IBM Multi-Cloud Data Encryption Powered by SPx®
Version 2.3

Administrator Guide

SC27-9557-01

Note

Before you use this information and the product it supports, read the information in “Notices” on page 109.

This edition applies to Version 2.3 of IBM Multi-Cloud Data Encryption (product number 5737-C67) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Introduction

Authorized Use Permission

Usage of this software is limited to the terms of the licensing agreement.

Point of Contact

For additional information about IBM Multi-Cloud Data Encryption (MDE), please visit IBM Support website at https://www.ibm.com/support/home/.

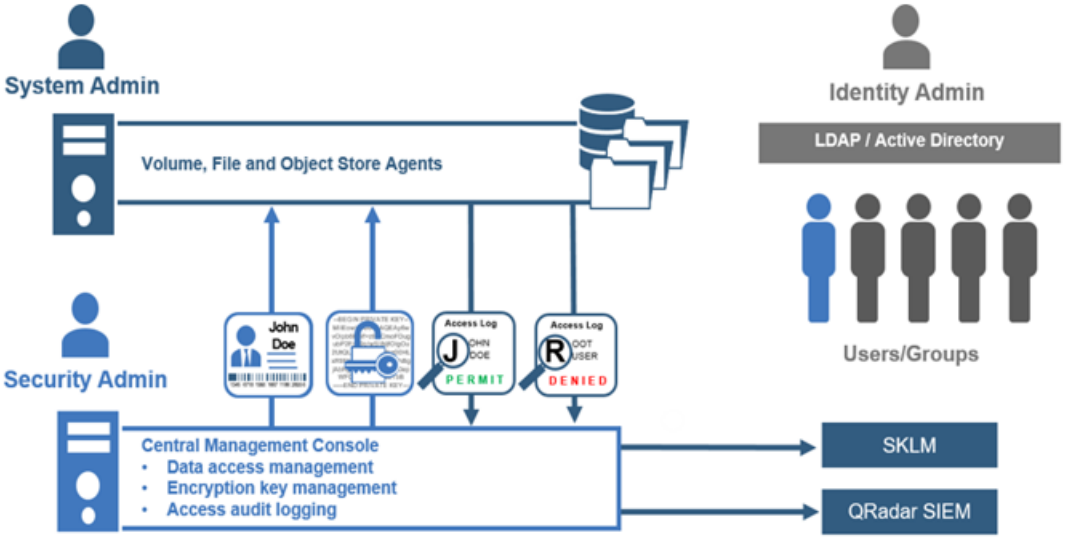
Background and Intention of the Administrator Guide

The Administrator Guide is the primary reference for installation, administration, and use of MDE for encryption agent provisioning and management, policy definition (access and cryptographic control), policy enforcement key management, and securing data at rest on selected servers that are using deployed agents. This document is intended for a System Administrator with administrative access and knowledge of their corporate network to install and administer the product.

Chapter 2. General Overview

Product Overview

The IBM Multi-Cloud Data Encryption (MDE) is a comprehensive data security product powered by SPx® technology that combines data-at-rest encryption (via Agents) with the additional powerful protection features of a Policy Provisioning Manager (PPM) that acts as a central management console. MDE enables the provisioning of agents, data access policy settings (operational and cryptographic access definition), and management (key lifecycle, agent updates and user access logging) of up to 25,000 agents from a single centralized location. MDE provides a seamless and secure system with the flexibility to assign agents that encrypt data at file system level or volume level using a unique cryptographic splitting technology. It provides data-centric protection that goes beyond standard encryption making data encryption much more robust and impenetrable from a brute force attack. It takes protection a step further with the ability to restrict, monitor, and audit data access at the user level by defining fine-grained access policies.

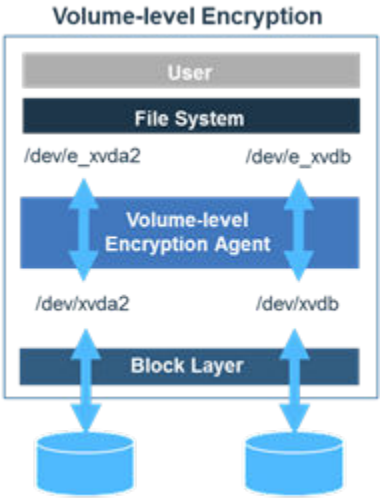


MDE provides a separation of duties with separate Administrator Roles: Product Administrator and Security Administrator. The Product Administrator role is entrusted with the permissions required to configure and maintain the MDE product. The Security Administrator role is entrusted with the permissions required to provision and manage the agents. These roles are further discussed in Section 7: MDE Administrative User Management.

MDE supports the installation of four agent types that provide the cryptographic data protection used to enforce the policy definitions.

Agent Types

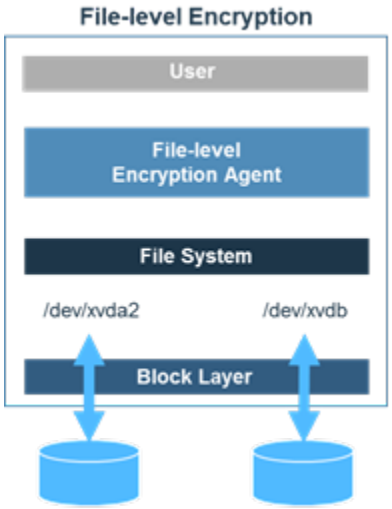
Volume Agent



The Volume Agent provides volume-level encryption with limited access policy controls. Volume-level encryption provides security in the form of a protected, predefined storage device via the block driver implementation in the OS.

An entire volume is defined and cryptographically protected as a unit. As data is added, edited, or deleted, the Volume Agent ensures all data within the volume is cryptographically secure with a PPM-managed encryption key.

File with Policy Agent



The File with Policy Agent combines file level encryption with data access policy. File-level encryption provides individual file protection at the file system level. File and storage environment sizes are only limited by the file system and not by File with Policy Agent. The location for the protected data is secured with the workgroup key for that path definition, and all the individual files stored within and beneath are encrypted separately using a unique and non-predictable initialization vector (IV). Protected data can be local to the file system or network mounted via NFS.

The unique file level keys are handled by an internal key management system. Policy-based access control is layered on top of the encryption, allowing for the definition of least-privileged access control, specification of access logging and limiting of access rights to specific system functions such as Read/

Read-Write/Copy/Delete. These policy controls work together with standard LDAP or Active Directory permissions. If a user does not have permissions to the data in LDAP or Active Directory, the Security Administrator cannot overwrite those access controls and authorize data access.

By default, all users are excluded from accessing the data covered by a policy. The Security Administrator needs to define who has access. This allows the Security Administrators to restrict system administrators, cloud vendor administrators and root users from accessing protected data.

Volume with Policy Agent

A Volume with Policy Agent leverages the volume-level encryption of a volume agent and file-based operational access control policies that can be applied and enforced for one or more protected file paths.

Object Store Agent

An Object Store Agent operates on an “M of N” model, which determines what number of pieces of data is required to rebuild the data (M) out of the total number of pieces created (N). The pieces of data stored, which can be on local or remote locations depending on the license, are referred to as “shares”. The use of multiple shares allows for improved data flow along with the added options for data resiliency and fault tolerance. The supported M of N distributed shares model is 1:1, 2:3, or 2:4.

An Object Store Agent (OSA) encrypts data that is sent to object storage. It acts as a pass through for files as they are transmitted to object storage encrypting and splitting data along the way. Files are retrieved from object storage through the Object Store Agent are decrypted on retrieval. The files at rest in object storage are encrypted. Only authorized users can send / receive data through the Object Store Agent.

Agent Feature Matrix

Agent Feature	Volume Agent	Volume with Policy Agent	File with Policy Agent	Object Store Agent
Encrypt Entire Volume	√	√		
Encrypt Files Individually in Designated Protected Directories			√	
File Level Policy		√	√	
File Access Audit Logs		√	√	
Protects Against Administrator Access to User Data			√	
Encrypt Data in Object Storage				√

Chapter 3. Planning Considerations

Prerequisites

Installation of IBM Multi-Cloud Data Encryption (MDE) is a straight forward process which includes the installation of a base Open Virtual Appliance (OVA) and running a Provisioning Policy and Management (PPM) installer.

In preparation, it is a good idea to review the installation instructions in their entirety prior to installing the software. Below is a list of prerequisites for successful installation and operation of IBM Multi-Cloud Data Encryption.

1. Operational server with licensed operating system and supported hypervisor (VMware ESXi™) to deploy and run PPM.
2. Packaged Base OVA
3. PPM Installer
4. 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.
5. Browsers: Google Chrome®, Microsoft Internet Explorer® 10+, Mozilla Firefox® ESR 52+.
6. Network Access between PPM and all agents.
7. Certificate Authority signed certificates (keystore, truststore, & CA certificate bundle) to establish a secure session between Management Server (PPM) and all Agents.

See Certificate Requirements and Server Certificate Settings for more details and Appendix B, “Sample Certificate Authority (CA) Certificates,” on page 85 for an example.

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

Critical Note: It is strongly advised that the MDE, external databases, and agents leverage NTP to coordinate system time. This will ensure event / audit log timestamps are sequenced properly.

Minimum System Requirements

PPM VM Minimum System Requirements

- CPU 4
- 8 GB RAM
- 40 GB of available storage
- Network Access Required

Linux Agent Minimum System Requirements

- One Core 64-Bit CPU @2GHz with AES-NI enabled
  - (recommended 2 Core 64-Bit CPU @2GHz with AES-NI enabled)

  - 2 GB RAM (recommended 4 GB RAM)
- 20 GB of available hard disk space
  - 300 MB or more is recommended for log file space
- Network Access Required
- Install / update the following packages: curl, openssl, and nss on Red Hat / CentOS
- Internet access or access to local repository during initial agent installation
- An SSL Certificate is required for agents

Windows Agent Minimum System Requirements

- One Core 64-Bit CPU @2GHz with AES-NI enabled - recommended 2 Core 64-Bit CPU @2GHz with AES-NI enabled
- 4 GB RAM - recommended 8 GB RAM
- 20 GB of available hard disk space - 300 MB or more is recommended for log file space
- Network Access Required
- An SSL Certificate is required for agents

Note: Requires an SSL (self-signed or Certificate Authority) certificate / key pair file prior to creating agents. The certificate is utilized to establish a secure TLS connection between the agent and the MDE Server.

Certificate Requirements

Certificates are required to establish a secure connection between the PPM Server and the agents. The certificate requirements include the following:

- PPM Server requires the certificate presented by an Agent must resolve to that Agent (DNS host name or IP Address)
- PPM Server requires the certificate presented by an Agent have the Client Authentication extended key usage set
- Agent requires that the certificate presented by the PPM Server must resolve to the PPM Server (DNS host name or IP Address)
- Agent requires that the certificate presented by the PPM Server have the Server Authentication extended key usage set

The PPM and Agent should be synchronized to a reliable time source to ensure certificates are within validity period.

Requires a unique certificate for each deployed Agent.

File System Support for Agents

Volume Agents perform encryption at the volume level. The File with Policy Agents will operate either with or on supported file systems of the host operating system. The File with Policy Agent and the Volume with Policy Agent support the following file systems:

Linux Servers

- EXT3
- EXT4
- XFS (on Red Hat / CentOS 6.5 or newer)
- NFS (NFSv3, NFSv4)

Windows Servers

- NTFS
- ReFS (on Windows Server 2012 R2 or newer)

AIX

- JFS2

Network Setup

About this task

MDE requires a consistent network connection between MDE PPM server(s) and agents. Internet Protocols IPv4 and IPv6 are supported. Using static IP assignments or DHCP with static leases would satisfy this need. Additionally, a properly working DNS infrastructure and the leveraging of host names across the ecosystem would work.

Network Ports

Function	Default Port	Configurable
Web	443	Yes
Database	5432	Yes
External LDAP	None	Yes
LDAP directories	None	Yes
Email event forwarding	None	Yes
Syslog event forwarding	None	Yes

OVA Configuration

The provided MDE OVA is pre-configured with MaxAuthTries set to 1. To successfully authenticate over SSH to the MDE VM, MaxAuthTries will need to be changed (not recommended) or SSH clients will need to set PubkeyAuthentication to "no" either on the command line or in the local SSH client configuration.

REST Interface

MDE supports a full programmatic REST interface. The root REST URL is:

https://<Virtual Machine IP>/rest/

Critical Note

The REST API will allow an administrator to perform advanced functions not accessible via the web interface. The REST API can be potentially used in a way that may get an agent into an unsupported state; therefore, an understanding of REST API programming knowledge is essential.

Reference the IBM Multi-Cloud Data Encryption (MDE) REST API Specification document for more details.

Chapter 4. Product Installation

Preparing for Installation

There are three steps for MDE's installation process:

1. Prerequisites
2. MDE Base Open Virtual Appliance (OVA) available
3. Supported Hypervisor (VMware ESXi™)

Licensing

MDE does not require a unique product license to run or to configure agents beyond that provided in the software license agreement.

MDE OVA/VM Management

After deploying the MDE OVA, update the system to ensure the latest security patches and software versions are installed.

Note: Periodically update the system to pick up security patches and newer software versions.

Installing MDE

About this task

To install MDE software:

Using example, file ibm_sw_mde_X.x.x-XX.bin, substitute the build number for XX for the version of the available software, and operate as a root user.

Procedure

1. Deploy the MDE base OVA into your hypervisor. In this example, it will be referred to as "MDE VM".
2. Login as admin and set a new password.

   MDE VM uses PAM standard criteria that is configurable by an administrator. The PAM password must be more than 8 characters and cannot contain 5 characters from previous password.
3. Take note of the IP address of the MDE VM.
4. Upload ibm_sw_mde_X.x.x-XX.bin to the MDE using SCP or similar file transfer method.
5. Make the bin file executable.

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

   ```
   [admin@localhost]$ ./ibm_sw_mde_X.x.x-XX.bin
   ```
7. Select English and hit Enter.
8. Read the license pages, tab to <OK>, hit 'Enter' to advance.

9. Select <Yes> and hit Enter to accept the license agreement.
10. Once extraction is complete, hit Enter on <OK> to return to the command line.
11. Install the RPMs as root.

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

12. MDE is now installed, but not yet configured.

    Note: Do not reboot the MDE VM until configuration is complete.

Language Setup

About this task

MDE supports multiple languages for the VM scripts and the PPM GUI. You will need to configure a default language preference prior to running the product.

Note: Languages are installed via RPM into the MDE VM. The installer binary comes with a built-in set of language RPMs. Additional languages can be added after initial install and may require a restart of the PPM service to take effect.

To configure the default language, follow the steps below:

Procedure

1. Run the spsd-langsetup script.

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

2. View the current default language code. If none is set, it will be blank.

```
Set the default language code.
The current default is:
```

3. View the list of available language codes. (The list below may show examples not available in your version of the product.)

```
Available language codes:
en_US
ja_JP
ko_KR
```

4. Enter the new default language code.

```
Enter the new default language code:  en_US
Default language code will be; en_US
```

5. Re-execute the spsd-langsetup script to validate default language code is set.

```
Set the default language code.
The current default is: en_US
```

Database Setup

About this task

MDE supports an internal or external database configuration. In either case, you will need to configure MDE to communicate with the configured database prior to starting MDE for the first time.

To associate a database with MDE, you will need to modify the MDE VM `/etc/spsd/db.props` file. You will need to edit this file as a root user.

Note: Running the spsd-pgsetup script will automatically modify the db.props file with the values entered in the prompts.

Configure the file properties to connect to the appropriate Internal or External database as described below. Database properties changes will not take effect until MDE is restarted.

Critical Note

When modifying db.props adhere to the following constraints:

- **no spaces between property name and =**
- **no spaces between = and property value**

Internal Database

Currently, MDE supports PostgreSQL as an internal database.

Internal Postgres Database

The MDE OVA comes pre-packaged with PostgreSQL software installed. To configure the database to work with MDE, follow the steps below:

1. Run the spsd-pgsetup script with the "--local" script option.

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

Note: The "--local" option configures a new, empty database on the internal "local" PostgreSQL Server.

After applying these settings, proceed to Server Certificate Settings. If you plan to set up the database on a remote target, proceed to External Database.

External Database

Currently, the only supported external database server is PostgreSQL. You must ensure that the following information is known prior to executing this process:

- Name (or IP address) of an accessible PostgreSQL database server
- Port number that the above PostgreSQL server is listening on
- Name of an existing database on the above server
- Name of an existing user defined as the owner of the above database
- Password of the above database user

To configure the database to work with MDE, run the spsd-pgsetup script. All values supplied in this command are examples:

```
$ sudo /opt/securityfirst/spsd/bin/spsd-pgsetup --host
ext.postgres.svr1 --port 5432 --dbname policyDB --user policyDBuser
--pass mypassword123
```

To upgrade the database to the latest schema, run the spsd-pgsetup script with the "--upgrade" script option

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

Note: Running the spsd-pgsetup script with the "upgrade" option ensures the database tables are properly configured to the current version of PPM.

After configuring these settings, proceed to Server Certificates Settings.

Server Certificate Settings

Keystore, Truststore, and Certificate Authority

Certificates are utilized to establish a secure communication session between the Management Server (PPM) and agents as well as 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.

Refer to Appendix B, “Sample Certificate Authority (CA) Certificates,” on page 85 for a sample of the Certificate Authority certificate process.

The server web certificate keystore and web certificate truststore are configured via

the setup script, spsd-certsetup, located in the /opt/securityfirst/spsd/bin directory of the MDE VM.

To configure the keystore and truststore and agent CA bundle, example input in **bold**:

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

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

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

Note

Server certificate components such as keystore, truststore, and CA bundle are not provided and must be generated and uploaded to MDE VM via the setup script. If a Common Access Card (CAC) will be used for authentication, PKI settings will need to be enabled.

Public Key Infrastructure (PKI) Settings

About this task

PKI configuration enables PPM to provide a secondary method of PPM user authentication. When configured, PPM will accept client certificates as an authentication method for web and REST sessions.

This certificate must be signed by a CA trusted by PPM. PPM will validate the certificate based on the rules defined in the spsd-certsetup script.

Example input in **bold**:

$ sudo /opt/securityfirst/spsd/bin/spsd-certsetup --crl-on --ocsp-on --pols-on oids x.x.x.x.x.x.x.x,Y.Y.Y.Y.Y.Y.Y

Note

PKI can be configured in the same script execution as keystore, truststore, and CA bundle. It is broken out here for instructional value.

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

Starting and First-time Login

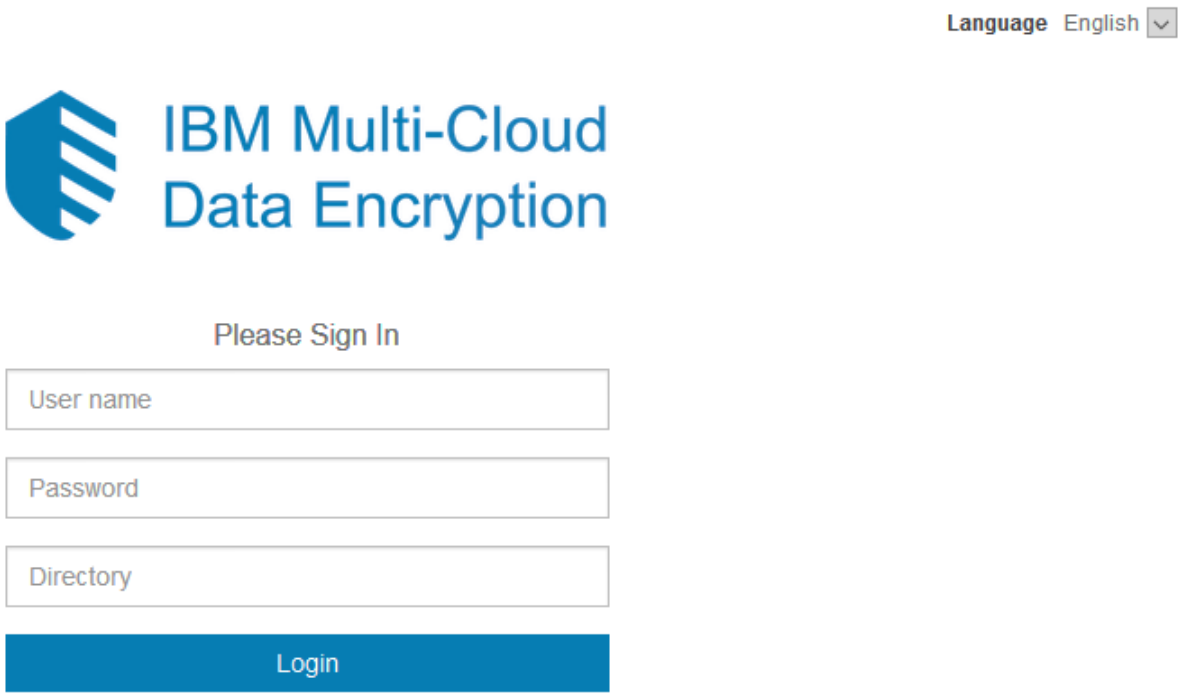
About this task

Once the deployment and configuration has been completed, reboot MDE server or simply start the service “spsd” from the MDE console to start the Web GUI. You will need to retrieve the IP address or host name of the virtual machine via the virtual machine console or host hypervisor.

Open a supported web browser and enter the IP address or hostname as the URL to reach the MDE login page.

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

At this point, you can change the language setting from the available list of support languages.



The default credentials are:

```
Username: admin
Password: admin
```

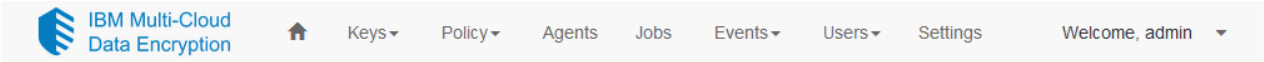
Note

- The default credentials are required to change after first login
- MDE supports most versions of Firefox, Chrome, Microsoft Edge, and Internet Explorer web browsers
- When using PKI client-authentication it may bypass the login page and go directly to the dashboard

Chapter 5. MDE Graphical User Interface (GUI)

Basic Product Navigation

MDE contains a top-of-the-page navigation menu. Some menu items contain sub-menu lists. Click on each menu item to navigate to the appropriate page or display the sub-menu list.



- **Home Icon** - A link to the product Dashboard home page.
- **Keys** - A menu containing key related sub-menu page links: External Keystores and Managed Keys.
- **Policy** - A menu containing policy related sub-menu page links: Datatypes, Path Sets, Processes, and Selectors.
- **Agents** - A link to the Agents page.
- **Jobs** - A link to the Jobs page.
- **Events** - A menu containing event related sub-menu page links: Forwarding and Logs.
- **Users** - A menu containing user related sub-menu page links: Accounts and LDAP directories.
- **Settings** - A link to the Settings page.

Note

MDE supports role-based access control (RBAC), which means that some navigation items will not be available based on the role of the logged-in user. Thus, some navigation items may not be available for all administrative users.

Product Dashboard

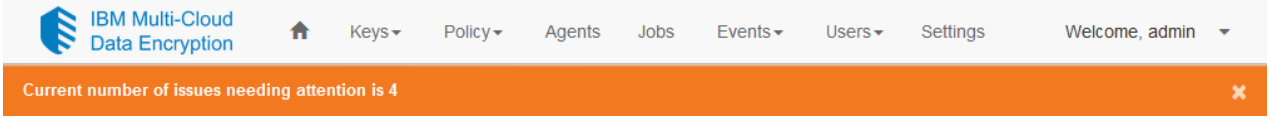
The product home page is the main landing dashboard page. It is intended to give a summary view of the current status of recent events to the logged in administrator. The home page contains recent events, event trends, and other summary data

Textbox Autocomplete

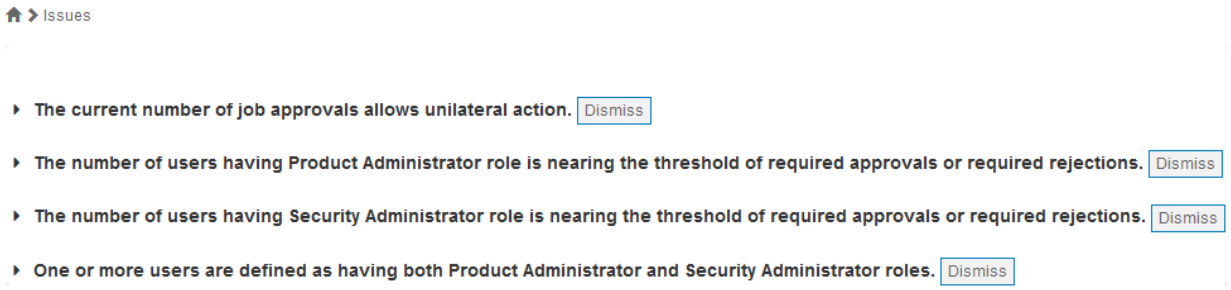
Throughout the user interface there are text entry fields. Some text entry fields will display match criteria based on an auto-completed list of entered characters. These fields may require multiple characters before an auto-complete suggestion list is presented

Attention Notifications

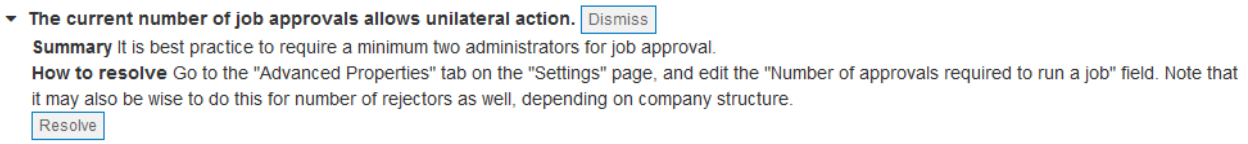
Upon first login, there will be a color banner at the top of the user interface indicating actions that need to be resolved.



Clicking the text in the banner will redirect the administrator to the “Issues” page where individual items are displayed.



