Password Synchronization	https://technet.microsoft.com/en-us/library/jj590288(v=ws.10).aspx

12.2.8 FIM Service

Ref. no.	Title (alphabetically)	URL
[29.]	Configure Message Delivery Restrictions	http://go.microsoft.com/fwlink/?LinkId=183625
[30.]	Configure Message Size Limits for a Mailbox or a Mail-enabled Public Folder	http://go.microsoft.com/fwlink/?LinkId=183626
[31.]	Configure Storage Quotas for a Mailbox	http://go.microsoft.com/fwlink/?LinkId=156929

12.2.9 FIM SSPR

Ref. no.	Title (alphabetically)	URL
[32.]	To allow SSPR for users that forgot their password you must allow anonymous access to the password reset portal.	https://technet.microsoft.com/en-us/library/ee534892(v=ws.10).aspx#allow_anony_access_pswd_reset_portal
[33.]	Password Reset Deployment Guide	https://technet.microsoft.com/en-us/library/ee534892(v=ws.10).aspx
[34.]	Password Registration and Reset Portal Deployment	https://technet.microsoft.com/en-us/library/jj134295(v=ws.10).aspx

12.2.10 FIM CM

Ref. no.	Title (alphabetically)	URL
[35.]	Create FIM 2010 CM service accounts using PowerShell	https://konab.com/create-fim-2010-cm-service-accounts-using-PowerShell/
[36.]	Create an OU and User Accounts for FIM CM Agents	https://technet.microsoft.com/en-us/library/gg430115(v=ws.10).aspx

12.2.11 FIM Reporting

Ref. no.	Title (alphabetically)	URL
[37.]	FIM 2010 R2 Reporting Permissions	http://aka.ms/fimreportingpermissions

12.2.12 BHOLD

Ref. no.	Title (alphabetically)	URL
[38.]	FIM 2010: Quick Guide to installing BHOLD Core	http://social.technet.microsoft.com/wiki/contents/articles/18334.fim-2010-quick-guide-to-installing-bhold-core.aspx
[39.]	Microsoft BHOLD Suite SP1 Installation Guide	https://technet.microsoft.com/en-us/library/jj134107(v=ws.10).aspx
[40.]	BHOLD Core Installation	https://technet.microsoft.com/en-us/library/jj134095(v=ws.10).aspx
[41.]	BHOLD Core technical reference	https://technet.microsoft.com/en-us/library/jj134937(v=ws.10).aspx

12.3 SQL Server

Ref. no.	Title (alphabetically)	URL
[42.]	Guidelines on choosing Service Accounts for SQL Server Services.	http://support.microsoft.com/kb/2160720
[43.]	Server Configuration - Service Accounts	https://msdn.microsoft.com/en-us/library/cc281953.aspx
[44.]	SQL Server 2005 Security Best Practices - Operational and Administrative Tasks	http://aka.ms/sql2005securitybestpractices
[45.]	SQL Server 2008 R2 Security Best Practice Whitepaper	http://aka.ms/sql2008securitybestpractices
[46.]	SQL Server 2012 Security Best Practice Whitepaper	http://aka.ms/sql2012securitybestpractices
[47.]	Service Account Types Supported for SQL Server Agent:	http://go.microsoft.com/fwlink/?LinkId=183624
[48.]	Selecting an Account for the SQL Server Agent Service	http://go.microsoft.com/fwlink/?LinkId=12295

12.4 SharePoint

Ref. no.	Title (alphabetically)	URL
[49.]	Plan for administrative and service accounts (Office SharePoint Server)	http://technet.microsoft.com/en-us/library/cc263445(v=office.12).aspx
[50.]	Plan administrative tasks in a least-privilege environment (SharePoint Server 2010)	https://technet.microsoft.com/en-us/library/hh377944(v=office.14).aspx
[51.]	Initial deployment administrative and service accounts (SharePoint Server 2010	https://technet.microsoft.com/en-us/library/ee662513%28v=office.14%29.aspx
[52.]	Administrative accounts	https://technet.microsoft.com/en-us/library/55b99d80-3fa7-49f0-bdf4-adb5aa959019(v=office.14)#Section2

Ref. no.	Title (alphabetically)	URL
[53.]	Harden SQL Server for SharePoint environments (SharePoint Server 2010)	https://technet.microsoft.com/en-us/library/ff607733(v=office.14).aspx

12.5 IIS

Ref. no.	Title (alphabetically)	URL
[54.]	Security Best Practices for IIS 8	http://technet.microsoft.com/en-us/library/cc263445(v=office.12).aspx

13 Useful resources

The list of references below are additional resources, helpful for getting more details where needed.

