|  |
| --- |
|  |
| Microsoft Identity manager  Security Baseline Configuration - Check list |
|  |
| Wednesday, 24 May 2023  Version 2.0.0. Draft |
|  |
| Prepared by  Peter Geelen  Executive Director - Microsoft MVP Security (Identity & Access) |

Revision

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

[Appendix A: Account overview for MIM basic configuration 5](#_Toc135861424)

[Appendix B: Documentation - Compact Check list 6](#_Toc135861425)

[Legend 6](#_Toc135861426)

[Check boxes 6](#_Toc135861427)

[Pre-installation: Backend configuration 6](#_Toc135861428)

[Set SPN 6](#_Toc135861429)

[Kerberos Constrained delegation 6](#_Toc135861430)

[Pre-installation: Account creation 6](#_Toc135861431)

[Back End 6](#_Toc135861432)

[All MIM Platforms 7](#_Toc135861433)

[MIM Synchronization 7](#_Toc135861434)

[MIM Sync MAs 7](#_Toc135861435)

[MIM Service 7](#_Toc135861436)

[MIM Portal 7](#_Toc135861437)

[MIM SSPR Registration Portal 8](#_Toc135861438)

[MIM SSPR Reset Portal 8](#_Toc135861439)

[MIM CM 8](#_Toc135861440)

[Pre-installation: Account lock down 8](#_Toc135861441)

[General 8](#_Toc135861442)

[MIM Sync 8](#_Toc135861443)

[AD 8](#_Toc135861444)

[Post-Installation 9](#_Toc135861445)

[Account Assignment 9](#_Toc135861446)

[MIM Service & MIM Portal 9](#_Toc135861447)

[MIM Sync 9](#_Toc135861448)

[Hotfix installation 9](#_Toc135861449)

[Account Assignment 9](#_Toc135861450)

[All MIM platforms 9](#_Toc135861451)

[MIM Service & MIM Portal 9](#_Toc135861452)

[MIM Sync 10](#_Toc135861453)

[Appendix C: Security Implementation Sign-off sheet 11](#_Toc135861454)

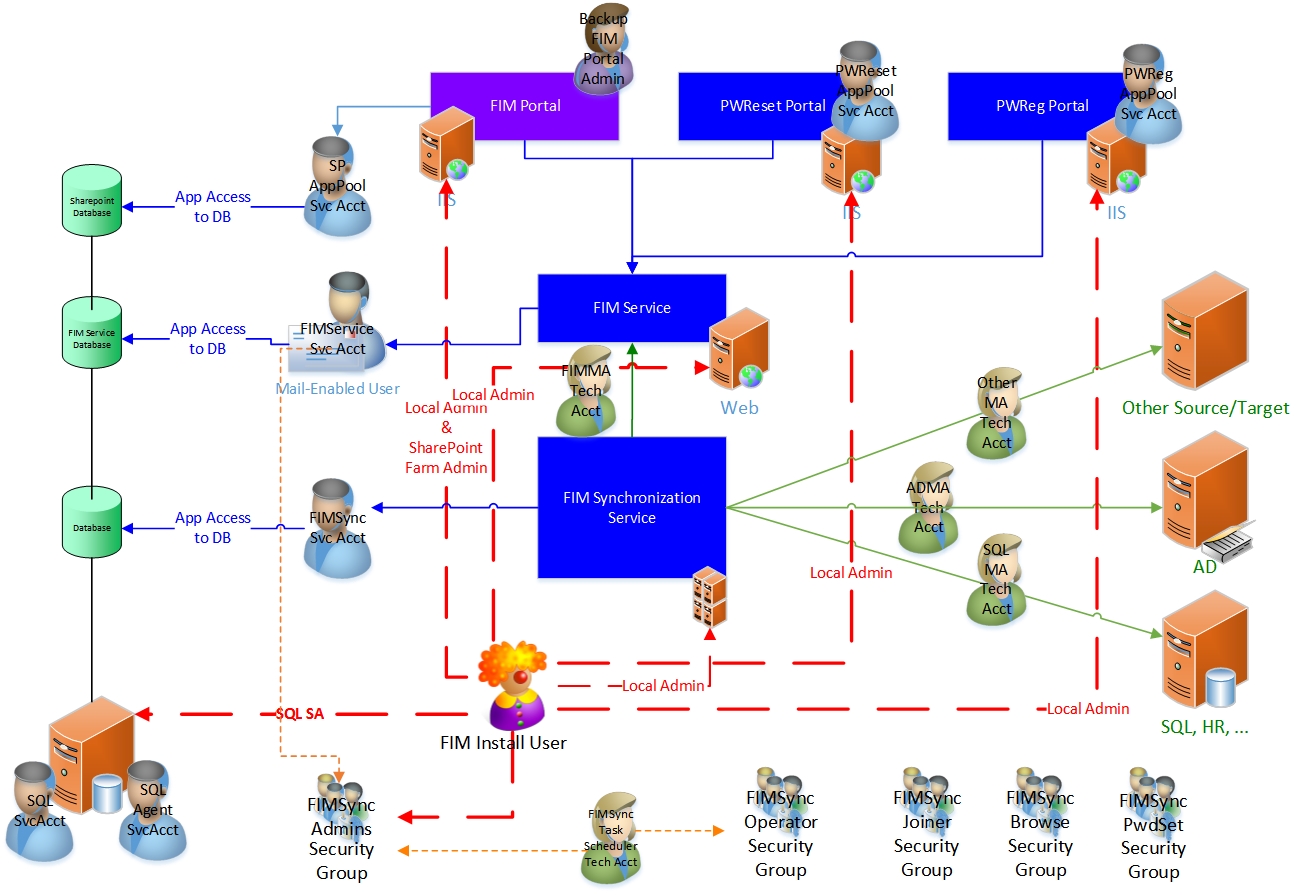
[CISO or authorized security delegate 11](#_Toc135861455)

