# Microsoft Identity Manager

## Microsoft Identity manager
## Security Baseline Configuration

**Wednesday, 24 May 2023**

**Version 2.0.0. Draft**


*Prepared by*

**Peter Geelen**

**Executive Director - Microsoft MVP Security (Identity & Access)**


# Revision and Signoff Sheet

## Change Record

| Date | Author | Version | Change reference |
|---|---|---|---|
| 17/dec/2015 | Peter Geelen | 0.9 | Draft for Review |
| 01/jan/2016 | Peter Geelen | 0.9.3 | Update layout & draft published on TN Wiki |
| 15/feb/2016 | Peter Geelen | 0.9.5 | Integrated feedback |
| 24/08/2022 | Peter GEELEN | 1.0.1 | Fixed layout and small issues |
| 23/05/2023 | Peter GEELEN | 2.0.0 | Update for Microsoft Identity manager (2016/2010) |

## Reviewers

| Name | Version Reviewed | Position | Date |
|---|---|---|---|
| Gil Olsen | 0.9.3 | Premier Field Engineer at Microsoft | 29/jan/2016 |
| Laurent Benmeziani | 0.9.3 | Premier Field Engineer at Microsoft | 27/jan/2016 |
| Thomas Vuylsteke | 0.9.3. | Premier Field Engineer at Microsoft | 15/jan/2016 |

# 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 implementing the security best practices of the FIM and MIM server components.

### 1.2.1 SharePoint

FIM and MIM require SharePoint to support the FIM/MIM Portal. This document is scoped to an infrastructure with a single server running SharePoint 2016 or 2019.

## 1.3 Out of scope

This document excludes a setup with a SharePoint farm (single server).

But in the additional references section (See page: paragraph 62, 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 MIM 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 59.

## 2.2 FIM vs MIM

In general, the current document applies to both FIM 2010, FIM 2010 R2, MIM 2016 SP1 or SP2.

If a configuration item is particular for a version, it will be mentioned explicitly.

### 2.2.1 MIM components

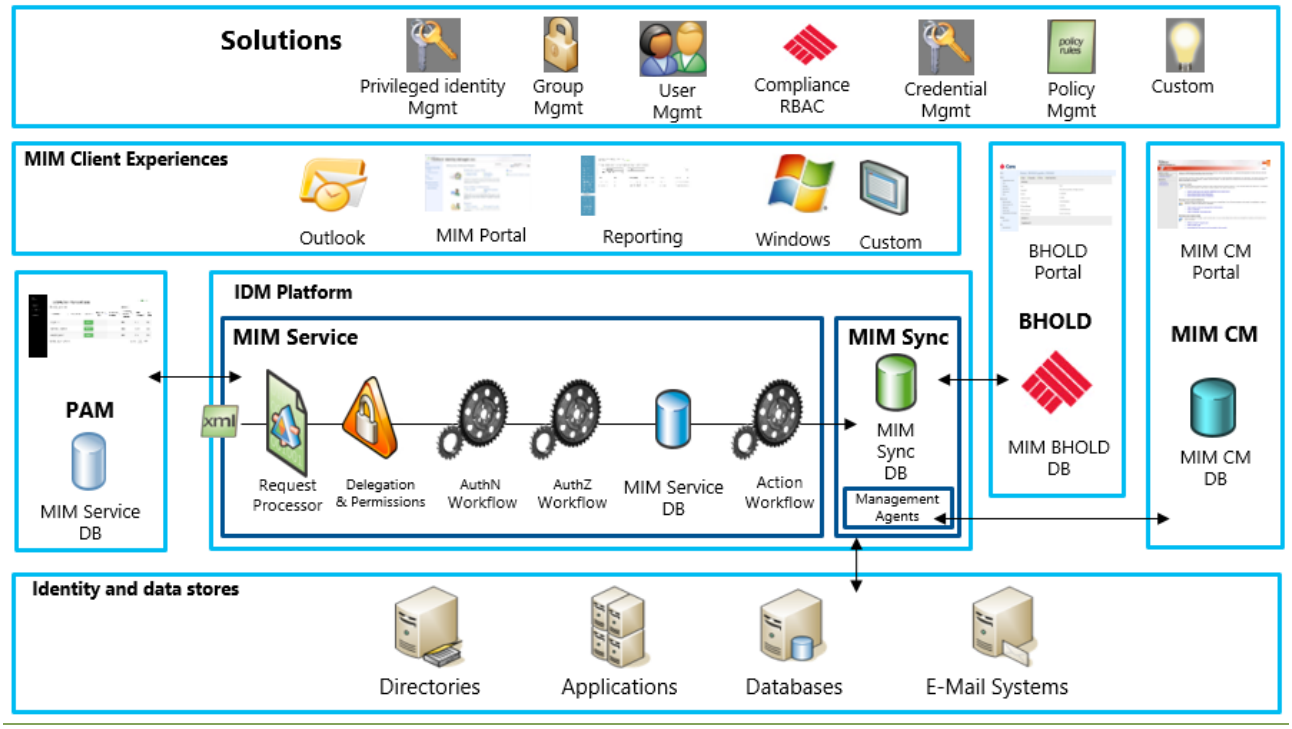



Figure 1: MIM components overview

Source: [9.] FIM 2010 Technical Overview

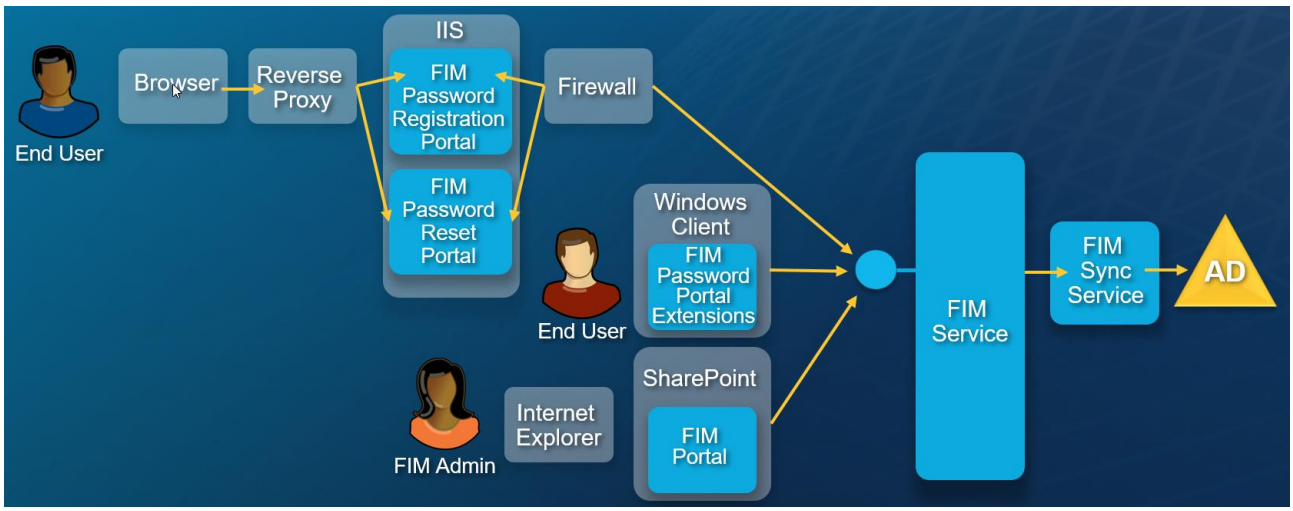



Figure 2: Typical MIM Infrastructure view

#### 2.2.1.1 MIM 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 MIM Synchronization Service is the fulfillment mechanism, creating and maintaining identities in other systems /../*

Please note that in some specific cases you do need to install 3rd party software on the MIM server to make the management agent (MA) connections work, eg Exchange requires the Exchange Management tools, Lotus Notes must have admin client, Oracle needs Oracle client software installed , …

#### 2.2.1.2 MIM Service

> *"/../ The MIM 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 MIM server and the built-in policy engine. /../"*

#### 2.2.1.3 MIM Portal

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

> *"/../ In the earlier figure, several clients to the MIM Service are shown: The MIM Add-in for Outlook, the Password Reset Add-in, and the **MIM Portal** as well as custom clients. In addition, the MIM Synchronization Service and Exchange 2007 can be considered **clients of the MIM Service**.*
>
> */../*
>
> *Users are allowed to interact with the MIM 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 MIM SSPR Portals: Password registration and reset portals

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

Essentially:

- **MIM Portal** must be hosted on **SharePoint**,
- while both MIM SSPR portals (Registration and Reset) only require IIS.

## 2.3 Naming conventions

The difference in behavior and the functionality of the MIM 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 68, 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<br>FIM Synchronization Service<br>Also applies to MIM Sync engine, ILM Sync Engine, MIIS Sync engine |
| **MIM Sync, MIMSync** | MIM Synchronization engine, or<br>MIM Synchronization Service |
| **ILM** | ILM 2007 FP1 |
| **MA** | Management Agent |
| **MIIS** | MIIS 2013 |
| **MIM** | Microsoft Identity Manager 2016, MIM 2016 (SP2) |
| **Sync** | MIM Sync |

This also means that:

- "MIM Service" (API, portal) IS NOT "MIM Sync" (sync engine)
- "MIM Service" IS NOT "MIM Sync Service"
- The "MIM service - Service Account" is NOT the "MIM 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 MIM 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 main account types

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

There are 2 more security items the need to be mentioned to implement the required security measures

- Security groups
- SPN (Service Principle Names)

### 2.4.1 Core account differentiators

| | Account Type | | | |
|---|---|---|---|---|
| **Task type** | Service Account | Technical Account | Functional Account | Personal Account |
| Run as a Background Service (continuously) | YES | NO | NO | NO |
| Running a batch job (Specific Task or script) | NO | YES | NO | NO |
| Interact with desktop/Physical Logon | NO | NO | YES | YES |
| Highly Privileged Rights | NO | NO | YES | YES/NO |
| 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)** | 'MIM Service' service, 'MIM Sync' Service, 'SQL Database server' service, … |
| **(2)** | Task Scheduler account to run MIMSync scripts on an **automated** schedule |
| **(3)** | MIM 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**

Only as of MIM 2016 SP2 virtual or managed accounts are supported.
More info: https://learn.microsoft.com/en-us/microsoft-identity-manager/preparing-domain-gmsa

From: https://learn.microsoft.com/en-us/microsoft-identity-manager/preparing-domain-gmsa (dd may 2023)
Following MIM components can have gMSA accounts configured to be used during the installation process:

- MIM Synchronization service (FIMSynchronizationService)
- MIM Service (FIMService)
- MIM Password Registration web site application pool
- MIM Password Reset web site application pool
- PAM REST API web site application pool
- PAM Monitoring Service (PamMonitoringService)

- PAM Component Service (PrivilegeManagementComponentService)

The following MIM components **do not support** running as gMSA accounts:

- MIM Portal. This is because MIM Portal is part of the SharePoint environment. Instead, you can deploy SharePoint in farm mode and Configure automatic password change in SharePoint Server.
- All Management Agents
- Microsoft Certificate Management
- BHOLD

These service accounts 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 configuration
- …

**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 technical 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.

Technical account require **complex passwords**.