13.1 Security Best practices

Title (alphabetically)	URL
Keys to the Kingdom: Monitoring Privileged User **Actions for Security and Compliance**	https://www.sans.org/reading-room/whitepapers/analyst/keys-kingdom-monitoring-privileged-user-actions-security-compliance-34890

13.2 FIM 2010

13.2.1 Product builds

Title (alphabetically)	URL
Microsoft Identity Software: Public Release Build Versions	http://aka.ms/IDMBuildversions
MIM 2016 Build Overview	http://aka.ms/MIMBuilds
FIM 2010 Build overview	http://aka.ms/FIMBuilds

13.2.2 FIM Prerequisites

Title (alphabetically)	URL
Step 6: Install FIM 2010 R2 Prerequisite Software	https://technet.microsoft.com/en-us/library/hh322909(v=ws.10).aspx

13.2.3 FIM Best practices

Title (alphabetically)	URL
Forefront Identity Manager 2010 R2 Best Practices	http://aka.ms/fim2010r2bestpractices
Forefront Identity Manager 2010 R2 Best Practices General	http://aka.ms/fim2010r2bestpracticesgeneral
Forefront Identity Manager 2010 R2 Best Practices for Security	http://aka.ms/fim2010r2bestpracticessecurity

13.2.4 FIM On-disk help

Title (Alphabetically)	URL
FIM 2010 R2 Synchronization Service On-disk Help	https://technet.microsoft.com/en-us/library/jj572795%28v=ws.10%29.aspx

13.2.5 FIM General Best practices

Items	URL
FIM 2010 Best practices	http://aka.ms/fim2010bestpractices

13.2.6 FIM Kerberos & SPN configuration

Items	URL
FIM 2010 R2 Kerberos Settings	https://technet.microsoft.com/en-us/library/jj134299(v=ws.10).aspx
FIM 2010: Kerberos Authentication Setup	http://social.technet.microsoft.com/wiki/contents/articles/3385.fim-2010-kerberos-authentication-setup.aspx
Kerberos and Self-Service Password Reset	https://technet.microsoft.com/en-us/library/jj134304(v=ws.10).aspx

13.2.7 FIM Sync

Items	URL
Management Agent Communication Ports, Rights, and Permissions	http://aka.ms/fim_portsrightspermissions
[DOWNLOAD] Management Agent Communication Ports, Rights, and Permissions	http://go.microsoft.com/fwlink/?LinkId=30737
Exchange recipient administration overkill in ILM and FIM	http://blog.msresource.net/2011/12/02/exchange-recipient-administration-overkill-in-ilm-and-fim/
Delegating the minimum set of permissions for mailbox-enabled user and linked mailbox provisioning	http://blog.msresource.net/2011/12/14/delegating-the-minimum-set-of-permissions-for-mailbox-enabled-user-and-linked-mailbox-provisioning/

13.2.8 FIM Portal

Items	URL
How to Use PowerShell to Fix an ObjectSID on an FIM Portal Object	http://social.technet.microsoft.com/wiki/contents/articles/3614.how-to-use-powershell-to-fix-an-objectsid-on-an-fim-portal-object.aspx

13.2.9 FIM SSPR

Items	URL
Maintaining Forefront Identity Manager 2010 R2 - Self-Service Password Reset	https://technet.microsoft.com/en-us/library/jj134290(v=ws.10).aspx
FIM 2010 R2 Password Registration Portal	https://technet.microsoft.com/en-us/library/jj134315(v=ws.10).aspx
FIM 2010 R2 Password Reset Portal	https://technet.microsoft.com/en-us/library/jj134281(v=ws.10).aspx

13.2.10 SharePoint

Items	URL
Installing FIM 2010 R2 on SharePoint Foundation 2013	https://technet.microsoft.com/nl-be/library/jj863242(v=ws.10).aspx
FIM 2010 - Bookmarks Collection	http://aka.ms/fimbookmarks

13.2.11 FIM Reference collections - Online

Items	URL
FIM 2010 – Short cuts collection	http://aka.ms/FIMShortcuts
FIM 2010 - Bookmarks Collection	http://aka.ms/fimbookmarks
Getting started with FIM 2010 - Resources for FIM starters	http://aka.ms/starttofim
Forefront Identity Manager Resources	http://aka.ms/fimresources
FIM 2010 Build Overview	http://aka.ms/fimhotfixes
FIM 2010 Best practices	http://aka.ms/fim2010bestpractices

