IBM Multi-Cloud Data Encryption

Version 2.3

Quick Start Guide

This guide gets you started with a typical IBM Multi-Cloud Data Encryption installation.

Product overview

IBM Multi-Cloud Data Encryption (MDE) is a comprehensive data security product that is powered by SPx® technology that combines data-at-rest encryption with powerful protection features of a Policy Provisioning Manager (PPM). The PPM acts as a management server console that enables the provisioning of encryption agents, data access policy settings, management of key lifecycle, agent updates, and user access logging for up to 25,000 agents from a single central location.

1 Step 1: Access the software and documentation

- Download the OVA for Multi-Cloud Data Encryption from Passport Advantage®.
- Review the Release Notes for Multi-Cloud Data Encryption before installation.
- For the complete documentation, see the IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/SSTD4E_2.3.0/doc/kc_welcome_mde23.html). The documentation is also available with the product.

2 Step 2: Evaluate your hardware and system configuration

Ensure that the following requirements are met:

a. Operational server with licensed operating system and supported hypervisor (VMware ESXi™) to deploy and run PPM.
b. Packaged Base OVA
c. PPM Installer
d. One or more targeted servers with a supported agent operating system (Red Hat® / CentOS 6.2+ or 7.2+, AIX 7.1 or 7.2, and Microsoft Windows Server® 2008 R2, Microsoft Windows Server® 2012 R2 or Microsoft Windows Server® 2016.
e. Browsers: Google Chrome®, Microsoft Internet Explorer® 10+, Mozilla Firefox® ESR 52+.
f. Network Access between PPM and all agents.
g. Certificate Authority signed certificates (keystore, truststore, & CA certificate bundle) to establish a secure session between Management Server (PPM) and all Agents.

For Object Store Agent (OSA), the following are additional requirements:

- S3 compatible Object Storage: Amazon Web Services S3 (AWS S3), IBM Cloud Object Storage (COS S3)
- Object Storage credentials: User ID and Secret Key (password)
- An application or utility that leverages AWS S3 REST API Library or Boto Python Library to point data to the OSA Agent

For complete information, see *Planning considerations*, *Server Certificate Settings* and *Appendix: Sample Certificate Authority (CA) Certificates* sections in the *IBM Multi-Cloud Data Encryption Administrator Guide*.

3 Step 3: Install IBM Multi-Cloud Data Encryption

Install MDE PPM, internal database configuration, and certificate setup.

Using example, file ibm_sw_mde_X.x.x-XX.bin, replace X with file name, version, and build numbers.

a. Deploy the MDE base OVA into your hypervisor. In this example, it is referred to as "Management Server VM".
b. Log in as admin and set a new password.

The OVA use PAM standard criteria that is configurable by the administrator. The PAM password must be more than 8 characters and cannot contain 5 characters from previous password.

c. Take note of the IP address of the MDE VM.
d. Upload `ibm-sw_mde_X.x.x-xx.bin` to the MDE by using `scp` or similar method.
e. Make the bin file executable.

```
[admin@localhost]$ chmod +x ./ibm_sw_mde_X.x.x-XX.bin
```

f. Run the bin file.

```
[admin@localhost]$ ./ibm_sw_mde_X.x.x-XX.bin
```

g. Select “English” and press Enter.
h. Read the License pages by using tab <OK>, press Enter to advance.
i. Select <Yes> and press Enter to accept the License Agreement.
j. After extraction is complete, press Enter on <OK> to return to the command line.
k. Note the rpm install location.
l. Install the RPMs as root.

```
[admin@localhost]$ sudo yum –y install rpms/*.rpm
```

The Management Server (PPM) is now installed, but not configured. Do not reboot until configuration is complete.

For detailed steps, see the *Product installation* section in the *IBM Multi-Cloud Data Encryption Administrator Guide*.

4 Step 4: Configure default language

Supported languages were installed during rpm installation onto Management Server VM above.

Steps to install:

a. Run the `spsd-langsetup` script:

```
$ sudo /opt/securityfirst/spsd/bin/spsd-langsetup
```

b. View the current default language code. If none is set, it is blank.
c. View the list of available language codes.
d. Enter the new default language code: **en_US** (example).
e. Rerun the spsd-language script to validate default language code is set. As in example, it displays “The current default is: **en_US**.

5 Step 5: Configure database

An internal or external database will need to be configured before starting MDE for the first time. The internal database supports PostgreSQL only and comes pre-packaged in the OVA.

To configure the database to work with MDE:

Run the `spsd-pgsetup` script with the "“--local" script option. This local option configures a new, empty database on the internal “--local” PostgreSQL Server.

```
$ sudo /opt/securityfirst/spsd/bin/spsd-pgsetup --local
```

If installing an external database, see the *Database Setup* section in the *IBM Multi-Cloud Data Encryption Administrator Guide*.

6 Step 6: Configure certificates

Certificates are used to establish a secure communication session between the Management Server (PPM) and Encryption Agents and web browsers. PPM requires all certificates to be signed by a Certificate Authority (CA). The CA establishes a root of trust that all participants in the communication session use to verify the identity of the other party.

- The CA signed certificate along with its corresponding key are combined into a java keystore.
- The certificate (or certificate bundle) from the CA used to sign the Agent certificates must be added to the PPM truststore.
- All three components (keystore, truststore, and CA certificate bundle) are used in the below PPM certificate setup process.

In this example, all certificate files have been copied to /etc/ppm/certs on the management server vm. Names noted by brackets are example names.

To configure a keystore, truststore, and CA bundle run:

For keystore:

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --ks /etc/ppm/certs/[ppm.jks] --
kw password
```

For truststore:

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --ts /etc/ppm/certs/[trust.jks] --
tw password
```

For CA Bundle:

```
$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --aca /etc/ppm/certs/
[ca_bundle.pem]
```

For more information on Certificate setup, see the *Server Certificate Settings* and *Appendix: Sample Certificate Authority (CA) Certificates*. sections in the *IBM Multi-Cloud Data Encryption Administrator Guide*.

7 Step 7: Reboot

After installing PPM, configuring a database, adding certificates, and optionally setting PKI, you can now reboot the MDE Management Server VM.

8 Step 8: Log in to the console

Once deployed, start the virtual machine via the hypervisor interface. You will need to retrieve the IP of the virtual machine.

Open the management server VM and login as admin and display the IP address of the MDE Management Server VM by running the command “ip address”.

To access the Management console, enter the following on a supported browser:

`https://<<MDE Server IP>>`

This directs the browser to the login page of MDE where you will be prompted to log in.

Default credentials for first login are and must be changed after login:

User name: admin

Password: admin

Note when using PKI client-authentication, the dashboard might be displayed bypassing the login page. (See the *Public Key Infrastructure (PKI) Settings* section in the *IBM Multi-Cloud Data Encryption Administrator Guide*.

After login, you are now ready to use IBM Multi-Cloud Data Encryption by provisioning an Encryption Agent.

There are four types of Encryption Agents: File with Policy Agent, Volume Agent, Volume with Policy Agent and Object Store Agent. These agents are provisioned to a supported Agent operating system (see Prerequisites). For specific information on Agent Provisioning, see the *Agent Provisioning and Management* section in the *IBM Multi-Cloud Data Encryption Administrator Guide*.

More information

? For more information, see IBM Multi-Cloud Data Encryption product support, at https://www.ibm.com/support/home/.

Document Number: GI13-4920-01