**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 infra-structure.

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/MIM service, you need local admin rights on the Windows server and you need SA rights on SQL, which are highly sensitive.
- After installation of MIM 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 infra-structure.

**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).

### 2.4.3 Security groups & SPN

#### 2.4.3.1 Security Groups

In an enterprise, managing security by assigning permissions to user accounts only, makes the security management impossible. Therefor you better assign permissions to groups as much as possible.

This is explained in reference [59.] below.

#### 2.4.3.2 SPN

Following authoritative references are used in this section.

- [58.] SPN

> *"A service principal name (SPN) is the name by which a client uniquely identifies an instance of a service. If you install multiple instances of a service on computers throughout a forest, each instance must have its own SPN. A given service instance can have multiple SPNs if there are multiple names that clients might use for authentication. For example, an SPN always includes the name of the host computer on which the service instance is running, so a service instance might register an SPN for each name or alias of its host. For more information about SPN format and composing a unique SPN"*
>
> *"Before the Kerberos authentication service can use an SPN to authenticate a service, the SPN must be registered on the account object that the service instance uses to log on. A given SPN can be registered on only one account. For Win32 services, a service installer specifies the logon account when an instance of the service is installed. The installer then composes the SPNs and writes them as a property of the account object in Active Directory Domain Services. If the logon account of a service instance changes, the SPNs must be re-registered under the new account."*

# 3 Generic security principles

## 3.1 References

Following authoritative references are used in this section.

- **[1.]** Microsoft Security Intelligence Report
- **[6.]** Principle of Least Privilege
- **[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. "*

You can also find more details explained on Implementing Least-Privilege Administrative Models:

> *"The principle is simple, and the impact of applying it correctly greatly increases your security and reduces your risk. **The principle states that all users should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more**. Doing so provides protection against malicious code, among other attacks. This principle applies to computers and the users of those computers.*
>
> *"One reason this principle works so well is that it forces you to do some internal research. For example, you must determine the access privileges that a computer or user really needs, and then implement them. For many organizations, this task might initially seem like a great deal of work; however, it is an essential step to successfully secure your network environment.*
>
> *"You should grant all domain administrator users their domain privileges under the concept of least privilege. For example, if an administrator logs on with a privileged account and inadvertently runs a virus program, the virus has administrative access to the local computer and to the entire domain. If the administrator had instead logged on with a nonprivileged (nonadministrative) account, the virus's scope of damage would only be the local computer because it runs as a local computer user.*

> *"In another example, accounts to which you grant domain-level administrator rights must not have elevated rights in another forest, even if there is a trust relationship between the forests. This tactic helps prevent wide-spread damage if an attacker manages to compromise one managed forest. Organizations should regularly audit their network to protect against unauthorized escalation of privilege."*

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

> *"An issue related to using least privilege is support for separation of privilege. This means removing high privilege operations to another process and running that process with the higher privileges required to perform its tasks. Day-to-day interfaces are executed in a lower privileged process…"*
>
> *"Similarly, systems and programs granting access to resources should do so when more than one condition is met. This provides a fine grained control over the resource, and additional assurance that the access is authorized."*

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 MIM documentation on TechNet clearly references to **use separate accounts** with **separate rights and permissions** to protect the various functional MIM 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 MIM functionality, the **different MIM components** serve a **different purpose**, executing **different tasks** thus you need;

- **different accounts,**
- **different groups**
- **separated per environment,**
- for **each environment**,

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

This also means that if you have multiple MIM setups running in the same environment, but serving different purposes, you need a proper segregation of duties.

The best example of this is using MIM for internal IDM, while using AADConnect for the communication to Azure/Office 365.

You will need a separate set of credentials, accounts and groups to run

- the intranet MIM functionality
- the AADconnnect functionality

The main reason for this SoD should be clear, they could / will have mutual impact.

### 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 Audit & monitoring

Although they are not active means of mitigation, the following counter measures are an essential part of the pack:

- monitoring (real time follow up of the operational environment)
- audit (regular, but not real-time platform event analysis, based on audit log collection)

## 3.8 Number of accounts vs. security risk

Only configure the required accounts related to the MIM feature you need to implement. No more, but also no less that what is needed.

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

For example, if you only implement MIM Sync, there is no need to implement the MIM Service required accounts.

But IF you implement a certain component, like MIM 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 MIM Sync and MIM Service, it is a violation of the Sod and PoLP to use one single account for multiple services, MAs, 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.

## 3.9 Conclusion

To mitigate security threats it's essential to apply a combination of counter measures:

- Principle of Least Privilege (assigning minimum permissions)
- Privilege separation (splitting permissions)
- SoD & account isolation (separating accounts & duties)

Applying these active counter measures, is also known as "account lockdown".

These active measures must be complemented with monitoring and audit to implement the required security counter measures.

## 3.10 Additional reading

More information is available in paragraph 13.1, Security Best practices at page 64.

# 4 MIM security principles

## 4.1 References

Authoritative references:

- **[11.]** Forefront Identity Manager 2010 R2 Best Practices General
- **[21.]** Forefront Identity Manager 2010 R2 Best Practices for Security

## 4.2 Best practices

### 4.2.1 Required settings

| Items | Ref. | Description |
|---|---|---|
| **Infrastructure Security** | **[11.]** | Proper setup of MIM 2016 in your test lab and careful planning of your **configuration migration** from test lab to production is essential to minimize deployment problems. |
| **Infrastructure Security** | **[11.]** | Proper setup of safe **data** migration procedures must be provided., with careful planning of your data migration from production lab to test environment. This is essential to minimize privacy issues and data exposure (preventing data leakage or unauthorized access). |
| **Back up** | **[11.]** | After installing MIM, 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.<br>Copy the encryption keys off the sync server and store them in a secure location.<br>For more information, see MIISkmu: Encryption Key Management Tool. |
| **Backup** | **[11.]** | Test your backup and restore procedures for Microsoft Forefront Identity Manager. |
| **DRP** | **[11.]** | 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** | **[21.]** | Control access with Microsoft Forefront Identity Manager security groups. |
| **Physical Access** | **[21.]** | Restrict physical access to computers to trusted personnel. |
| **Least Privilege** | **[21.]** | Implement user rights and permissions to restrict software access to trusted accounts. |
| **Least Privilege** | **[21.]** | For each management agent allow only minimum access required |
| **Account Security** | **[21.]** | Enforce strong password policies for **all user accounts**. |
| **Account Security** | **[21.]** | Lock down the Microsoft Forefront Identity Manager service account |
| **Account Security** | **[21.]** | Periodically change the Microsoft Forefront Identity Manager service account password. |

# 5 Compact Check list for account & group configuration

## 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<br>Critical risk on MIM systems, linked systems & general infrastructure<br>Real & proven danger<br>High impact on recovery<br><br>Impact of risk is critically higher than operational burden | High business impact<br>Risk of setting up a configuration that cannot be recovered using a normal DRP planning.<br>Critical impact on security, violation of common security best practices<br>Critical impact on linked systems like HR, AD, O365 |
| **MEDIUM (ORANGE)** | Strongly advised to follow best practice | Possible, Realistic danger<br>Significant impact on MIM systems, linked systems & general infrastructure<br><br>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<br>Low risk<br>Theoretical, low frequency<br>Easy to recover<br><br>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.<br><br>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/<MIM Service Server> | MIM Service Account |
| ☐ | HIGH | D | SPN | HTTP/<MIM 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/<MIM CM Server> | MIM CM Web Pool Agent Account |

## 5.3 SPN Delegation

You need to set delegations for the MIM service account and the Sharepoint service account, refer to section 7.1.1.4, SPN Delegation on page 36.