Expanding an individual item will give details on how to resolve the issue.



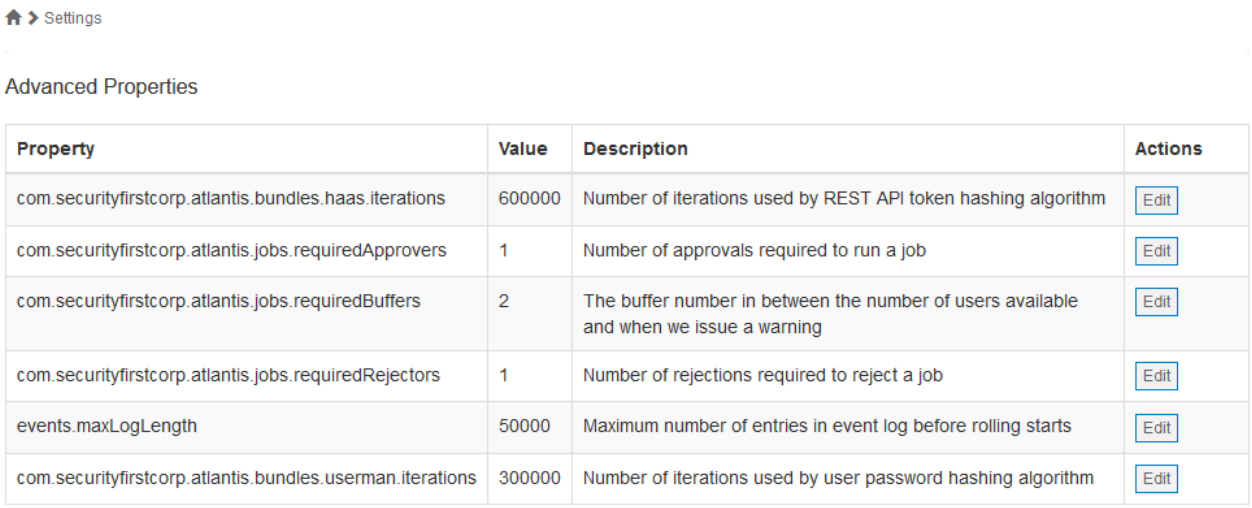
Once all open issues have been resolved, the banner will not be displayed; however, an administrator can choose to dismiss the banner for the current page.

Note

New conditions might arise that create new “needs attention” issues and the banner will reappear.

Advanced Properties

The Product Administrator is allowed to configure advanced properties that define product behavior. The advanced properties are accessible via the settings page. These properties are scoped to either the local instance or potentially, if leveraging High Availability (HA) or multi-tenant functionality, the MDE ecosystem.

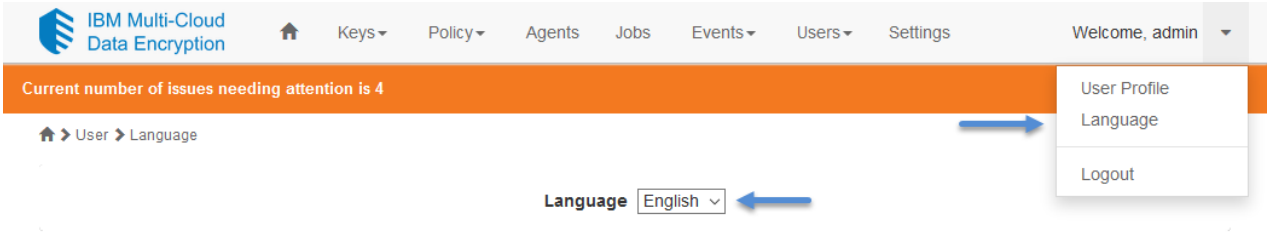


To edit a property, a Product Administrator must click the “Edit” button. Once the appropriate changes have been made, click the “Save” button and a job will be created.

GUI Language Setting

From the GUI, you may change to one of the supported languages installed during the initial installation when selecting from the login page or home page.

- **Login page** - Found at the top right on page. Click the pull-down menu for a list of supported languages.
- **Home page** - Found at the top right pull-down menu, select “Language” for a list of supported languages.

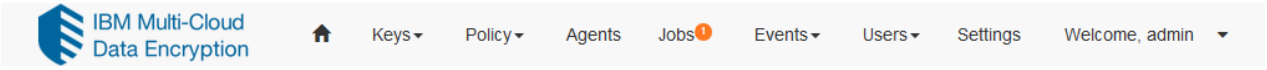


The language displayed in the GUI is determined by the following hierarchy (first present setting is used):

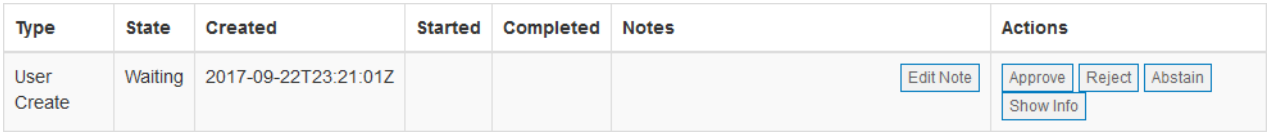
1. The value of the language cookie set via PPM’s user interface.
2. The value of the user’s browser language setting.
3. The value of the language code set via the PPM CLI script-langsetup.
4. The first found installed PPM language pack.

Chapter 6. Jobs

MDE incorporates a jobs system to manage the approval and timing of running tasks. Many features utilize the job system to wait for approval before being confirmed. When a job is created, a new job will be added to the list on the Jobs page.



Administrators will have the option to approve, reject, or abstain on each job. Each administrator can take action only once per job.



Job Descriptions

Job	Description	Category	Role
Advanced Properties	Modify an advanced property	Product Management	Product Administrator
Modify Keystore	Change the location/ details of the policy enforcement keystore	Product Settings	Product Administrator
Key Rotation	Rotate a set of keys in the agent ecosystem	Key Management	Security Administrator
Key Revocation	Revoke a set of keys from the agent ecosystem	Key Management	Security Administrator
Key Shred	Permanently remove a set of keys from the agent ecosystem causing the data to be lost.	Key Management	Security Administrator
Add Agent	Provision and add a new agent into the ecosystem	Agent Management	Security Administrator
Delete Agent	Remove agent from MDE management	Agent Management	Security Administrator
Modify Agent	Modify information relating to an agent	Agent Management	Security Administrator
Policy Update	Modify the policy associated with an agent	Agent Management	Security Administrator
Create New Administrative User	Create a new MDE Administrator	MDE Administrative User Management	Product Administrator

Delete Administrative User	Remove a MDE Administrator	MDE Administrative User Management	Product Administrator
Add Administrative User Role	Add a role to a MDE Administrator	MDE Administrative User Management	Product Administrator
Remove Administrative User Role	Remove a role from a MDE Administrator	MDE Administrative User Management	Product Administrator
Change Administrative User Password	Change the password of a MDE Administrator	MDE Administrative User Management	Product Administrator
Change Administrative User Status	Enable or disable a MDE administrative user account	MDE Administrative User Management	Product Administrator
Register Directory	Configure LDAP Server directories for MDE Administrative users	MDE Administrative User Management	Product Administrator
Delete Directory	Remove LDAP server directory from MDE	MDE Administrative User Management	Product Administrator
Update Directory	Modify LDAP server directory	MDE Administrative User Management	Product Administrator

Multi-Administrator Approval

The required number of approvers and rejecters is configurable within MDE. By default, MDE is configured for single administrator approval. It is strongly recommended that two or more administrators be required for job approval. Multi-Administrator approval prevents a single administrator from enacting a change within MDE itself or to any managed agent instances.

User	Time	Actions	Required Approvals	Required Rejections	Notes
admin	2017-09-22T23:22:35Z	Approve	1	1	

Critical Note

The number of administrative users must meet or exceed the number of job “Required Approvals” or “Required Rejections”. Make sure that there are the required number of administrative users before changing these values.

The approval and rejection thresholds may be overridden by job type. Each job type defined by the system, except the Property Change job, has both an approval and rejection threshold in Advanced Properties that when set will override the system default. Once a property is set, it may not be unset

The Property Change job is the only job type without an approval and rejection threshold because it controls the modification of the Advanced Properties. For this job, the approval and rejection thresholds will always be the higher of the system default or the highest override value defined for any other job type. This action will ensure that no other job type threshold can be subverted through a property change process.

Job Approval

To approve a job, an administrator with the proper permissions must navigate to the Jobs page, find the appropriate job, and click the “Approve” button. Once the required number of administrator approvals is reached, the job will execute.

Job Rejection

To reject a job, an administrator with the proper permissions must navigate to the Jobs page, find the appropriate job, and click the “Reject” button. Once the required number of administrator rejections is reached, the job will be permanently cancelled.

Job Abstain

Abstaining from a job indicates an administrator has seen the job but does not want to approve or reject it. An abstain might best be described as an “audit” position and prevents the administrator from selecting a different position on the same job in the future.

Job Info

Each job within MDE has different information that describes it. The “Show Info” button can be clicked and job specific information will appear. Additionally, any actions (approve, reject, abstain) taken on the job by different administrators will appear along with the user name of the administrator that took the action.

Chapter 7. MDE Administrative User Management

Administrative User Roles

MDE leverages a flat static Role Based Access Control (RBAC) design. Certain functionality within MDE requires specific permissions. The complete set of MDE permissions are grouped into two distinct roles: Product Administrator and Security Administrator. Additional administrators of each role may be added at any time.

Product Administrator Role

The Product Administrator role is entrusted with the permissions required to configure and maintain the MDE product.

Security Administrator Role

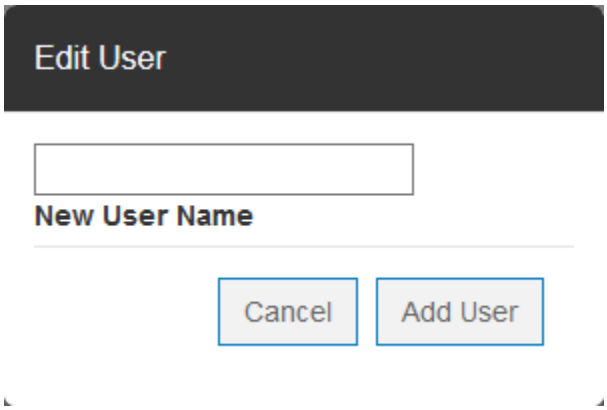
The Security Administrator role is entrusted with the permissions required to provision and manage the agents. These include but are not limited to: Policy definition and specifications, key management, datatype definition, agent management, external keystore configuration, and external LDAP configuration of external groups for policy.

Administrative User Management

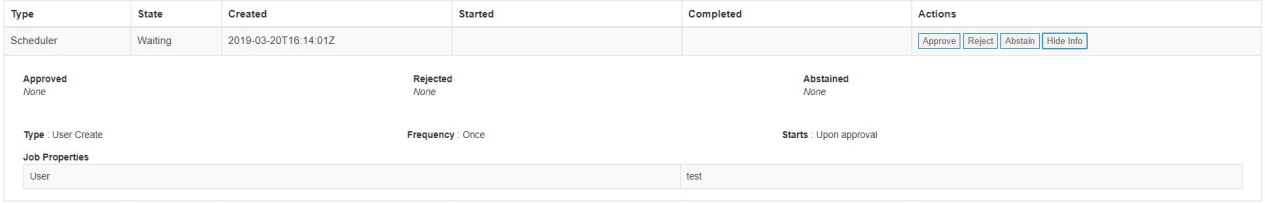
A Product Administrator possesses the permissions that are required to add, modify, and remove other administrative users within MDE.

Adding a New Administrative User

When adding a new administrative user, a Product Administrator will be prompted to enter the new administrative user name.



Fill in a unique user name and a job will be created to add this administrative user to MDE.

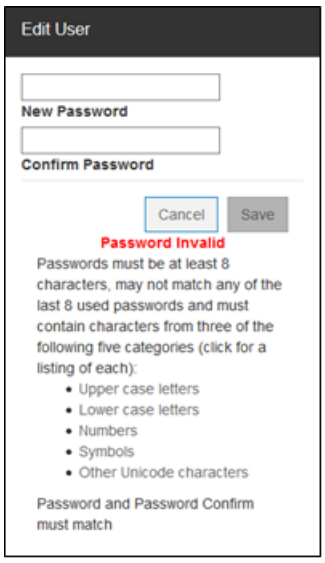


The required number of Product Administrators must approve the job for the user to be created.

A newly added administrative user is created with an expired password and no defined role. A Product Administrator must edit the initial password, the role, and status. Each of these updates will generate a job. The jobs must be approved before the new administrative user can become active in MDE.

Editing an Administrative User Password

To edit an administrative user's password, navigate to the appropriate user and select the "Edit Password" button. A password entry dialogue will appear.



Enter a password that conforms to the identified rules. Once entered, save the changes and a job will be created.

The required number of Administrative users must approve the job for the password change to take effect

Note: The newly added administrator will be prompted to change password upon initial login.

Editing the Administrative User Role

To edit an administrative user's role, locate the user row and select the "Edit Roles" button. Role entry check boxes will appear inline.

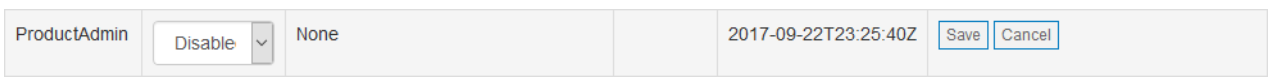
The administrative user performing an edit will be able to apply the same role as they possess, such as "built-in admin user" which is the initial user that can apply both the Product Administrator and Security Administrator roles. A user given the same roles will then be able to do the same.

Select the desired role(s) and click the "Save Changes" button, and a job will be created.

The required number of Administrator users must approve the job for the role change to take effect.

Editing the Administrative User Status

To edit an administrative user's status, navigate to the effected user and select the "Edit Status" button. A status entry dropdown will appear inline.



Status values are: enabled, disabled, and locked.

- **Enabled** - The administrative user is active and able to perform actions.

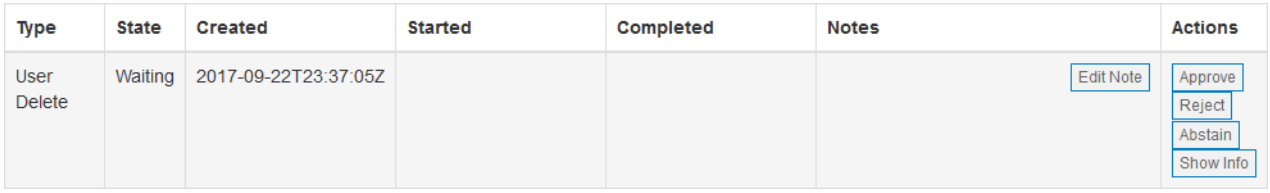
- **Disabled** - The administrative user is inactive and cannot perform actions
- **Locked** - The administrative user is locked and cannot perform actions.

Select the desired status and click “Save”, a job will be created to modify the user status.

The required number of Administrative users must approve the job for the status change to take effect.

Removing an Administrative User

To remove an administrative user, locate the target user row and click the “Delete” button. A job will be started to remove the user from MDE. This action can only be performed by a user with the Product Administrator role.



The required number of administrative users must approve the job for the user to be removed.

Critical Note

- Removing an administrative user is a permanent action.
- Must maintain enough administrative users to meet the required job approvals condition (See “Multi-Administrator Approval” section.
- Jobs cannot be successfully accepted if there are not enough administrative users.

User Account Lockout

To protect the system and user accounts from brute force password attacks, user accounts are locked after ten (10) consecutive failed login attempts. The user account will be locked until the account is explicitly enabled (See section, Editing the Administrative User Status) or the server service is restarted.

Note

- To restart the server service, run **systemctl restart spsd** in the Virtual Machine console.
- Account Lockout is on a per-server basis. An account locked out on one server in a cluster is not automatically locked out of the other servers within the cluster.
- The Account Lockout threshold is not user configurable.

LDAP Directory List

A Product Administrator can configure LDAP directories for MDE user management. LDAP directories can be added, modified, or deleted. Each action will create a job for approval before taking affect.

When adding / modifying a LDAP directory the available settings are:

- **Directory ID** - The identity of the LDAP directory.
- **Type -** drop-down option for LDAP or Active Directory
- **Bind DN** - The full distinguished name that is used to bind to the LDAP server.

  Bind DN sample syntax is as follows:

```
uid={$username},ou=users,dc=company,dc=com
```

Note: When selecting the type “Active Directory”, the Bind DN section is greyed out, as this information is not required.

- **Host** - IP/Hostname of the LDAP server
- **Port** - Port of the LDAP Server
- **Secure** - Identifier of secure or non-secure LDAP connection
- **Actions** - select Save or Cancel

Directory ID	Type	Bind DN	Host	Port	Secure	Actions
LDAP1	LDAP	uid={$username},ou=users,dc=company,dc=com	10.10.10.1	636	☑	Save Cancel

User Source

MDE can simultaneously support internally and externally defined users. Externally defined users will show a value in the “Directory” column of the User List. Internally defined users will have that field blank.

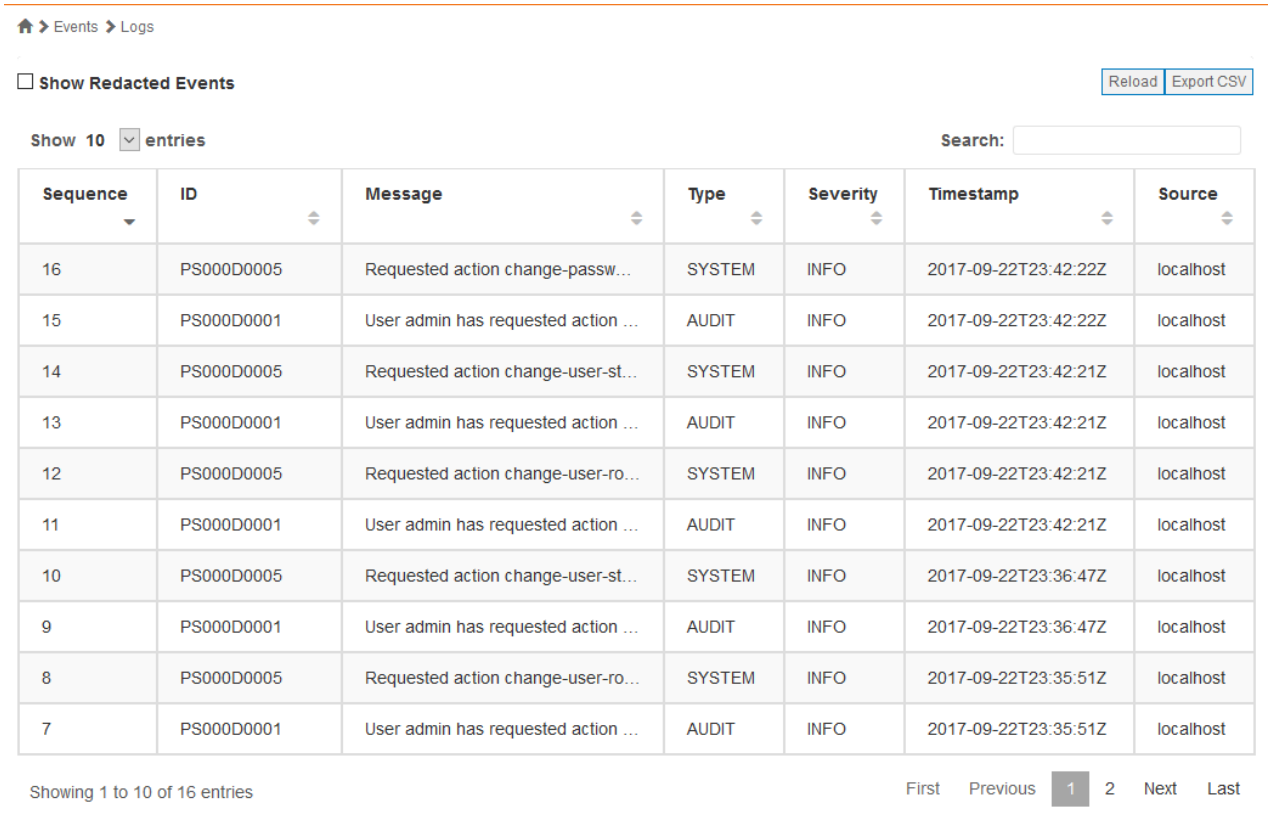
Name	Status	Roles	Directory	PW Modified	Actions
admin	Enabled	Product Administrator, Security Administrator		2017-09-22T23:09:44Z	Edit Password Edit Roles Delete
ProductAdmin	Enabled	Product Administrator		2017-09-22T23:25:40Z	Edit Password Edit Status Edit Roles Delete
SecurityAdmin	Enabled	Security Administrator		2017-09-22T23:42:22Z	Edit Password Edit Status Edit Roles Delete

Chapter 8. Events

MDE includes an event aggregation and forwarding system. This system aggregates events from managed agents along with internally generated events and stores them in an internal event log. Additionally, it can be configured to forward events to one or more recipients

Event Log

The MDE event log can be seen by selecting the Events menu item on the top-level menu bar.



This page shows all events in a single sequential list. Each event has a sequence number, ID, message, type, severity, receipt timestamp, and source as defined below:

- **Sequence number** - number attributed to the order in which the event is received. It is unique (even if the same event is repeated) and will increment over time.
- **ID** - unique identifier of the event. Multiple instances of the same event will have a common ID.
- **Message** - descriptive text identifying the condition being evented. Some events might support variable insertion so while the event ID might be common the text could be slightly different.
- **Type** - describes if the event origination is from a system action or a user action. The type is:
  - **SYSTEM** - events that are originated by an automated MDE action.
  - **AUDIT** - events that are originated by a user action.
- **Severity** - relative indication of the awareness level of the event. The severity categories are:
  - **INFO** - no action is required, for informational purposes only
  - **WARN** - no immediate action is required; condition monitoring is advised
  - **CRITICAL** - immediate action is required

- **Timestamp** - coordinated universal time (UTC) formatted indication of event origination time.
- **Source** - hostname or IP of the system (Agent or MDE) originating the event.

The MDE event log size is configurable via the Advanced Settings. Once the set size limit is reached the oldest events will be rotated out as new events are received.

Event Details

An event(s) may have extended arguments that are not part of the event message. If present, the event will display a Details link in the message column of the event log. Clicking the Details button will display the extended arguments

Event Export

MDE allows an administrator to export the events list as a CSV file format from the Export CSV button on Events page.

Clicking the “Export CSV” button will download the events file to the client machine. Each row in the events file is an event from the log.

The columns in the events file are as follows: event sequence number, event ID, redacted flag, event message string (with arguments omitted), event type, event severity, event arguments, event timestamp, and event source.

Event Forwarding

Every event received will be forwarded to each configured event recipient. Events are forwarded in parallel upon insertion into the internal event log.

A Product or Security Administrator can modify the event recipients of the product. Once configured, any event created or received by MDE will be forwarded to the recipient(s). Supported recipient type is Syslog.

MDE also supports multiple formats for the forwarded events. Supported formats are: Log Event Extended Format (LEEF), Common Event Format (CEF), and Cloud Auditing Data Federation (CADF) event models.

Event Arguments

In addition to the normal event message string, event arguments will be sent as key / value parameters. These parameters will be identified by the concatenated string of the prefix with “spx” and the argument name. For example, if an event contains username, the string key / value pairing may be “spxuser=user1”.

Agent Events

MDE aggregates system and audit events from each managed (and connected) agent. These events are displayed in the MDE event log and are forwarded to any configured event recipients.

Note

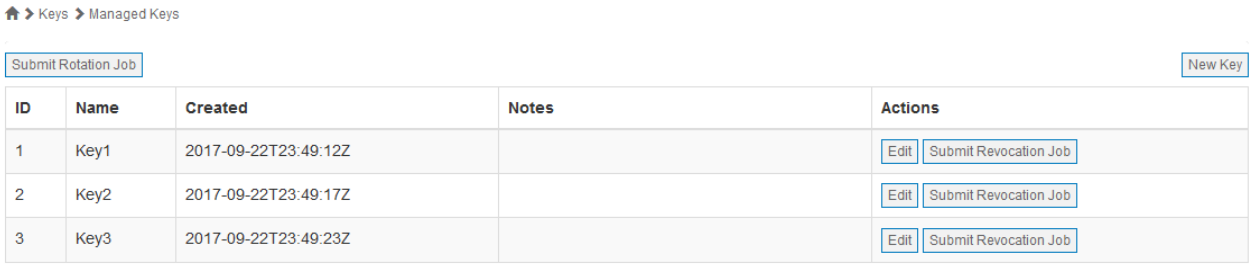
It is strongly advised that MDE, external databases, and all agents leverage NTP to coordinate system time. This will ensure event / audit log timestamps are sequenced properly.

Reliable Events

The events sent from an individual agent to MDE are handled in real time. This ensures that if an event is missed, MDE will reach back to the agent, request the missed event, and insert it into the event log in the proper sequence.

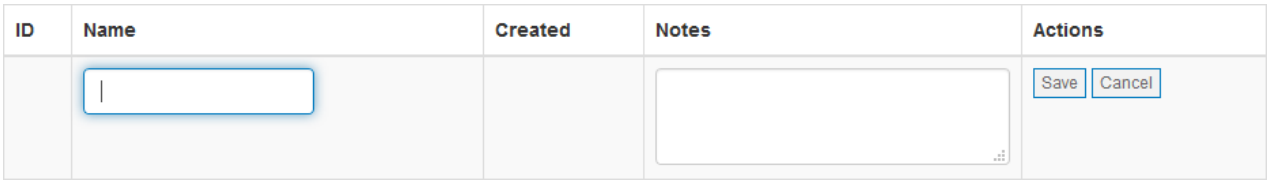
Chapter 9. Policy Enforcement Key Management

A Security Administrator can define policy enforcement keys for secure storage within MDE. These keys can be associated with datatypes, and volumes to secure data and provide cryptographic access control.