[Sign off 11](#_Toc135861456)

[MIM Options implemented 11](#_Toc135861457)

[Derogations - Exceptions implemented 12](#_Toc135861458)

# 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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Importance | 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 | <domain>\<account> | |

### Kerberos Constrained delegation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Importance | LOC | Acct. Type | Account Reference | Name (to fill) |
| 🞎 | HIGH | D | msDS-AllowedToDelegateTo | FIMService/<MIM Service Server> | MIM Service Account  <domain>\<account> | |
| 🞎 | HIGH | D | msDS-AllowedToDelegateTo | FIMService/<MIM Service Server> | SharePoint Service Account  <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](javascript:void(0)) | <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> |
| 🞎 | 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[[1]](#footnote-2)  Grant local admin rights |

### MIM Sync

|  |  |  |
| --- | --- | --- |
|  | Action | Account |
| 🞎 | Account creation |  |
| 🞎 | Account Configuration |  |

### AD

|  | Importance | LOC | Account Type | Account Reference | Procedure |
| --- | --- | --- | --- | --- | --- |
| 🞎 | HIGH | D | Functional | MIM ADMA | [Replicating Directory Changes](https://support.microsoft.com/en-us/kb/303972) |
| 🞎 | HIGH | D | Functional | MIM ADMA | Lock down the account to the minimum required permissions to the minimum required containers |

## Post-Installation

### Account Assignment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Importance | LOC | Account Type | Account Reference | Procedure |
| 🞎 | HIGH | D | Functional | MIM Installer account | After installation[[2]](#footnote-3)  Remove   * local admin rights * SQL SA permissions   where applicable |

### 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   * SQL SA * 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 |
| 🞎 |  |  |  |
| 🞎 |  |  |  |
| 🞎 |  |  |  |
| 🞎 |  |  |  |
| 🞎 |  |  |  |
| 🞎 |  |  |  |
| 🞎 |  |  |  |
| 🞎 |  |  |  |
| 🞎 |  |  |  |
| 🞎 |  |  |  |
| 🞎 |  |  |  |
| 🞎 |  |  |  |
| 🞎 |  |  |  |

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. [↑](#footnote-ref-2)
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. [↑](#footnote-ref-3)