### 5.3.1 Kerberos Constrained delegation

| | Importance | LOC | Acct. Type | Account Reference | Name (to fill) |
|---|---|---|---|---|---|
| ☐ | HIGH | D | msDS-Al-lowedToDel-egateTo | FIMService/<MIM Service Server> | MIM Service Account |
| ☐ | HIGH | D | msDS-Al-lowedToDel-egateTo | FIMService/<MIM Service Server> | SharePoint Service Account |

## 5.4 Pre-installation: Account creation

### 5.4.1 Back End

#### 5.4.1.1 SQL

Reference:

- [19.] Server Configuration - Service Accounts

This section only has informational purposes, but has been added as a reminder to secure the MIM 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."*

#### 5.4.1.2 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> |

### 5.4.2 All MIM Platforms

| | Importance | LOC | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Functional | MIM installer administrator account* | <domain>\<account> |

### 5.4.3 MIM Synchronization

| | Importance | LOC | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Service | MIM Sync service SVCA | <domain>\<account> |
| ☐ | HIGH | D | Security Group | MIMSyncAdmins | <domain>\<account> |
| ☐ | HIGH | D | Security Group | MIMSyncOperators | <domain>\<account> |
| ☐ | HIGH | D | Security Group | MIMSyncJoiners | <domain>\<account> |
| ☐ | HIGH | D | Security Group | MIMSyncBrowse | <domain>\<account> |
| ☐ | HIGH | D | Security Group | MIMSyncPasswordSet | <domain>\<account> |
| ☐ | HIGH | D | Technical | MIM Task scheduler | <domain>\<account> |

#### 5.4.3.1 MIM Sync MAs

| | Importance | LOC | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Technical | ADMA Account | <domain>\<account> |
| ☐ | HIGH | D | Technical | MIMMA Account | <domain>\<account> |
| ☐ | HIGH | D | Technical | SQL MA Account | <domain>\<account> |
| ☐ | HIGH | D | Technical | Other MAs:<br>- 1 account per type of MA<br>And by preference 1 account per MA. | <domain>\<account> |

### 5.4.4 MIM Service

| | Importance | LOC | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Service | MIM service SVCA | <domain>\<account> |
| ☐ | HIGH | D | Technical | MIMMA Account | <domain>\<account> |

### 5.4.5 MIM Portal

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

### 5.4.6 MIM SSPR Registration Portal

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

### 5.4.7 MIM SSPR Reset Portal

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

### 5.4.8 MIM CM

Source: [39.] Create an OU and User Accounts for MIM CM Agents

> *"The following table summarizes the accounts and permissions required by MIM CM. You can allow the MIM 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 | MIM CM Agent | <domain>\<account> |
| ☐ | HIGH | D | Technical | MIM CM Authorization Agent | |
| ☐ | HIGH | D | Technical | MIM CM CA Manager Agent | |
| ☐ | HIGH | D | Technical | MIM CM Enrollment Agent | |

| | | | | | |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Technical | MIM CM Key Recovery Agent | |
| ☐ | HIGH | D | Technical | MIM CM Web Pool Agent | |

## 5.5 Pre-installation: Account lock down

### 5.5.1 All MIM Platforms

| | Importance | LOC | Account Type | Account Reference | Procedure |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Functional | MIM Installer account | Just before installation[1]<br>- Grant local server admin rights<br>- Grant SQL SysAdmin (SA)<br>- Grant SharePoint farm admin rights |

### 5.5.2 MIM Sync

| | Importance | LOC | Account Type | Account Reference | Procedure |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Service | MIM Sync Svc SVCA | Lock down MIM Sync Service SVCA |
| ☐ | HIGH | D | Technical | MIM ADMA | Lock down ADMA Technical Account |
| ☐ | HIGH | D | Security Groups | Security Groups | Minimize memberships to MIM Sync security groups |
| ☐ | HIGH | D | Security Groups | Security Groups | Minimize administrative memberships to the MIM Servers |

#### 5.5.2.1 MIM Sync MAs

| | Importance | LOC | Account Type | Account Reference | Procedure |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Technical | MIM MA | Lock down the MIM MA technical account |
| ☐ | HIGH | D | Technical | MIM MA | Block/Filter the administrative accounts from the MIM Service connector space |
| ☐ | HIGH | D | Technical | MIM ADMA | Replicating Directory Changes |
| ☐ | HIGH | D | Technical | MIM 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> |

[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.

## 5.6 Post-Installation: Set operational admins

### 5.6.1 MIM Portal

| | Importance | LOC | Account Type | Account Reference | Procedure |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Functional | MIM Portal Backup Account | Add a functional account as backup root account to the MIM Potal |

## 5.7 Hotfix installation

### 5.7.1 All MIM Platforms

| | Importance | LOC | Account Type | Account Reference | Procedure |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Functional | MIM Installer account | Just before hotfix installation[2]<br>- Grant local admin rights<br>- Grand SQL SysAdmin<br>- Grant SharePoint farm admin rights |

[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 MIM backend infrastructure

## 6.1 SQL Server

Although MIM heavily relies on SQL Server, SQL security configuration is out of scope for MIM 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 MIM.

- **[45.]** Guidelines on choosing Service Accounts for SQL Server Services.
- **[49.]** 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: **[14.]** Before You Begin

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

If you are using MIM 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:

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

**Important**

The **SQL Server service account** should a domain account, not a local computer account. A local account cannot impersonate domain accounts and the MIM 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 MIM.

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

### 6.2.2 Action items

Please find below a list of configuration items relevant to MIM, 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.<br>Separate different applications into different sites with different application pools. |
| Web Application Isolation | Implement the principle of least privilege.<br>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).<br>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:

- **[35.]** 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 MIM Portal back-end services.

### 6.3.1 References

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

- **[54.]** 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:<br>- MSSQLSERVER<br>- SQLSERVERAGENT<br>If you do not use the default SQL Server instance, in the Windows Services console, these services will be shown as the following:<br>- MSSQL$InstanceName<br>- SQLAgent$InstanceName | Use either a Local System account or a domain user account.<br>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$).<br>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:<br>- Setup<br>- SharePoint Products Configuration Wizard | - Domain user account.<br>- Member of the Administrators group on each server on which Setup is run.<br>- SQL Server login on the computer that runs SQL Server.<br>- Member of the following SQL Server security roles:<br>- securityadmin fixed server role<br>- dbcreator fixed server role<br>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:<br>- Configure and manage the server farm.<br>- Act as the application pool identity for the SharePoint Central Administration Web site.<br>- Run the Microsoft SharePoint Workflow Timer Service. | - **Domain** user account.<br>Additional permissions are automatically granted for the server farm account on Web servers and application servers that are joined to a server farm.<br>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:<br>- **dbcreator** fixed server role<br>- **securityadmin** fixed server role<br>- **db_owner** fixed database role for all SharePoint databases in the server farm |

# 7 Pre-installation: Securing MIM Components

## 7.1 MIM general

### 7.1.1 SPN

#### 7.1.1.1 References

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

- **[18.]** 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: [18.] 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 MIM SPN Configuration

From: [18.] 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 MIM Service database. Allows clients the ability to locate an instance of SQL. |
| **FIMService/<MIM Service Server>** | MIM Service Account | SPN required for the MIM Service. Allows clients the ability to locate an instance of the MIM Service. |
| **HTTP/<MIM 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. |

| SPN | Account | Description |
|---|---|---|
| **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 MIM 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 MIM Password Service account. |
| **HTTP/<MIM CM Server>** | MIM 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 MIMServices, ensure that each MIMService has constrained delegation configured so that each MIMService 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 MIMService that is polling. In all cases, the Approval Response will be directed to the MIMService machine that processed the original Request so cross-server communication: MIMPortal -> MIMService AND MIMService -> MIMService must work properly."*

### 7.1.2 Changing MIM Sync Service account

#### 7.1.2.1 References

Source: [12.] 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 MIM 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** | [12.] | To complete this procedure, you must be logged on as a member of the MIMSyncAdmins security group. |
| **Account Security** | [12.] | See the Account security requirement of the MIM Sync service account, section below. |
| **Backup** | [12.] | Back up the encryption key set by running MIISkmu.exe. |
| **Installation** | [12.] | You can change the account in 2 ways<br>1. Run Setup from the MIM installation CD in maintenance mode, or<br>2. Run the Change configuration from the Control Panel (Programs/Software)<br>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. |
| **Account Lock down** | [12.] | Local Security Policy<br>- Deny logon locally<br>- Deny access to this computer from the network<br>- Deny logon as a batch job<br>- Deny log on through Terminal Services.<br>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. |

#### 7.1.2.3 Risks

| Items | Ref. | Description |
|---|---|---|
| **Attacks** | [12.] | 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 separation** | | |

## 7.2 MIM Setup

### 7.2.1 MIM Installer account – functional account

#### 7.2.1.1 References

- **[14.]** Before you begin
- **[19.]** Considerations for New Installation of MIM 2016
- **[20.]** Installing the MIM 2016 Server Components
- **[5.]** Segregation of duties

#### 7.2.1.2 Required settings

| Items | Ref. | Description |
|---|---|---|
| **Account type: domain account** | [20.] | You must create a user account to run installation of the MIM components.<br>This installer account must be a **domain user** account.<br>The most important reason is that the MIM installer account is assigned root administrator in the MIM 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** | [20.] | **ONLY DURING INSTALLATION**<br>To be able to install MIM Synchronization Service or MIM Service, the account must be a SQL sysadmin.<br>The account that you use does not have to be a SQL sysadmin after the installation is complete.<br>The user account used to install the MIM Service must be granted the sysadmin role in SQL Server.<br>**By default, members of the Local Administrators group do not have the necessary permissions.**<br>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: Sharepoint** | [20.] | To be able to install the MIM Portal, the account must be a SharePoint administrator.<br>To be able to install the MIM 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 MIM Portal is authorized as an administrator of that SharePoint site. |
| **Account Security** | [20.] | **ONLY DURING INSTALLATION**<br>This account **should be** a local administrator account (by membership of the local admins group). |
| **Account Security** | [20.] | **ONLY DURING INSTALLATION**<br>The MIM installer accounts should **be member of the local administrators** group. |
| **Account Security** | [20.] | The MIM installer account **should only be** a **member of the security group** MIMSyncAdmins during installation |
| **Account Security** | [20.] | The MIM installer account **should only have elevated rights during initial installation and/or hotfix installation.** When these operations are finished, the elevated rights must be revoked. |
| **Account security** | [20.] | Use the following restrictions on the MIM installer account:<br>• Deny logon as a batch job<br>• Deny run as a service |

| Items | Ref. | Description |
|---|---|---|
| **Account separation** | [5.] | Due to the fact that the MIM installer account is only used to install MIM component, during initial setup or during application of a hotfix, do not use this account for other purposes.<br>DO NOT<br>- use the MIM Installer account for operational, day-to-day management.<br>- Use the MIM installer account as service account<br>As other services require other privileges, the PoLP demands to use separate accounts. |