Adding a Key

When adding a new key, a unique name must be entered. Key names are not case sensitive. The key value is not exposed and cannot be edited by a user. The notes field is optional.



Note

Key names can be changed, but the actual key value cannot be modified by a user.

Keys can be created on the ‘Keys’ page, or during the agent creation wizard. All “system defined” keys created during the agent wizard are autogenerated and cannot be managed. Keys can only be edited on the ‘Keys’ page.

Editing a Key

After key creation, the Security Administrator can modify the name of a key. Changing the key name does not change the actual underlying key values. Additionally, the notes field can be modified.

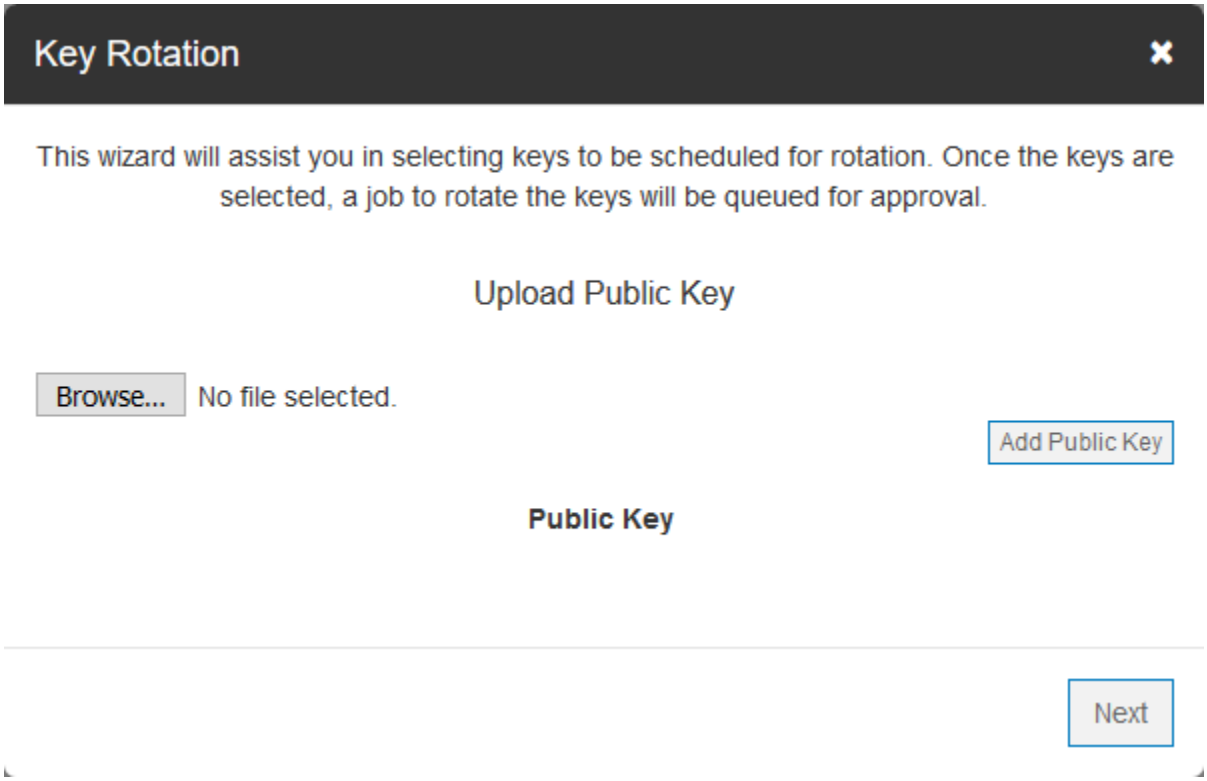
Key Rotation

MDE enables the Security Administrator to rotate keys within the agent ecosystem. From the Keys page, click the “Submit Key Rotation Job” button.

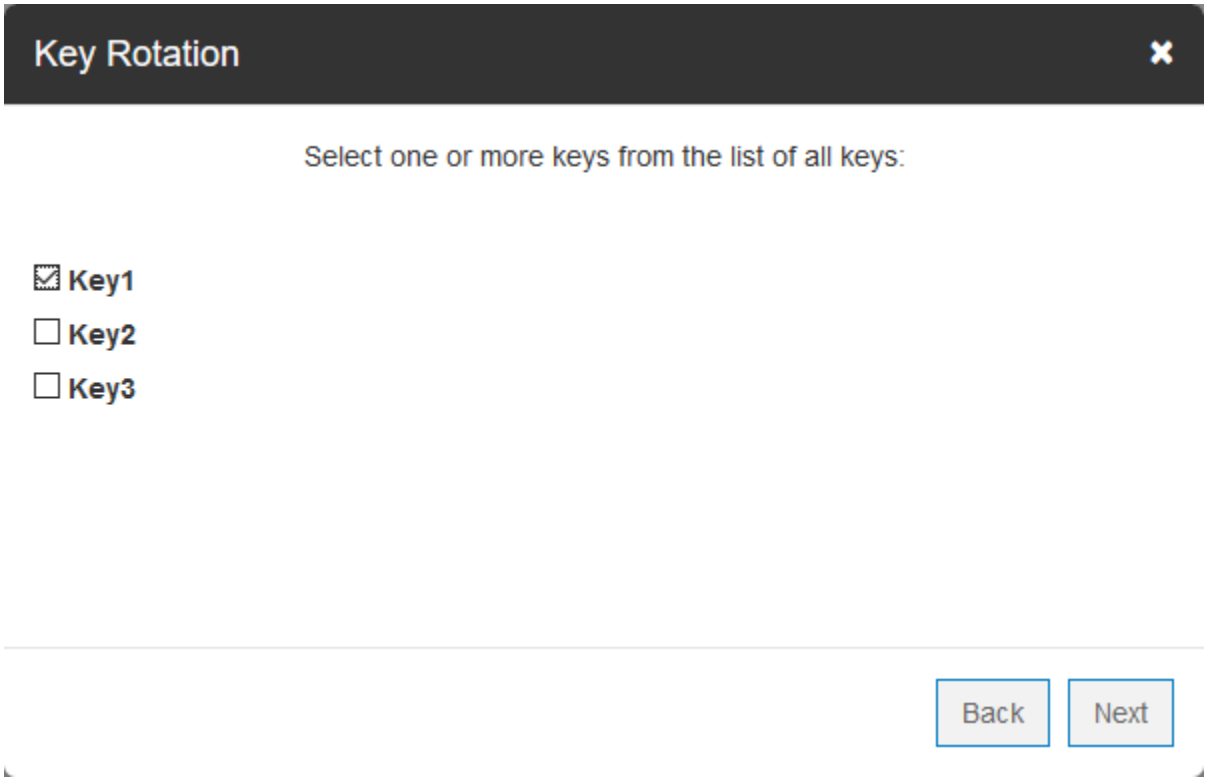
You will be prompted to upload a public key. This key will be used to encrypt the key escrow for the rotated key. Choose an appropriate key, add the key, and click “Next”.

Critical Note

The SSL key must be RSA and PEM encoded.



A list of all user-created keys will be displayed. The Security Administrator can select any number of keys to rotate.



After selecting the desired key(s), a job will be created.

Critical Note

If a key is associated with more than one agent, all agents using that key will be affected.

Upon job approval, all impacted agents will be notified of the key rotation. The job will continue to run until all impacted agents have completed the key rotation process. Depending upon the number of impacted agents, this job could take a long time to complete.

Note

When using an external keystore, it must be **online** for key rotation to succeed. If an error occurs, ensure that the external keystore is online and reboot the PPM server or restart the PPM service (spsd).

Key Revocation

Key revocation removes a key from MDE and places that key in escrow. Key revocation can only be done on a key that is currently unassociated to any active policy. Prior to revoking a key, the Security Administrator must remove policies that reference that key.

Removing the path that leverages the key from an agent policy association will not decrypt the data on disk, therefore if data accessibility is desired the data must be migrated out of the protected directory prior to removing policy associated to that path.

After revocation is complete, any data remaining in the protected path will be inaccessible. The revoked key will be stored in escrow and removed from normal PPM operation.

WARNING

The Security Administrator must update agent policy to disassociate the targeted key from all agents before revoking that key. See the section on "Editing an Agent" for more information on deleting a path.

Key Shredding

Key shredding operates the same way as key revocation; however, once the key shredding operation is completed the key will not be put into escrow leaving the data permanently inaccessible.

Note

This function is only available via REST API, refer to the REST API documentation for more details.

Auto-generated Keys

If a Security Administrator does not want to manage policy enforcement keys, MDE can auto-generate a key for each newly created policy. Auto-generated Keys are always unique when created and are not visible on the key management page.

Critical Note

Auto-generated Keys cannot be rotated or revoked. If you need the ability to rotate or revoke keys, use named keys instead.

External Keystore

Keys can be stored in one of two places: internal secure database or external keystore. MDE is initially setup to use the internal secure database only. If the Security Administrator plans to leverage an external keystore, one must be configured. External keystores are used for key protection only. Key management for external keystores must be done via MDE.

Note

Instructions to setup an external keystore are supplied by the external keystore vendor.

KMIP Keystores

About this task

A Security Administrator will need to upload a Java Keystore and a Java Truststore. Follow these steps to create a Java Keystore and a Java Truststore:

Procedure

1. Gather the client certificate file and a client private key file in PKCS12 (Public Key Cryptography Standard #12) format. For later steps we will call this "client.p12". (See Appendix C, "Sample Conversion to Create a PKCS12 File," on page 89 for a sample on combining a client certificate and client private key into a PKCS12 formatted file.
2. Gather a public CA certificate file. For later steps, we will call this file "sklm_ca.pem".

   [user@localhost]$ keytool -importkeystore -srckeystore client.p12 -keystore client.jks -storetype JKS
3. Import the PKCS12 file into a new Java Keystore:

   Critical Note

A password will be asked for during this step. Retain this password for later.

   [user@localhost]$ keytool -v -list -keystore client.jks
4. Get the alias from the file:
5. Import the CA Certificate file into a new Java Truststore:

   ```
   [user@localhost]$  keytool -import -trustcacerts -alias sklm
   -file sklm_ca.pem -keystore sklmtrust.jks
   ```

   Critical Note

A password will be asked for during this step. Retain this password for later.
6. Get the alias from the file:

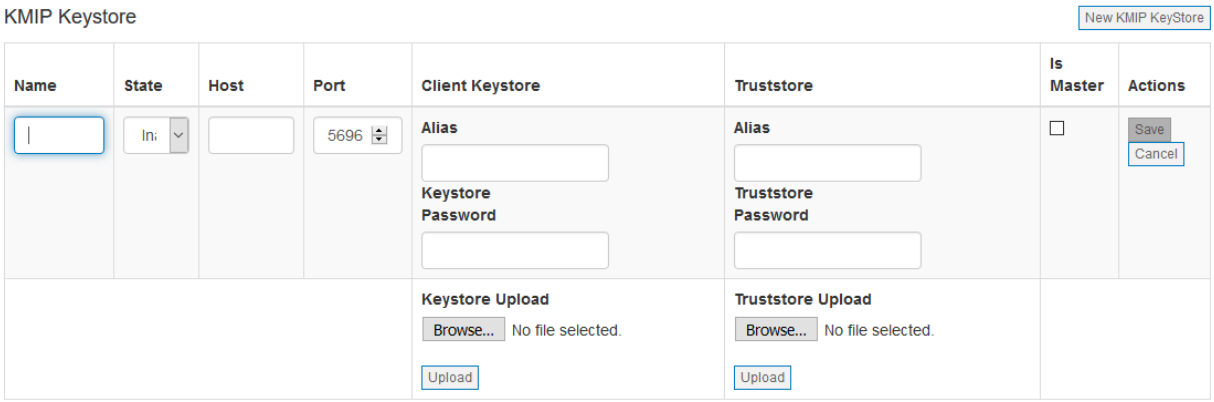
   keytool -v -list -keystore trust.jks

   The settings that will need to be filled in for the external keystore to be active:

   - **Name** - User defined reference for the external keystore
   - **State -** This will tell MDE the defined external keystore should override the current active keystore. If the state is *active*, MDE will start using the keystore. If the state is *inactive,* MDE will no longer use the keystore.
   - **Host -** The IP address of the external keystore.
   - **Port -** The port number of the external keystore.
   - **Client Keystore**
     - **Keystore Alias** - The gathered keystore alias.
     - **Keystore File** - Java Keystore file.
     - **Client Keystore Password** - The password setup on the keystore creation.
   - **Truststore**
     - **Truststore Alias -** The gathered truststore alias.
     - **Truststore File -** Java Truststore file.

- **Truststore Password -** The password setup on the truststore creation.

- **Is Master** - Identifies external keystore used as the master keystore for all read and write operations
  - Defaults to “true” for the first keystore defined.
  - If not selected, will be treated as a “clone” keystore and will only be used for read operations.
  - Only one external keystore can be designated as the master.



Note

Currently, MDE supports an external keystore product: IBM Security Key Lifecycle Manager (SKLM) configured for KMIP.

Hardware Security Modules (HSM)

About this task

When using an HSM as the external keystore, you will need to ensure that the 3rd party product is fully configured and operational per Manufacturer’s instructions.

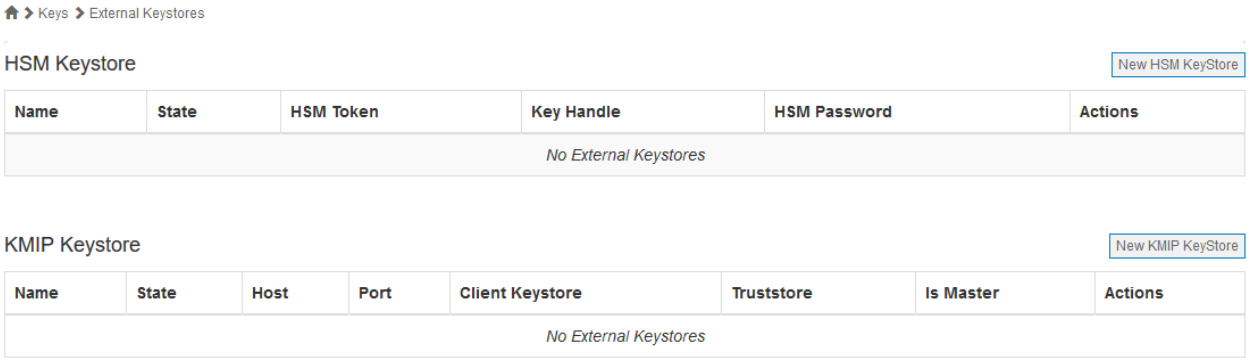
The HSM’s 64-bit version client software needs to be copied to the MDE VM by the PPM Product Administrator. The software should be extracted and installed along with SDK option using the HSM manufacturer’s product instructions for setting up and configuring communication.

A utility that comes with the client software or a utility that has been proven to work with HSM is used to create a wrapper key. A wrapper key is a 256-symmetric key that needs to be available for use with PPM.

When this symmetric wrapper key is created on the HSM, a handle is assigned to it. This handle will be needed when configuring the HSM in the PPM GUI page. The PPM will pass this handle and the policy key to the HSM for wrapping of the policy key and HSM will return the wrapped key to be stored in the PPM database.

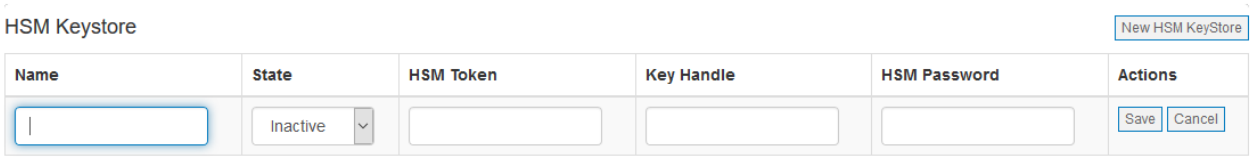
After installation and configuration of the software, ensure that PPM can communicate with the HSM, reboot the PPM VM.

From the External Keystores screen, select New HSM Keystore.



The following settings need to be filled in for an external keystore to be active:

- **Name** - User defined reference for the external keystore
- **State** - This sets the intended state for the keystore
- **HSM Token** - HSM uses the slot number of the partition
- **Key Handle** - This is the handle that is assigned to the key that will be used to wrap the policy keys
- **HSM Password** - This is the password associated with the partition that the customer will be using.



Note: Supported HSM product: SafeNet® Luna HSM configured for an HSM Keystore.

Chapter 10. File Level Policy Definition

MDE enables the Security Administrator to define file level control (operational and cryptographic) on various types of data. The terms below are used when defining file level data control.

- **Selectors -** an unordered list of users and groups which defines who is to be allowed access to any resource (or Path Set). Optionally, a defined process can be identified as another component for a selector.
- **Path Sets -** list of file paths to be protected by policy
- **Datatypes -** an ordered list of access definition rows assigned to a specified type of data. Each row is comprised of a selector, I/O (read/write) operation, and policy action.
- **Processes -** a file path to an executable. Used in a selector to define access controls with an identified executable. Optional for more enhanced access control.

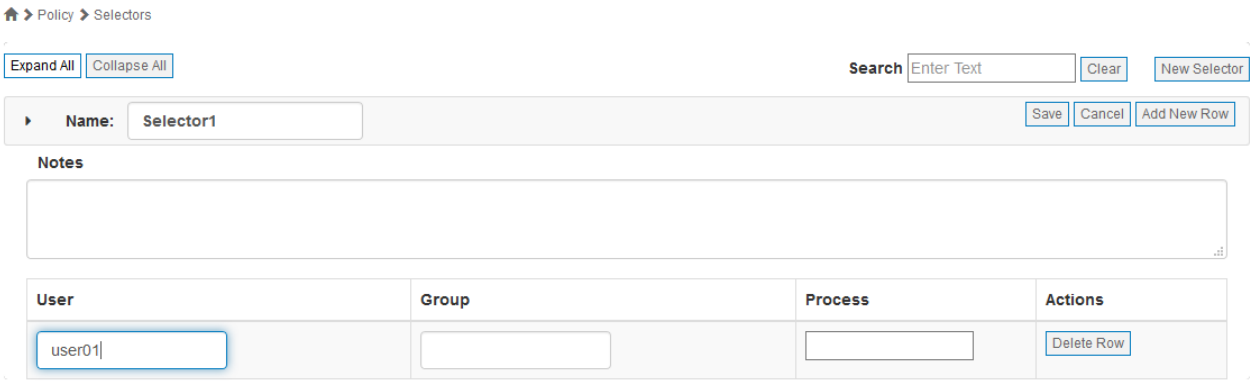
Once a Datatype is created, it can be associated with one or more provisioned agents. The following sections will describe the configuration of a Policy.

Selectors

A Selector is a Policy object that defines a set of users and / or user groups via one or more selector rows. When adding a new selector, the Security Administrator must supply a name prior to saving. Selector notes and rows can be added at any time by editing the selector.

Each selector row contains the following fields: user, group, process. One of the fields must be populated prior to being saved.

- **User** - the short-name of a target system defined user. This is matched to a user in the target Agents operating system. This field is optional.
- **Group** - the short-name of a target system or LDAP defined user group. This is matched to a user group in the target Agents operating system. This field is optional.
- **Process** - a reference to a product defined process name. This is matched to the process file path (and optional hash values) in the target Agent's operating system. This field is optional.



The values in each selector row are combined using a logical AND operation. If multiple fields are set in a single row, all fields must match for the row to match. A selector matches if any of the defined rows match. The ordering of rows within a selector do not impact the policy matching algorithm.

User	Group	Process	Agent Match Behavior
√			Matches on user

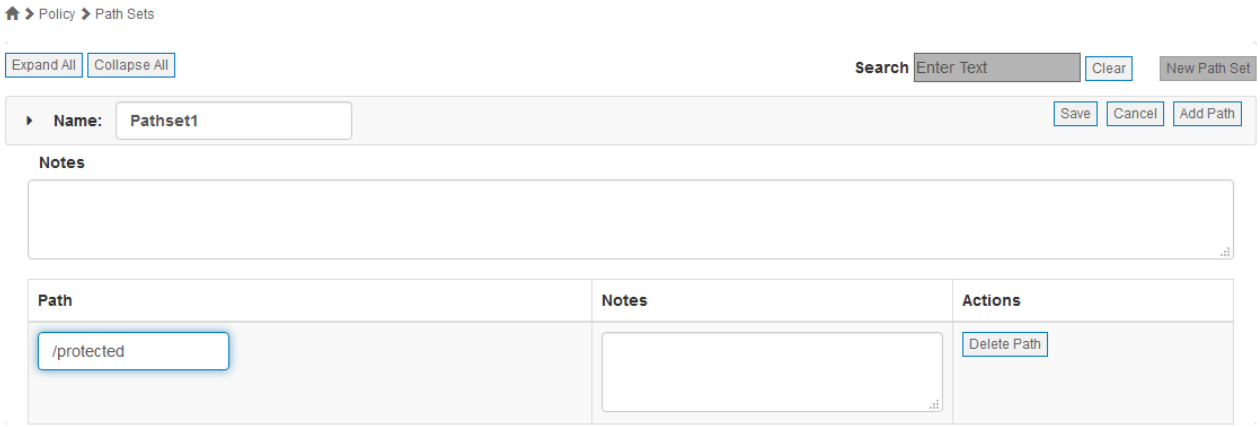
	√		Matches on any user in the defined group
		√	Matches on the process path defined and potentially restricts to any provided hash values
√	√		Matches on user only if acting as a member of the defined group
√		√	Matches on user only if acting via the defined process
	√	√	Matches on any user in the defined group only if acting via the defined process
√	√	√	Matches on user only if acting as a member of the defined group and acting via the defined process with process

Note

Selector user and/or group resolution works with the configured external LDAP or Active Directory server where the File Agent is installed.

Path Sets

A Path Set is a collection of one or more unordered file path rows. When adding a Path Set, the Security Administrator must supply a name for the Path Set. To add a row to the Path Set, click the “Add Path” button. Each row contains a file path, and notes.



The Security Administrator must supply a file path. Protection is recursive from the provided path down through any sub-directories. The notes field is optional.

Datatypes

A Datatype is an ordered collection of Datatype Row definitions enabling the file level operational and/or cryptographic access control of data. Each Datatype contains a name, policy enforcement key, user notes, and an ordered list of rows.

- **Name -** user defined reference to the Datatype
- **User Notes -** Security Administrator defined notes field.

Datatype Row

Each Datatype row contains the following fields: order, selector, operation, and action.

- **Order -** the priority in which each policy row will be checked. First matching row is used. This field is required but will not show if only one row is present.
- **Selector -** a selection of previously defined selectors. The policy row will match if any of the rows in the selector match. This field is required. MDE provides a “select all” Selector that will match on any user.
- **Operation -** a selection of file operations that can be performed. The options are “read” and “read/write”. This field is required.
- **Action -** a selection of access actions that associate to the operation. The options are “permit”, “deny”, “permit, log”, and “deny, log”. This field is required.

Datatype Row Variables

The Selector, Operation, and Action fields can be optionally set to be variable. This allows for a Security Administrator to create templates for a Datatype that will be completed during Agent creation. The available field settings are: May Edit, Must Edit, and Not Editable.

May Edit

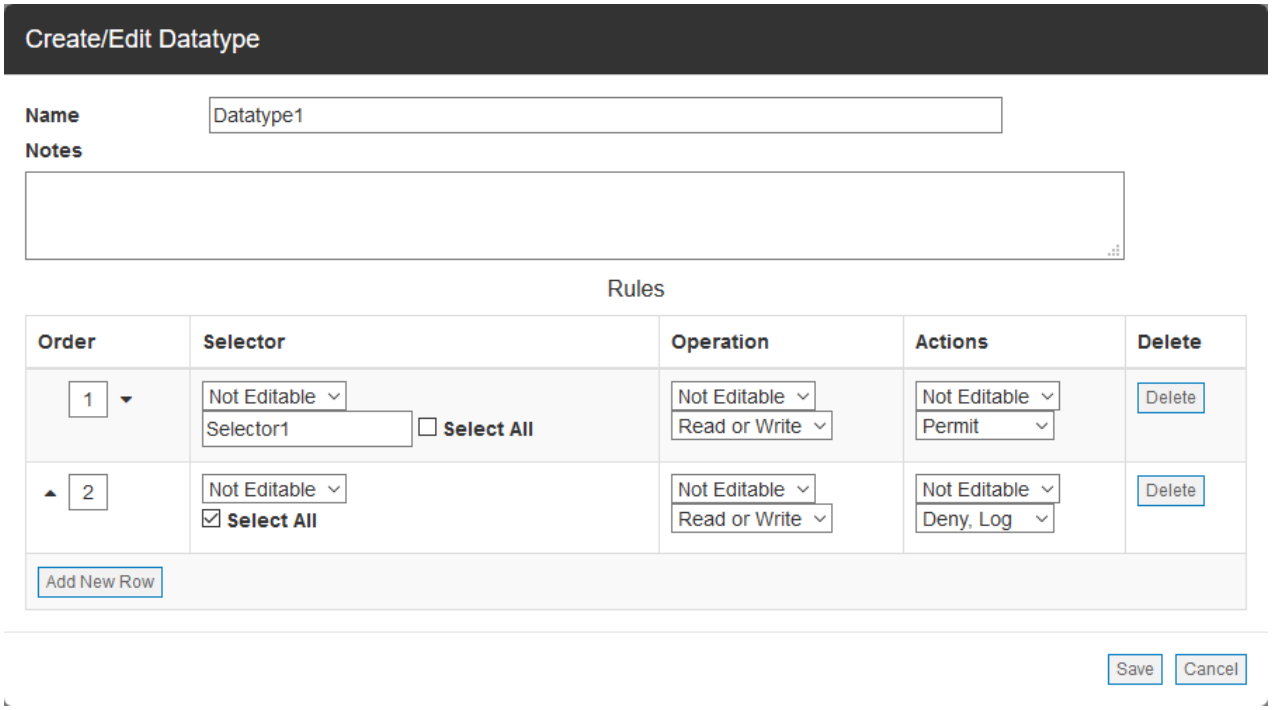
This field can optionally be overwritten during Agent creation.