13.2.12 SQL

Items	URL
SQL Builds	http://aka.ms/SQLBuilds

13.3 MIM 2016 Product info

Title (alphabetically)	URL
MIM 2016	http://aka.ms/MIM2016
MIM 2016 Product documentation	http://microsoft.com/mim

13.4 IIS

Items	URL
Best Practices Analyzer for Internet Information Services: Security	https://technet.microsoft.com/nl-nl/library/dd391934(v=ws.10).aspx

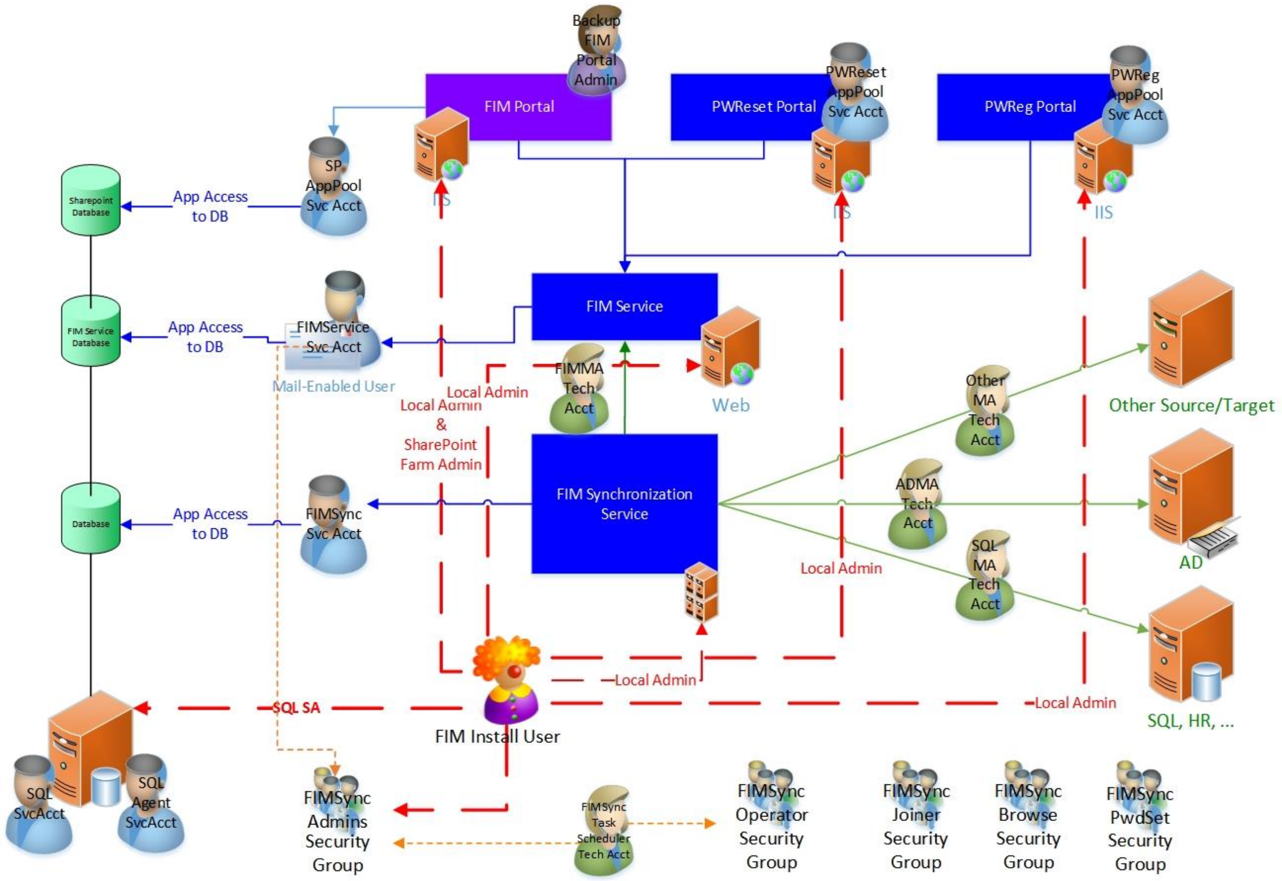
14 Glossary, abbreviations & acronyms

Acronym	Description	See also
AAD	Azure AD	
AAD Connect	Azure AD Connect = successor of AADSync	
AADSync	Azure AD Sync	ADSync, AAD Connect
AADConnect	See AAD Connect	
ACC	Acceptance environment	
AD	Active Directory	
ADDS	Active Directory Domain Services	
ADSync	Azure Active	
CM	Certificate Manager, Certificate Management	
CS	Connector space Component of FIM Sync	
DBA	Database administrator	
DBO	Database Owner	
DEV	Development	
DirSync	First version of O365 Directory Synchronization. Now deprecated and replaced by AADSync and AADconnect	
DTAP	Development, Test, Acceptance & Production environments	
FIM Sync Svc	FIM Synchronization Service	
FIMSync	FIM Synchronization	
FIM Sync	FIM Synchronization	
FIM	Forefront Identity Manager 2010 (R2)	FIM 2010, FIM 2010 R2
FIMCM	FIM Certificate Manager	
LSG	Local Security Group	
DLSG	Domain Local Security Group	
HPA	Highly priviledged account	
MIIS	Microsoft Identity Integration Server 2003	MIIS 2003
MIM	Microsoft Identity Manager 2016	MIM 2016
MV	Metaverse, Component of FIM Sync	
O365	Office 365	
PCNS	Password Change Notification Service	
PROD	Production	
PW	Password	

Pwd	Password	
SG	Security Group	
WF	Workflow	
MA	Management Agent	FIM Sync
DSG	Domain Security	
USG	Universal Security Group	
DL	Distribution List	
DG	Distribution Group	DL
MPR	Management Policy Rule	FIM Service component
SCCM	System Center Configuration Manager	
SA	SQL System Administrator	
SCSM	System Center Service Manager	
SPF	SharePoint Foundation	
SVC	Service	
SVCA	Service Account	
SVR	Server	
TST	Test Environment	

15 Index

Appendix A: Account overview for FIM basic configuration



Appendix B: Documentation - Compact Check list

Pre-installation: Backend configuration

SPN