#### 7.2.1.3 Risks

| Items | Ref. | Description |
|---|---|---|
| **Same account** | [20.] | The MIM Sync Service account has HPA access to the MIM Sync Service operations, using the same account for other operations bestows too many unneeded privileges to the MIM Sync service account |

### 7.2.2 MIM Synchronization Service SVCA

#### 7.2.2.1 References

- **[25.]** MIM 2016: Same Account being used for MIM Synchronization Service and MIM MA
- **[26.]** MIM 2016: MIM Service or the MIM Synchronization Service Account does not have Deny Logon As Batch Job set
- **[14.]** Before you begin
- **[19.]** Considerations for New Installation of MIM 2016

#### 7.2.2.2 Required settings

| Items | Ref. | Description |
|---|---|---|
| **Account type: domain account** | [14.] | You must create a service account to run the MIM Synchronization Service.<br>This service account must be a domain service account. |
| **Account Security** | [14.] | This account should **not be a local administrator account**. |
| **Account Security** | [14.] | The service accounts should **not be members of the local administrators** group. |
| **Account Security** | [14.] | The MIM Synchronization Service SVCA should not be a **member of the security groups** that are used to control access to MIM Synchronization Service (groups starting with MIMSync, for example, MIMSyncAdmins). |

| Items | Ref. | Description |
|---|---|---|
| **Account security** | [14.] | On the server running the **MIM Synchronization Service**, you must restrict only the **MIM Synchronization Service - service account** and not the MIM Service - service account.<br>On the server running the **MIM Service**, you must only **restrict the MIM Service - service account**, and not the MIM Synchronization Service - service account.<br>Use the following restrictions on the service accounts:<br>- Deny logon as a batch job<br>- Deny logon locally<br>- Deny access to this computer from the network<br>- Deny log on through Remote Desktop Services |
| **Account separation** | [14.], [19.] | Due to the fact that the MIM Synchronization account is only used to run the MIM Synchronization services, do not use this account for other purposes.<br>As other services require other privileges, the PoLP demands to use separate accounts. |
| **Account Separation** | [14.], [19.] | The MIM Sync service SVCA must not be part of the MIM Sync Security Groups<br>The MIM Service SVCA must be part of the MIM Sync Admins security group. (See Ref. 4)<br>**This requirement excludes the use of 1 single account for both the MIM Service and the MIM Synchronization service.** |

#### 7.2.2.3 Exceptions

| Items | Ref. | Description |
|---|---|---|
| **Password reset** | [14.] | 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** | [14.] | Due to the fact that the MIM Synchronization account is only used to run the MIM Synchronization services, do not use this account for other purposes.<br>As other services require other privileges, the PoLP demands to use separate accounts. |
| **Same account** | [14.] | If you choose to use the same account for both service accounts and you separate the MIM Service and the MIM Synchronization Service, you cannot set **Deny access to this computer from the network** on the MIM Synchronization Service server.<br>If access is denied, that action prohibits the MIM Service from contacting the MIM Synchronization Service to change configuration and manage passwords. |
| **Same account** | [14.] | The MIM Sync Service account has HPA access to the MIM Sync Service operations, using the same account bestows too many unneeded privileges to the MIM Sync service account |

### 7.2.3 MIM Administrative Security Groups

#### 7.2.3.1 References

- [15.] Using Security Groups

#### 7.2.3.2 Purpose

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

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

| Items | Ref. | Description |
|---|---|---|
| **MIMSyncAdmins** | [15.] | Members of this group have full access to everything in Synchronization Service Manager GUI. |
| **MIMSyncOperators** | [15.] | Members of this group have access to Operations in the Synchronization Service Manager only.<br>MIMSyncOperators can run MAs, view synchronization statistics for each run, and save the run histories to a file. Members of the MIMSyncOperators group must also be members of the MIMSyncBrowse group to open links in synchronization statistics. |
| **MIMSyncJoiners** | [15.] | Members of this group have access to Joiner and Metaverse Search in Synchronization Service Manager. MIMSyncJoiners can join or project disconnectors by using Joiner, and they can use Metaverse Search to view object properties and disconnect objects from the metaverse. |

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

| Items | Ref. | Description |
|---|---|---|
| **MIMSyncBrowse** | [15.] | Can gather information about a user's lineage when resetting passwords by using Windows Management Instrumentation (WMI) queries. |
| **MIMSyncPasswordSet** | [15.] | Members of this group have permission to perform all operations by using the password management interfaces with WMI. Members in this group inherit all MIMSyncBrowse permissions.<br>For more information about setting passwords by using WMI, see the MIM Developer Reference. |

#### 7.2.3.3 Required configuration

| Items | Ref. | Description |
|---|---|---|
| **Account type: domain local groups** | [15.] | By default, MIM setup creates these groups as local computer groups, rather than domain local groups.<br>But local computer groups are known **only to that server**, whereas domain local groups can be recognized throughout the domain.<br>There might be cases where you need to use domain local groups for these roles. For example:<br>- If the MIM configuration needs to be moved from one server to another, using domain local groups enables you manage access from a single location.<br>- If you plan to have two servers running MIM 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 MIM. You can accomplish this by using domain local groups.<br>- …<br>And also:<br>- Disaster recovery<br>- Server fail over<br>- Server migration |
| **Account creation** | [15.] | If you plan to use domain local groups, create the groups **before** installing MIM. |
| **Account creation** | [15.] | Add the MIM Sync Service installer account to the domain group MIM Sync admins |

### 7.2.3.4 Risk

| Items | Ref. | Description |
|---|---|---|
| **Group creation by wizard** | [15.] | During installation and setup, MIM adds the user account that is running the installation to the MIMSyncAdmins group, but **only if the MIMSyncAdmins group is also created during setup**.<br>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** | [15.] | If you do not create the groups in advance, MIM setup will suggest to create these groups as local computer groups, rather than domain local groups.<br>There might be cases where you need to use domain local groups for these roles. For example:<br>- Two servers running MIM with a shared database for the purposes of redundancy<br>- MIM management is distributed across the organization, using domain local groups grant access to the appropriate people within your organization.<br>- When the MIM configuration must be moved from one server to another<br>- Centralized or remote log management, you can use domain local groups to control access remote servers.<br>- If you are enabling password synchronization on MIM, you must use a domain account for the MIM Synchronization Service - service account. |

### 7.2.3.5 Group type selection

Source: **[15.]** Using Security Groups

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

- Two servers running MIM with a shared database for the purposes of redundancy
- MIM management is distributed across the organization, using domain local groups grant access to the appropriate people within your organization.
- When the MIM 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 MIM, you must use a domain account for the MIM Synchronization Service - service account.

| **Important** |
|---|
| If you plan to use domain local groups, create the groups **before** installing MIM. |

#### 7.2.3.6 MIM 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 MIM Task scheduler jobs.<br>Due to the fact the MIM 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 MIM task scheduler account must be a **member of the security group** MIMSyncAdmins, to allow for cleaning the run history |
| **Account security** | | On the server running the **MIM Synchronization Service**, you must allow the **MIM Task scheduler account**<br>- Allow logon as a batch job<br><br>Use the following restrictions on the MIM task scheduler account:<br>- Deny Logon as a service<br>- Deny access to this computer from the network<br>- Deny logon on through Remote Desktop services |
| **Account Security – Folder access** | | The MIM task scheduler account might need specific access on files and folders on the server to<br>- Run scripts<br>- Create log files<br>- … |
| **Account separation** | | Due to the fact that the MIM Task scheduler account is only used to execute the tasks, do not use this account for other purposes.<br>As other services require other privileges, the PoLP demands to use separate accounts. |

### 7.2.4 PCNS

## 7.3 MIM Service

### 7.3.1 MIM Service – service account

#### 7.3.1.1 References

- **[26.]** MIM 2016: MIM Service or the MIM Synchronization Service Account does not have Deny Logon As Batch Job set
- **[14.]** Before you begin
- **[19.]** Considerations for New Installation of MIM 2016
- **[20.]** Installing the MIM 2016 Server Components

### 7.3.1.2 Required settings

| Items | Ref. | Description |
|---|---|---|
| **Account type: domain account** | [14.] | To run the MIM Service component, you must have a dedicated domain service account |
| **Account type: mail enabled** | [14.] | To be able to use the Office Outlook integration feature, an Exchange Server mailbox must also be created for this account. To use the MIM 2016 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** | [26.] | This account should **not be a local administrator account**. |
| **Account Security** | [14.] | The service accounts should **not be members of the local administrators** group. |
| **Account Security** | [19.] | The MIM Service SVCA must be **member of the security groups**:<br>- MIMSyncAdmins<br>For SSPR, only if using SSPR,<br>- MIMSyncBrowse and MIMSyncPasswordSet |
| **Account security** | [26.] | On the server running the **MIM Synchronization Service**, you must restrict only the **MIM Synchronization Service - service account** and not the MIM Service - service account.<br>On the server running the **MIM Service**, you must only **restrict the MIM Service - service account**, and not the MIM Synchronization Service - service account.<br>Use the following restrictions on the service accounts:<br>- Deny logon as a batch job<br>- Deny logon locally<br>- Deny access to this computer from the network<br>For SSPR<br>- WMI and DCOM permissions for SSPR |
| **Account separation** | [14.], [19.] | Due to the fact that the MIM Service account is only used to run the MIM Service - service, do not use this account for other purposes.<br>As other services require other privileges, the PoLP demands to use separate accounts. |
| **Account Separation** | [14.], [19.] | The MIM Service SVCA must be part of the MIM Sync Admins security group. (See Ref. 4)<br>The MIM Sync service SVCA must not be part of the MIM Sync Security Groups<br>**This requirement excludes the use of 1 single account for both the MIM Service and the MIM Synchronization service.** |
| **Account Separation** | [14.] | You must reserve the domain service e-mail account for the exclusive use of the MIM Service. If e-mail messages are being processed by other applications, such as Office Outlook 2007, the functionality of MIM Service might be affected. |
| **Account settings: mail** | [20.] | See page 54, par. 9.1, post-installation MIM Service |

#### 7.3.1.3 Risks

| Items | Ref. | Description |
|---|---|---|
| **Same account** | [19.] | Due to the fact that the MIM Synchronization account is only used to run the MIM Synchronization services, do not use this account for other purposes.<br>As other services require other privileges, the PoLP demands to use separate accounts. |
| **Same account** | [19.] | If you choose to use the same account for both service accounts and you separate the MIM Service and the MIM Synchronization Service, you cannot set **Deny access to this computer from the network** on the MIM Synchronization Service server.<br>If access is denied, that action prohibits the MIM Service from contacting the MIM Synchronization Service to change configuration and manage passwords. |
| **Same account** | [19.] | The MIM Service account has HPA access to the MIM Service operations, using the same account bestows too many unneeded privileges to the MIM Sync service account |

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

### 7.3.2 MIM MA account

#### 7.3.2.1 References

- [14.] MIM 2010 Installation Guide > Before you begin [14.]