Must Edit

This field must be set during agent creation.

Not Editable

This field must be set during Datatype creation and cannot be changed during Agent creation.

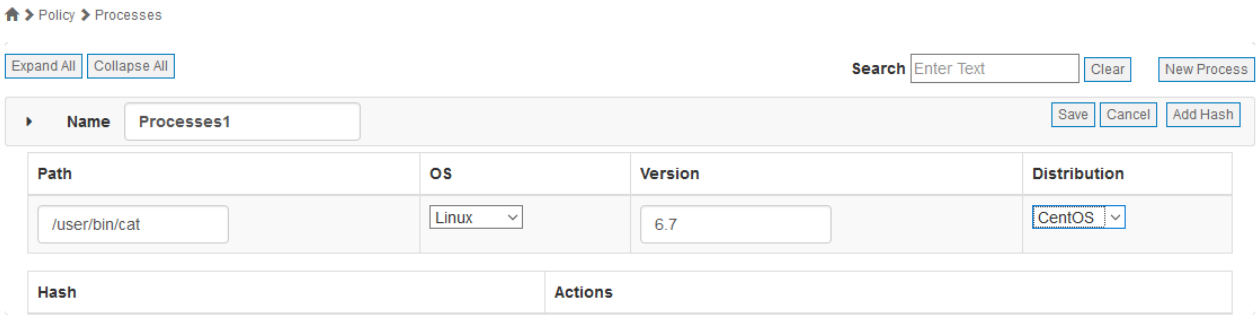


A Datatype cannot be saved until all rows have values and/or a variable setting.

Processes

A process identifies a file system path to an executable. A process is composed of the following fields:

- **Name** - name of process
- **Path** - absolute path to a file system executable
- **OS** - field used to reference operating system type (Linux, Windows, AIX).
- **Version** - field used for the operating system version.
- **Distribution** - field used for operating system distribution name (Red Hat, CentOS, Windows, AIX).



A process can be defined as a file path only or with a list of process hash values. When one or more hash values are defined, the process match will be limited to the listed hashes.

Note

Process hash values are generated via an agent tool and should be copied into PPM. The tool will output a hash value for the current version of the executable.

spxhash -p <path to executable>

Example:

[root@blkdr ~]# spxhash -p /usr/bin/vim

1202E81EF41273904A6DD381C35B2561F838F7E35B6B26959F8EEB646297A36A7C2

Chapter 11. Agent Provisioning and Management

MDE supports four types of agent installations: Volume, File with Policy, Volume with Policy, and Object Store. Each agent type enables a different method of data protection.

- **Volume** - agent protects data at a block device level
- **File with Policy** - agent protects data at a file level and provides file-based operational access control policies
- **Volume with Policy** - agent protects data at a block device level and also provides file-based operational access control policies
- **Object Store** - agent protects data sent to object storage

Adding an Agent

To add an agent, a Security Administrator must navigate to the Agents page of MDE and click the “Add Agent” drop down list. The available agent options will be listed.

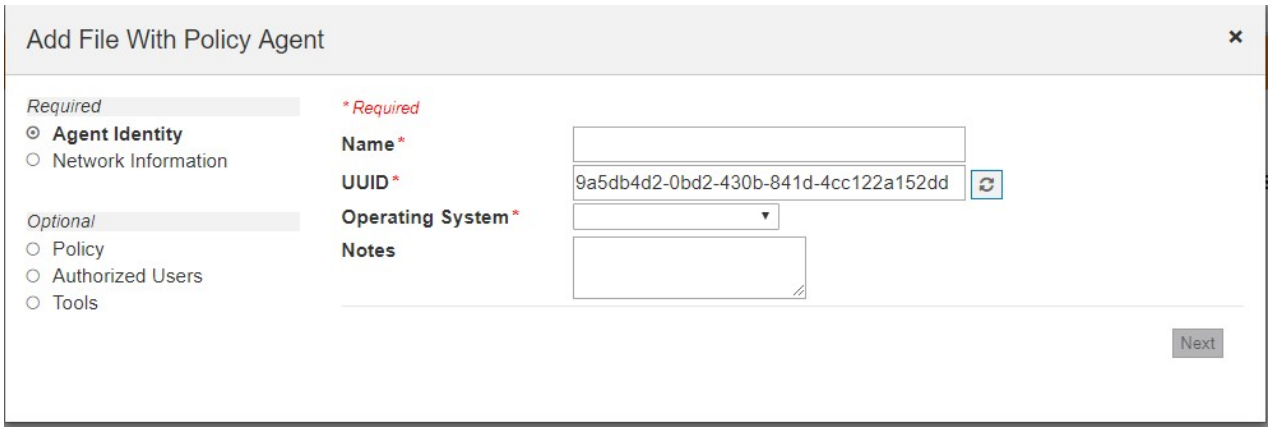
After selecting the agent type, a wizard opens to enable you to create the agent.

Note: It is recommended to add all intended policy components (Selectors, Path Sets, Keys, Datatypes, and Processes before starting the Add Agent process as these components cannot be created during process.

There are six sections to provisioning an agent: Agent Identity, Network Information, Policy, Volumes, Authorized Users, and Tools. All required sections must be completed before the agent can be added.

Identity

The Identity section requires the Security Administrator define a Name, UUID, Operating System, and Notes.



- **Name** - a user defined reference for the agent.
- **UUID** - a unique identifier MDE uses to identify the agent.
- **Operating System** - operating system of the target agent.
- **Notes** - Security Administrator notes for this agent.

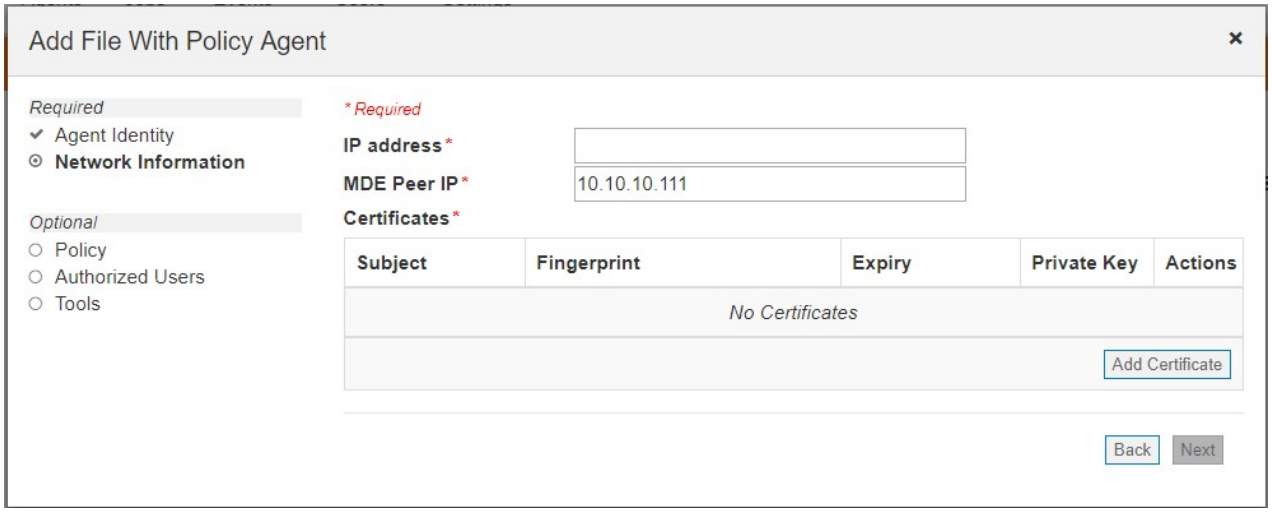
Once all the required fields are entered, click **Save** to go to the next step.

Note:

- MDE autofills the UUID but the Security Administrator can replace it if required.
- Required fields are indicated in the GUI
- Name for agents are not unique; therefore, if using the same name for multiple agents, event log messaging may misrepresent the message source

Network

The Network step requires the Security Administrator to define the hostname or IP address of the agent as well as MDE, and the certificates needed to establish a secure connection between MDE and the target agent.



- **IP Address**- IP address or host name of the server where the agent is being installed.
- **MDE Peer IP** - IP address or host name of MDE as seen from the target agent server instance.

  Note: MDE auto-fills the MDE Peer IP, but the Security Administrator can modify it if required.
- **Certificates** - list of uploaded certificates used to establish a secure connection between MDE and the installed agent. This certificate is used to establish a mutually authenticated TLS1.2 connection between the agent and MDE PPM Server.

To upload a certificate, the Security Administrator must click **Add Certificate**, navigate to the desired certificate and open it. It will display in the New Agent-Network screen.

Note: The Agent and PPM will not communicate and the agent will not encrypt data and enforce policies if the keystore and truststore certificates have not been uploaded to MDE and the agent is not assigned the matching certificate. Please refer to the section “Server Certificate Settings” for more details.

Once all the required fields are entered, click **Next** to go to the next step.

File with Policy, Volume with Policy, and Volume Agent Creation

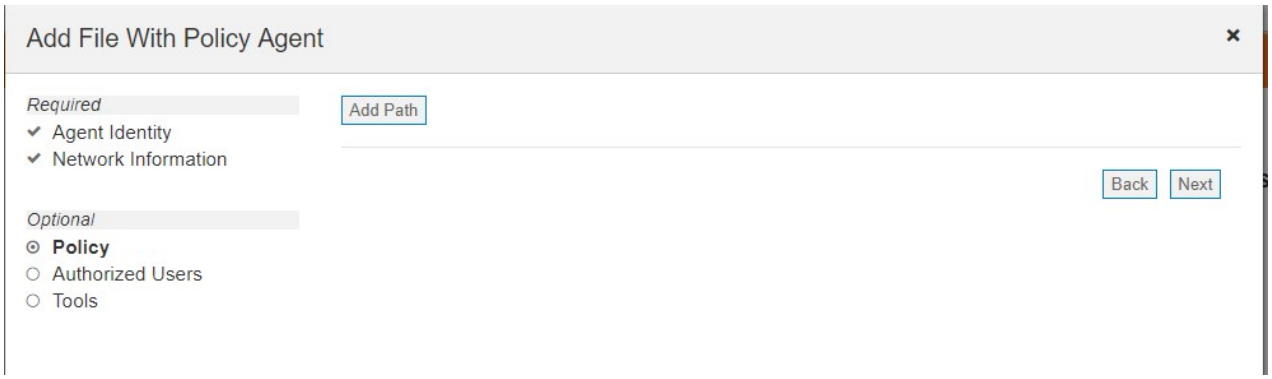
The Policy step requires the Security Administrator to define the operational and cryptographic controls to file paths on the targeted agent.

Add Path

File with Policy and Volume with Policy agents can add a path definition to the agent policy. Each added path protects an individual or grouping of file paths on the targeted agent. The number of paths added is defined by the Security Administrator.

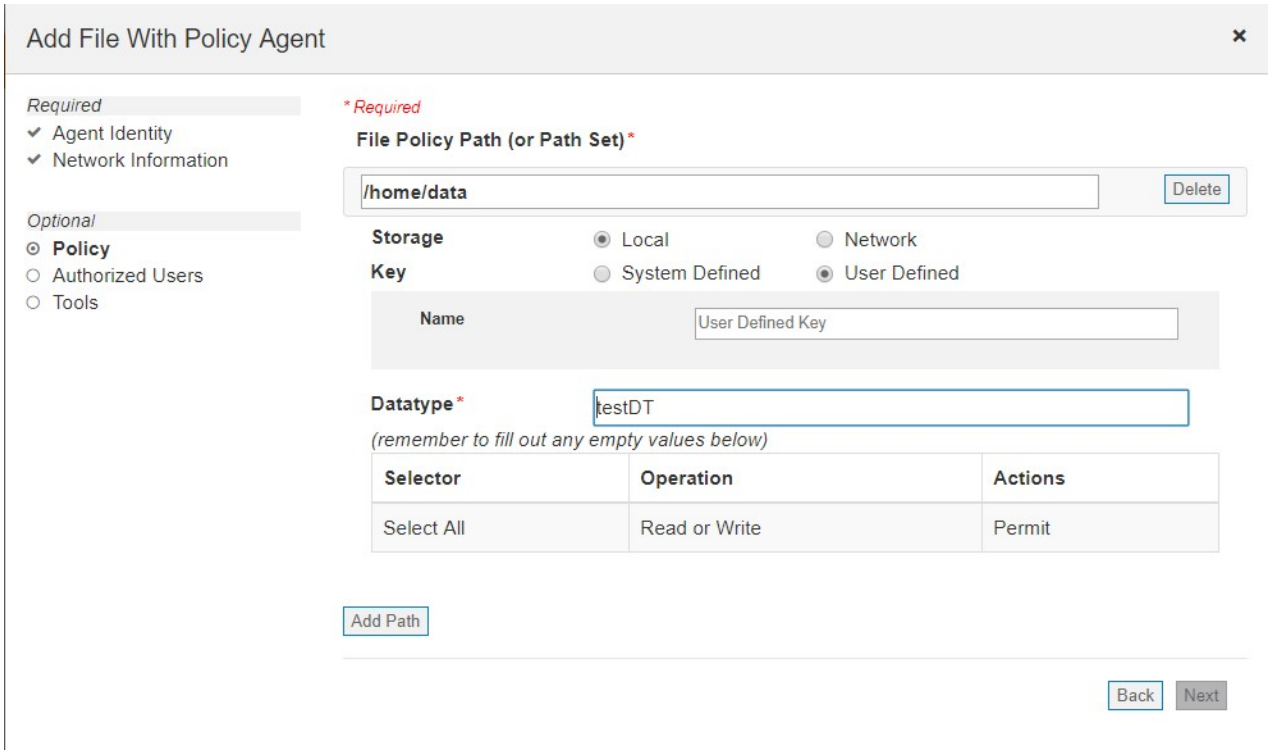
Critical Note

- **Paths protected via policy must exist at time of policy application or the policy application will fail.**
- **Existing files and sub-directories must be manually processed with the spxconvert command available after installation of File with Policy Agent. Policy will be in effect even if the files are not encrypted.**
- **New Files and directories added after installation will automatically be encrypted and protected via policy.**



To add a path, click the **Add Path**.

Each added path requires the entry of file path or path set, key, and a datatype.



- **File Policy Path (or Path Set) -** identifies the path or group of paths to be protected by the identified Datatype access control definition. Protection is recursive from the provided file path into any sub-directories.
- **Storage –** Identifies the location of the file path. Options are Local or Network. If Network is selected, additional parameters must be entered to properly configure the network storage. (See configuration information below)

- **Key -** key used to encrypt paths associated with the Datatype. Any previously defined User Defined key or the MDE managed System Defined key can be used. This field may or may not be visible depending upon whether File with Policy or Volume with Policy is used (see Note).
- **Datatype -** selection of a pre-created Datatype. Once selected, the Datatype information is added inline. If a Datatype with variables is used, the variables must be entered prior to saving.

Note:

- If using a Path Set, it must be created prior to adding the new agent. Otherwise, a single manual path may be defined.
- The Datatype used must be created prior to adding the new agent.
- If the new agent is Volume with Policy type, Path Sets will not contain policy enforcement keys as protection is accomplished via volume policy definition.

Local Storage Configuration

If using local storage when defining your file policy path, select the **Local Storage** option. This will direct the agent to protect the absolute file path (or path set) defined. No additional parameters are needed.

Network Storage Configuration

If using network storage when defining your file policy path, select the “Network Storage” option. This will direct the agent to mount the defined network storage to the absolute file path defined. Path sets cannot be used with network defined storage. Additional parameters are required.

Network storage requires the definition of: protocol, hostname/IP, share, username, password, and advanced mount options.

- **Protocol –** identifies the type of network storage being leveraged. Options are: NFSv4, NFSv3
- **Hostname/IP –** the hostname/IP of the network storage system
- **Share –** the network file system exported location
- **Username –** (not required for NFSv3) The authentication username to the network file system
- **Password –** (not required for NFSv3) The authentication password to the network file system
- **Advanced Mount Options –** Comma separated options to apply to NFS definition

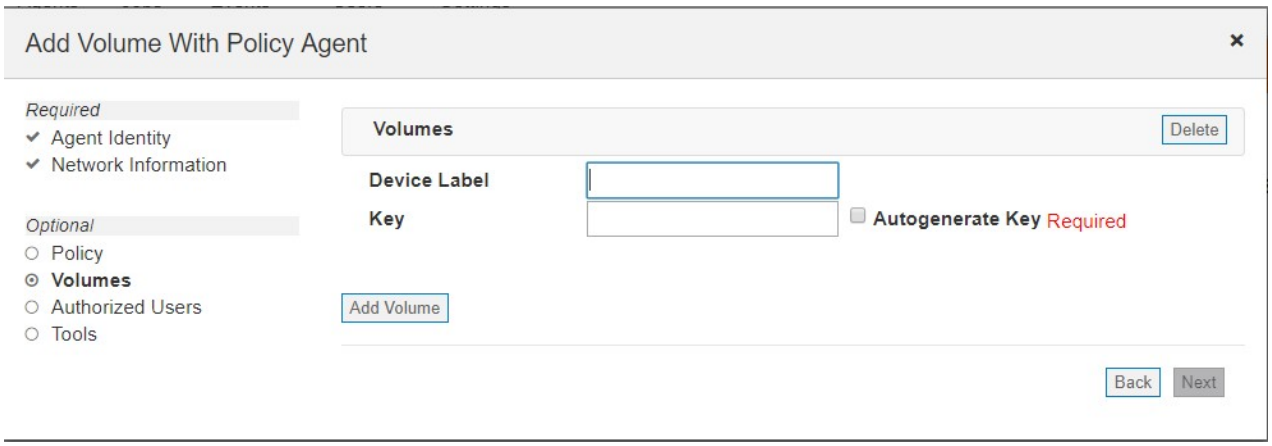
After all the required fields are entered, click **Next** to go to the next step.

Volumes

Add Volume

About this task

Volume and Volume with Policy agent types can add one or more volume definitions to the agent policy. Each volume added is a new protected block device on the targeted agent.



To add a volume, click **Add Volume**. Each added volume requires the entry of an underlying device label and a policy enforcement key.

- **Device Label** - identifies the device being protected. After policy is deployed to an agent, the device label will need to be associated to the volume via running the spxdevice command (See the *Installing an Agent* section).
- **Key** - key used to encrypt the volume. Any previously defined key or the MDE managed Auto-generate Key can be used.

Critical Note

Unless using the "Autogenerate Key" option, the policy enforcement key added must be defined prior to adding the agent. See the *Policy Enforcement Key Management* section.

After all the required fields are entered, click **Next** to go to the next step.

Object Store Agent Creation

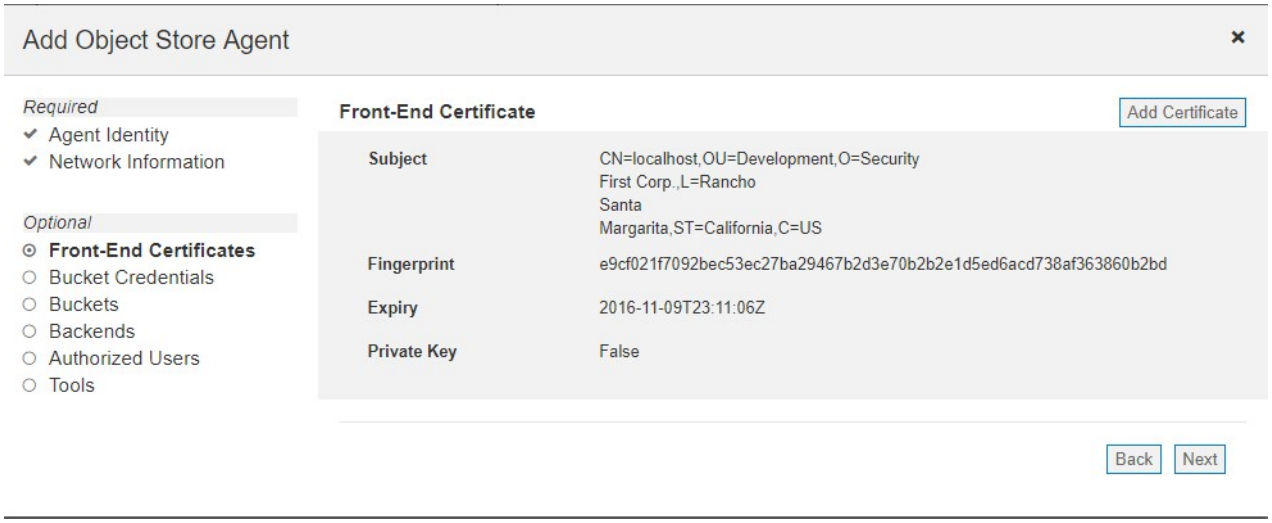
MDE Object Storage agent (OSA) acts as an intermediary between a client and the backend object storage. Object storage clients connect to OSA using bucket credentials instead of the backed object storage credentials.

Administrators can configure OSA to connect to one or more object storage providers. OSA encrypts and enforces policy on data sent through OSA to the configured backend object storage. If more than one backend is configured, the data is split and pieces of the data is sent to each backend.

Front-End Certificates

Object Store agents require the configuration of a certificate to establish a secure connection between the object store client and the Object Store agent.

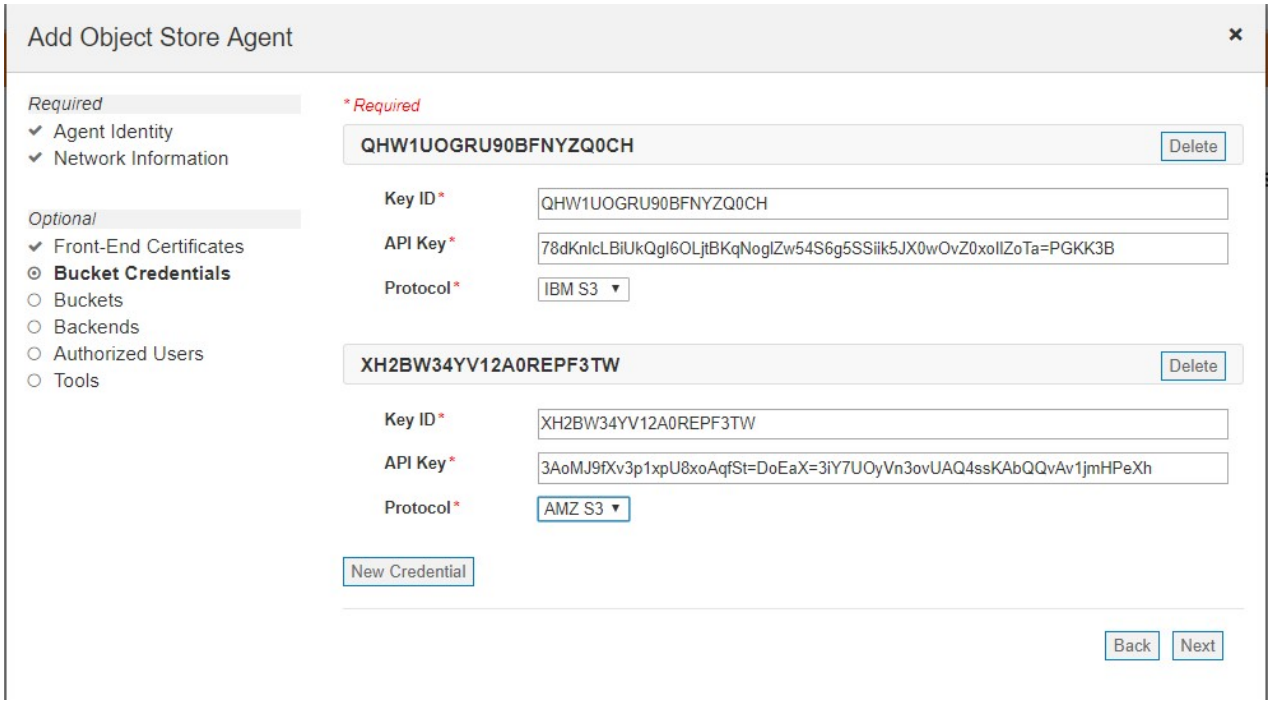
To upload a certificate, the Security Administrator must click the "Add Certificate" button, navigate to the desired certificate and open it.



Once all the required fields are entered, click “Next” to go to the next step.

Bucket Credentials

MDE can be configured to communicate with multiple object storage providers. Each provider will require the configuration of a bucket and bucket credentials.



To add a new credential set, click the "New Credential" button.

Bucket Credentials require the definition of: Key ID, API Key, and Protocol.