	Importance	LOC	Acct. Type	Account Reference	Name (to fill)
□	HIGH	D	SPN	SQL Database Account	<domain>\<account>
□	HIGH	D	SPN	FIM Service Account	<domain>\<account>
□	HIGH	D	SPN	SharePoint Service Account	<domain>\<account>
□	HIGH	D	SPN	Password Registration Server Account	<domain>\<account>
□	HIGH	D	SPN	Password Reset Server Account	<domain>\<account>
□	HIGH	D	SPN	FIM CM Web Pool Agent Account	

Pre-installation: Account creation

Back End

SQL

	Importance	LOC	Acct. Type	Account Reference	Name (to fill)
□	HIGH	D	Service	SQL Server Database engine acct.	<domain>\<account>
□	HIGH	D	Service	SQL Server Agent service* acct.	<domain>\<account>
□	HIGH	D	Service	SQL Server Analysis Services acct.	<domain>\<account>
□	HIGH	D	Service	SQL Server Reporting Services acct.	<domain>\<account>
□	HIGH	D	Service	SQL Server Browser acct.	<domain>\<account>

SharePoint

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Functional	SharePoint Setup administrator acct*	<domain>\<account>
□	HIGH	D	Functional	Farm service account	<domain>\<account>
□	LOW	D	Functional	search service account	<domain>\<account>
□	LOW	D	Functional	search content access account	<domain>\<account>
□	LOW	D	Functional	SharePoint Application pool account	<domain>\<account>

All FIM Platforms

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Functional	FIM setup administrator account*	<domain>\<account>

FIM Synchronization

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Service	FIM Sync service	<domain>\<account>
□	HIGH	D	Security Group	FIMSyncAdmins	<domain>\<account>
□	HIGH	D	Security Group	FIMSyncOperators	<domain>\<account>
□	HIGH	D	Security Group	FIMSyncJoiners	<domain>\<account>
□	HIGH	D	Security Group	FIMSyncBrowse	<domain>\<account>
□	HIGH	D	Security Group	FIMSyncPasswordSet	<domain>\<account>
□	HIGH	D	Technical	FIM Task scheduler	<domain>\<account>

FIM Sync Management agents

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Technical	ADMA Account	<domain>\<account>
	See below	D	Technical	FIMMA Account	
□	HIGH	D	Technical	SQL MA Account	<domain>\<account>
□	HIGH	D	Technical	Other Management agents: 1 account per type of MA and by preference 1 account per MA.	<domain>\<account>