#### 7.3.2.2 Required settings

| Items | Ref. | Description |
|---|---|---|
| **Configuring the Service Accounts Running the MIM 2016 Server Components in a Secure Manner** | [14.] | There are three service accounts that are used to run the MIM server components. They are called the MIM Service - service account, the MIM Synchronization Service - service account, and the MIM Password service account in this guide.<br>The **MIM MA account is not considered a service account**, and it should be a regular user account.<br>For the MIM Synchronization Service - service account to be able to impersonate the MIM MA account, the MIM MA must be able to log on locally. |

| Items | Ref. | Description |
|---|---|---|
| **Account type** | [14.] | You must create a domain account that is reserved for the exclusive use of the MIM Service MA (MIM MA) used by the MIM Synchronization Service to communicate with the MIM Service. |
| **Account Security** | [14.] | The MIM Service has to know the name of the account that the MIM 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 MIM Service MA Account

The purpose of this account is to make it possible for the MIM Service to be able to identify the MIM Synchronization Service when it is exporting to the MIM Service through the Web services. When the MIM 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** | [14.] | The account that you use for the MIM MA should be considered a trusted account. You should not use it to access the MIM Portal. If you do, all requests that are made through the MIM Portal with this account will skip AuthN and AuthZ. |
| **Account Change** | [14.] | If you later change this account in the MIM Synchronization Service, you must also run a change install on the MIM Service to update the service with the new account information. |

## 7.4 MIM 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 MIM configuration part is rather applying on the installation or reconfiguration.

### 7.4.1 IIS

Reference: [57.]: Security Best Practices for IIS 8

## 7.5 Management agents

### 7.5.1 General

General: https://learn.microsoft.com/en-us/previous-versions/mim/cc720599(v=ws.10)

### 7.5.2 MIM MA

MIM MA Account security

### 7.5.3 ADMA

How to grant the "Replicating Directory Changes" permission for the Microsoft Metadirectory Services ADMA service account: http://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

### 7.5.4 GALSync

- Permissions for GALSync User MA User Account

### 7.5.5 SQL MA

### 7.5.6 Other MAs

## 7.6 MIM Certificate Management

### 7.6.1 References

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

> *"The following table summarizes the accounts and permissions required by MIM CM. You can allow the MIM 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 MIM CM Agent

Provides the following services:

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

| Items | Ref. | Description |
|---|---|---|
| **Account Type** | [39.] | Domain account |
| **Account Security** | [39.] | - Allow logon locally user right.<br>- Issue and Manage Certificates user right.<br>- Read and Write permission on the system Temp folder at the following location: %WINDIR%\Temp.<br>- A digital signature and encryption certificate issued and installed in the user store. |

### 7.6.3 MIM CM Key Recovery Agent

Provides the following services:

- Recovers archived private keys from the CA.

| Items | Ref. | Description |
|---|---|---|
| **Account Type** | [39.] | Domain account |
| **Account Security: Local permissions** | [39.] | - Allow logon locally user right.<br>- Membership in the local Administrators group. |
| **Account Security: Certificates** | [39.] | - 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** | [39.] | - Read permission and Write permission on the system Temp folder at the following location: %WINDIR%\Temp. |

### 7.6.4 MIM CM Authorization Agent

Provides the following services:

- Determines user rights and permissions for users and groups.

| Items | Ref. | Description |
|---|---|---|
| **Account Type** | [39.] | Domain account |
| **Account Security:** | [39.] | - Membership in the Pre-Windows 2000 Compatible Access domain group.<br>- Granted the Generate security audits user right. |

### 7.6.5 MIM CM CA Manager Agent

Provides the following services:

- Performs CA management activities.

| Items | Ref. | Description |
|---|---|---|
| **Account Type** | [39.] | Domain account |
| **Account Security: PKI** | [39.] | - This user must be assigned the Manage CA permission. |

### 7.6.6 MIM CM Web Pool Agent

Provides the following services:

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

| Items | Ref. | Description |
|---|---|---|
| **Account Type** | [39.] | Domain account |
| **Account Security: Local permissions** | [39.] | - Membership in the local IIS_WPG group.<br>- Membership in the local Administrators group. |
| **Account Security: Audit** | [39.] | - Granted the Generate security audits user right. |
| **Account Security: Special Rights** | | - Granted the Act as part of the operating system user right.<br>- Granted the Replace process level token user right.<br>- |
| **Account Security: IIS** | [39.] | - Assigned as the identity of the IIS application pool, CLMAppPool. |
| **Account Security: Registry** | [39.] | - Granted Read permission on the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CLM\v1.0\Server\WebUser registry key. |
| **Account Security: AD Special Rights** | [39.] | - This account must also be trusted for delegation. |

### 7.6.7 MIM CM Enrollment Agent

Provides the following services:

- Performs enrollment on behalf of a user.

| Items | Ref. | Description |
|---|---|---|
| **Account Type** | [39.] | Domain account |
| **Account Security: PKI** | [39.] | - An Enrollment Agent certificate that is issued and installed in the user store.<br>- Enroll permission on the Enrollment Agent certificate template (or the custom template, if one is used). |
| **Account Security: Special Rights** | [39.] | - Allow logon locally user right. |

## 7.7 MIM Reporting (SCSM)

### 7.7.1 Reference

- [40.] MIM 2016 Reporting Permissions

### 7.7.2 SCSM Installer Account

| Items | Ref. | Description |
|---|---|---|
| **Account Type** | [39.] | Domain account |
| **Account Security: Local Rights** | [39.] | - Local admin on the SCSM and SCSMDW server.<br>- member of the local Administrators group on the SQL Server. |
| **Account Security: SQL Rights** | [39.] | 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** | [39.] | Security group in AD |
| **Account Security: Rights** | [39.] | The Installer account is added automatically. |
| **Account Security: Rights** | [39.] | • The group is added to the Service Manager Administrators role automatically.<br>• The group is added to the Data Warehouse Administrators role automatically. |

### 7.7.4 Service Manager Service Account

| Items | Ref. | Description |
|---|---|---|
| **Account Type** | [39.] | Domain account |
| **Account Security: Local Rights** | [39.] | Local admin on the SCSM and SCSMDW server. |

| Items | Ref. | Description |
|---|---|---|
| **Account Security** | [39.] | 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<br><br>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** | [39.] | Domain account |
| **Account Security: Local Rights** | [39.] | Member of the local Users security group. |
| **Account Security: Local Rights** | [39.] | If email notifications are required, this account must be mail enabled. |

### 7.7.6 Reporting Account

| Items | Ref. | Description |
|---|---|---|
| **Account Type** | [39.] | Domain account |
| **Account Security: SQL** | [39.] | - Used by SSRS to access the DWDataMart data<br>- In SQL, it is added to the db_datareader and reportuser roles on the DWDataMart database. |

## 7.8 BHOLD

### 7.8.1 References

See: [41.] FIM 2010: Quick Guide to installing BHOLD Core

### 7.8.2 BHOLDApplicationGroup

| Items | Ref. | Description |
|---|---|---|
| **Account Type** | [41.] | Domain group |

### 7.8.3 BHOLD Core Service Account

| Items | Ref. | Description |
|---|---|---|
| **Account Type** | [41.] | Domain user |
| **Account Security** | [41.] | Log on as a Service |
| **Account Security** | [41.] | Password never expires |
| **Account Security** | [41.] | Add this user to the following groups:<br>- IIS_IUSRS<br>- II. ii. BHOLDApplicationGroup |

# 8 Security during Installation

## 8.1 MIM setup account – functional account

### 8.1.1.1 References

- **[14.]** Before you begin
- **[19.]** Considerations for New Installation of MIM 2016
- **[20.]** Installing the MIM 2016 Server Components
- **[5.]** Segregation of duties

### 8.1.1.2 Required settings

| Items | Ref. | Description |
|---|---|---|
| **Account type: domain account** | [20.] | You must create a user account to run installation of the MIM components.<br>This installer account must be a **domain user** account.<br>The most important reason is that the MIM installer account is assigned root administrator in the MIM 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** | [20.] | **ONLY DURING INSTALLATION**<br>To be able to install MIM Synchronization Service or MIM Service, the account must have the SQL sysadmin role on SQL Server.<br>The account that you use does not have to be a SQL sysadmin after the installation is complete, except when you deploy MIM hotfixes.<br>**By default, members of the Local Administrators group do not have the necessary permissions.**<br>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: Sharepoint** | [20.] | To be able to install the MIM Portal, the account must be a SharePoint administrator.<br>To be able to install the MIM 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 MIM Portal is authorized as an administrator of that SharePoint site. |
| **Account Security** | [20.] | **ONLY DURING INSTALLATION**<br>This account **should be** a local administrator account. |
| **Account Security** | [20.] | **ONLY DURING INSTALLATION**<br>The MIM installer accounts should **be member of the local administrators** group. |
| **Account Security** | [20.] | The MIM installer account **should only be** a **member of the security group** MIMSyncAdmins. |
| **Account security** | [20.] | Use the following restrictions on the MIM installer account:<br>• Deny logon as a batch job<br>• Deny run as a service |

| Items | Ref. | Description |
|---|---|---|
| **Account separation** | [5.] | Due to the fact that the MIM installer account is only used to install MIM component, during initial setup or during application of an hotfix, do not use this account for other purposes.<br>DO NOT<br>- use the MIM Installer account for operational, day-to-day management.<br>- Use the MIM installer account as service account<br>As other services require other privileges, the PoLP demands to use separate accounts. |

#### 8.1.1.3 Risks

| Items | Ref. | Description |
|---|---|---|
| **Same account** | [20.] | The MIM Sync Service account has HPA access to the MIM Sync Service operations, using the same account bestows too many unneeded privileges to the MIM Sync service account |

## 8.2 MIM 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 MIM configuration part is rather applying on the installation or reconfiguration of the MIM SSPR portals for assword registration or password reset.

