IBM_logo_87x30

IBM® OpenPages® GRC Platform

Migrate\_ePolicy Service  
a POC\_MVP SDI Solution

Install/Update Instructions

Readme File

POC\_MVP development team:

Anil Pandey (anpde186@in.ibm.com)

Thapaswi Jagadhapi (tjagad09@in.ibm.com)

Eddie Hartman ([eddie.hartman@no.ibm.com](mailto:eddie.hartman@no.ibm.com))

Updated Oct 13 2020

TABLE OF CONTENTS

[Installation Instructions 3](#_Toc54001675)

[The POC\_MVP Solution Overview 3](#_Toc54001676)

[Updating POC\_MVP 4](#_Toc54001677)

[Verifying Certificates and Settings 5](#_Toc54001678)

# Installation Instructions

First locate the SDI Server’s *Solution Directory* (abbreviated SolDir). The SolDir is the current working directory for the SDI Server, and is the location for the following important sub-folders:

* serverapi – the location of the keystore file used for storing SSL certificates
* logs – the location of log files

The location of the SolDir is defined by an environment variable, TDI\_SOLDIR, just as the SDI installation folder (e.g. V7.2) is set in the TDI\_HOME\_DIR variable. These values are set/exported in scripts found in ${TDI\_HOME\_DIR}/bin folder, with defaultSoldir.sh (or .bat for Windows) used to set the SolDir and setupCmdLine.sh (.bat) defining several, including TDI\_HOME\_DIR.

The Solution Directory is also the location of the solution.properties file which holds Java properties that control both the JVM and the SDI Server itself. Among the settings defined here are the API ports (RMI and REST), the location and password(s) to key- and truststores used, and authentication settings for the web-based Admin.

## The POC\_MVP Service Overview

The POC\_MVP solution itself consists of a set of text files that must be present in a sub-folder of the SDI SolDir. This folder is named after the solution itself. In the case of the Migrate ePolicy Service, the solution framework is *POC\_MVP* and therefore the solution folder will be:

/local/IBM/TDI/SolDir/POC\_MVP

The following files must be present in this folder:

|  |  |
| --- | --- |
| POC\_MVP.xml | The SDI solution Config file |
| POC\_MVP.properties | Configuration settings for the solution |
| id\_rsa.pub | Key used to access GSA via scp |
| id\_rsa | Private key used for scp |
| fields\_evidencelog.txt | List of fields used for Evidence Log |
| fields\_historylog.txt | List of fields used for History Log |
| fields\_validationlog.txt | List of fields used for Validation Log |
| map\_csd\_to\_Policy.map | Map from CSD to Policy |
| map\_csd\_to\_techspec.map | Map from CSD to TechSpec |
| map\_csddoc.map | Map for CSD doc to Policy doc |
| map\_evidence.map | Map for Evidences |
| map\_evidencedoc\_techspec.map | Map for Evidence doc for TechSpec |
| map\_evidencedoc.map | Map for Evidence doc for Policy |
| map\_evidencelog.map | Map for Evidence Log for Policy |
| map\_evidencelogdoc\_techspec.map | Map for Evidence Log doc for TechSpec |
| map\_evidencelogdoc.map | Map for Evidence Log doc for Policy |
| map\_historylog.map | Map for History Log for Policy |
| map\_historylogdoc\_techspec.map | Map for History Log doc for TechSpec |
| map\_historylogdoc.map | Map for History Log doc for Policy |
| map\_migrationlog.map | Map for Abstract of Migration Log |
| map\_procedure.map | Map for Clauses |
| map\_proceduredoc.map | Map for Clauses doc |
| map\_techspec\_doc.map | Map for TechSpec doc |
| map\_validationlog.map | Map for Validation Log |
| map\_validationlogdoc\_techspec.map | Map for Validation Log doc for TechSpec |
| map\_validationlogdoc.map | Map for Validation Log doc for Policy |
| query\_control\_clause\_rr.txt | Query for RR Clauses |
| query\_control\_clause\_rv.txt | Query for RV Clauses |
| query\_controls.txt | Query for Clause Controls |
| query\_csd\_document.txt | Query for CSD doc |
| query\_evidence\_attachment.txt | Query for Evidence doc(s) |
| query\_evidence\_log.txt | Query for Evidence logs |
| query\_evidence.txt | Query for Evidences |
| query\_history\_log.txt | Query for History Logs |
| query\_policy.txt | Query for CSDs (Policies) |
| query\_technicalspecifications.txt | Query for TechSpecs |
| query\_techspec\_document.txt | Query for TechSpec docs |
| query\_validation\_log.txt | Query for Validation Logs |