FIM Service

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Service	FIM service	<domain>\<account>
□	HIGH	D	Technical	FIMMA Account	<domain>\<account>
□	HIGH	D	Functional	Backup Portal Administrator	<domain>\<account>

FIM Portal

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	MEDIUM	D	Functional	Backup Portal Administrator	<domain>\<account>
□	HIGH	D	Functional	FIM Portal - Application Pool Account	<domain>\<account>

FIM SSPR Registration Portal

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Functional	FIM SSPR Registration Portal - Application Pool Account	<domain>\<account>

FIM SSPR Reset Portal

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Functional	FIM SSPR Reset Portal - Application Pool Account	<domain>\<account>

FIM CM

	Importance	LOC	Account Type	Account Reference	Name (to fill)
□	HIGH	D	Functional	FIM CM Agent	<domain>\<account>
□	HIGH	D	Functional	FIM CM Authorization Agent	
□	HIGH	D	Functional	FIM CM CA Manager Agent	
□	HIGH	D	Functional	FIM CM Enrollment Agent	
□	HIGH	D	Functional	FIM CM Key Recovery Agent	
□	HIGH	D	Functional	FIM CM Web Pool Agent	

Pre-installation: Account lock down

General

	Importance	LOC	Account Type	Account Reference	Procedure
□	HIGH	D	Functional	FIM Installer account	Just before installation[3] Grant local admin rigths

FIM Sync

☒☑□	Action	Account
□	Account creation	
□	Account Configuration	

AD

	Importance	LOC	Account Type	Account Reference	Procedure
□	HIGH	D	Functional	FIM ADMA	Replicating Directory Changes
□	HIGH	D	Functional	FIM ADMA	Lock down the account to the minimum required permissions to the minimum required containers

Post-Installation

Account Assignment

FIM Service & FIM Portal

	Account Type	Account Reference	Name (to fill)
□	Functional account	Add Backup Portal Administrator account to Administrators set	

[3] This applies both to fresh installation of FIM component or implementation of an hotfix or service pack. Only during implementation of a service pack, the installation account that runs the installation needs the elevated rights. Only DURING installation, not before, not after.

FIM Sync

	Account Type	Account Reference	Name (to fill)
□	Personal account	Add FIM Administrator account to FIMSyncAdmins group	

Hotfix installation

Account Assignment

All FIM platforms

	Account Type	Account Reference	Name (to fill)
□	Functional account	Add FIM Setup account to - SQL SA - Local server admin (via AD)	

FIM Service & FIM Portal

	Account Type	Account Reference	Name (to fill)
□	Functional account	Add Backup Portal Administrator account to Administrators set	

FIM Sync

	Account Type	Account Reference	Name (to fill)
□	Personal account	Add FIM Administrator account to FIMSyncAdmins group	

Appendix C: Security Implementation Sign-off sheet

The sheet below can be used to sign-off for a FIM implementation, to validate that a FIM configuration has been setup following best practices, or not.

In case the security configuration base line has not been implemented as described, it's mandatory to make sure that the CISO (Chief Information Security Officer) that is responsible and accountable for the FIM infrastructure, or his authorized direct delegates signs off for the exceptions.

CISO or authorized security delegate

Item	**<FIIL IN>**
Company	
Name	
Function	
Manager name / Direct report of	
Manager Function	
Signature	
Date	

Sign off

Item	
I have fully read & understood the guidelines and best practices in this document	□
I agree that the exceptions below were implemented	□

FIM Options implemented

Please check which FIM options are installed to determine which security configurations must be applied.

In next section you must provide in detail which best practices were not implemented and clearly state the reason.

	Component	**Implemented**	**Not implemented**
□	FIM Sync Server	□	□
□	PCNS	□	□
□	FIM Service	□	□
□	FIM Portal	□	□
□	SSPR: Password registration Portal	□	□
□	SSPR: Password reset Portal	□	□
□	FIM CM	□	□
□	FIM Reporting	□	□
□	BHOLD	□	□
□	(0365) AADConnect, DirSync	□	□

Derogations - Exceptions implemented

Please explain in detail, which best practices were **not implemented** and **clearly state the reason**.

	Section in document	Topic / configuration	Reason
□			
□			
□			
□			
□			
□			
□			
□			
□			
□			
□			
□			
□			