### 8.2.1 Change mode install

#### 8.2.1.1 Reference

From: [37.] 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 MIM Password Registration and Password Reset portals you must also run a change mode install on the server that is running the MIM 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 MIM Service** and associate it with the new application pool account or accounts."*

# 9 Post-installation: Securing MIM

## 9.1 MIM Service

### 9.1.1.1 References

- [20.] Installing the MIM 2016 Server Components
- [32.] Configure Message Delivery Restrictions
- [33.] Configure Message Size Limits for a Mailbox or a Mail-enabled Public Folder
- [34.] Configure Storage Quotas for a Mailbox

### 9.1.1.2 Required settings

| Items | Ref. | Description |
|---|---|---|
| **Account type: domain account** | [20.] | Configuring the MIM Service SVCA Exchange mailbox<br>1. Configure the service account so that it can accept mail only from internal e-mail addresses<br>2. Configure the service account so that it rejects mail messages with sizes greater<br>3. Configure the service account so that it has a mailbox storage quota of 5 gigabytes (GB). than 1 MB. |

## 9.2 MIM Portal (SharePoint)

### 9.2.1 Reference

- [17.] Step 7: Perform MIM 2016 Prerequisite Tasks

| Items | Ref. | Description |
|---|---|---|
| **Account type** | [17.] | Change the SharePoint Application Pool Account to Use CORP\SPService |

### 9.2.2 SharePoint in depth

See, page 62, 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<br>- logon name = corresponding AD sAMAccountName<br>- Domain = logondomain (NetBIOS) of domain user is logging on to<br>- objecSid = objectSid of user account |

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

- synchronizing the accounts into the portal from AD, via the MIM 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 MIM Service / MIM portal will be assigned as **primary portal administrator**, as it will be added to the Administrators set in the MIM Portal.

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

# 10 Post-installation: Securing MIM 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 MIM portal:

- synchronizing the accounts into the portal from AD, via the MIM 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 MIM Service / MIM portal will be assigned as primary portal administrator, as it will be added to the Administrators set in the MIM Portal .This account must be filtered from the MIM MA to avoid accidental deletion or modification which blocks access to the MIM portal.

### 10.1.3 MIM Service

The account that is used to run the MIM Service / MIM portal will be assigned elevated rights in these platforms.

This account must be filtered from the MIM MA to avoid accidental deletion or modification which MIM Service and portal operations.

### 10.1.4 Secondary / personal administrator accounts

To manage the portal additional administrators must be added to the 'Administrators' set.

But its key to limit the accounts for the administrators in the portal to the absolute minimum.

To setup a delegated access model to the MIM portal, you must use other MPRs for fine grained access.

# 11 Operational best practices

## 11.1 References

- [15.] Using Security Groups

## 11.2 MIM Default folders

| | Importance | Items | Ref. | Description |
|---|---|---|---|---|
| ☐ | MEDIUM | Default File and folder permissions | [14.] | Do not change permissions on the default files and folders<br>When reinstalling MIM component or applying a MIM hotfix, these permissions will be reset. |

## 11.3 Database

| | Importance | Items | Ref. | Description |
|---|---|---|---|---|
| ☐ | MEDIUM | Database backup | | MIM databases backup must be executed same time or within very short time frame (as they need to be restored from the same point in time) |
| ☐ | MEDIUM | Default Database permissions | [14.] | Do not change permissions on the default database settigns<br>When reinstalling MIM component or applying a MIM hotfix, these permissions will be reset. |
| ☐ | MEDIUM | Database restoration | | MIM database restoration (at least MIM Service and MIM Sync DB) must happen from databases at the same point of time. Do not restore MIM Service and MIM Sync DB from different time frames, different backups… |
| ☐ | MEDIUM | Database restoration | | MIM database restoration (at least MIM Service and MIM Sync DB) must happen from databases at the same point of time. Do not restore MIM Service and MIM Sync DB from different time frames, different backups… |

## 11.4 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… |

## 11.5 DTAP & debug tools

| | Importance | Items | Ref. | Description |
|---|---|---|---|---|
| ☐ | MEDIUM | Debug tools | | Only install debug tools on the production server, when no other options left, and only for the time required during debugging. |

| | Importance | Items | Ref. | Description |
|---|---|---|---|---|
| ☐ | HIGH | DTAP environment | | Make sure to have a separation between dev, pre-production and production environment, to avoid any deployment issues in production |

## 11.6 DRP

| | Importance | Items | Ref. | Description |
|---|---|---|---|---|
| ☐ | HIGH | Backup | | Make sure to have a backup of the MIM databases within the shortest time frame possible (as the database require restoration from the same status) |
| ☐ | HIGH | Restore | | If you need to restore the MIM Service or MIM Sync database, both need to be restored at the same time, to keep the MIM service objects in line with the MIM Sync database (requests, workflows…) |

## 11.7 Hotfixes and patching

| | Importance | Items | Ref. | Description |
|---|---|---|---|---|
| ☐ | HIGH | Patching | | Mare sure all MIM components are updated to the latest hotfix level, unless a very clear contra-indication is present (like hotfix breaking your environment) |
| ☐ | HIGH | Patching | | Mare sure all MIM components are updated with the same hotfix level. Hotfix levels must be in sync on all MIM components |

# 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<br>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<br>Click here to download The Administrator Accounts Security Planning Guide from the Microsoft Download Center. |
| [5.] | Segregation of duties aka. Separation of duties | Separation of Duties in Information Technology |
| [6.] | Principle of Least Privilege | Implementing Least-Privilege Administrative Models |
| [7.] | Privilege separation | https://buildsecurityin.us-cert.gov/articles/knowledge/principles/separation-of-privilege |
| [8.] | 4-eyes principle | http://whatis.techtarget.com/definition/four-eyes-principle |

## 12.2 MIM

### 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 |
| [10.] | Release Notes for Forefront Identity Manager 2010 R2 | https://technet.microsoft.com/en-us/library/hh322889 |

### 12.2.2 MIM Best practices

| Ref. no. | Document | Description |
|---|---|---|
| [11.] | Microsoft Identity Manager 2016 Best Practices | https://learn.microsoft.com/en-us/microsoft-identity-manager/mim-best-practices |
| [12.] | 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 Deprecated features

| Ref. no. | Document | Description |
|---|---|---|
| **[13.]** | Deprecated Features And Planning For The Future | https://learn.microsoft.com/en-us/microsoft-identity-manager/microsoft-identity-manager-2016-deprecated-features |

### 12.2.4 MIM Security

| Ref. no. | Document | Description |
|---|---|---|
| **[14.]** | FIM 2010 Installation Guide > Before you begin | https://ffwd2.me/fimbeforeyoubegin |
| **[15.]** | Using Security Groups | http://technet.microsoft.com/en-us/library/jj590183(v=ws.10).aspx |
| **[16.]** | Test Lab Guide: Installing Forefront Identity Manager 2010 R2 | http://technet.microsoft.com/en-us/library/hh322905(v=ws.10).aspx |
| **[17.]** | Step 7: Perform MIM 2016 Prerequisite Tasks | http://technet.microsoft.com/en-us/library/hh322882(v=ws.10) |
| **[18.]** | FIM 2010 R2 Kerberos Settings (SPN Configuration) | http://technet.microsoft.com/en-us/library/jj134299(v=ws.10).aspx |
| **[19.]** | Considerations for New Installation of FIM 2020 R2 | http://technet.microsoft.com/en-us/library/jj134293(v=ws.10).aspx |
| **[20.]** | Installing the MIM 2016 Server Components | https://technet.microsoft.com/en-us/library/hh332711(v=ws.10).aspx |

### 12.2.5 MIM Best practices for security

| Ref. no. | Title (alphabetically) | URL |
|---|---|---|
| **[21.]** | Forefront Identity Manager 2010 R2 Best Practices for Security | https://learn.microsoft.com/en-us/previous-versions/mim/jj590274(v=ws.10) |
| **[22.]** | FIM 2010 (R2): Well-known GUIDS | https://ffwd2.me/FIMGuids |
| **[23.]** | Best practices for the FIM Portal Administrator account | http://www.wapshere.com/missmiis/best-practices-for-the-fim-portal-administrator-account |

### 12.2.6 MIM Best practice analyzer (BPA)

| Ref. no. | Title (alphabetically) | URL |
|---|---|---|
| **[24.]** | Best Practice Analyzer for Forefront Identity Manager 2010 R2 | https://technet.microsoft.com/en-us/library/jj203402(v=ws.10).aspx |
| **[25.]** | MIM 2016: Same Account being used for FIM Synchronization Service and FIM MA | https://technet.microsoft.com/en-us/library/jj204553(v=ws.10).aspx |
| **[26.]** | MIM 2016: MIM Service or the MIM Synchronization Service Account does not have Deny Logon As Batch Job set | https://technet.microsoft.com/en-us/library/jj204563(v=ws.10).aspx |