There may be other files in the folder, however these do not have an effect on the Migrate\_ePolicy solution, and will be part of other *POC\_MVP*-based solutions.

## Updating POC\_MVP.xml

Typically the only file replaced for most updates is the Config xml itself: POC\_MVP.xml

Sometimes changes may be required for the POC\_MVP.properties file. At present this configuration file looks similar to this:

##{PropertiesConnector} savedBy=06857S744, saveDate=Fri Aug 07 17:55:31 IST 2020

#

# OpenPages Settings

op.uri.root=/grc/api

op.url=https://gtsus-uat01.op.ibmcloud.com

op.username=eddie.hartman@no.ibm.com

{protect}-op.password={encr}Acehrttw234ff…..

#

# Policy Template in OpenPages

policy.template=POLT-102

#

# GSA Setting Below

gsa.username=itrmop

gsa.folder.path=/gsa/pokgsa-p7/03/sarmecm\_prd/Openpages/

gsa.hostname=pokgsa.ibm.com

#

# Schedule for running Risk\_2\_csv

schedule=\* \* \* 0 0 0

#

# GEO this solution is running - it is appended to the CSV filename

geo=EMEA

#

# Settings for the SMTP service used to send email notifications

smtp.hostname=smtp.gmail.com

smtp.port=465

smtp.username=service\_user@gmail.com

smtp.password=thepassword

**For installation and configuration of production server, ensure the GTS SDI Service Account credentials for openpages are set to the values of these properties :**

**op.username**

**op.password**

**Furthermore, the hostname, port and credentials to access the Mail server must also be entered here. A mentioned below, to have SDI encrypt any property in the file, simply prepend the property name with {protect}- and this value will we encrypted the next time the solution is loaded – e.g. when the SDI Server is restarted.**

Note that if encrypted property values must be updated, simply replace everything to the right of the equals sign with the new value in clear text, removing {encr} but leaving {protect}- in place at the start of the line. The next time the SDI Server starts up it will re-write the property file to encrypt these protected property values.

## Verifying Certificates and Settings

In order to test settings and connectivity, ensure that the SDI Server is **not** running, for example with this linux commandline:

ps x | grep V7.2 | cut -c -80

The output will look something like this:

A screenshot of a cell phone

Description automatically generated

The process that starts the ServerLauncher is the SDI Server. Killing this process brings down the Server. Note that when restarted, the solution will automatically reschedule.

Once you are sure the SDI Server is not running then you can use the following command to verify the installation:

%TDI\_INSTALLDIR%/ibmdisrv -c POC\_MVP/POC\_MVP.xml -r verify

The resulting output should look something like this:

A screenshot of a social media post

Description automatically generated

You can ignore any errors that occur before the *OS detected:* message appears, although please note these down and inform the POC\_MVP development team.

The above output indicates that the installation is correct.

Note however, the Migrate ePolicy service will be passed the hostname and credentials to an ePolicy database to be used for the migration. As a result, the certificates required for a secure connection to the database must be pre-installed to the SDI keystore. For the AG and AP geos there will be only a single database instance. However, for EMEA there will be more than one, and the certificates for all servers must be pre-loaded.

For more information on how to request and load certificates, see the Readme\_SDI Setup.pdf document.