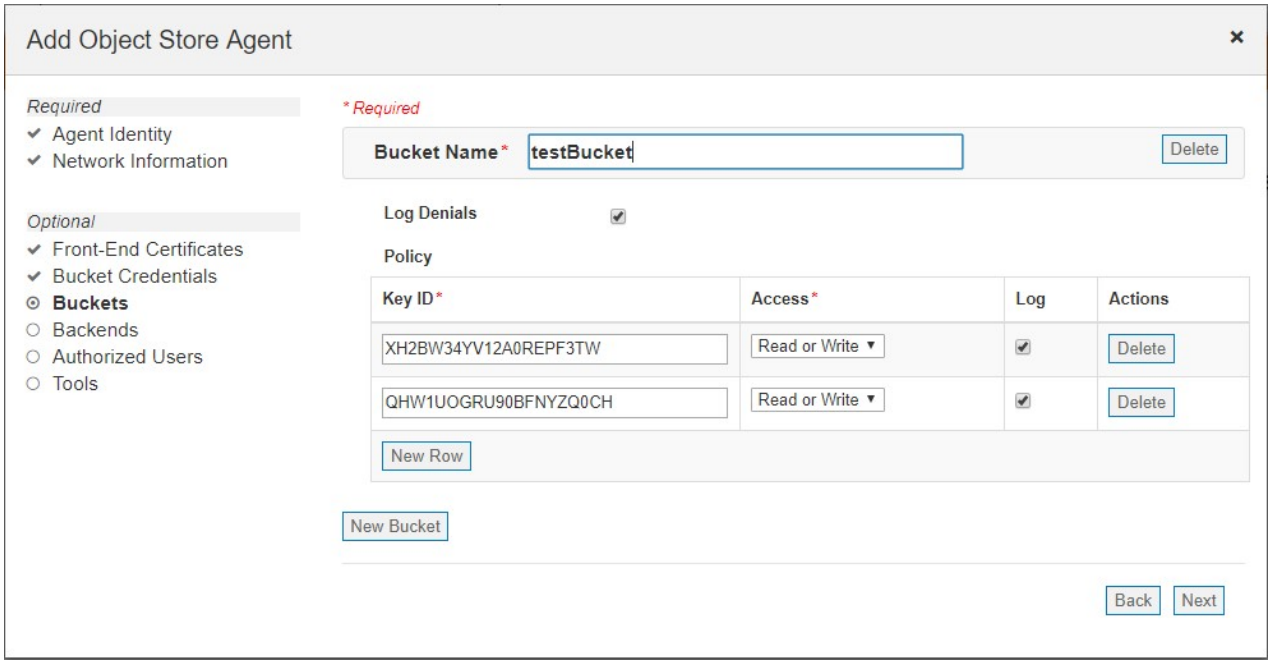
- **Key ID –** the identification of the object store accessor
- **API Key –** a string password to provide to the S3 API to correlate to the Key ID
- **Protocol –** the identification of the protocol leveraged to communicate with the object storage provider (Swift, IBM S3, and Amazon S3).

MDE will generate a Key ID and API Key pairing. Administrators can override these generated values if desired. An administrator will need to select the desired protocol from the supported object storage providers.

Once all the required fields are entered, click “Next” to go to the next step.

Buckets

MDE defines object storage policy via the association of buckets. Each bucket requires the definition of: Name, Log Denials, and Policy.

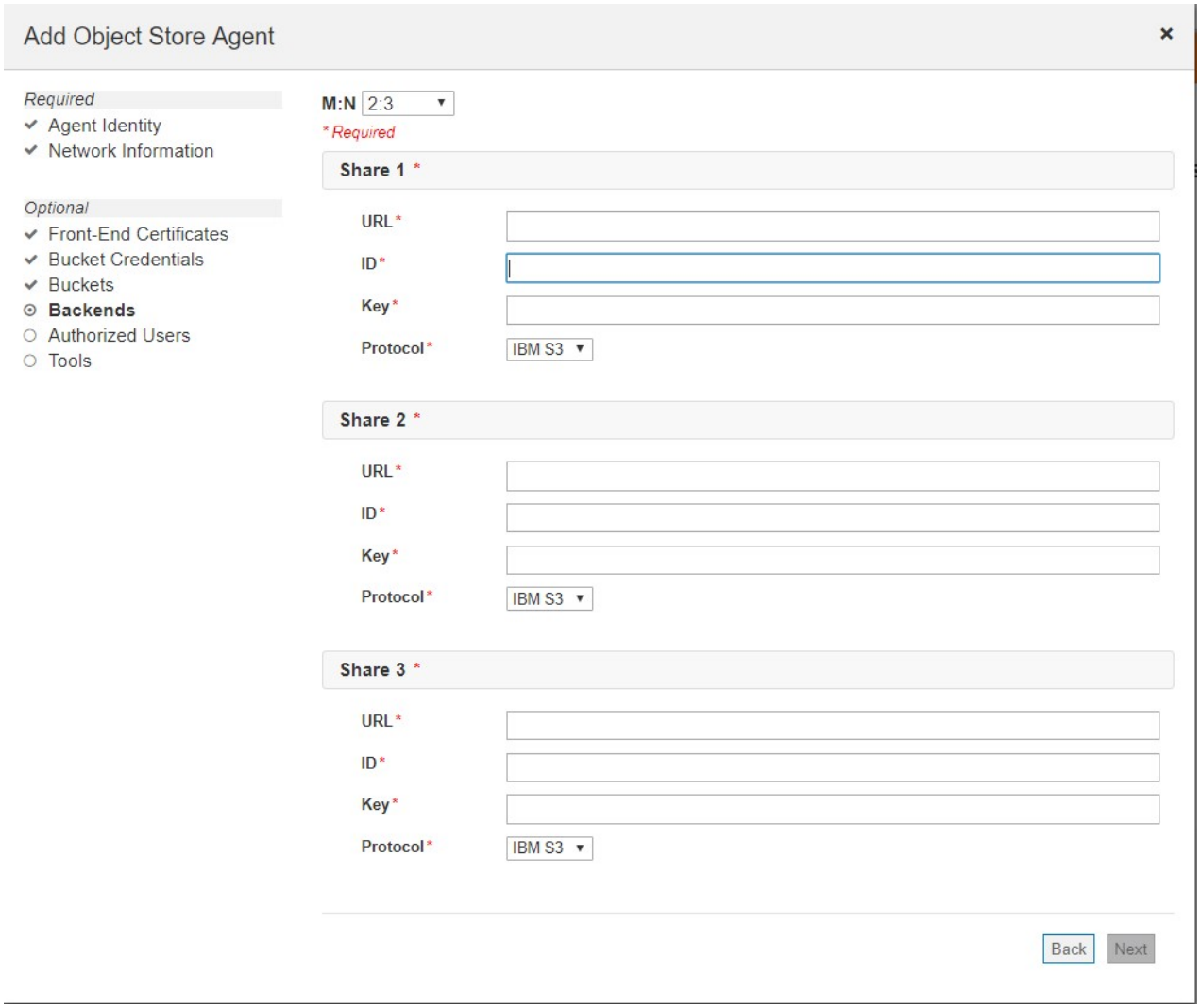


- **Name –** the name of the object storage bucket
- **Log Denials –** a checkbox selection. If checked the Object Store agent will create audit logs for access denials.
- **Policy –** The definition of the bucket access controls. Policy can be comprised of multiple rows. Each row of policy definition requires: Key ID, Access, Log,
- **Key ID** – the entry of a pre-created Bucket Credential Key ID.
- **Access** – the selection of either: Read or Write, Read, or Write access privileges.
- **Log** – a checkbox selection. If checked the Object Store agent will create audit logs on access permits of the provided row behavior.

Once all the required fields are entered, click “Next” to go to the next step.

Backends

Backend connection information is defined via a M:N selection. This selection defines the redundancy and security of the object storage data. N represents the number of backend object storage providers being configured or “shares”. M represents the number of shares required to reconstruct the data. The supported configurations are 1:1, 2:3, 2:4.



Each share requires the configuration of: URL, ID, Key, and Protocol.

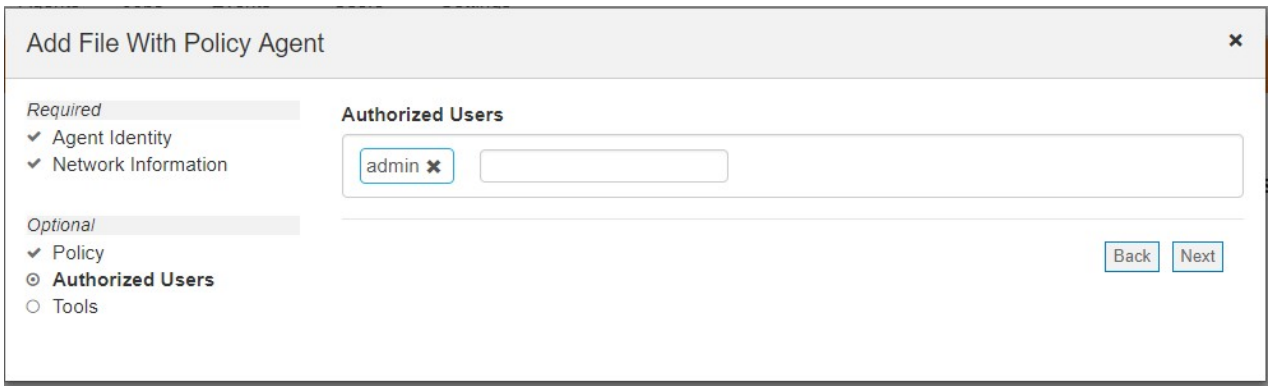
- **URL –** the access URL for the object storage provider
- **ID –** the account user id to access the object storage provider.
- **Key –** the user id account key to access the object storage provider.
- **Protocol** -- the identification of the protocol leveraged to communicate with the object storage provider (Swift, IBM S3, and Amazon S3).

Once all the required fields are entered, click “Next” to go to the next step.

Authorized Users

The Users step requires the Security Administrator to define the MDE user accounts that have privileges to download the agent install bundle.

If a user is not listed as an authorized user, and if that user logs in and views the agent, that user will not see the download links in the Agent Info page.



After all the required fields are entered, click **Next**to go to the next step.

Agent Tools

Agents support specialized tools that aid the transfer of data in an encrypted form. There are two types of tools: Backup/Restore and Object Store.

Tools are configured during agent provisioning or on the Agent Info page. The Backup/Restore tool is used to backup and restore encrypted data. It leverages an associated key to backup encrypted data and provides the ability to restore the encrypted data at a later time even if the policy key has been rotated. The backup/restore tool is optional with no requirement to associate a tool to an agent. The Object Store tool is required for the Object Store Agent

Agent Tools Matrix

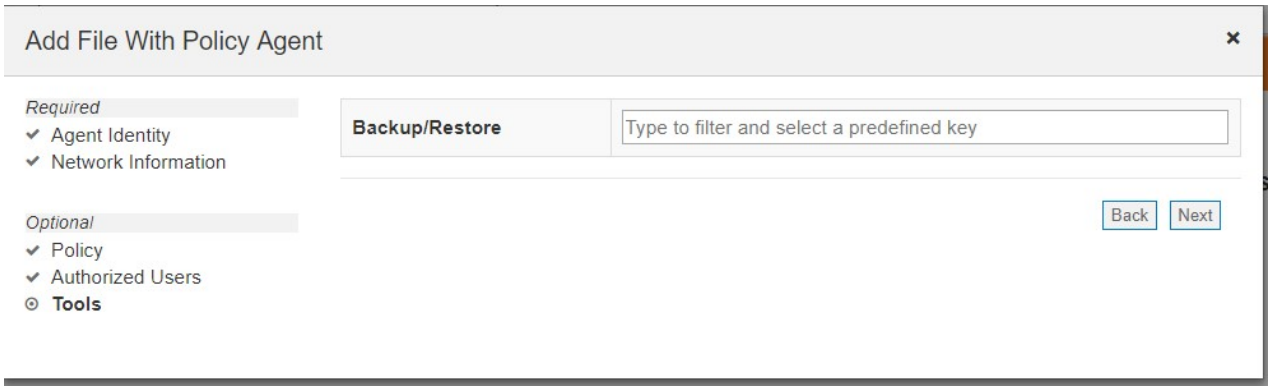
Tool availability is based upon agent type and enabled by associating a key. The tools matrix by agent type is as follows:

Tool Type	Volume	Volume with Policy	File with Policy	Object Store
Backup/Restore	√	√	√	
Object Store				√

Tool Key Association

To associate a key to a tool, start typing a previously defined key name into the text box next to the desired tool and then select the appropriate key from the list.

Click **Save** and a job will be created. Once approved, the configured tool will be enabled on the agent.



Note: Auto-generated keys are not supported on Tools. Keys must be defined prior to creating the agent.

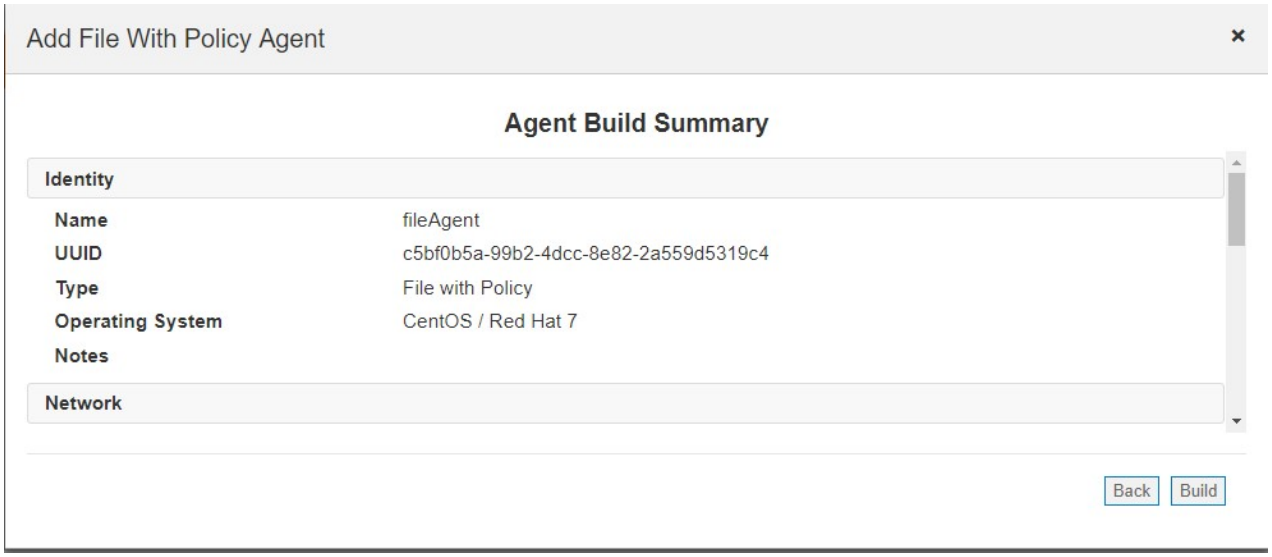
After all the required fields are entered, click **Next** to go to the next step.

Review and Build

About this task

When all provisioning steps are complete, the user will be navigated to the Review screen.

The review page of the provisioning setup will display a complete view of all the configuration information.



Review the contents for completeness and correctness and click **Build** to complete the provisioning process. A job will be created to add the agent.

Upon job approval, the agent will be created, and the installation package will be available to download and install.

Agent Activation

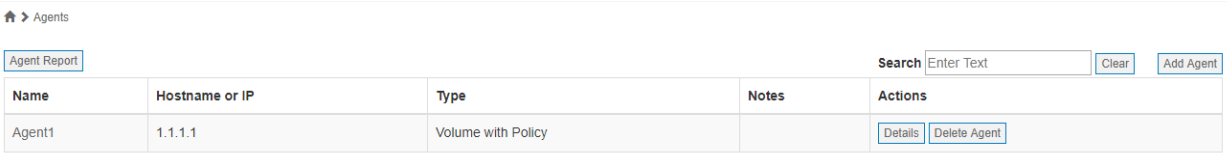
Upon agent build job approval, the newly created agent is active within MDE. Once the agent is installed, it will use the configured MDE Peer IP and provided certificates to create a mutually-authenticated TLS1.2 connection to MDE.

The agent will request policy on initial installation and subsequent startup. MDE will respond with the configured policy configuration. Once the policy is received it is enforced at the agent.

Viewing Agents

About this task

The Agents page will display a summary list of created agents.



To see the details for any specific agent, click the agent name in the Name column or click the Details button in the Actions column. This will open an agent detail view page which displays provisioning information, installation bundle downloads, and other useful information.

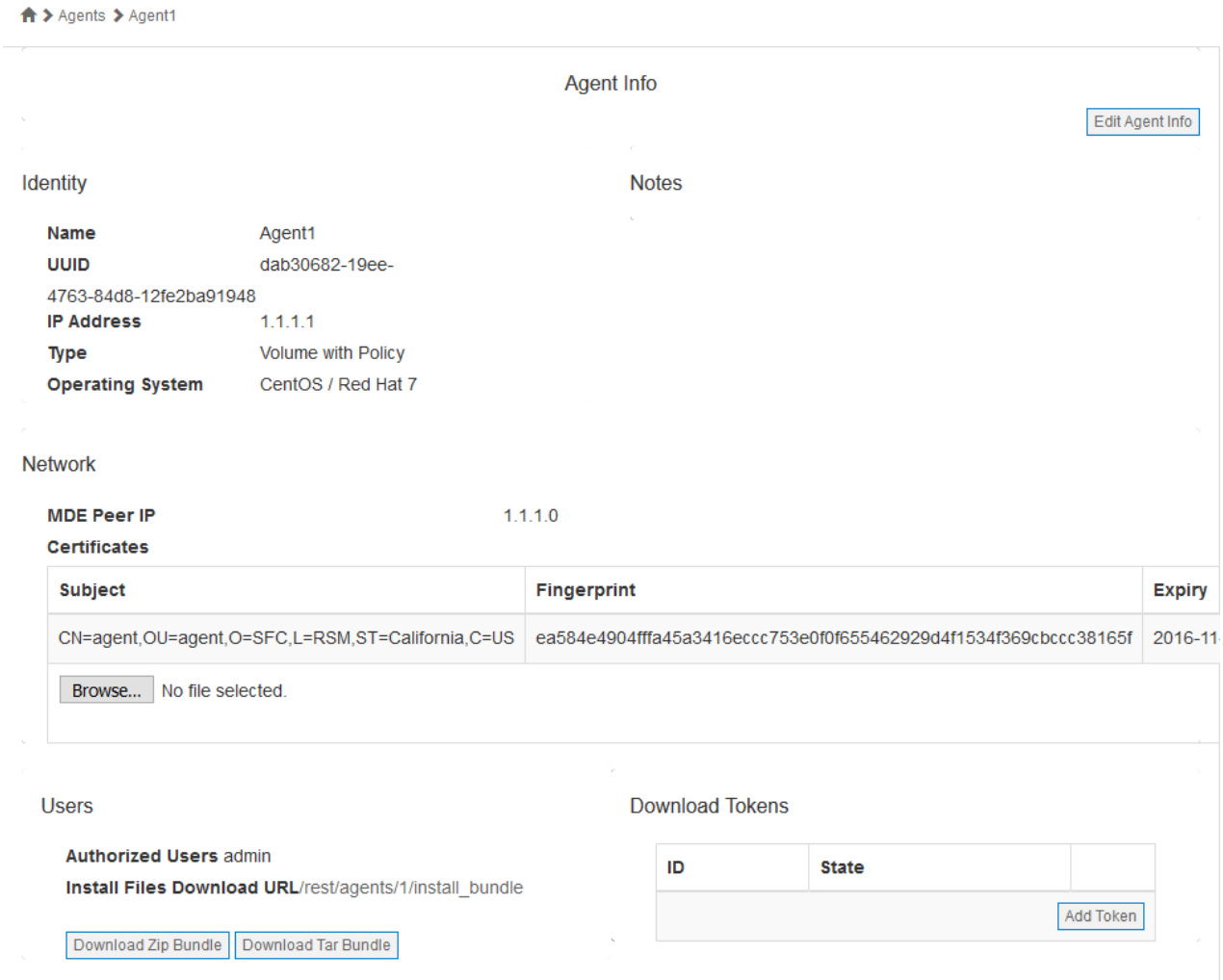
Agent Report

The MDE Security Administrator can create an Agent Report. This report contains information on: total number of agents, agent counts by type and operating system, and agents logged in within 30 days from report generation. The date is based on the PPM time, which is UTC time. The data will be broken down in to agent type.

Installing an Agent

About this task

The provisioning step configured all the information necessary for agent install and deploy policy to a target server instance. To install the agent, download the installation package, copy it to the target system, unpack the contents, and run the setup script.



Critical Note

Ensure all users, groups and paths or devices identified in the provisioning policy are created, attached and configured to the agent system.

Installing an Agent for Linux

There are 4 Agent types: Volume Agent, File with Policy Agent, Volume with Policy Agent, and Object Store Agent. Use the Agent Type designated during Agent Provisioning.

Linux Volume Agent Device Configuration

About this task

Procedure

1. Create a Volume in PPM (remember device label used in Section 11.1.5).
2. Install the “gettext” package on your agent VM.
3. Install the agent – see Appendix A, “Sample Agent Installation Processes,” on page 81 for details
4. Reboot agent VM when installation completes.
5. As root, run spxdevice -e <label given in PPM> -m <mount point> -f <file sytem> -u <disk to use>

```
spxdevice -e COS6VOL -m /protected -f ext4 -u /dev/sdb
```

Linux File with Policy Agent Device Configuration

About this task

Procedure

1. Create a File with Policy Agent in PPM
2. Create any required users
3. Create any required sub-directories
4. Set proper permissions on directories
5. Install “gettext” package on your agent VM
6. Install the agent – see Appendix A, “Sample Agent Installation Processes,” on page 81 for details
7. Reboot agent VM when installation completes
8. Validate the file policy is correct via the command “spxinfo -l”

Note

An asterisk next to a path indicates that there is pre-existing data that is pending encryption. To perform encryption in place on pre-existing directory structures and data and to determine the status of data at any time, MDE provides a command line utility called “spxconvert”

See Appendix E, “Encryption in Place,” on page 93 for detailed description of the command and its use.

Linux Volume with Policy Agent Device Configuration

About this task

Procedure

1. Create a Volume with Policy Agent in PPM (remember device label used)
2. Install the “gettext” package on your agent VM
3. Install the agent – see Appendix A, “Sample Agent Installation Processes,” on page 81 for details

4. Reboot agent VM when installation completes
5. As root, run spxdevice -e <label given in PPM> -m <mount point> -f <file sytem> -u <disk to use>

   [root@localhost]# spxdevice -e COS6VOL -m /protected -f ext4 -u /dev/sdb
6. Create any required sub-directories and users
7. Set proper permissions on directories
8. Reboot the agent VM
9. lsblk – use to verify disk exists and may take ~30 seconds sometimes
10. Validate the file policy is correct via command “spxinfo -l”

Note

On Linux, volume encryption can be setup on full devices or partitions. To use a single partition simply specify an empty partition (e.g. /dev/sdb1) when using the spxdevice -u option.

Linux Object Store Agent Configuration

About this task

Procedure

1. Create a Object Store Agent in PPM
2. Install the agent - see Appendix A, “Sample Agent Installation Processes,” on page 81 for details
3. Reboot agent VM when installation completes

Installing an Agent for AIX

AIX supports a single agent type: File with Policy Agent. Use the Agent Type designated during Agent Provisioning.

AIX File with Policy Agent Device Configuration

1. Create a File with Policy Agent in PPM
2. Create any required users
3. Create any required sub-directories
4. Set proper permissions on directories
5. Install the agent – see Appendix A, “Sample Agent Installation Processes,” on page 81 for details
6. Reboot agent VM when installation completes
7. Validate the file policy is correct via the command “spxinfo -l”

Note: An asterisk next to a path indicates that there is pre-existing data that is pending encryption. To perform encryption in place on pre-existing directory structures and data and to determine the status of data at any time, MDE provides a command line utility called “spxconvert”

See Appendix E, “Encryption in Place,” on page 93 for detailed description of the command and its use.

Installing an Agent for Windows

There are 3 Agent types: Volume Agent, File with Policy Agent and Volume with Policy Agent. Use the Agent Type designated during Agent Provisioning.

Windows Volume Agent Device Configuration

About this task

Procedure

1. Create a Volume in PPM (remember device label used).
2. Install the agent -see Appendix A, “Sample Agent Installation Processes,” on page 81 for details
3. Reboot agent VM when installation completes
4. Run “spxdevice -e <label given at PPM> -d <disk number to use>” to attach to the entire disk. Must run as Administrator.

   ```
   spxdevice -e PRODISK -d 1
   ```

5. Or run spxdevice -e <label given at PPM> -d <disk number to use> -m <drive letter> -f <file system> to attach to the entire disk that will be formatted and mounted with a drive letter.

   ```
   spxdevice -e PRODISK -d 1 -m E -f NTFS
   ```

6. Alternatively, run “spxdevice -i <disk number to use>” to stage the disk to attach to a specific partition

   ```
   spxdevice -i 1
   ```

7. Next run “spxdevice -e <label given at PPM> -v <drive letter> -f <filesystem>” to attach to a specific partition and format the partiton with a filesystem

   ```
   spxdevice -e PRODISK -v E -f NTFS
   ```

   Note: On Windows, volume encryption can be setup on full devices or partitions.

   - For entire disk encryption, the disk must be online and initialized and disk space must not be formatted. Drive letters must be available.
   - For partition encryption, the backing device must be created via “spxdevice -i <disk number>” on a clean disk. Then, a RAW partition with a drive letter must be created.

   Refer to the help in the “spxdevice” command for more options.

Windows File with Policy Agent Device Configuration

About this task

Procedure

1. Create a File with Policy Agent in PPM
2. Create any required users
3. Create any required sub-directories
4. Set proper permissions on directories
5. Install the agent – see Appendix A, “Sample Agent Installation Processes,” on page 81 for details
6. Validate the file policy is correct via command: spxinfo -l

   Note

   An asterisk next to a path indicates that there is pre-existing data that is pending encryption. To perform encryption in place on pre-existing directory structures and data and to determine the status of data at any time, MDE provides a command line utility called “spxconvert”

   See Appendix E, “Encryption in Place,” on page 93 for detailed description of the command and its use.

   Note

   On Windows, make sure that an administrative user is permitted to create the target directories via policy as the policy is in effect once the policy is retrieved.

Windows Volume with Policy Agent Device Configuration

About this task

Procedure

1. Create a Volume with Policy Agent in PPM (remember device label used)
2. Install the agent – see Appendix A, “Sample Agent Installation Processes,” on page 81 for details
3. Reboot agent VM when installation completes
4. Run “spxdevice -e <label given at PPM> -d <disk number to use>” to attach to the entire disk. Must run as Administrator.

   PS C:\> spxdevice -e PRODISK -d 1
5. Or run “spxdevice -e <label given at PPM> -d <disk number to use> -m <drive letter> -f <file system>” to attach to the entire disk that will be formatted and mounted with a drive letter

   PS C:\> spxdevice -e PRODISK -d 1 -m E -f NTFS
6. Alternatively, run “spxdevice -I <disk number to use> to stage the disk to attach to a specific partition.

   PS C:\> spxdevice -i 1
7. Next run “spxdevice -e <label given at PPM> -v <drive letter> -f <filesystem>” to attach to a specific partition and format the partiton with a filesystem.

   PS C:\> spxdevice -e PRODISK -v E -f NTFS

   Note

   On Windows, volume encryption can be setup on full devices or partitions.
   - For entire disk encryption, the disk must be online and initialized and disk space must not be formatted. Drive letters must be available.
   - For partition encryption, the backing device must be created via “spxdevice -i <disk number>” on a clean disk. Then, a RAW partition with a drive letter must be created.

   Please refer to the help in the “spxdevice” command for more options.
8. Add protected directory(ies) onto volume
9. Restart computer
10. spxinfo -l (should show list of all protected directories)

    Note

    On Windows, make sure that an administrative user is permitted to create the target directories via policy as the policy is in effect once the volume is attached and available.

Active Policy

Each agent can have only one active policy. Agents do not store their policy in a persistent way. On every agent reboot the agent requests the currently active policy from MDE. If MDE is inaccessible by the agent, then the default deny access will be applied to all protected directories on the agent.

When a new policy is sent to the agent, the agent will send an event to MDE on successful (or unsuccessful) application of the policy. If policy activation issues persist, refer to the kernel_policy.log file in the following locations:

- Linux/AIX: `/var/log/spxagent/spx-policyagent`
- Windows: `C:\Windows\spxagent\PolicyAgent`

Editing an Agent

After an agent is successfully provisioned and approved any changes to that agent must be made by editing the agent through the GUI on the “Agent Info” page. To edit an agent, view the agent details. On the Agent Info page, sections of the agent can be edited independently.

Edit Agent Info

Clicking the “Edit Agent Info” button will allow the modification of some agent information: Name, IP Address, MDE Peer IP, and Notes.

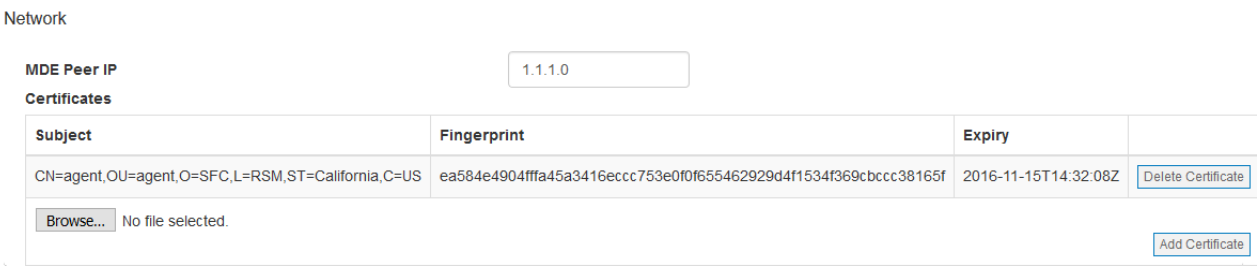
Changes to MDE Peer IP will be immediate within MDE, but if the agent was already installed a new install package must be created and installed before changes will be in effect.

Note

UUID, Operating System, and Agent Type are not editable after initial provisioning.

Add/Delete Certificates

Agent certificates can be added and deleted by clicking the appropriate buttons in the certificates section of the Agent Info page.



To update an Agent Certificate, follow these steps:

1. Generate new certificate for the agent

2. Upload new certificate to PPM via the Management Console
    a. From the Agents page, click on the agent to be updated to display the Agent Info page
    b. Click the “Add Certificate” button, select the new certificate file and click “OK” button
    c. The new certificate should be displayed
3. Delete the old certificate
    a. From the Agents page, click on the Agent to be updated to display the Agent Info page
    b. Determine the certificate that is to be deleted
    c. Click the “Delete Certificate” button, a job will be created
    d. Click the “Dismiss” button
    e. From the Jobs page, click “Approve” button on the desired job
4. Verify certificate has been deleted from the agent
    a. From the Agents page, click on the agent to be updated to display the Agent Info page
    b. Verify proper certificate is remaining

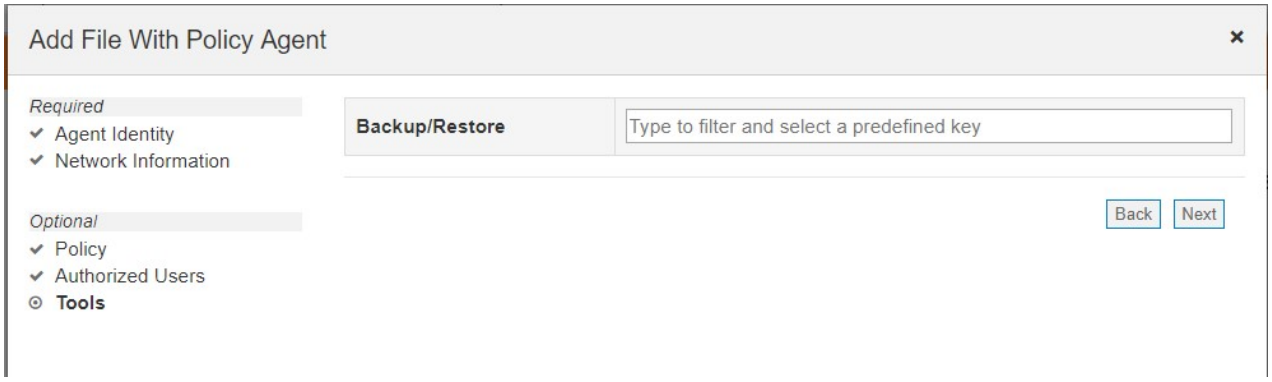
If the agent was already installed a new install package must be created and installed before certificate changes will be in effect.

Agent Tools

The tools that were not configured during agent provisioning can now be added on the Agent Info page. Additionally, configured tools can be modified.

Associate a Key

To associate a key, type the key name into the text box next to the tool and select the key from the list. Click “Save” and a job will be created. Once approved, the configured tool will be enabled on the agent.



Modify a Key

To modify a key, click the edit button and type the key name into the text box next to the tool and select the key from the list.

Click “Save” and a job will be created. Once approved, the configured tool will be enabled on the agent.

SU Data Access

When applying policy access controls, the default setting is to deny SU data access. There may be a scenario where SU data access is allowed. If so, there is a check box on the Agent Info page that allows setting to be modified.

Toggling the check box will create a job. Once approved, the SU data access setting will change accordingly.

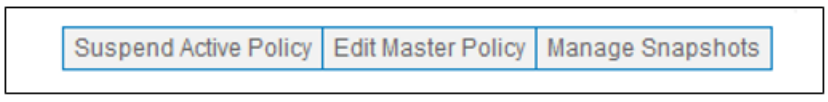
The following table shows the SU Data Access Controls:

Agent Type	Operating System	SU Data Access Default	SU Data Access Configurable
Volume	CentOS6/RedHat6	N/A	N/A
Volume	CentOS7/RedHat7	N/A	N/A
Volume	Windows	N/A	N/A
Volume with Policy	CentOS6/RedHat6	Blocked	Yes
Volume with Policy	CentOS7/RedHat7	Blocked	Yes
Volume with Policy	Windows	N/A	N/A
File with Policy	CentOS6/RedHat6	Blocked	Yes
File with Policy	CentOS7/RedHat7	Blocked	Yes
File with Policy	AIX	Blocked	Yes
File with Policy	Windows	N/A	N/A
Object Store	CentOS7/RedHat7	N/A	N/A

Policy Suspend

The Volume with Policy and File with Policy Agents support the ability to suspend a defined active policy. When a policy is suspended all actions against the protected directories will be denied. Suspending an active policy can be done without changing the active snapshot definition.

To suspend policy, click the “Suspend Active Policy” button in the right-hand corner of the Agent Info policy section and it will create a job.



Once the job is approved, the policy will be immediately suspended and the button will toggle and display “Reenable Active Policy”.

To reenable the suspended policy, click the “Reenable Active Policy” button and a job is created. After approving the job, the last active snapshot policy will be immediately in effect.

Policy Changes

Policy changes can be made by either modifying a policy applied to a protected path, adding a new protected path, or adding an encrypted volume.

Changes to policy do not modify the encryption status of current data. They will only impact the handling of data created after the policy is redeployed.

Critical Note

> Do not delete a volume policy from an active agent. Doing so is unsupported and could put the target system in an inconstant state.
>
> You can create a new volume on an active agent and leave the old volume as unused.
>
> Alternately, you can create and deploy a new agent.

Edit Policy

Editing an agent's policy allows the modification of File Policy Path, Path Set and Datatype association, or encrypted volumes.

If the Datatype is changed to one that can be edited, inline editing of those fields will be available. To edit the policy, click the "Edit Master Policy" button.

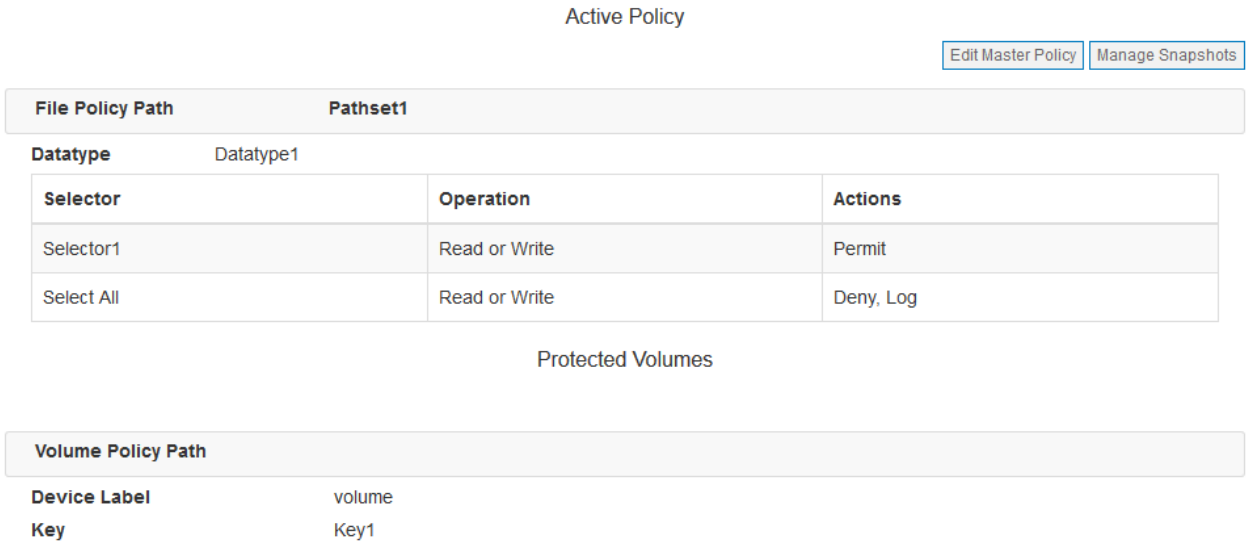
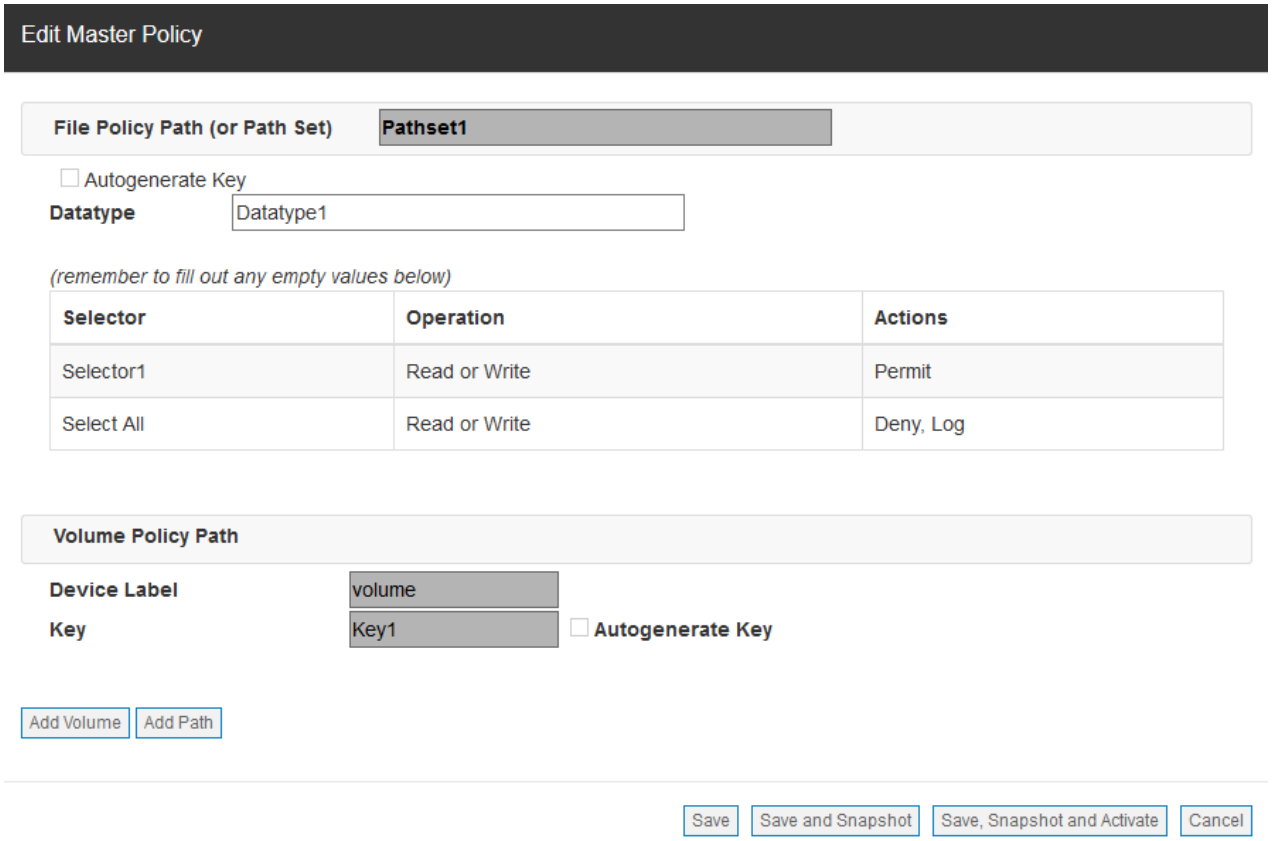


Figure 1. Volume with Policy Agent Example

This will launch Edit Master Policy page.



Note

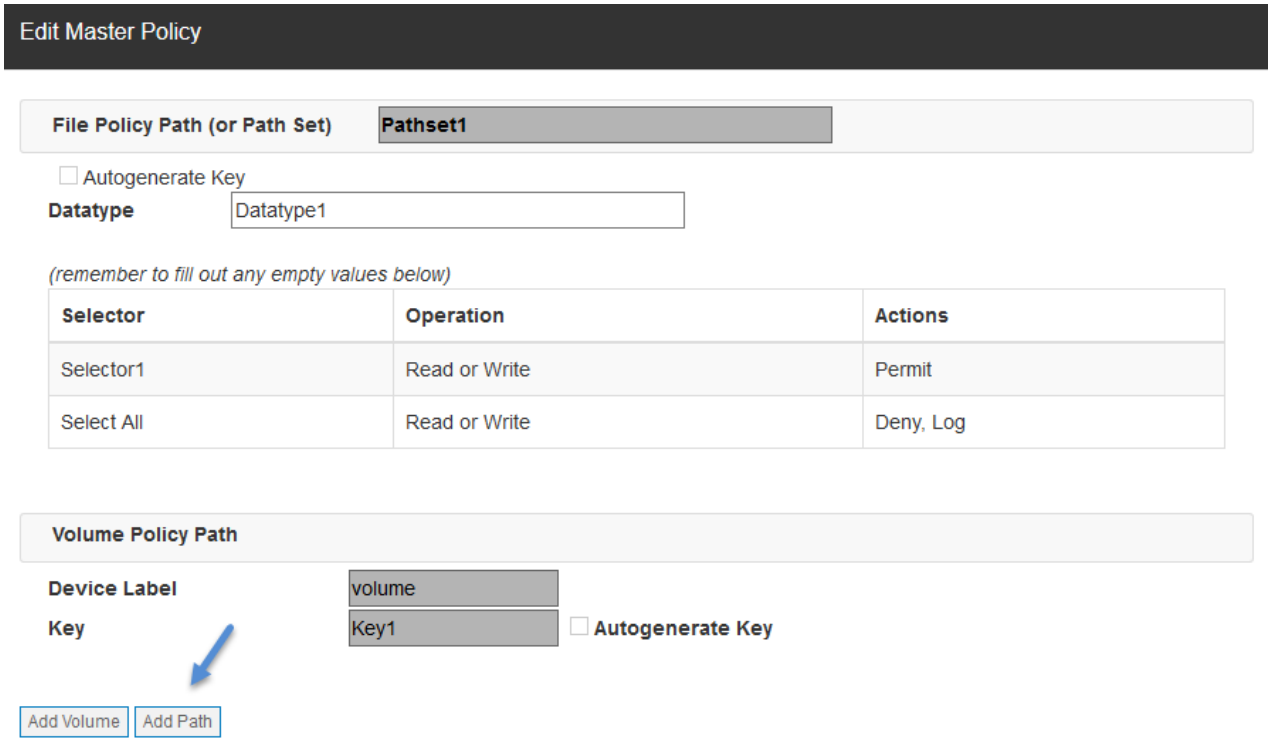
Editing the Master Policy does not modify any snapshots.

•

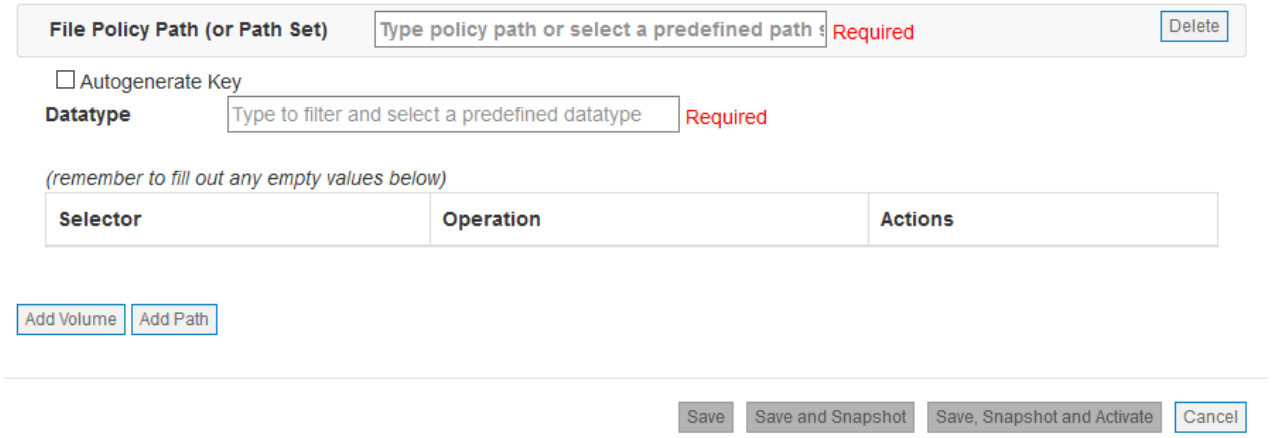
Add Path

About this task

To add a new path to place under policy, click the “Add Path” button.



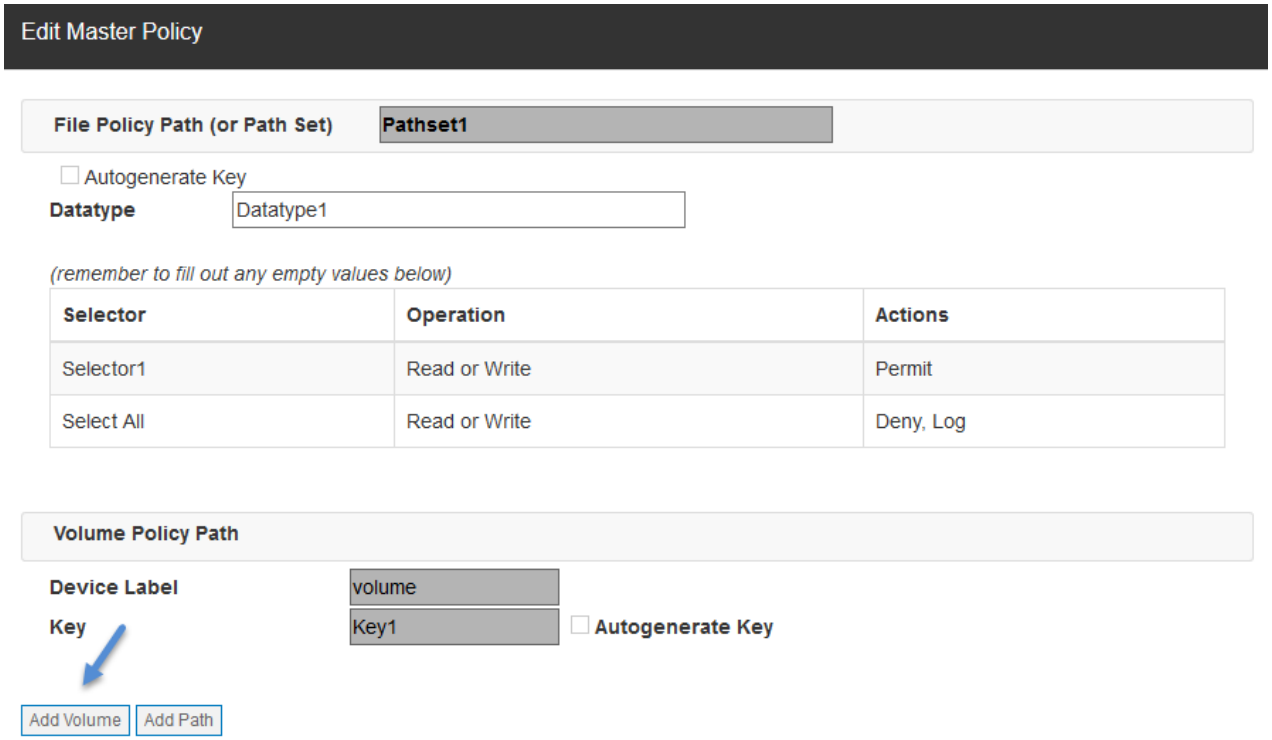
This will open a new section for input of policy (similar to original provisioning).



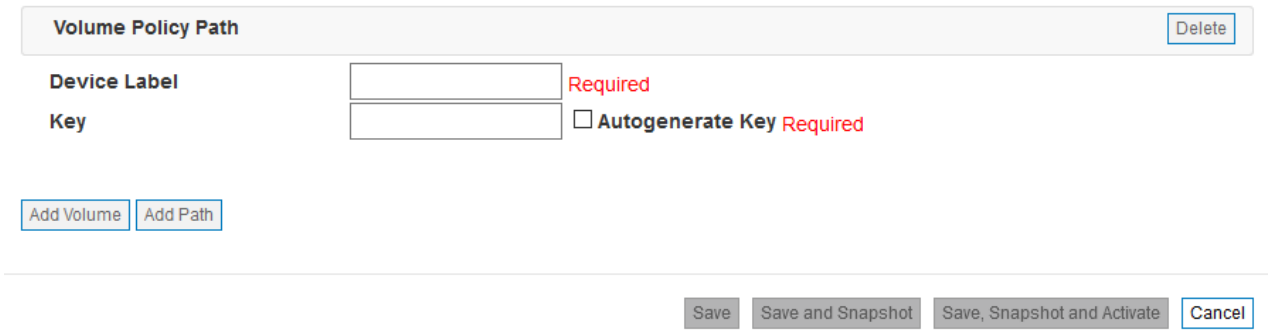
Add Volume

About this task

To add a new volume to encrypt, click the “Add Volume” button.



This will open a new section for input (similar to original provisioning).

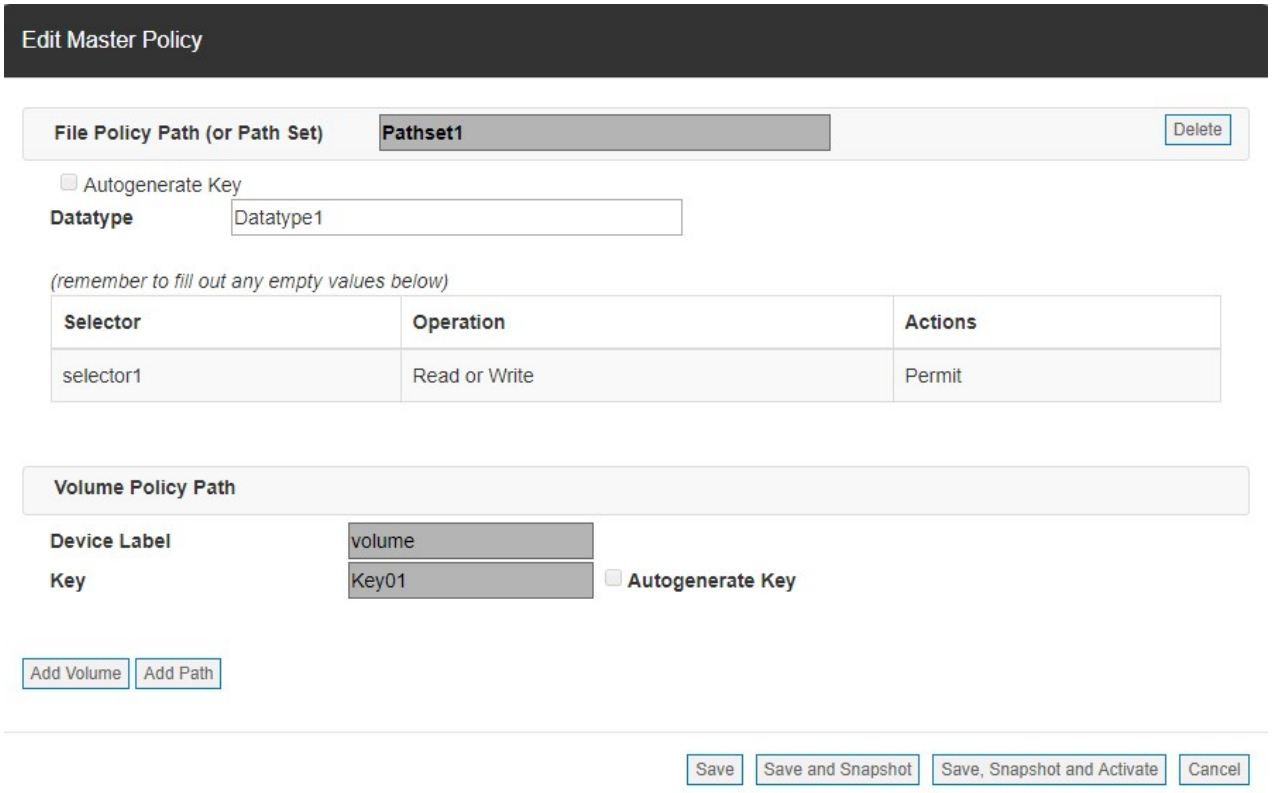


Delete Path

About this task

To delete a path from policy protection, click the “Delete” button for the intended path. Once the policy configuration has been saved, snapshot, and activated that path will no longer be protected by access control policy. New files written into the directory will no longer be encrypted. Existing file will remain in encrypted state and will not be accessible.

Note: To ensure uninterrupted access to the data, copy/move the data out of the protected directory path prior to deleting the path from policy.



Agent Snapshots

Agent snapshots are the permanent storage of agent associated policy configurations. Snapshots are indexed and have a state of Active or Inactive. There is only one active snapshot per agent. This is the policy configuration currently applied to the agent. To modify the agent policy configuration, the administrator must create a new snapshot that reflects the desired changes and activate the new snapshot.

Saving Agent Edits and Snapshots

When completing the editing of Agent policy, you can either Cancel the changes, Save the changes, Save and Snapshot the changes, or Save and Snapshot and Activate the changes.

Cancel Changes

Canceling the changes will revert to the policy configuration that was in place prior to modifying.

Save Changes

Saving the changes will store them for future use, but does not create a snapshot and therefore the changes cannot be applied to the agent.

Save and Snapshot

Saving and snapshotting the changes will store them for future use and creates a snapshot that can be viewed and activated at a later time.

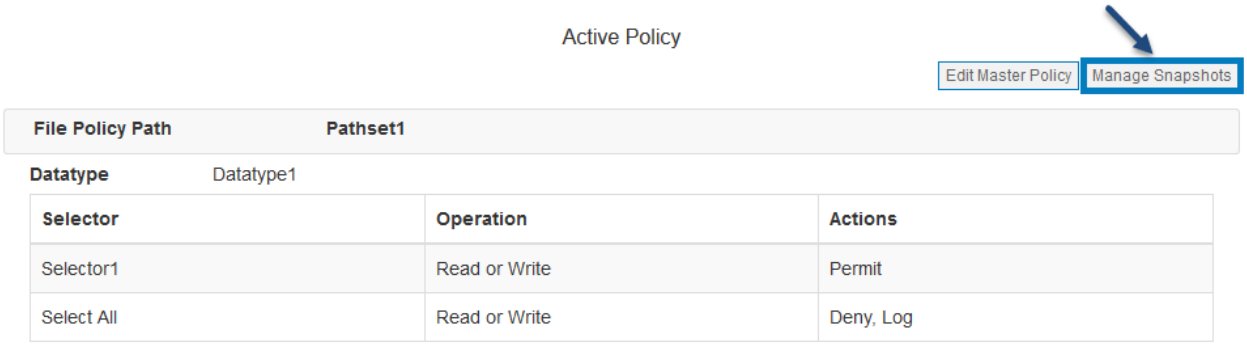
Save, Snapshot and Activate

Saving, snapshotting and activating the changes will store them for future use and creates a snapshot that can be viewed and immediately creates a job to apply these changes to the agent.

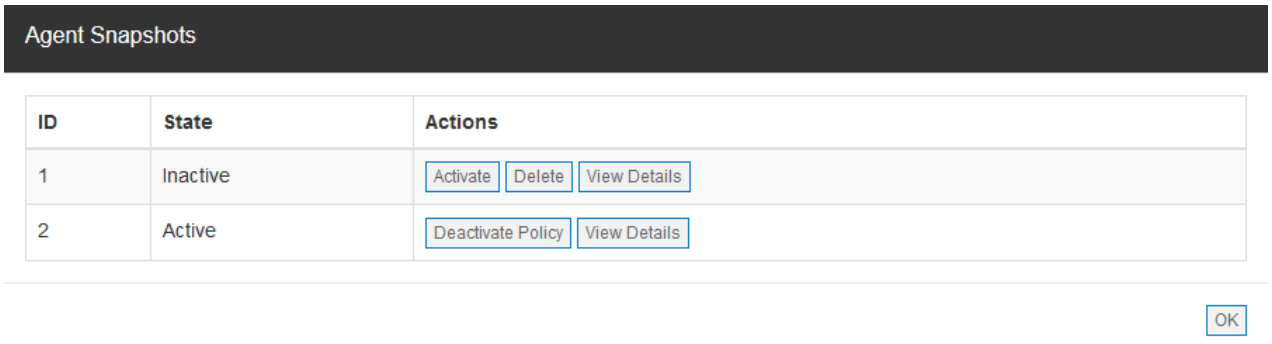
Note: Any snapshot changes or updates will not take effect until the agent is able to communicate to the PPM Server. The created job will remain running until successful communication between PPM and Agent or the Agent is removed from the PPM Server.

Managing Snapshots

All snapshots associated with an agent can be viewed via the “Manage Snapshots” button on the Agent Info view.



Clicking the button will bring up a snapshot management dialogue. From here, a Security Administrator can view snapshot details, activate a snapshot, deactivate policy associated with a snapshot, and delete a snapshot.

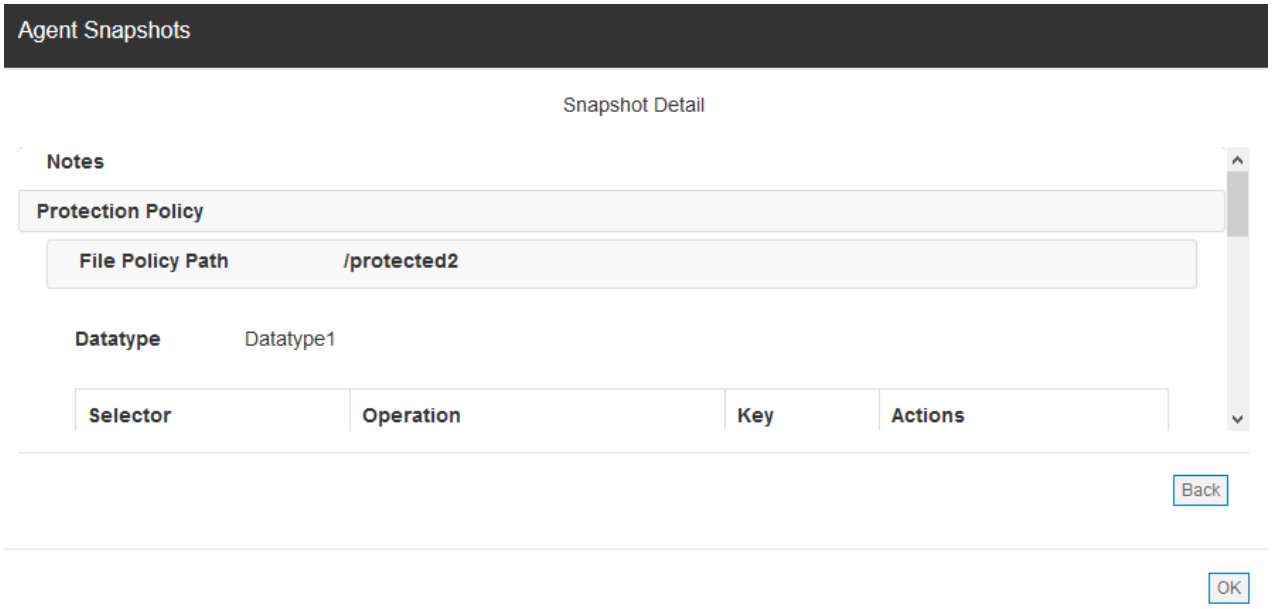


Note

Changing the active snapshot does not modify the Master Policy.

View Details

This button brings up a summary view of the policy associated with the snapshot.



Activate Snapshot

Activating a snapshot creates a job to send the policy to the agent. Once approved, the snapshot will transition into the active state and its policy will overwrite any policy present on the agent.

Note: Any snapshot changes or updates will not take effect until the agent is able to communicate to the PPM Server. The created job will remain running until successful communication between PPM and Agent or the Agent is removed from the PPM Server.

Delete Snapshot

An inactive snapshot can be deleted. Deleting a snapshot will permanently remove it from MDE.

Uninstalling a File Agent

About this task

If it is desired to remove a File Agent, this can be achieved via the following steps:

Copy data out of protected directories. This will ensure data is not inaccessible after policy is deactivated.

Perform the following steps to remove the agent software:

Procedure

1. Linux – run as root
   a) Stop the spx-policyagent service
      - Using CentOS 7 run

        ```
        systemctl stop spx-policyagent
        ```

      - Using CentOS 6 run

        ```
        service spx-policyagent stop
        ```

   b) Run `cd /opt/ibm/mde/spxagent/spx-fileagent/`.
   c) Run `./fileagent_uninstall.sh`.
   d) Type y to acknowledge the destructive action.

e) Reboot.

2. AIX - run as root

a) Stop the spx-policyagent service.

```
stopsrc -s spx-policyagent
```

b) Stop the kernel modules.

```
/opt/ibm/mde/spxagent/spx-fileagent/module/spx_kctrl_stop
```

c) Remove RPM.

```
rpm -e fileagent*
```

Note: If you want exact rpm name instead of a wildcard run, use

```
rpm -qa | grep fileagent
```

d) Reboot.

3. Windows – run as Administrator

- Via Windows GUI
  - Navigate to Add/Remove Programs in the Control Panel
  - Select “FileAgent” for uninstall
  - Reboot system when prompted
- Via PowerShell CLI
  - msiexec /x <path to FileAgent.msi>
  - Reboot system when prompted

Important: Authorized user(s) should not use the mv (move) command to move data to/from the encrypted location as this may create issues with MDE policy.

Back up data first using the cp (copy) command to/from protected (encrypted) directories.

Uninstalling Volume Agents

Uninstalling a Volume Agent

- Linux – run as root.

1. Unmount protected volume

```
umount /dev/mapper/<e_volume>
```

2. Stop the spx-policyagent service
   - Using CentOS 7 run

```
systemctl stop spx-policyagent
```

   - Using CentOS 6 run

```
service spx-policyagent stop
```

3. Run `cd /opt/ibm/mde/spxagent/spx-volumeagent/`.
4. Run `./volumeagent_uninstall.sh`.
5. Type y to acknowledge the destructive action.
6. Reboot

- Windows – run as administrator
  - Via Windows GUI
    - Navigate to Add/Remove Programs in the Control Panel
    - Select “VolumeAgent” for uninstall
    - Reboot system when prompted
  - Via PowerShell CLI
    - msiexec/x <path to VolumeAgent.msi>
    - Reboot system when prompted

Uninstalling a Volume with Policy Agent

About this task

Procedure

1. Linux – run as root
   a) Unmount protected directory

   ```
   umount /dev/mapper/<e_volume>
   ```

   b) Stop the spx-policyagent service
   - Using CentOS 7 run

     ```
     systemctl stop spx-policyagent
     ```

   - Using CentOS 6 run

     ```
     service spx-policyagent stop
     ```

   c) Run `cd /opt/ibm/mde/spxagent/spx-hybridagent/`.
   d) Run `./hybridagent_uninstall.sh`.
   e) Type y to acknowledge the destructive action.
   f) Reboot.
2. Windows – run as administator
   - Via Windows GUI
     - Navigate to Add/Remove Programs in the Control Panel.
     - Select “HybridAgent” for uninstall.
     - Reboot system when prompted.
   - Via PowerShell CLI
     - Run `msiexec /x <path to HybridAgent/msi>`.
     - Reboot system when prompted.

Uninstalling Object Store Agent

About this task

All user accounts and permissions will remain stored in the PPM until the agent is deleted from PPM.

Procedure

1. Linux – run as root
2. Stop the spx-policyagent service

```
systemctl stop spx
```

3. **cd** `/opt/ibm/mde/spxagent/spx-objectagent`

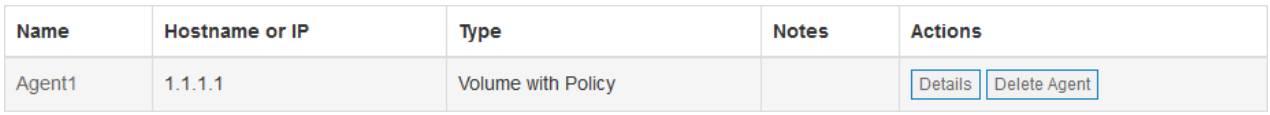
```
./objectagent_uninstall.sh
```

4. Type y to acknowledge the destructive action
5. Reboot.

Removing an Agent from MDE

An agent managed by MDE can be removed from the ecosystem using the MDE user interface (GUI).

To remove an agent, click the “Delete Agent” button and a job will be created. Once the job has been approved the agent will be removed from MDE.



Name	Hostname or IP	Type	Notes	Actions
Agent1	1.1.1.1	Volume with Policy		Details Delete Agent

Critical Note

- Removing an agent from MDE will prevent the agent from being able to connect to MDE resulting in the currently protected data becoming inaccessible on the next agent restart.
- Removing an agent does not decrypt the data.

Agent utilities

MDE agents provide multiple utilities to aid in the configuration of an agent and the protection of sensitive information. For more details on each, run the utility with the “--help” option.

Utility	Function	Volume	Volume with Policy	File with Policy	Object Store
spxbackup	Creates an encrypted backup of the identified data.	Yes	Yes	Yes	No
spxconvert	Converts preexisting data in a protected directory from unencrypted to encrypted based on the defined policy.	No	No	Yes	No
spxdevice	Maps a disk volume/ partition to a defined device name.	Yes	Yes	No	No

spxhash	Generates a version-specific hash of an indicated process.	No	Yes	Yes	No
spximport	Imports encrypted data into a directory without double-encrypting the data.	No	No	Yes (Windows only)	No
spxinfo	Lists directories protected via defined policy	No	Yes	Yes	No
spxobject	Lists object store	No	No	No	Yes
spxrestore	Restores an encrypted backup of identified data.	Yes	Yes	Yes	No

Chapter 12. Operations

Product Data Backup and Restore

MDE supports the ability to do a point-in-time backup of MDE PPM data. This point-in-time backup can be restored to return MDE to the state at time of backup collection.

Note: Before performing a backup or restore, please stop the MDE service via the “systemctl stop spsd” command in the MDE VM.

```
sudo systemctl stop spsd
```

Product Data Backup

About this task

Product backups are done via a command line script run within the MDE VM.

The backup script spsd-backup is located in the MDE VM in the `/opt/securityfirst/spsd/bin` directory. It will automatically create a new file and name it with a timestamp of when this backup was made.

```
sudo /opt/securityfirst/spsd/bin/spsd-backup --help
Usage: spsd-backup [--nodb] [--help]
---------------------------------
    --nodb      Don't backup the database
    --help      Show this help
```

To run a backup:

```
sudo /opt/securityfirst/spsd/bin/spsd-backup
Dumping local buildinfo
Dumping local spsd properties
Dumping local PostgreSQL database a
Done - created spsd-backup-2017-04-04T144448-0700.tar.gz
```

Product Data Restore

About this task

Product restore is done via a command line script run within the MDE VM.

The restore script spsd-restore is located in the `/opt/securityfirst/spsd/bin` directory.

```
sudo /opt/securityfirst/spsd/bin/spsd-restore --help
Usage: spsd-restore [--nodb] [--noprops] [--help] FILE
---------------------------------
    --nodb      Don't write the database
    --noprops   Don't write local properties
    --help      Show this help
```

To run a restore:

```
sudo /opt/securityfirst/spsd/bin/spsd-restore
spsd-backup-2017-04-04T144448-0700.tar.gz
```

Note: After restoring a backup file, the next start of MDE will apply the changes.

Kernel Update

About this task

When a kernel update is required on an Agent running a Red Hat Enterprise Linux 7 or CentOS 7 Operating System, please use the following guidelines:

- If the OS / kernel update is within the same release, the new kernel is automatically supported.
- If the OS / kernel upgrade is to a higher release (i.e. RHEL 7.2 -> 7.4), then run the following steps to build support for new kernel:
  - Example: agent installation bundle was untarred to /root/agent

```
cd /root/agent/spx-installer
./agent_setup.sh -d /root/agent
Reboot
```

These steps are not required for Agents running on Red Hat Enterprise Linux 6 or CentOS 6.

Upgrade

Follow these steps to upgrade MDE product to a new version.

Note: These steps apply to the MDE Open Virtualization Appliance. If a non-OVA install was performed the directories might change.

For the MDE Server

About this task

Procedure

1. As root, stop the PPM policy service.

```
systemctl stop spsd
```

2. Backup the MDE data:

```
/opt/securityfirst/spsd/bin/spsd-backup
```

3. Move the new version MDE bin file to the `/home/admin` directory.
4. Delete existing rpms directory.

```
rm -fr /home/admin/rpms
```

5. Change the access permission to the MDE bin file.

```
chmod +x /home/admin/ibm_sw_mde_X.x.x-XX.bin
```

6. Run the MDE bin file of the new version.

```
/home/admin/ibm_sw_mde_X.x.x-XX.bin
```

7. Install the RPMs.

```
yum -y install /home/admin/rpms/*
```

8. Run the Upgrade script.

```
/opt/securityfirst/spsd/bin/spsd-pgsetup --upgrade
```

9. Start the PPM policy service back up again:

```
systemctl start spsd
```

Upgrading from previous version

About this task

These steps must be performed to allow policy to operate!

Procedure

1. Navigate to Agent Info page
2. Click on “Edit Master Policy”
3. Click on “Save, Snapshot, and Activate”
4. Approve the job
5. Go back to Agent VM and attempt to perform a read/write action on a directory in policy, logged in as a user in policy that has rights to that directory, and verify that non-defined user are not allowed.

For the Agent Target VM

Linux/AIX Agents

About this task

Procedure

1. Create a new agent directory and change to new Agent directory

```
mkdir [agent_new_directory]
cd [agent_new_directory]
```

2. Download or curl down the respective Agent’’s install bundle

```
curl --header "Accept: application/x-tar" -u
username:password
https://<PPM IP address/rest/agents/Agent ID #/install_bundle> install_bundle_name.tar
```

3. Untar the install bundle

```
tar xvf <install_bundle_name>.tar
```

4. Run the setup.sh scripts to reinstall the Agent

```
./setup.sh
```

5. Answer yes to reboot the Agent when prompted.
6. You can delete all the previous installer files from previous Agent directory, if desired.

```
rm -rf [/previous Agent directory]
```

Windows Agents

About this task

Procedure

1. Download the respective Agent’s install bundle
2. Un-zip the install bundle

3. Run the .msi installer to install the new Agent software
4. Answer yes to reboot the Agent when prompted

Service Data

Collecting service data

Service Data Collection is done via a script run within the MDE VM.

The spsd-service script is located in the MDE VM in the /opt/securityfirst/spsd/bin directory.

```
sudo /opt/securityfirst/spsd/bin/spsd-service --help
Usage: spsd-service [OPTIONS]
---------------------------------
    OPTIONS:
    --nodb      Don't dump the database
    --norest    Don't pull any data from the REST API
    --nosys     Don't pull system data (/var/log, /proc, and so on)
    --withcore  Pull in a core dump of spsd
    --help      Show this help
```

To run a service data collection:

```
sudo /opt/securityfirst/spsd/bin/spsd-service
```

Removing sensitive information from PPM logs

To help protect the privacy of a PPM installation when service data leaves the PPM logical boundary, the following MDE debug logs have sensitive information tagged using a specialized tag syntax:

- bundleAll.log
- bundleWarnPlus.log
- debug.log
- warn.log

Note: Inside a service data tarball (the result of the above service data collection process), these logs may be found in the logs folder.

The tags are formatted as #<tagname>(<tagdata>) where <tagdata> is replaced with the data to be tagged and <tagname> is one of the following:

- user - to tag usernames, whether they are MDE users or users of an external service that MDE integrates with. *Example: #user(admin)*
- group - to tag group names. *Example: #group(domainusers)*
- email - to tag email addresses. *Example: #email(example@example.com)*
- ip - to tag IP addresses. *Example: #ip(192.168.0.5)*
- host - to tag network hostnames. *Example: #host(dns.example.com)*
- key - to tag **public** cryptographic keys or a related value such as a managed key name. *Example: #key(HRKey2)*
- cert - to tag certificate data such as a distinguished name of a connecting agent. *Example: #cert(C=US, ST=UT, L=Provo, O=Example Corp., OU=architecture, CN=docserver4*
- fingerprint - to tag certificate fingerprints. *Example: #fingerprint(41:1A:B9:89:DB:77:90:77:39:D0:DF:5E:98:90:B7:17*

Tags can be removed from service data using a process such as in this example that removes #user tagged data from the bundleAll.log:

```
gunzip spsd-service-2018-01-24T141620-0800.tar.gz
tar xf spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
sed -i '/\#user/c\REDACTED' logs/bundleAll.log
tar --delete --file=spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
tar --append --file=spsd-service-2018-01-24T141620-0800.tar ./logs/bundleAll.log
gzip spsd-service-2018-01-24T141620-0800.tar
```

Appendix A. Sample Agent Installation Processes

The following sections outline the general process for installation of the agent install bundle. These are only example methods and are not supported installation instructions.

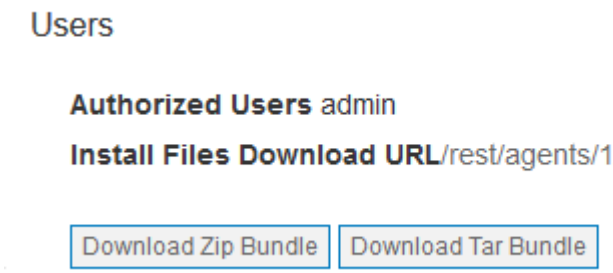
Red Hat / CentOS Process

About this task

Transferring install bundle via CURL:

Procedure

1. Login to the target system
2. Ensure a valid network connection with the MDE server
3. Ensure that all users, groups and paths or devices that are identified in policy are created, attached, and configured to the system
4. Login to MDE
5. Within MDE, provision an agent for the target system
6. Within MDE, view the agent details and note the Download URL



7. From the target system, create a directory for Agent download and change to that directory
8. Download the tar bundle using the following curl command:

   [user@localhost]$ curl -k --header “Accept: application/x-tar” -u admin:admin https://<PPM IP>/<Download URL> > package.tar

   Example using PPM defined user:

   [user@localhost]$ curl -k --header “Accept: application/x-tar” -u admin:admin-password https://1.1.1.10/rest/agents/1/install_bundle > package.tar

   Example using PPM LDAP defined user:

   [user@localhost]$ curl -k --header "X-Directory: tenant1" --header “Accept: application/x-tar” -u john:secret https://1.1.1.10/rest/agents/1/install_bundle > package.tar

   (assuming directory identifier "tenant1", with user "john" and password "secret")
9. From the target system, untar the package:

   [user@localhost]$ tar -xf package.tar
10. From the target system, run the setup script as root

    [user@localhost]$ ./setup.sh

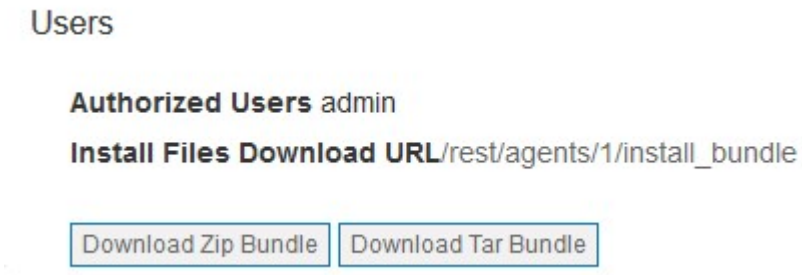
11. Once the setup script has completed the agent is installed and policy will be downloaded from MDE and will be in effect.

AIX Process

About this task

Transferring install bundle:

1. Login to the target system
2. Ensure a valid network connection with the MDE server
3. Ensure that all users, groups and paths or devices that are identified in policy are created, attached, and configured to the system
4. Login to MDE
5. Within MDE, provision an agent for the target system
6. Within MDE, view the agent details and note the Download URL



7. From the target system, create a directory for Agent download and change to that directory
8. Transfer the bundle to the target system.
9. From the target system, untar the package:

```
[user@localhost]$ tar -xf package.tar
```

10. From the target system, run the setup script as root.

```
[user@localhost]$ ./setup.sh
```

11. Once the setup script has completed the agent is installed and policy will be downloaded from MDE and will be in effect.

Windows Server Process

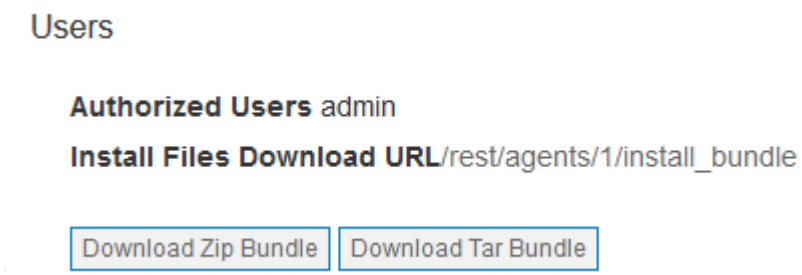
About this task

Transferring install bundle:

Procedure

1. Login to the target system
2. Ensure a valid network connection with the MDE server
3. Ensure all users, groups and paths or devices identified in policy are created, attached and configured to the system
4. Login to MDE

5. Within MDE, provision an agent for the target system
6. Within MDE, view the agent details and note the Download URL



7. Click “Download Zip Bundle” to download the zip file bundle for the agent software to the local system
8. Transfer the install bundle to the target system
9. On the target system, extract the contents of the zip file bundle
10. Execute the msi file of the install bundle

    FileAgent-<version>.msi

    Example:

    PS C:\> FileAgent-4.2.11-0030.msi
11. Once the setup script has completed and the agent is installed properly, policy will be in effect.

    Note: A reboot is required. To bypass the requested reboot prompt, you can run the command with the no reboot option: **msiexec /i <agent_filename_version.msi> NO_REBOOT_PROMPT=1**

Appendix B. Sample Certificate Authority (CA) Certificates

About this task

MDE requires certificates that are signed by a Certificate Authority to establish a secure session between the Management Server (PPM) and Agents. It will require:

- keystore
- truststore
- CA certificate bundle

An internal company RSA based Certificate Authority or 3rd party Certificate Authority can be used to sign certificates. In the below Linux example, the following items are created:

- Certificate Signing Request (CSR) is created and sent to Certificate Authority to be signed. The signed certificate and key are combined to create a keystore.
- A truststore is created using the Certificate Authority's certificate bundle.
- An agent certificate is created. These certificates are required for communication between PPM and Agents.

This example is provided for your convenience, you should adhere to your Certificate Authority when generating certificates to be signed. Names within brackets [name.pem] represent file names that may be different or changed when using company or 3rd party certificates.

To create a keystore, you will need to submit a CSR to internal company Certificate Authority or a 3rd Party Certificate Authority.

Procedure

1. Create an OpenSSL configuration file (i.e. ppm.cnf) that contains the following information:

```
[req]
default_bits          = 4096
distinguished_name     = req_distinguished_name
req_extensions         = v3_req
prompt           =   no

[req_distinguished_name]
C   =  your_country
ST  =  your_state_or_province
L   =  your_locale_(city)
O   =  your_organization
OU  =  your_org_unit_(department)
CN  =  your_ppm_host.your_domain

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints    = CA:FALSE
extendedKeyUsage    = serverAuth
subjectAltName      = @alt_names

[alt_names]
DNS.1   =   your_ppm_host.your_domain
IP.1    =   your_ppm_ip_address
```

   You need to update the [req_distinquishd_name] and [alt_names] sections to reflect your organization's information.

2. Create a PPM CSR

```
openssl req -out [csr.pem] -new -newkey rsa:2048 -keyout [key.pem] -outform pem
```

3. CSR [csr.pem] must be signed by Certificate Authority (CA)
4. After receiving signed certificate from CA, verify the extended key usage and subject alternative names are present

```
openssl x509 -in [signed cert] -noout -text
```

5. Combine signed certificate and key (key from step 2)

```
a.    openssl pkcs12 -export -out [ppm.p12] -inkey [key.pem] -in [signed-cert] -name ppm
b.    keytool -importkeystore -srckeystore [ppm.p12] -keystore [ppm.jks]        -storetype
JKS
```

To create a truststore, you will need the Certificate Authority's certificate that it uses to sign CSRs. This is also referred to as the CA Certificate bundle. Replace "ca_bundle.crt" below with the actual name of this certificate.

a. Create truststore using Certificate Authority (CA) certificate bundle. If there are multiple certificates in the CA certificate bundle, they must be separated and imported into a truststore individually.

```
a.    keytool -import -trustcacerts -file [ca_bundle-1.crt] -alias CA1 -keystore
[trust.jks]
b.    keytool -import -trustcacerts -file [ca_buncle-2.crt] -alias CA2 -keystore
[trust.jks]
c.    continue for each certificate in bundle
```

b. Copy the resulting *.jks and [ca_bundle.crt] files to the PPM server in a secure directory (i.e. /etc/ppm/certs). This location will be specified when you update the web and agent properties files using the spsd-certsetup script. (see Management Server Setup below)

An MDE Agent Certificate is also required.

a. Create an OpenSSL configuration file (i.e. host01.cnf) that contains the following information:

```
[req]
default_bits       = 2048
distinguished_name = req_distinguished_name
req_extensions     = v3_req
prompt = no

[req_distinguished_name]
C  = your_country
ST = your_state_or_province
L  = your_locale_(city)
O  = your_organization
OU = your_org_unit_(department)
CN = your_agent_host.your_domain

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
extendedKeyUsage = clientAuth
subjectAltName   = @alt_names

[alt_names]
DNS.1 = your_agent_host.your_domain
IP.1  = your_agent_ip_address
```

You need to update the [reg_distinguished_names] and [alt_names] sections to reflect your organization's information.

b. Create an MDE Agent CSR

```
a. openssl req -out [host01.csr] -nodes -sha256 -newkey rsa:2048 -keyout
[host01.key] -config [host01.cnf]
```

c. Request CSR signed by Certificate Authority (CA)

d. After receiving signed certificate from CA, verify the extended key usage and subject alternative names are present

```
a. openssl x509 -in [signed-agent] -noout -text
```

e. If the agent certificate was signed by a different CA than the PPM certificate, then the CA_bundle certificate must be imported into the PPM truststore. Please refer to step 5 in the PPM certificate creation process (CSR) above

f. Combine signed certificate and key

```
a. cat [signed-agent] [host01.key] > [host01.pem]
```

g. Use the [host01.pem] cert / key pair when creating an agent for this host in MDE

```
a. [host01.pem] is uploaded using a browser during the PPM agent creation.
```

Copy the [host01.pem] to your workstation or a shared resource so it is accessible during the PPM agent creation.

Follow this process for each host that an agent will be installed on.

Management Server Setup

The Management Server Setup must have the certificates updated prior to configuring any Policy Agents. This will require executing the provided script (/opt/securityfirst/spsd/bin/spsd-certsetup) on the Server (See Administrator Guide for Server Certificate Settings section) after uploading your company's keystore and truststore, and a CA certificate bundle. It will also require a restart of the spsd service or reboot of the Management Server (PPM). Failure to do so will result in agents being unable to communicate to the MDE Management Server.

If certificates have not been updated and an agent has been configured, running the certificate update script and then updating the agent certificate on the Agent Info page will restore communication between the agent and the MDE Management server.

Appendix C. Sample Conversion to Create a PKCS12 File

About this task

Use the following steps to combine the client private key and client certificate into a single PKCS12 (Public Key Cryptography Standard #12) file:

[user@localhost]$ openssl pkcs12 -export -out ppmclient.p12 -inkey client_key.pem -in client_cert.pem -name ppmclient

[user@localhost]$ keytool -v -list -keystore ppmclient.p12 -storetype pkcs12

Appendix D. Do's and Don'ts

Changing Assigned Keys

Overview

I have data within a protected directory and I want to modify the key associated with that directory.

Background

Data within a directory is encrypted with the key defined at time of data creation (or movement into that directory). Changing a policy key does not migrate the pre-existing data to the new key.

When a policy has been applied to an agent and is active, it is potentially very dangerous to modify the key values of the protected directories. While not strictly forbidden, modifying a key value can lead to loss of data.

Do

If the administrator wishes to migrate an entire directory from one key to another key, the data would first have to be moved out of that directory. Once the directory is empty, the key value associated via policy can be changed and applied. Then the data can be moved back into that directory and the data will be encrypted with the new key.

Don't

Don't modify the key value associated to the policy and activate the policy without first migrating the data out of the directory. If the best practice methodology is not followed than the data originally present in the directory will continue to be encrypted with the original key. Once modifying policy to a new key, the data will become inaccessible. Furthermore, if the original key is rotated, the data will be permanently inaccessible as there would be no way to modify policy back to the original key value.

Rotating Keys with Encrypted Backups

Overview

I want to backup data from a protected directory.

Background

Backup up data in its encrypted format ties that data to the key value at time of backup. If the key is rotated after the backup operation is performed, it cannot be properly restored.

Keys should be associated with a protected location, not data. This will prevent unintentional data access problems on a restore.

Do

Data within a directory is encrypted with the key defined at time of data creation (or movement into that directory). It is a best practice to backup the data prior to rotating the key. The agent utility "spx-backup" can be used to perform this operation. This will backup the data with a key that is not based on the protected directory and not impacted by key rotation.

Don't

Use caution when copying the protected directory in its encrypted form (e.g. a disk image or VM snapshot). If this is done, the data could become inaccessible once the original key is rotated.

Appendix E. Encryption in Place

In order to allow encryption on pre-existing directory structures and data and to determine the status of data at any time, MDE provides a command line utility called “spxconvert”.

This feature is not only capable of encrypting pre-existing data but is also useful when going through an audit such as Payment Card Industry (PCI) or Health Insurance Portability and Accountability Act (HIPAA).

Note: This feature will only work with File Agents and does not cover volumes which will require a formal data migration.

Command Options

spxconvert usage: (params are indicated with the square [ ] brackets and include type)

-h (-?, ?) 'Print this help dialog'

-a 'Perform encrypted file audit'

-p [STR] 'Audit path'

-e [STR] 'Encrypt any unprotected files in path'

-c 'Dump all checksums of pre/post file conversion'

-v 'Verbose - extra print for added information'

Audit (-a)

By default, the audit is performed for all in policy directories. This can be narrowed to a single directory by using the -p option. An audit will print any files for a directory that are not encrypted, and print a file count for the total number of files within a directory that are encrypted.

Encrypt (-e)

Convert any unprotected files in the specified directory. Upon completion, any files with mismatched checksums will be displayed to the user. The optional -c flag will print checksums for all files upon completion, not just any that conflict. Checksums can only be printed upon completion for performance as the system cache must be flushed after the convert. Flushing the caches after each file would be a huge negative impact on performance.

Audit Steps

1. Show if there are any items pending encryption:

spxinfo -l

1. Show detailed information on data:

spxconvert -a -v

1. Show detailed information on a specific directory:

spxconvert -p -v <*path*>

Encrypt Steps

1. Show items that are pending encryption:

spxinfo -l

1. Show all checksums before encryption:

spxconvert -c -p <*path*>

1. Encrypt any files in a specific path:

spxconvert -p -v <*path*>

1. Show all checksums on a specific path after encryption:

spxconvert -c -p <*path*>

Appendix F. Agent Debug Logging

By default, Policy Agents operate with debug-level messages omitted from logging. To capture debug-level messages in the agent's log, the system administrator of the agent must enable the feature and then restart the agent for the debug-level messages to begin being captured.

Valid values are 1-6; however, the default value is '4' and setting any value less than '4' may omit any useful information.

Critical Note

- Enabling debug-level logging may disclose sensitive system information
- Due to the nature of debug messaging, agent log files may drastically increase in file size.

Linux Agents

About this task

Enable debugging by locating the configuration file located at **/etc/sysconfig/spx-policyagent** and set the writable flag (**chmod +w /etc/sysconfig/spx-policyagent**).

Append to the bottom of the file, "**LOG_LEVEL=6**" without quotes.

AIX Agents

About this task

Windows Agents

About this task

Enable debugging by locating the registry key located at **HKLM\SYSTEM\CurrentControlSet\Services\Spx Policy Agent\log level** and set the value to '**6**'.

Appendix G. Non-OVA Deployment

These are example instructions on how to setup a non-OVA environment for PPM deployment. These instructions are only applicable if you are not deploying the supplied PPM OVA, but instead are creating your own RHEL or CentOS 7.x environment into which to deploy the PPM software.

Install these packages on all the PPM nodes.

Note: This is only one example setup. There are many environmentally specific needs that will cause these instructions to be invalid. Please contact support for additional assistance.

1. Install java 1.8 and postgresql 9.2.

   Note: You will be prompted for a password during the initdb process. This will be the postgres “superuser” password.

   ```
   yum install -y postgresql-server java-1.8.0-openjdk-headless
   passwd postgres
   su - postgres
   initdb --auth=md5 -W
   exit
   ```

2. Install firewall policies.

   The example below shows how to install the firewall policies using iptables. Other methods may work equally well and can be used according to your site preferences. Example: `yum install -y iptables iptables-services`

   The next two commands assume you have firewalld installed and enabled. If firewalld is not installed, running these commands will do no harm.

   ```
   systemctl stop firewalld
   systemctl disable firewalld
   ```

   Start and flush the IP Tables firewall service

   ```
   systemctl start iptables.service
   iptables -F
   ```

   Enable the iptables service - Optional step - you can skip If you don’t require a local software-based firewall

   ```
   systemctl enable iptables.service
   ```

   Define a base firewall - Optional step - you can skip If you don’t require a local software based-firewall

   ```
   iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --
   update --seconds 60 --hitcount 4 --name DEFAULT --rsource -j LOG --log-prefix
   "SSH BruteForce: "
   iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --
   update --seconds 60 --hitcount 4 --name DEFAULT --rsource -m recent --set --name
   ssh --rsource
   iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
   iptables -A INPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
   service iptables save
   ```

3. Install Keepalive, HAProxy and PSMisc packages.

   ```
   yum install -y haproxy keepalived psmisc
   ```

4. Download Zookeeper.

   Note: If wget is not installed, then please install it:

   ```
   yum install -y wget
   wget http://apache.claz.org/zookeeper/zookeeper-3.4.10/zookeeper-3.4.10.tar.gz
   ```

```
mkdir /home/admin
mv zookeeper-3.4.10.tar.gz /home/admin
```

5. Install and configure a reliable network time source.

   The example shows NTP configuration, but other reliable time sources may work equally well and can be used according to your site preferences.

```
yum install -y ntp
sed -i "/server\ [0-9].rhel/ s/rhel/us/" /etc/ntp.conf
sed -i "/server\ [0-9].centos/ s/centos/us/" /etc/ntp.conf
systemctl stop chronyd
systemctl disable chronyd
systemctl start ntpd
systemctl enable ntpd
```

6. Install the Extra Packages for Enterprise Linux (EPRL) repository

```
yum install -y epel-release
```

7. Install Unpredictable Random Number Generator (Requires EPEL).

```
yum install -y haveged
```

8. Install net-tools for service data collection.

```
yum install -y net-tools
```

Appendix H. Software Version Check

Check the following commands to check the software version.

PPM version

From the PPM VM Shell, execute the following command:

```
cat /etc/ppm/buildinfo/release
```

Linux agent version

From the Linux CLI, run the following command:

```
yum list policyagent
```

AIX agent version

From the AIX CLI, execute the following command:

```
rpm -qa | grep fileagent
```

Windows agent version

Navigate to **Add/remove programs** in Windows. Scroll to find the agent name.

Agent type	Agent name in Windows
File with Policy	FileAgent
Volume	VolumeAgent
Volume with Policy	HybridAgent

Appendix I. Glossary

Term	Definition
Advanced Encryption Standard New Instructions (AES-NI)	Specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001; encryption protocol used by SPx based products.
Agent	A managed server running Security First encryption and access control software.
Amazon Web Services (AWS) S3	A simple storage service that stores and retrieves data and is highly scalable and inexpensive object storage.
Auto-Generated Keys	Policy Enforcement Keys created and managed by MDE. These are indicated during policy creation by the Autogenerate Key.
Certificate Authority	An organization that is trusted to sign digital certificates. The CA verifies identity and legitimacy of the submitted certificate request. If verification of request is successful, CA issues signed certificates.
Certificate Revocation List (CRL)	Published list of certificates that have been revoked by the Certificate Authority (CA) that issued the corresponding certificates.
Certificate Revocation List Distribution Point (CRLDP)	A starting point field within certificate that holds information about the revoked certificate by the issuing CA that includes name, optionally reasons for revocation, and CRL issuer name.
Cloud Auditing Data Federation (CADF)	A common event format syntax type that is forwarded to a Security Information and Event Management (SIEM) system.
Comma Event Format (CEF)	A common event format syntax type that is forwarded to a Security Information and Event Management (SIEM) system.
Comma Separated Value (CSV)	A data format that uses comma as a field delimiter and a return as a record delimiter.
Command Line Interface (CLI)	Type of interaction where the user issues commands to the application in the form of text lines (command lines)
Coordinated Universal Time (UTC)	The primary time standard by which the world regulates clocks and time.
Cryptographic Access Controls	The ability to separate user access by leveraging different encryption material.
CURL	CURL is a computer software project providing a library and command-line tool for transferring data using various protocols.

Distinguished Encoding Rules (DER)	DER is one of ASN.1 encoding rules defined in ITU-T X.690, 2002, specification. An encoding rule to data structure provides a transfer syntax that governs how bytes in a stream are organized when sent between computers.
Domain Name (DN)	An internet resource name that is universally unique and linked to IP destination information
Domain Name Service (DNS)	An Internet Service that translates domain names into IP addresses.
Dynamic Host Configuration Protocol (DHCP)	A client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
File Agent	A file agent enforces file based operational access policy definitions and association of one or more protected file paths. Each protected file path can have its own operational and cryptographic access control.
Graphical User Interface (GUI)	A type of user interface that allows users to interact with MDE through graphical icons as opposed to text-based interfaces and typed commands
Health Insurance Portability and Accountability Act (HIPAA)	HIPAA Privacy regulation requires providers and organizations to ensure confidentiality and security of protected health information (PHI)
High Availability (HA)	System operations continue even if components fail because of redundancy (redundant power supplies, CPUs, drives, software, etc.)
Hypertext Transfer Protocol (HTTP)	An application protocol that is the foundation of data communications for the World Wide Web.
Hypervisor	Also, called Virtual Machine Monitor. A hypervisor or virtual machine monitor (VMM) is a piece of computer software, firmware or hardware that creates, runs and manages virtual machines. A computer on which a hypervisor runs one or more virtual machines is called a host machine; and each virtual machine is called a guest machine. The VMware Hypervisor is also called an ESXi Host.
IBM Cloud Object Storage (COS S3)	Storage platform that holds large amounts of data such as backups, archives, videos files, and image files providing data-at-rest and high availability.
Initialization Vector (IV)	An arbitrary or unpredictable random number that can be used along with a secret key for data encryption that is is employed only one time in any session.

Java KeyStore (JKS)	A Java KeyStore (JKS) is a repository of security certificates – either authorization certificates or public key certificates – plus corresponding private keys. The Java Development Kit (JDK) provides a tool (keytool) to manage keys and certificates in the keystore. jks extension is a Java-specific file format.
Key Revocation	The removal of policy enforcement keys from an agent environment resulting in recoverable cryptographic data access restriction. This action makes the data temporarily unreadable.
Key Rotation	The migration of policy enforcement keys within an agent environment resulting in no user-visible change to data access.
Key Shredding	The removal of policy enforcement keys from an agent environment resulting in an unrecoverable cryptographic data access restriction. This action makes the data permanently unreadable.
Keystore	The configured storage location of policy enforcement keys.
Lightweight Directory Access Protocol (LDAP)	An open, vendor neutral, industry standard protocol for accessing and maintaining distributed directory information over a network. This software protocol enables anyone to locate organizations, individuals and other resources such as files and devices in a network.
Log Event Extended Format (LEEF)	LEEF is a customized event format for IBM Security QRadar that contains readable and easily processed events for QRadar. It supports several predefined event attributes for the event payload.
Logical Volume Manager (LVM)	A storage device manager that uses a device mapper Linux kernel framework to gather storage devices into groups and allocates logical units from the combined space as needed. Most Linux distributions are LVM-aware.
M of N (M:N)	A model that determines what number of pieces of data is required to rebuild the data (M) out of the total number of pieces (shares) created (N).
NT File System (NTFS)	A proprietary file system developed by Microsoft in Windows NT operating system and used to store and retrieve files on a hard disk that supported file-level security, compression, and auditing.
Network Time Protocol (NTP)	A networking protocol for clock synchronization between computer systems.
Object Identifier (OID)	An identifier standardized mechanism for naming any object or concept with a globally unambiguous persistent name.

Object Store Agent	Object Store Agent encrypts and splits data to be sent and securely stores in highly scalable, efficient, object storage – in the cloud, on-prem, or both.
Online Certificate Status Protocol (OCSP)	An internal protocol used to obtain the revocation status of X.509 digital certificates.
Open Virtualization Archive (OVA)	A tar archive file. It is all the OVF files zipped and or compressed into a single file.
Payment Card Industry (PCI)	A standard to increase controls and security around cardholder data to reduce fraud.
PEM	A widely used encoding format for security certificates with syntax and content defined by X.509 v3 standards.
PostgreSQL	PostgreSQL (pronounced “post-gress-Q-L” is an open source relational database management system (DBMS) developed by a worldwide team of volunteers. PostgreSQL is not controlled by any corporation or other private entity and the source code is available free of charge.
Protected	Any data that has been processed.
Public Key Cryptography Standard #12 (PKCS12)	A public-key cryptographic standard that defines an archive file format for storing many cryptography objects as a single file. It is commonly used to bundle a private key with its X.509 certificate or to bundle all the members of a chain of trust. It may be encrypted and signed.
Public Key Infrastructure (PKI)	A set of roles, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
ReFS	Microsoft’s new file system that was introduced with Windows Server 2012 and designed to maximize data availability, scalability, and data integrity.
Representational State Transfer Application Program Interface (REST API)	A RESTful API, also known as RESTful web service, is based on representational state transfer (REST) technology, an architectural style and approach to communications often used in web services development.
Role Based Access Control (RBAC)	A method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file.
RSA	Public-key cryptography developed by Rivest, Shamir, and Adelman (RSA) using a public and private key to secure data.
Secure Copy Protocol (scp)	The scp command is used in Linux to transfer files between systems via Secure Shell (SSH) protocol.

Secure Socket Layer (SSL)	A cryptographic protocol that encrypts data communication over the Internet utilizing an asymmetric-key to exchange symmetric keys. A certificate authority and public-key infrastructure is necessary to allow verification of the certificate and the owner, as well as to generate, sign and administer the validity of the certificates.
Secure Socket Shell (SSH)	A network protocol that provides administrators with a secure way to access a remote computer. SSH also refers to the suite of utilities that implement this protocol.
Selector	OS defined users and groups that can access data, path sets, and other policy related features.
Transport Layer Security (TLS)	A cryptographic protocol that provides communications securely over a computer network
Truststore	A truststore stores certificates from trusted Certificate Authority (CA) that is used to verify certificates by Server in SSL connection.
Unique Identifier (UUID)	Universally Unique Identifier (UUID) is an identifier standard used in software construction. A UUID (128-bit number) is used to uniquely identify some object or entity on the internet.
Virtual Machine (VM)	An emulation of a computer system that is based on the computer architecture and functions of a real or hypothetical computer.
VMware ESXi™	An emulation of a particular computer system that is based on computer architecture and functions of a real or hypothetical computer.
Volume Agent	A volume agent enforces the volume policy definition and association of one or more protected volumes on a target system.
Volume with Policy Agent	It leverages the volume policy protection of a volume agent and allows for file-based operational access control policies to be applied and enforced for one or more protected file paths. Also, known as hybrid agent

Notices[r]

This information was developed for products and services offered in the U.S.A.

This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing

IBM Corporation

North Castle Drive, MD-NC119

Armonk, NY 10504-1785 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for

which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs. Depending on how you are viewing this information, some images and illustrations may not appear.

Trademarks[r]

SPx and Security First Corp are trademarks or registered marks of Security First Corp., registered in many jurisdictions worldwide. Other products and services may be trademarks of Security First Corp. or other companies.

IBM, the IBM logo, and ibm.com are trademarks or registered marks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at: http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

The Apache Software Foundation (ASF) owns all Apache-related trademarks, service marks, and graphic logos on behalf of our Apache project communities, and the names of all Apache projects are trademarks of the ASF.

Node.JS is a registered trademark of Joyent, Inc. CORPORATION DELAWARE 345 California Street; Suite 2000 San Francisco CALIFORNIA 94104.

Unicode and the Unicode Logo are registered trademarks of Unicode, Inc. in the U.S. and other countries.

The CentOS Marks are trademarks of Red Hat, Inc. (“Red Hat”).

“Red Hat,” Red Hat Linux, the Red Hat “Shadowman” logo, and the products listed are trademarks or registered trademarks of Red Hat, Inc. in the US and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Terms and conditions for product documentation[r]

Permissions for the use of these publications are granted subject to the following terms and conditions:

Applicability: These terms and conditions are in addition to any terms of use for the IBM website.

Personal use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights: Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein. IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed. You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED,

INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations[r]

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below. This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Product Number: 5737-C67

Printed in the USA

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

SPx and Security First Corp are trademarks or registered marks of Security First Corp., registered in many jurisdictions worldwide. Other products and services may be trademarks of Security First Corp. or other companies.

IBM, the IBM logo, and ibm.com are trademarks or registered marks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at: http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

The Apache Software Foundation (ASF) owns all Apache-related trademarks, service marks, and graphic logos on behalf of our Apache project communities, and the names of all Apache projects are trademarks of the ASF.

Node.JS is a registered trademark of Joyent, Inc. CORPORATION DELAWARE 345 California Street; Suite 2000 San Francisco CALIFORNIA 94104.

Unicode and the Unicode Logo are registered trademarks of Unicode, Inc. in the U.S. and other countries.

The CentOS Marks are trademarks of Red Hat, Inc. (“Red Hat”).

“Red Hat,” Red Hat Linux, the Red Hat “Shadowman” logo, and the products listed are trademarks or registered trademarks of Red Hat, Inc. in the US and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below. This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

SC27-9557-01