### 12.2.7 MIM Sync

| Ref. no. | Title (alphabetically) | URL |
|---|---|---|
| [27.] | Forefront Identity Manager Password Management | https://technet.microsoft.com/en-us/library/jj590203(v=ws.10).aspx |
| [28.] | Management Agent Communication Ports, Rights, and Permissions | https://learn.microsoft.com/en-us/previous-versions/mim/cc720599(v=ws.10)?redirectedfrom=MSDN |

### 12.2.8 MIM PCNS

| Ref. no. | Title (alphabetically) | URL |
|---|---|---|
| [29.] | Forefront Identity Manager Password Management | https://technet.microsoft.com/en-us/library/jj590203(v=ws.10).aspx |
| [30.] | Pcnscfg: Password Change Notification Service (PCNS) Configuration Utility | https://technet.microsoft.com/en-us/library/jj590227(v=ws.10).aspx |
| [31.] | Using Password Synchronization | https://technet.microsoft.com/en-us/library/jj590288(v=ws.10).aspx |

### 12.2.9 MIM Service

| Ref. no. | Title (alphabetically) | URL |
|---|---|---|
| [32.] | Configure Message Delivery Restrictions | http://go.microsoft.com/fwlink/?LinkId=183625 |
| [33.] | Configure Message Size Limits for a Mailbox or a Mail-enabled Public Folder | http://go.microsoft.com/fwlink/?LinkId=183626 |
| [34.] | Configure Storage Quotas for a Mailbox | http://go.microsoft.com/fwlink/?LinkId=156929 |

### 12.2.10 MIM SSPR

| Ref. no. | Title (alphabetically) | URL |
|---|---|---|
| [35.] | 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 |
| [36.] | Password Reset Deployment Guide | https://technet.microsoft.com/en-us/library/ee534892(v=ws.10).aspx |
| [37.] | Password Registration and Reset Portal Deployment | https://technet.microsoft.com/en-us/library/jj134295(v=ws.10).aspx |

### 12.2.11 MIM CM

| Ref. no. | Title (alphabetically) | URL |
|---|---|---|
| [38.] | Create FIM 2010 CM service accounts using PowerShell | https://konab.com/create-fim-2010-cm-service-accounts-using-PowerShell/ |
| [39.] | Create an OU and User Accounts for MIM CM Agents | https://technet.microsoft.com/en-us/library/gg430115(v=ws.10).aspx |

### 12.2.12 MIM Reporting

| Ref. no. | Title (alphabetically) | URL |
|---|---|---|
| [40.] | MIM 2016 Reporting Permissions | http://aka.ms/fimreportingpermissions (deprecated) |

### 12.2.13 BHOLD

| Ref. no. | Title (alphabetically) | URL |
|---|---|---|
| [41.] | 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 |
| [42.] | Microsoft BHOLD Suite SP1 Installation Guide | https://technet.microsoft.com/en-us/library/jj134107(v=ws.10).aspx |
| [43.] | BHOLD Core Installation | https://technet.microsoft.com/en-us/library/jj134095(v=ws.10).aspx |
| [44.] | 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 |
|---|---|---|
| [45.] | Guidelines on choosing Service Accounts for SQL Server Services. | http://support.microsoft.com/kb/2160720 |
| [46.] | Server Configuration - Service Accounts | https://msdn.microsoft.com/en-us/library/cc281953.aspx |
| [47.] | SQL Server 2005 Security Best Practices - Operational and Administrative Tasks | (download) https://download.microsoft.com/download/8/5/e/85eea4fa-b3bb-4426-97d0-7f7151b2011c/SQL2005SecBestPract.doc |
| [48.] | SQL Server 2008 R2 Security Best Practice Whitepaper | https://www.microsoft.com/en-gb/download/details.aspx?id=436 |
| [49.] | SQL Server 2012 Security Best Practice Whitepaper | https://download.microsoft.com/download/8/f/a/8fabacd7-803e-40fc-adf8-355e7d218f4c/sql_server_2012_security_best_practice_whitepaper_apr2012.docx |
| [50.] | Service Account Types Supported for SQL Server Agent: | http://go.microsoft.com/fwlink/?LinkId=183624 |
| [51.] | Selecting an Account for the SQL Server Agent Service | http://go.microsoft.com/fwlink/?LinkId=12295 |

## 12.4 SharePoint

| Ref. no. | Title (alphabetically) | URL |
|---|---|---|
| [52.] | Plan for administrative and service accounts (Office SharePoint Server) | http://technet.microsoft.com/en-us/library/cc263445(v=office.12).aspx |
| [53.] | Plan administrative tasks in a least-privilege environment (SharePoint Server 2010) | https://technet.microsoft.com/en-us/library/hh377944(v=office.14).aspx |

| Ref. no. | Title (alphabetically) | URL |
|---|---|---|
| [54.] | Initial deployment administrative and service accounts (SharePoint Server 2010) | https://technet.microsoft.com/en-us/library/ee662513%28v=office.14%29.aspx |
| [55.] | Administrative accounts | https://technet.microsoft.com/en-us/library/55b99d80-3fa7-49f0-bdf4-adb5aa959019(v=office.14)#Section2 |
| [56.] | 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 |
|---|---|---|
| [57.] | Security Best Practices for IIS 8 | http://technet.microsoft.com/en-us/library/cc263445(v=office.12).aspx |

## 12.6 AD

| Ref. no. | Title (alphabetically) | URL |
|---|---|---|
| [58.] | Service Principal Names | https://msdn.microsoft.com/en-us/library/windows/desktop/ms677949(v=vs.85).aspx |
| [59.] | Group types | https://technet.microsoft.com/en-us/library/cc781446(v=ws.10).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 |
| Improving security through least-privilege practices | http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/improving-security-through-least-privilege-practices.html |
| Dev and Test Domains do not belong in your Production forest! | http://blog.joeware.net/2013/02/20/2674/ |
| Highly Available Active Directory | http://blog.joeware.net/2009/03/11/1623/ |
| You do, in fact, have a lab environment. What you do not have is a production environment. | http://www.activedir.org/MailingList/tabid/55/view/topic/postid/33143/Default.aspx |

## 13.2 Microsoft Identity Manager

### 13.2.1 Product builds

| Title (alphabetically) | URL |
|---|---|
| Identity Manager version release history | https://learn.microsoft.com/en-us/microsoft-identity-manager/reference/version-history |
| FIM 2010 Build overview | https://social.technet.microsoft.com/wiki/contents/articles/2229.fim-2010-build-overview.aspx |

### 13.2.2 MIM Prerequisites

| Title (alphabetically) | URL |
|---|---|
| Step 6: Install MIM 2016 Prerequisite Software | https://technet.microsoft.com/en-us/library/hh322909(v=ws.10).aspx |

### 13.2.3 MIM Best practices

| Title (alphabetically) | URL |
|---|---|
| Forefront Identity Manager 2010 R2 Best Practices | https://learn.microsoft.com/en-us/previous-versions/mim/jj590305(v=ws.10) |
| Forefront Identity Manager 2010 R2 Best Practices General | https://learn.microsoft.com/en-us/previous-versions/mim/jj590345(v=ws.10) |
| Forefront Identity Manager 2010 R2 Best Practices for Security | https://learn.microsoft.com/en-us/previous-versions/mim/jj590274(v=ws.10) |
| Microsoft Identity Manager 2016 Best Practices | https://learn.microsoft.com/en-us/microsoft-identity-manager/mim-best-practices |

### 13.2.4 MIM On-disk help

| Title (Alphabetically) | URL |
|---|---|
| MIM 2016 Synchronization Service On-disk Help | https://technet.microsoft.com/en-us/library/jj572795%28v=ws.10%29.aspx |

### 13.2.5 Deprecated Features

| Items | URL |
|---|---|
| Deprecated Features And Planning For The Future | https://learn.microsoft.com/en-us/microsoft-identity-manager/microsoft-identity-manager-2016-deprecated-features |

### 13.2.6 MIM 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 MIM Sync

| Items | URL |
|---|---|
| Management Agent Communication Ports, Rights, and Permissions | http://technet.microsoft.com/en-us/library/cc720599(WS.10).aspx |
| [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 MIM 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 MIM 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 |
| MIM 2016 on Sharepoint 2019/2016 | https://learn.microsoft.com/en-us/microsoft-identity-manager/prepare-server-sharepoint |

### 13.2.11 MIM Reference collections - Online

| Items | URL |
|---|---|
| FIM 2010 - Bookmarks Collection | https://social.technet.microsoft.com/wiki/contents/articles/32588.mim-2016-bookmarks-collection-curation.aspx?WT.mc_id=ES-MVP-5002204 |
| Getting started with FIM 2010 - Resources for FIM starters | https://social.technet.microsoft.com/wiki/contents/articles/33620.fimmim-resources-for-starters.aspx |
| Forefront Identity Manager Resources | https://social.technet.microsoft.com/wiki/contents/articles/399.forefront-identity-manager-resources.aspx |
| FIM 2010 Build Overview | https://social.technet.microsoft.com/wiki/contents/articles/2229.fim-2010-build-overview.aspx |
| FIM 2010 Planning and Architecture Collection | https://www.microsoft.com/en-us/download/details.aspx?id=9094 |

### 13.2.12 SQL

| Items | URL |
|---|---|
| SQL Builds | https://learn.microsoft.com/en-US/troubleshoot/sql/releases/download-and-install-latest-updates |

## 13.3 MIM 2016 Product info

| Title (alphabetically) | URL |
|---|---|

| | |
|---|---|
| **MIM 2016** | https://learn.microsoft.com/en-us/microsoft-identity-manager/microsoft-identity-manager-2016 |
| **MIM 2016 Product documentation** | https://learn.microsoft.com/en-us/microsoft-identity-manager/ |

## 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 |

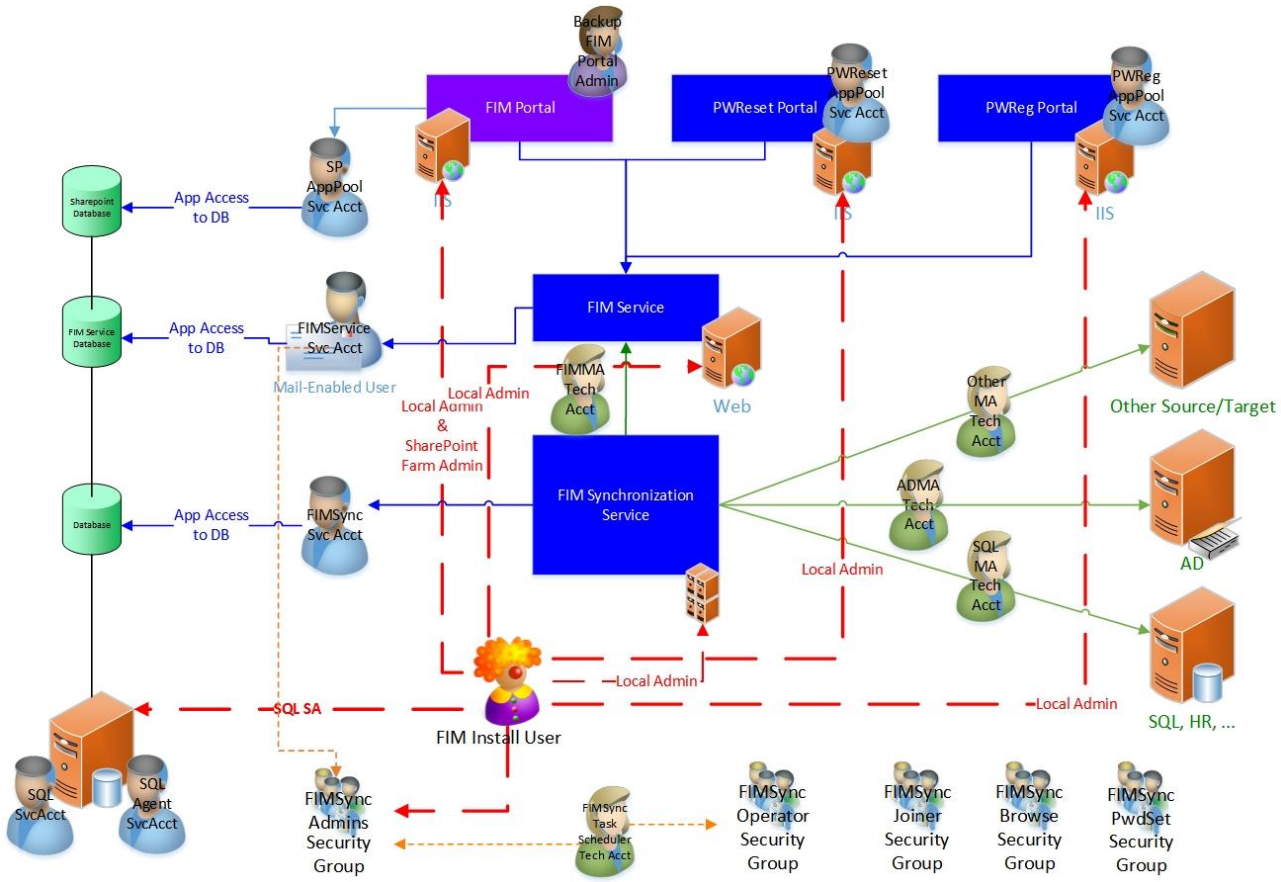
# 14 Glossary, abbreviations & acronyms

| Acronym | Description | See also |
|---|---|---|
| **AAD** | Azure AD | |
| **AAD Connect** | Azure AD Connect<br>= 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 Directory Sync | |
| **CM** | Certificate Manager,<br>Certificate Management | |
| **CS** | Connector space<br>Component of MIM 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 | |
| **MIM Sync Svc** | MIM Synchronization Service | |
| **MIMSync** | MIM Synchronization | |
| **MIM Sync** | MIM Synchronization | |
| **FIM** | Forefront Identity Manager 2010 (R2) | FIM 2010, FIM 2010 R2 |
| **MIMCM** | MIM Certificate Manager | |
| **LSG** | Local Security Group | |
| **DLSG** | Domain Local Security Group | |
| **HPA** | Highly privileged account | |
| **MIIS** | Microsoft Identity Integration Server 2003 | MIIS 2003 |
| **MIM** | Microsoft Identity Manager 2016 | MIM 2016 |
| **MV** | Metaverse, Component of MIM Sync | |
| **O365** | Office 365 | |
| **PCNS** | Password Change Notification Service | |
| **PROD** | Production | |
| **PW** | Password | |

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

# 15 Index

# Appendix A: Account overview for MIM basic configuration



# Appendix B: Documentation - Compact Check list

## Legend

- LOC = location
- D : Domain

### Check boxes

☒ not applicable

☑ implemented

☐ not implemented

## Pre-installation: Backend configuration

### Set SPN

| | Im-portance | LOC | Acct. Type | Account Reference | Name (to fill) |
|---|---|---|---|---|---|
| ☐ | HIGH | D | SPN | SQL Database Account | <domain>\<account> |
| ☐ | HIGH | D | SPN | MIM 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 | MIM CM Web Pool Agent Account | |

### Kerberos Constrained delegation

| | Importance | LOC | Acct. Type | Account Reference | Name (to fill) |
|---|---|---|---|---|---|
| ☐ | HIGH | D | msDS-Al-lowedToDel-egateTo | FIMService/<MIM Service Server> | MIM Service Account<br><domain>\<account> |
| ☐ | HIGH | D | msDS-Al-lowedToDel-egateTo | FIMService/<MIM Service Server> | SharePoint Service Account<br><domain>\<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 MIM Platforms

| | Importance | LOC | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Functional | MIM installer administrator account* | <domain>\<account> |

## MIM Synchronization

| | Importance | LOC | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Service | MIM Sync service | <domain>\<account> |
| ☐ | HIGH | D | Security Group | MIMSyncAdmins | <domain>\<account> |
| ☐ | HIGH | D | Security Group | MIMSyncOperators | <domain>\<account> |
| ☐ | HIGH | D | Security Group | MIMSyncJoiners | <domain>\<account> |
| ☐ | HIGH | D | Security Group | MIMSyncBrowse | <domain>\<account> |
| ☐ | HIGH | D | Security Group | MIMSyncPasswordSet | <domain>\<account> |
| ☐ | HIGH | D | Technical | MIM Task scheduler | <domain>\<account> |

## MIM Sync MAs

| | Importance | LOC | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Technical | ADMA Account | <domain>\<account> |
| ☐ | See below | D | Technical | MIMMA Account | |
| ☐ | HIGH | D | Technical | SQL MA Account | <domain>\<account> |
| ☐ | HIGH | D | Technical | Other MAs: 1 account per type of MA and by preference 1 account per MA. | <domain>\<account> |

## MIM Service

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

## MIM Portal

| | Importance | LOC | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|---|---|
| ☐ | MEDIUM | D | Functional | Backup Portal Administrator | <domain>\<account> |

| | Importance | LOC | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Functional | MIM Portal - Application Pool Account | <domain>\<account> |

### MIM SSPR Registration Portal

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

### MIM SSPR Reset Portal

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

### MIM CM

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

## Pre-installation: Account lock down

### General

| | Importance | LOC | Account Type | Account Reference | Procedure |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Functional | MIM Installer account | Just before installation[3]<br>Grant local admin rigths |

### MIM Sync

| | Action | Account |
|---|---|---|
| ☐ | Account creation | |
| ☐ | Account Configuration | |

### AD

| | Importance | LOC | Account Type | Account Reference | Procedure |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Functional | MIM ADMA | Replicating Directory Changes |

[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.

| | Importance | LOC | Account Type | Account Reference | Procedure |
|---|---|---|---|---|---|
| ☐ | HIGH | D | Functional | MIM ADMA | Lock down the account to the minimum required permissions to the minimum required containers |

# Post-Installation

## Account Assignment

### MIM Service & MIM Portal

| | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|
| ☐ | Functional account | Add Backup Portal Administrator account to Administrators set | <domain>\<account> |

### MIM Sync

| | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|
| ☐ | Personal account | Add MIM Administrator account to MIMSyncAdmins group | <domain>\<account> |
| ☐ | Service Account | Add MIM Servcie account to MIMSyncAdmins group | <domain>\<account> |

# Hotfix installation

## Account Assignment

### All MIM platforms

| | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|
| ☐ | Functional account | Add MIM Setup account to<br>- SQL SA<br>- Local server admin (via AD) | <domain>\<account> |

### MIM Service & MIM Portal

| | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|
| ☐ | Functional account | Add Backup Portal Administrator account to Administrators set | <domain>\<account> |

### MIM Sync

| | Account Type | Account Reference | Name (to fill) |
|---|---|---|---|
| ☐ | Personal account | Add MIM Administrator account to FIMSyncAdmins group | <domain>\<account> |

# Appendix C: Security Implementation Sign-off sheet

The sheet below can be used to sign-off for a MIM implementation, to validate that a MIM 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 MIM infrastructure, or his authorized direct delegates signs off for the exceptions.

## CISO or authorized security delegate

| **Item** | **<FILL 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** | ☐ |

## MIM Options implemented

Please check which MIM 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** |
|---|---|---|---|
| ☐ | MIM Sync Server | ☐ | ☐ |
| ☐ | PCNS | ☐ | ☐ |
| ☐ | MIM Service | ☐ | ☐ |
| ☐ | MIM Portal | ☐ | ☐ |
| ☐ | SSPR: Password registration Portal | ☐ | ☐ |
| ☐ | SSPR: Password reset Portal | ☐ | ☐ |
| ☐ | MIM CM | ☐ | ☐ |
| ☐ | MIM 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 |
|---|---|---|---|
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |