# DPM easyCipher

## System User Guide

Version 8.3
March 2023

randtronics

# DPM easyCipher

## System User Guide

Version 8.3

## Contents

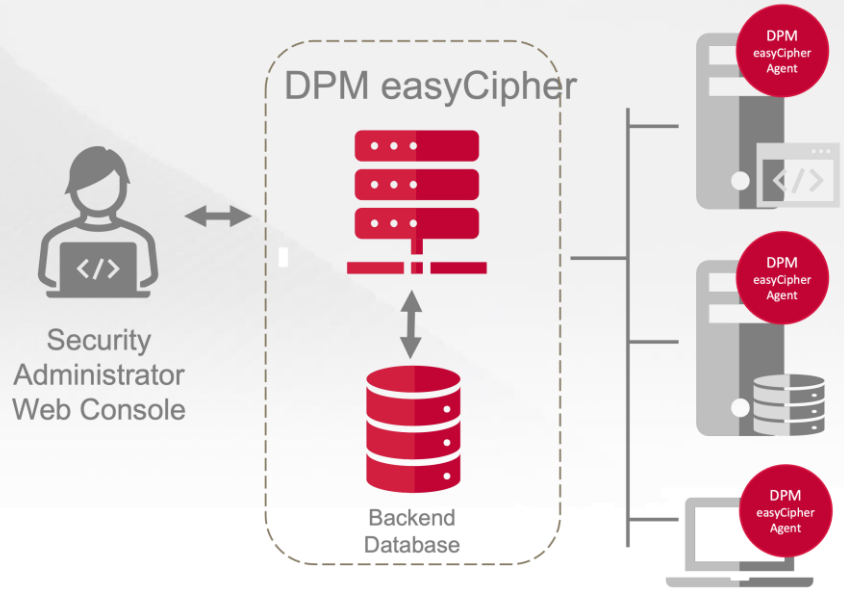
# 1. Purpose

This document serves as a user guide for system administrators of the DPM easyCipher software. It is assumed the DPM easyCipher manager and agent is either already installed on-premise as per the Installation Guide, or is remotely provisioned through Randtronics easyCloudPlus SaaS offering.

# 2. System Overview

The DPM easyCipher software provides management of encryption and access control to protect data stored in files on target computer systems.

The software consists of two components: DPM easyCipher Agent and DPM easyCipher.




DPM easyCipher – provides a web-based management system which allows centralized configuration and distribution of encryption and access control policies for DPM easyCipher Agents, administering DPM easyCipher settings, performing key management tasks. It also provides a centralized point for auditing and reporting.

DPM easyCipher Agent - is installed on every computer where it is required to protect data. It can be a laptop/desktop or a server. It applies polices created by the Manager to the devices, performs encryption transparently and controls access to the secured folders on the devices.

The DPM easyCipher software is designed to provide a secure environment for sensitive data protection. Access to secure folders on a PC is controlled from the Manager, which allows the contents of that folder to be encrypted, as well as provide access control based on an access control list.

# 3. Software Installation

For installation of DPM easyCipher software, please refer to the document “DPM easyCipher Installation Guide”.

# 4. Upgrade DPM easyCipher

For upgrade of DPM easyCipher software, please refer to the document “DPM easyCipher Installation Guide”.

DPM easyCloudPlus is maintained at the latest version by Randtronics.

# 5. Data Protection Polices

DPM easyCipher offers three types of protection policies on folders:

- Encryption
- Access Control

Encryption and Access Control

Data Protection polices determine which users and applications are allowed to access and encrypt and decrypt data in the folders to be protected.

## 5.1 Encryption

When a new policy (Encryption or Encryption and Access Control type) is created a new symmetric key will be generated automatically or it can be chosen from a prior created key list. Any files that are created in the protected folder, or are moved into the protected folder by authorized users and applications (in Standard mode) will be encrypted using the encryption key. A user/application with 'Encryption' permission will be able to encrypt and decrypt files using the nominated key.

## 5.2 Access Control

When a new policy (Access Control or Encryption and Access Control type) is created permissions can be set to allow to block users and applications from accessing the protected folder.

DPM easyCipher can configure the following access control permissions:

- Read – permission to read folder, open and read files in the protected directory
- Write – permission to change the contents of a file and save it in the protected directory
- Modify – permission to create or rename files in the protected directory
- Delete – permission to delete files in the protected directory.

## 5.3 Encryption and Access Control

Combination of both Encryption and Access Control.

# 6. Network access

## 6.1 On-premise

| | |
|---|---|
| DPM easyCipher console URL | https://<server>:8443/dpmeasycipher |
| Ports (TCP) | Need to be open in a firewall:<br>On the Manager side:<br>8443 - HTTPS Web console port<br>8448 – AWS SNS listening port (if using AWS autoscaling)<br>10000 – Agent policy port<br>10005 – Agent registration port<br><br>On the Agent side:<br>20000 – to browse folders and ping from DPM easyCipher<br>If this port is not opened encryption will still work but policy path will need to be configured manually. |
| Initial login | Username: admin<br>Password: admin |

## 6.2 easyCloudPlus SaaS

| | |
|---|---|
| DPM easyCipher console URL | URL to access manager as provided by Randtronics |
| Ports (TCP) | The connecting ports from agent to manager will be provided by Randtronics.<br><br>The connection from the manager to the agent requires the following to be configured:<br><br>1) public IP address mapped to the agent<br>2) Port 20000 opened for external connections<br><br>These are used to browse folders when configuring policies and pinging from the manager. If your are unable to provide public IP address the policy can still be configured but the path will need to be entered manually. |
| Initial login | Username: admin<br>Password: admin |

# 7. First time access

Once the DPM easyCipher has started, it can be accessed by via a web browser:

***https://ip_address:8443/dpmeasycipher***

If you are using easyCloudPlus then use the URL provided by Randtronics.

## 7.1 First time login

On initial login, the credentials to use are:

- Username: admin
- Password: admin

Note: you will be asked to change a default password after uploading a license.

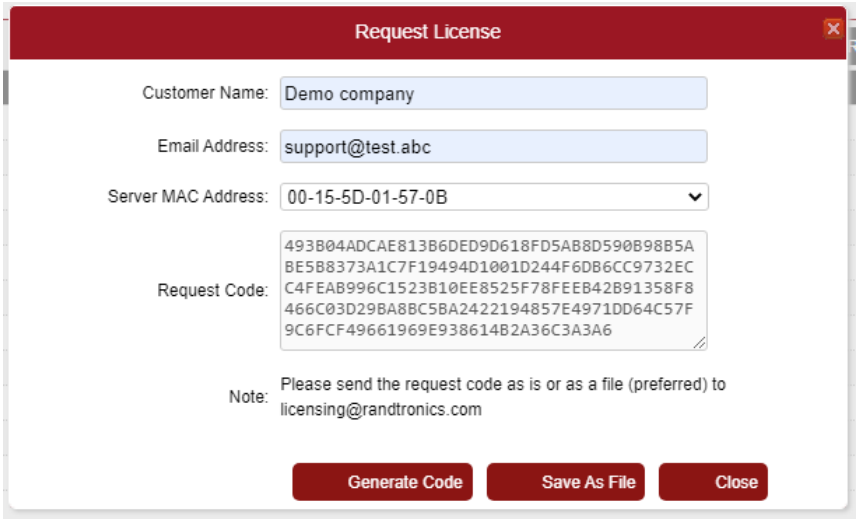
## 7.2 Licensing

The first time the DPM easyCipher instance is installed it is necessary to generate a license request and import a new software license.

### 7.2.1 Generate a license code

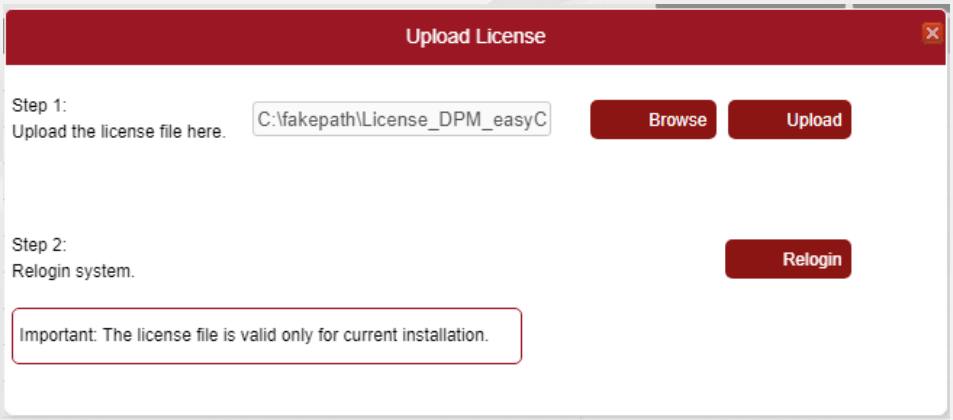
1. After initial login click “Request License”.
2. Populate required fields and click “Generate Code”.
3. Click “Save As File” and save a request file on a local system

Send the request file to licensing@randtronics.com



### 7.2.2 Import license

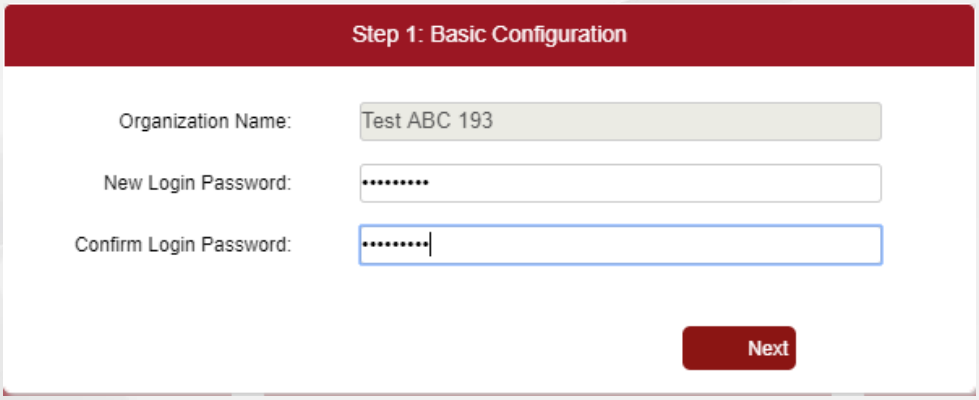
1. Once received a license file, login to the web console and click “Import License”
2. Click “Browse” and select the license file.
3. Click “Upload”
4. Click ‘Relogin”



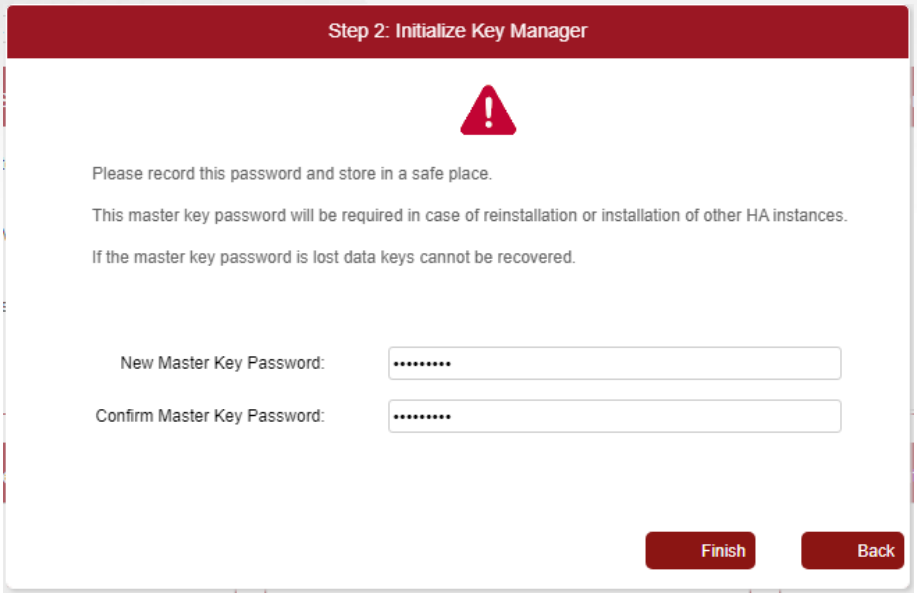
## 7.3 Initial configuration

Once the DPM easyCipher instance has been licensed, accessing a Web console for the first time will take the user through the basic configuration screens.

First. you will be asked to change a password for ‘admin’ user.




1. Set a new password for ‘admin’ user. Confirm the password.
2. Click ‘Next’




3. Provide a Master Key password that will be used to derive a local Master Key.
4. Click ‘Finish.

The Master Key and internal Encrypting Key will be generated.

IMPORTANT!!!

Please record your master password and keep it in a safe place. It is required to re-enter a master password in case of reinstallation or when an additional node is deployed for high availability. If the master password is entered incorrectly no keys can be decrypted and data cannot be decrypted.

# 8. DPM easyCipher backup and restore

## 8.1 Backup - Master key password backup

During installation and initial configuration of DPM easyCipher a system user enters a master key password that is used for initialization of internal key management module. The master key password is used to derive a master key for protection of other keys and configurations.

The same master key password is required to be entered during reinstallation of DPM easyCipher, rebuilding a system or installation of another node for high availability.

DPM does not store master key password in clear format. So a master key password need to be recorded during installation and stored in a safe place so they can be accessed when recovery as needed.

## 8.2 Backup - Database backup

DPM easyCipher stores most configurations, policies and encryption keys in its backend database.

It is recommended that a database backup is scheduled as per company policy to perform a backup of all database configurations. This can be done using native database tools or 3rd party tools.

The following database needs to be backed up:

- dpm_ec

Also the following database users have been created for DPM access to the database:

dpm_ec

It is recommended to backup information about those database users as well so they can be restored.

DPM easyCloudPlus is backed up by Randtronics.

## 8.3 Backup - Configurations backup

There are a few configurations that DPM easyCipher does not store in its database but rather in files on a file system where it is installed. During upgrade or system failure (e.g. hard disk crash) those files may be lost. So it is very important to perform a backup of DPM easyCipher installation folder.

DPM easyCloudPlus is backed up by Randtronics.

## 8.4 Restore - Replacing one DPM node with a new one (in HA configuration)

This section is only applicable to On-premise deployment.

If only one DPM node fails while the database and another node is still running a recovery process is simple. Follow the steps to build a new node:

1. Install a new instance of DPM easyCipher on a new system pointing to the same database
2. Generate a new license request
3. Import a new license and relogin
4. Provide the same master key password as per original installation
5. Configure server TLS certificates as needed
6. All other configurations will be synchronized with another running instance

## 8.5 Restore - Complete system restore

This section is only applicable to On-premise deployment.

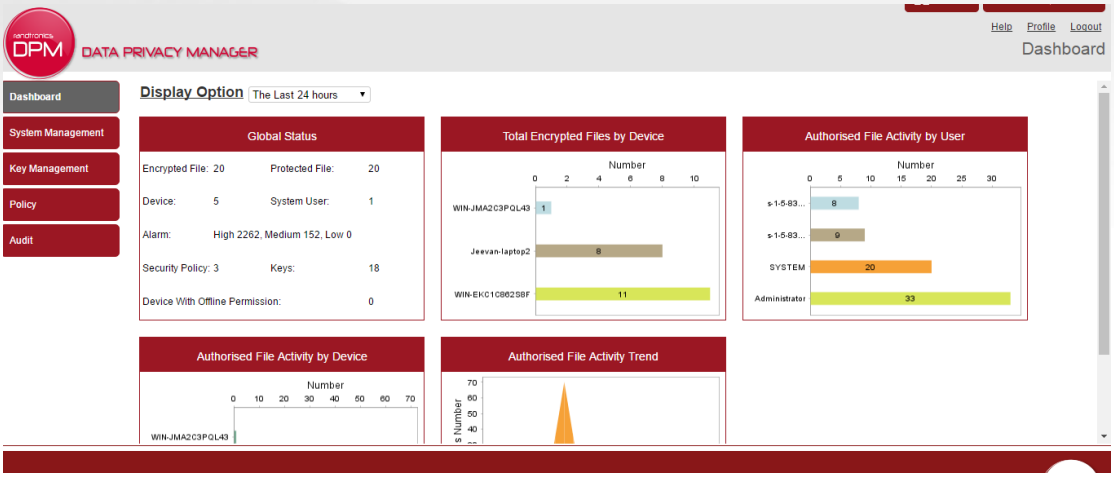
When it is required to restore the entire DPM system:

1. Install new a DPM easyCipher instant of the same version
2. Stop DPM easyCipher services service
3. If user dpm_ec does not exist restore it from the database backup
4. Restore the latest database backup of the DPM database using database restore tools
5. Restore configuration files from installation folder backup
6. Start DPM services
7. Request a replacement license for DPM easyCipher from Randtronics and import it
8. Relogin
9. Provide the same master key password per the original installation
10. Restart DPM easyCipher services

# 9. Dashboard

## 9.1 Dashboard page

The Dashboard screen displays various status information about the system and summary of user access events.




A number of reports are displayed using various graphs, which are described below:

- **Global Status** – displays the DPM easyCipher system status at a glance, including the number of registered devices, files encrypted, the number of security policies, the number of system users and number of encryption keys generated.
- **Unauthorized File Activity Trend**– displays the number of alarms triggered over the last 24 hours
- **Unauthorized File Activity by Department** – displays the number of alarms triggered per department over the last 24 hours
- **Unauthorized Attempts by User** – shows a list of detected illegal file activity, along with the user responsible for the activity over last 24 hours
- **Unauthorized Attempts by Device** – shows a list of detected illegal file activity, along with the device that activity is occurring on over last 24 hours
- **Authorized File Activity by User** – shows the amount of file access events performed by users during last 24 hours

- **Authorized File Activity by Device** – shows the amount of file access events performed within a device during 24 hours
- **Authorized File Activity Trend** – shows the amount of file access events over last 24 hour period.

If your easyCipher instance is running on Linux and some dashboards don't show any text please install fontconfig.

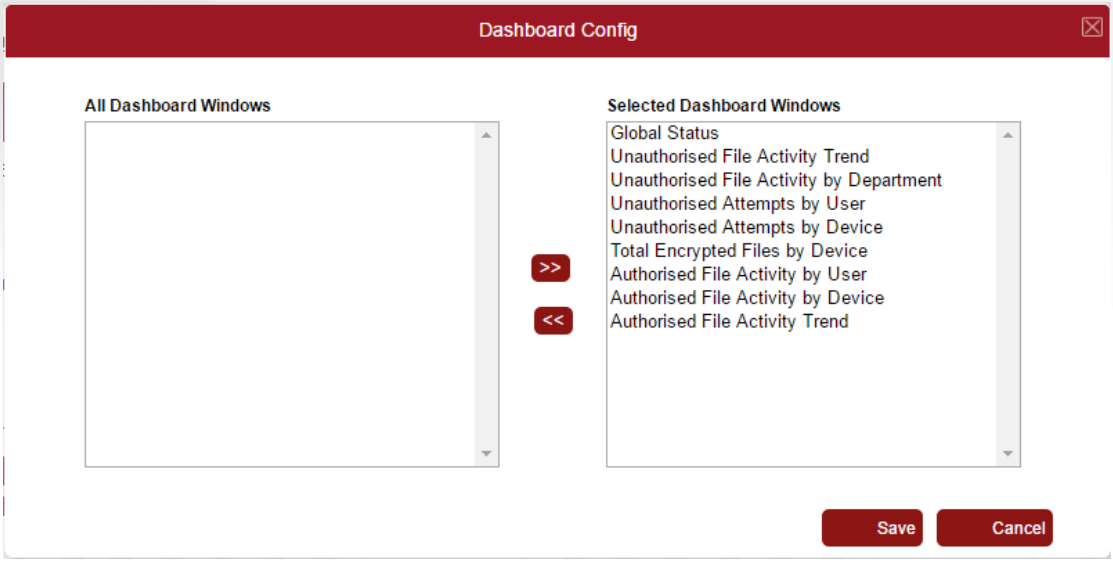
sudo apt-get install fontconfig

or

sudo yum install fontconfig

### 9.1.1 Configure Dashboard screen

1. To hide or to show dashboards, click on 'Display Options'.
2. The Dashboard Config box will be displayed.



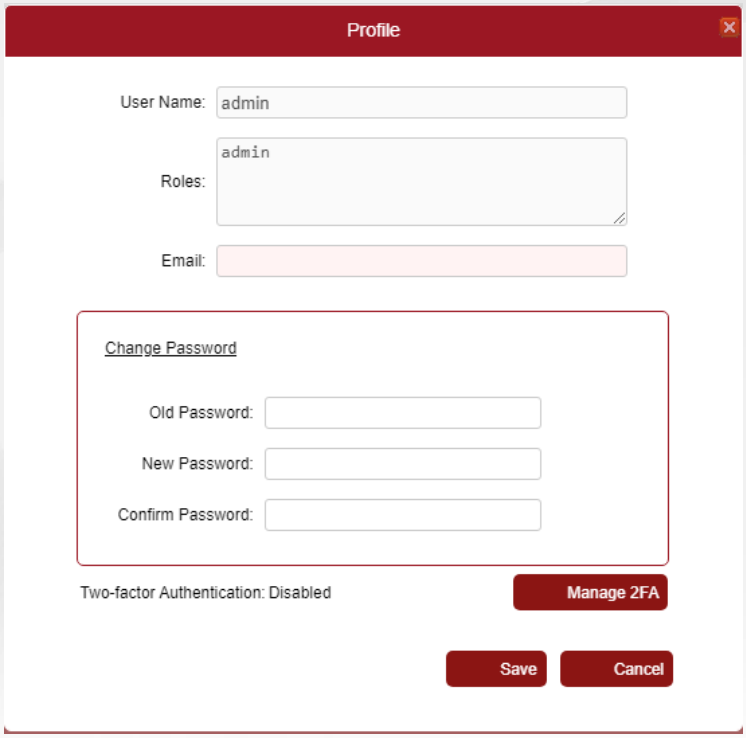

3. Move items that you want to hide from the right list to the left and move items that you want to display from left to right.
4. Click 'Save'.

Each system user can configure their own dashboard view.

## 9.2 Profile

The Profile page shows information about the currently logged in system User.

Click on ‘Profile’ link in the top right corner to see ‘Profile’ window.




The Profile popup will display information about the currently logged in user:

- User Name – a user name that is used to login to the management console
- Roles – a list of system roles that the user belongs to
- Email – the email address of the user. This email address is used to send a temporary password when the user uses ‘Forgot password’ link.
- Two-factor Authentication – Disabled or Enabled.

You can change both the user password and email from the page. Please note that password change is not available for users imported from Active Directory.

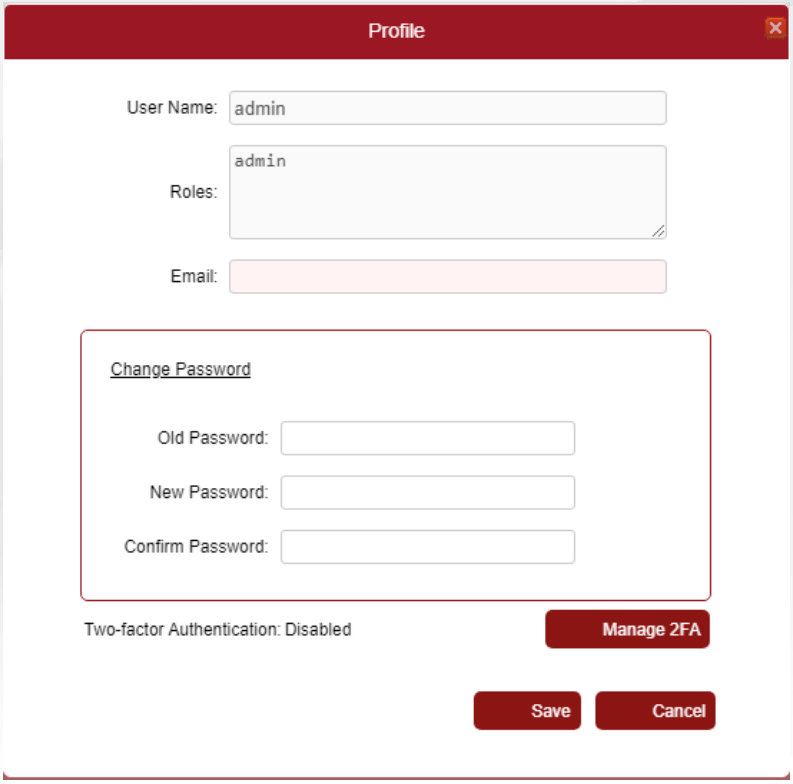
You can also manage 2 factor authentication configuration for the user by clicking ‘Manager 2FA’.

### 9.2.1 Change your password

Changing password can only be performed for native DPM users (not AD users).

To change password for the current user:

1. Open 'Profile' dialog



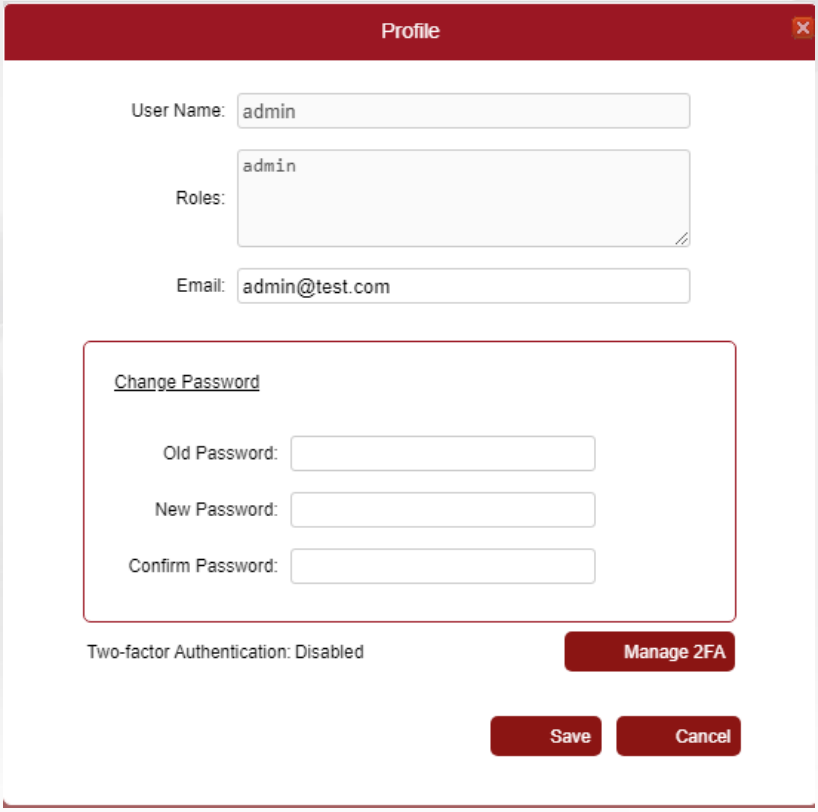

2. Input the current password into the Old Password field
3. Input the new password into the New Password and Confirm Password fields
4. Click on the Save button

The new password will be validated against the password restrictions configured in the Password management tab. See the Password Management tab for more information.

## 9.2.2 Change your email

To change the Email address of the current user:

1. Open ‘Profile’ dialog by clicking ‘Profile’ link in the top right corner.




2. Enter the new email address into the Email field
3. Click on the Save button

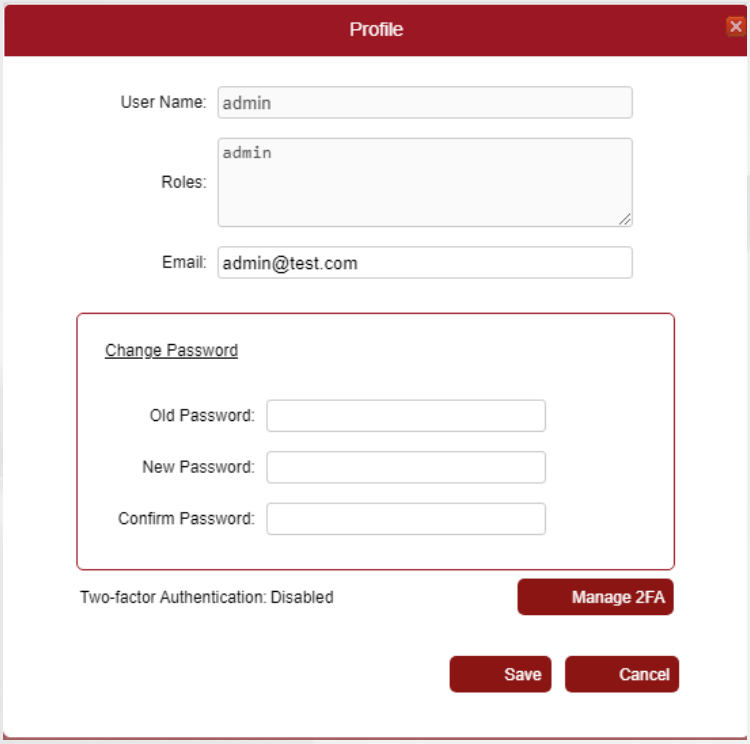
## 9.2.3 Manage two-factor authentication

Each system user can enable two-factor authentication (2FA). 2FA increases the security of your account. Even if somebody guesses your password, they won’t be able to login.

### 9.2.3.1 Turn on two-factor authentication

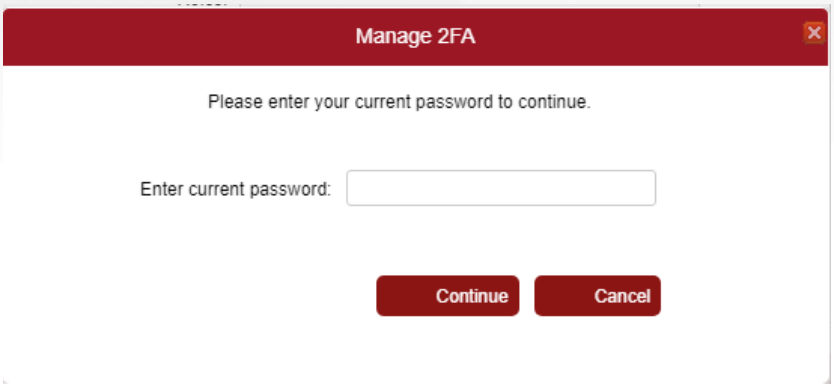
To enable 2FA for the current user:

1. Open ‘Profile’ dialog by clicking ‘Profile’ link in the top right corner.



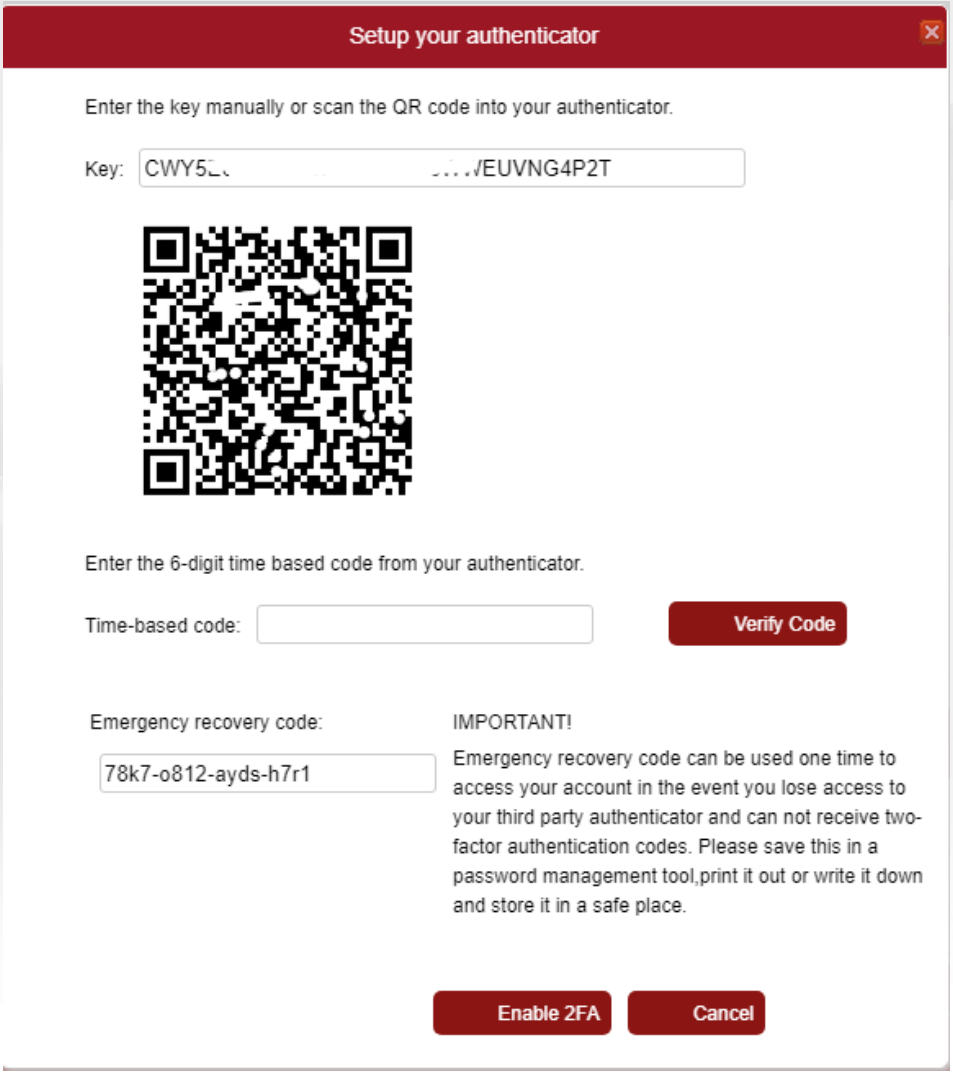

2. Click ‘Manage 2FA’

Enter the current password for your user and click ‘Continue’.




3. Details for setting up 2FA will be presented.

You can use any authenticator app on your phone such as Google Authenticator, Microsoft Authenticator and others.




Scan the QR code in you Authenticator app or enter the key manually.

Once you add the entry to the Authenticator app, you will see a one-time code that iwill be generated every 30 seconds.

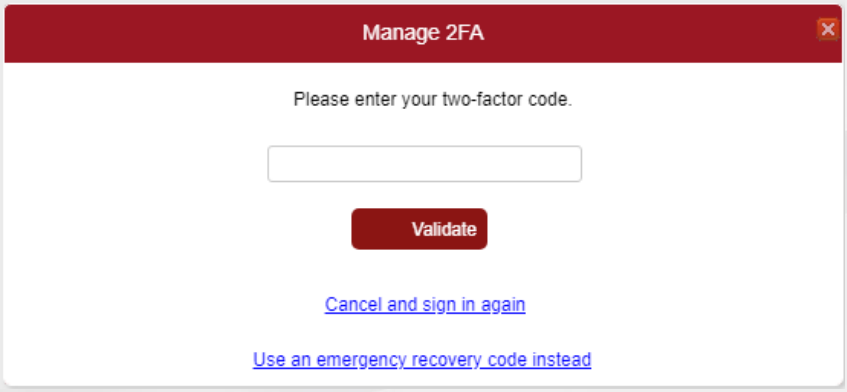
Please enter the one time code from the Authenticator app into 'Time-based code' field and click 'Verify Code'. It should display 'Code verified successfully on the top.

You can only see 'Emergency recovery code' which you should save and store in a safe place. This is a one-time use recovery code that can be used instead of Authenticator app code in case you don't have access to it. Once this recovery code is used it will be regenerated automatically. If you use the recovery code to login you must go to 'Profile – Manage 2FA' and get the new recovery code again.

4. Click 'Enable 2FA' to enable two-factor authentication for your account.

### 9.2.3.2 Login using two-factor authentication

Once 2FA is enabled for the system user all logins into the management console by that system user will require entering two-factor code.



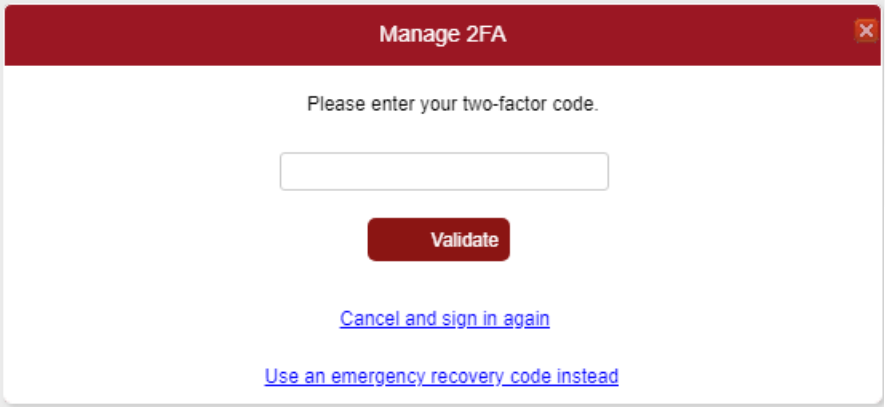

Open your Authenticator app and type the one-time code displayed in the app. Click ‘Validate’.

If the code is correct you will be taken to the management console.

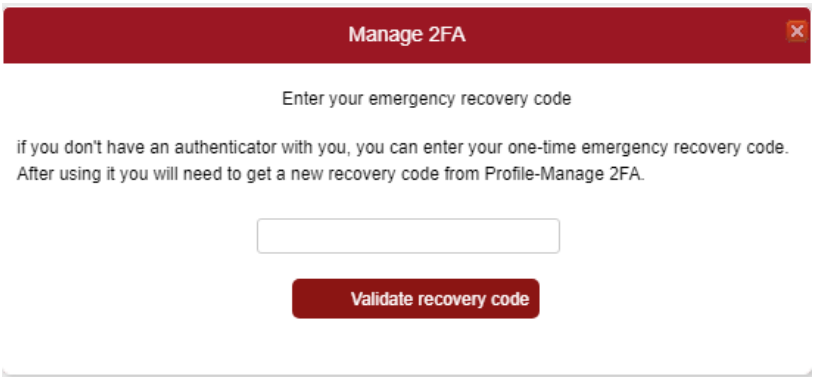
#### 9.2.3.3 Using emergency recovery code

If you have lost your Authenticator app, you can still login by using emergency recovery code.

After entering username and password you will be presented with a dialog to enter two-factor code.



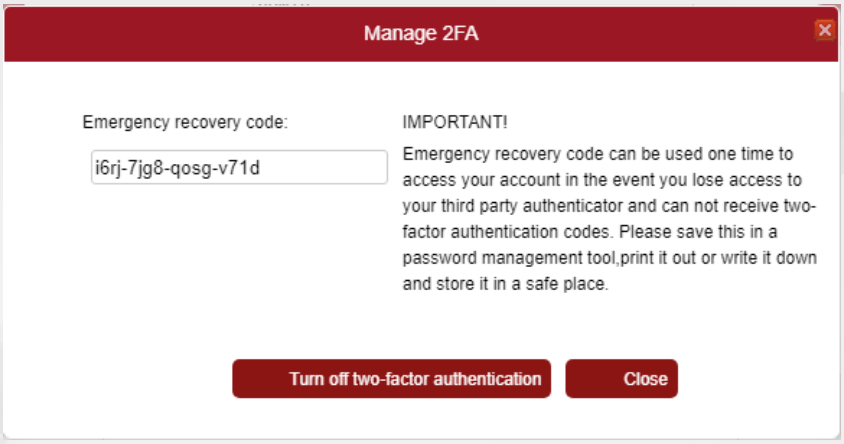

Click ‘Use and emergency recovery code instead’.




Type your emergency recovery code and click ‘Validate recovery code’.

After login, navigate to ‘Profile – Manage 2FA’.

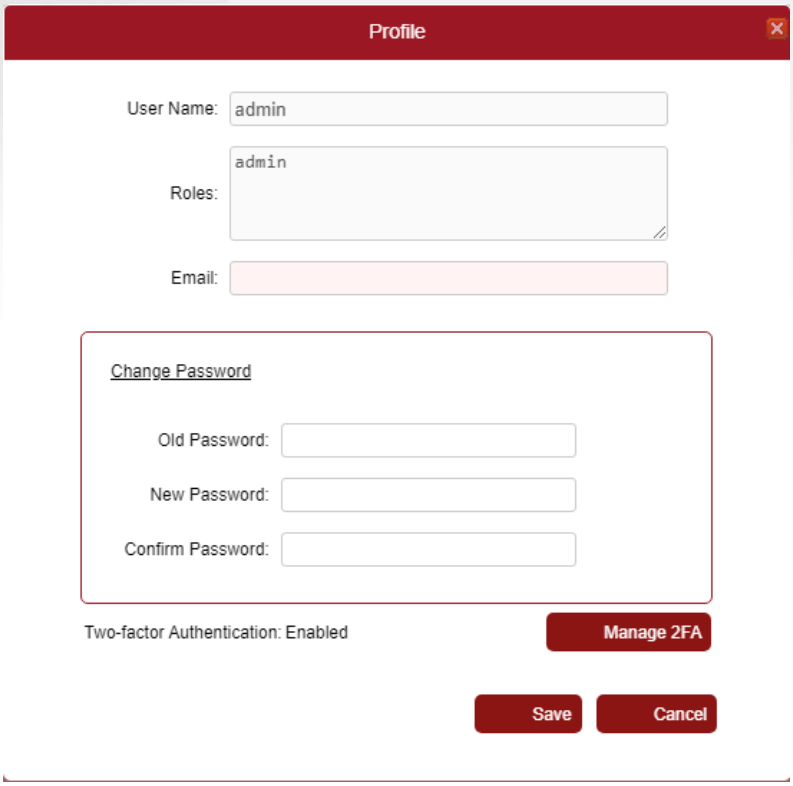
The new emergency recovery code will be displayed. Store  in a safe place for future use.




### 9.2.3.4 Turn off two-factor authentication

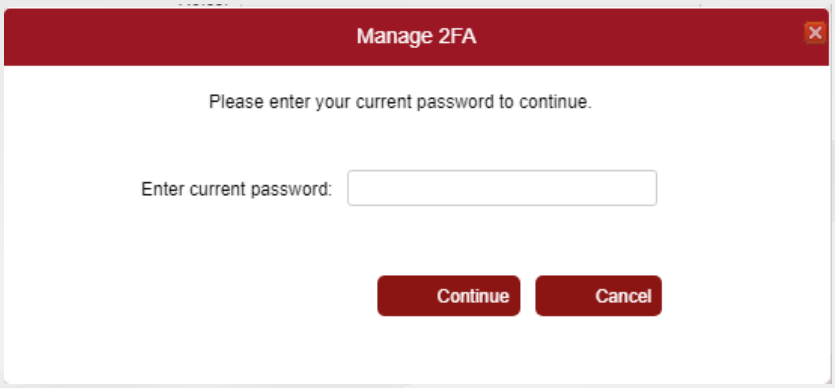
To disable 2FA for the current user:

1. Open ‘Profile’ dialog by clicking ‘Profile’ link in the top right corner.

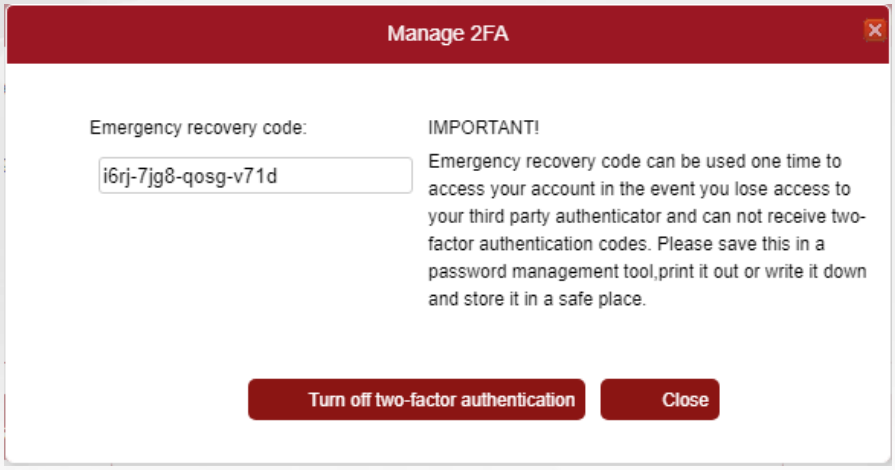



2. You will see that 2FA is Enabled. Click ‘Manage 2FA’

Enter the current password for your user and click ‘Continue’.




3. Click ‘Turn off two-factor authentication’ on the next screen.



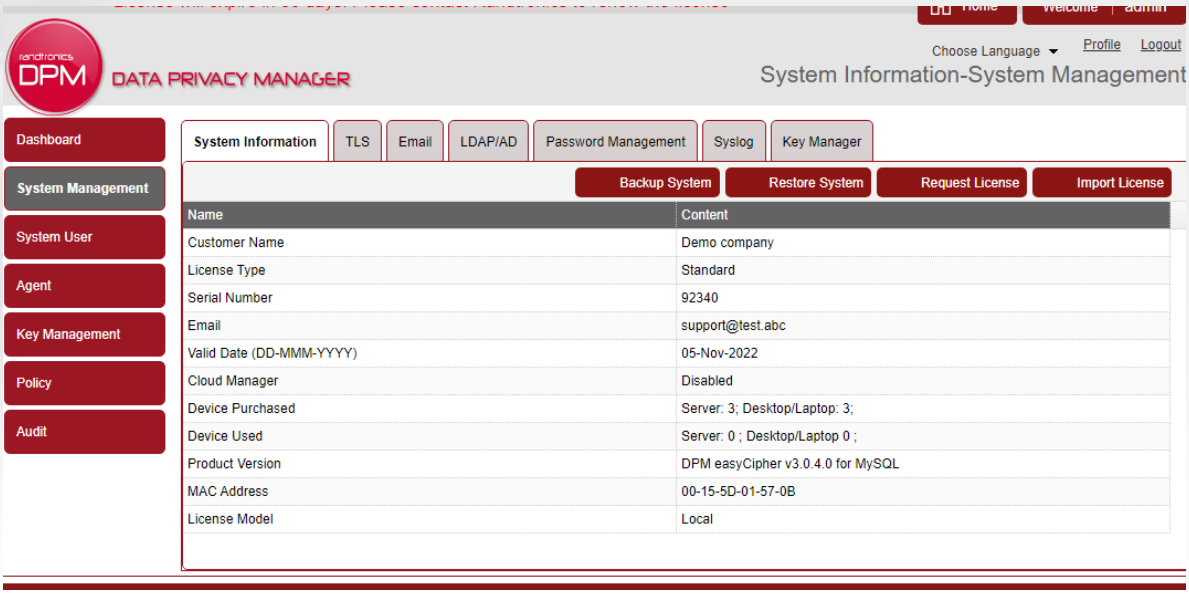

4. Now 2FA is disabled and it will no longer require a 2FA code.

# 10. System Management

The System Management area allows the user to configure the DPM easyCipher system, including updating the DPM easyCipher license, managing system roles and system users, Key Manager connection configurations, creating password complexity rules and managing agents and groups.

## 10.1 System Information tab

To access the System Information tab, click on the 'System Management' menu, then click on the 'System Information' tab.




The System Information tab contains the following:

- Displays the current license information
- Displays DPM easyCipher system information – product version, the number of devices allowed to be managed and restricted by the license and the actual number of devices used
- Allows the user to request a new license
- Allows the user to import a new license
- Allows the user to take a system backup
- Allows the user to restore a system backup

The page will display the following:

**Customer name** – the name of the customer configured during installation

**License type** – will display either Standard or Enterprise, depending on the type of license

**Serial Number** – the license serial number

**Email** – the email address of the user who requested the license

**Valid Date** – the date that the current license will expire

**Cloud Manager** – whether integration with cloud groups is enabled. Cloud Manager requires an additional license.

**Device Purchased** – the number of Agent devices allowed by the license

**Device Used** – the number of Agent devices currently in use by the system

**Product Version** – the version of the Manager

**MAC Address** – MAC address that this system is licensed for

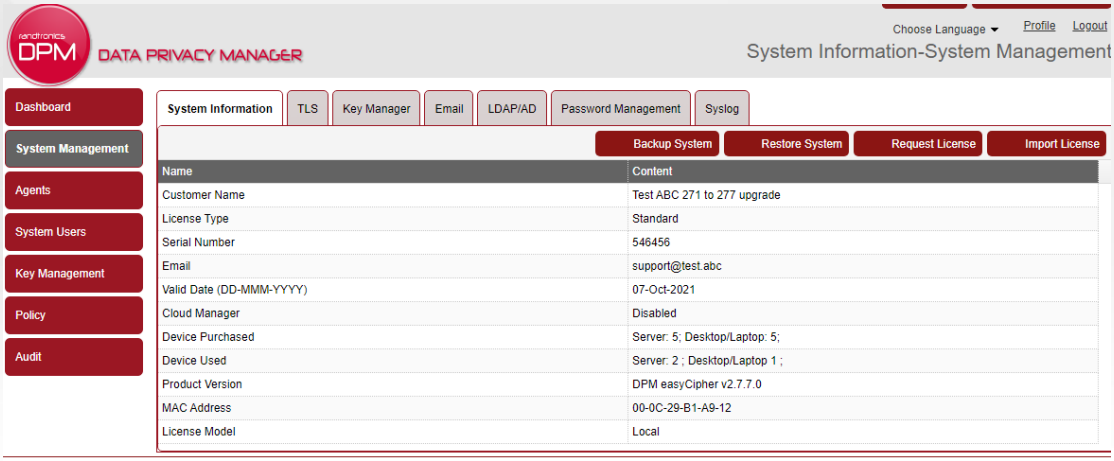
**License Model** – whether it is using a local or hosted license

### 10.1.1 Request a new license

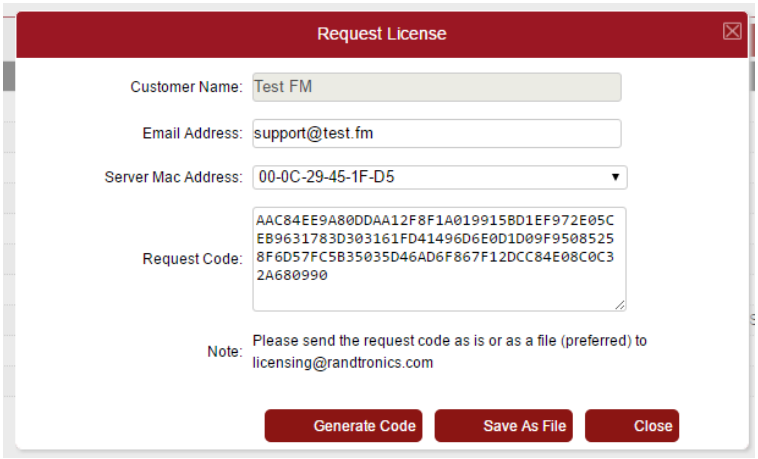
Before the DPM easyCipher software can be used, it is necessary to install a license. There are two steps to installing the license, the first step is to generate a license request and send the request to Randtronics. Randtronics will then issues the license which needs to be imported into the DPM easyCipher.

To request a new license, please perform the following steps:

1. Click on the System Management button in the left hand menu
2. Then click on the System Information tab




1. Click on 'Request License'



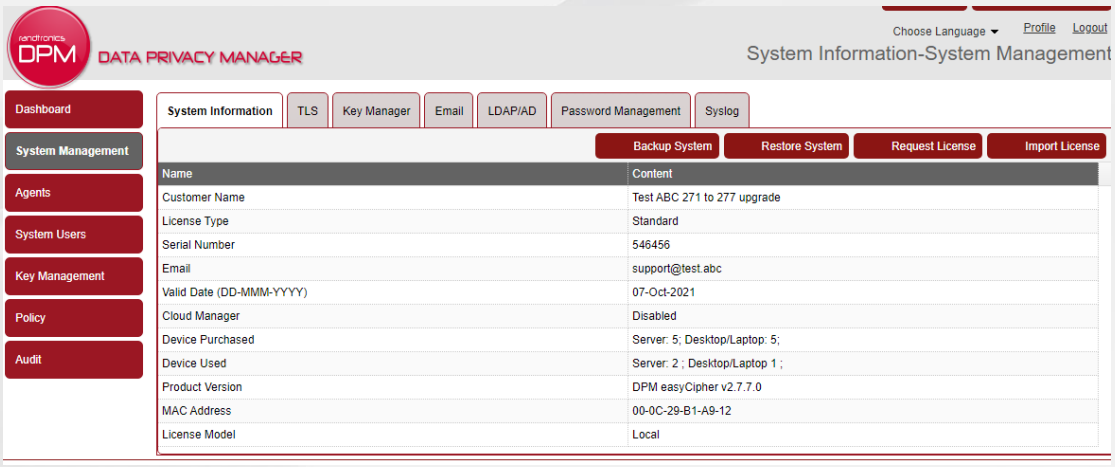

2. Enter your Customer Name (if requesting for the first time), email address, select MAC address that you want to assign this license to and click 'Generate Code'
3. Click 'Save as file' to download a license request to your local system. Close the window.
4. Send the license request file to licensing@randtronics.com

## 10.1.2 Import a license

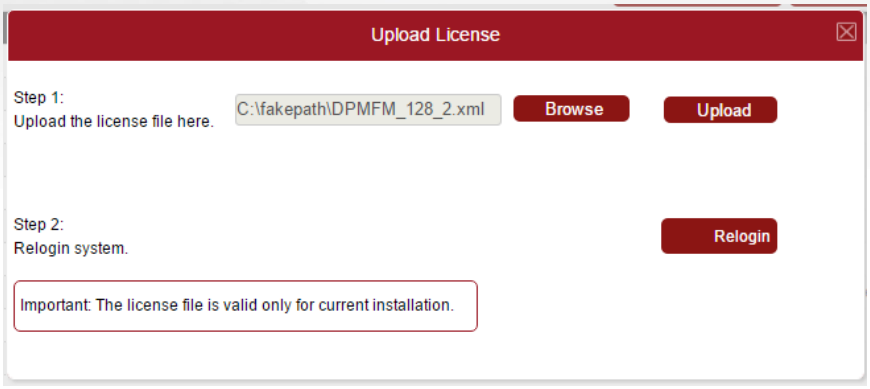
Once Randtronics has processed the license request and responded with a license file, it is necessary to import the new license into the DPM easyCipher.

To import a new license, please perform the following steps:

1. Click on the System Management button in the left hand menu
2. Then click on the System Information tab




3. Click on 'Import License'

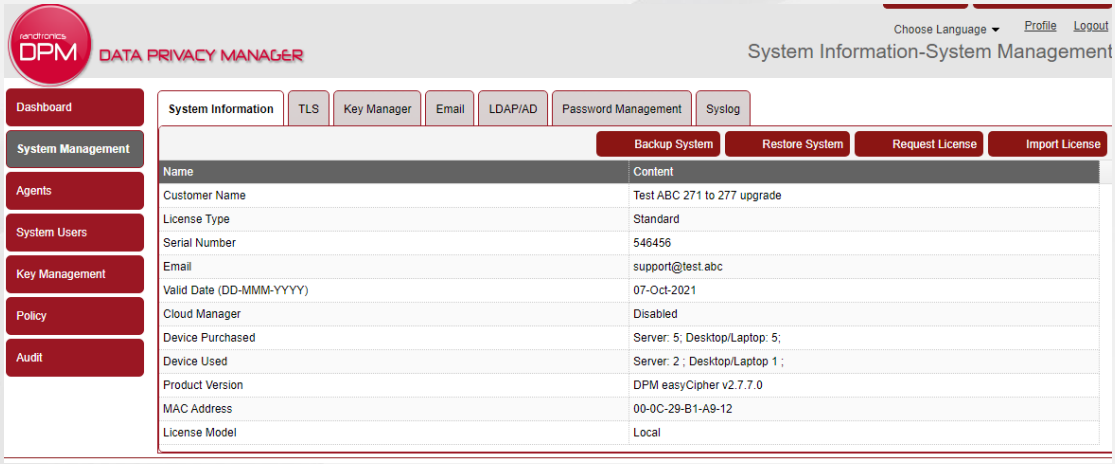



4. Browse to the license file and upload it.
5. Relogin to the system.

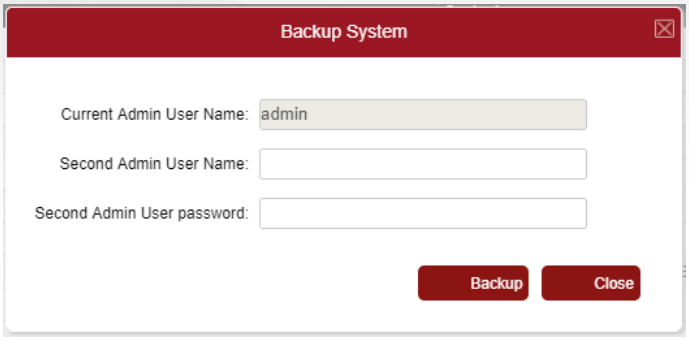
## 10.1.3 System Backup

To backup configuration files please follow the steps:

1. Login to the management console with 'System Management' rights and click on the 'System Management' Menu in the left hand menu




2. Click 'Backup System' button.

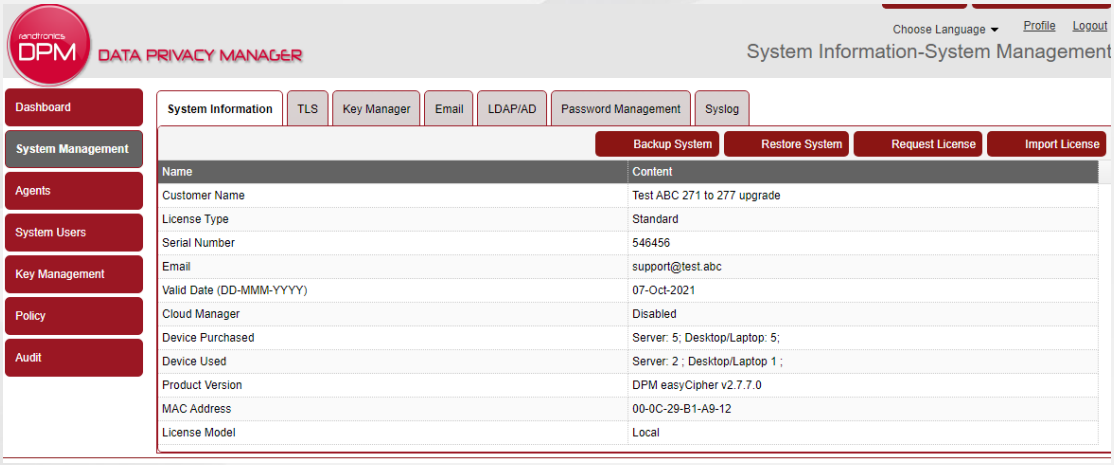



3. A second admin user requires to enter their user name and password to complete the operation.
4. Click 'Backup' and save a file into your local folder.
5. Backup the database as per normal database backup procedures. It is important to run the database backup after the System Backup file has been downloaded, as the DPM easyCipher will store backup related information in the database

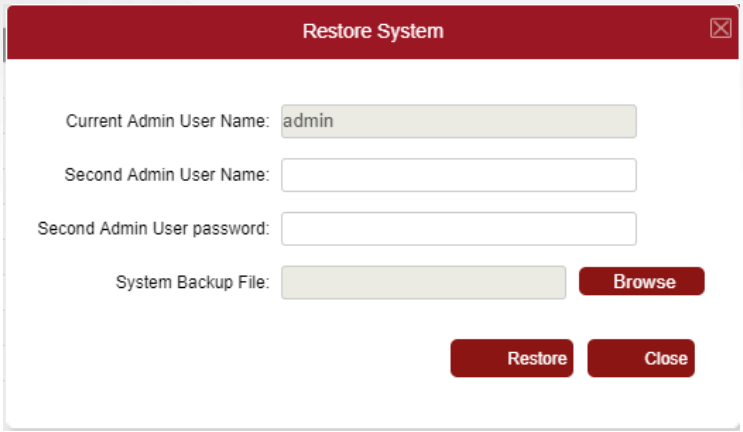
## 10.1.4 System restore

1. If necessary, restore the latest database backup of the DPM easyCipher database

2. Login to the management console with 'System Management' rights and navigate to 'System Management'-'System Information' menu




3. Click on 'Restore System'




Restoring the system is a privileged operation and requires a second admin user to complete the operation. Ask another admin user to enter their username and password

4. Browse to the system backup file and type the password that was used during creation of the backup.
5. Click 'Restore'.
6. Login to OS and restart DPM services:
    a. For Windows:
        i. DPM easyCipher Server
        ii. DPM easyCipher Web
    b. For Linux
        i. dpmeasyciphermanager
        ii. dpmeasycipherserver

## 10.2 TLS tab

For users of DPM easyCloudPlus we advise retaining the default settings.

DPM easyCipher utilizes secure TLS (Transport Layer Security) in both internal and external communications, in order to preserve confidentiality, integrity and authenticity of data transmitted through its authorized channels. Digital Certificates (X.509) are used to establish trust between two parties during a TLS communication. In this section, you will learn how to review, configure and update the certificates used by DPM easyCipher, as well as other parameters specific to services and network communication.

Secure TLS connections are employed in two distinct contexts:

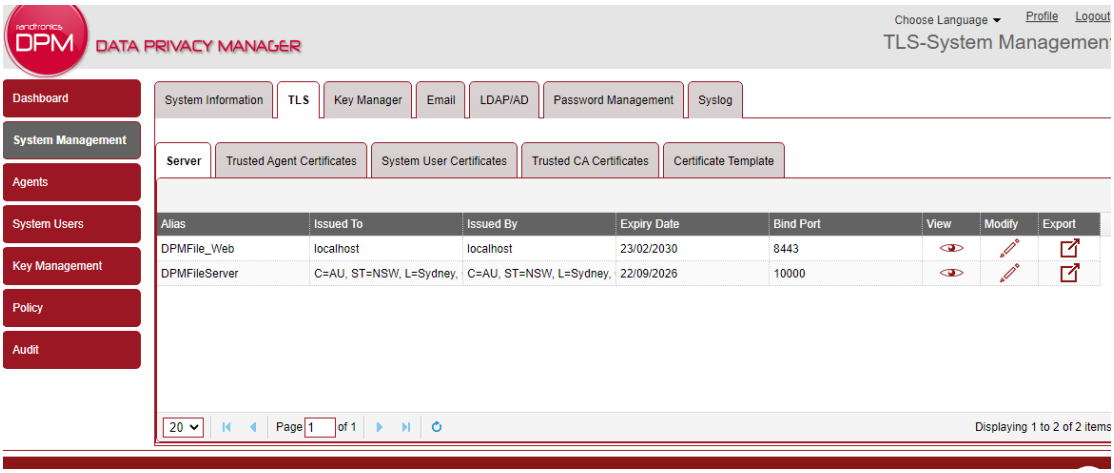
- Web Management Console Sessions: when a user authenticates to the DPM Management console, all data exchanged travels through an encrypted TLS tunnel underlying the HTTP protocol (also known as HTTPS). This secure connection is used to protect sensitive information such as user credentials or configuration details;
- DPM Server/Agent Communications: in order to provide transparent encryption to local files and folders, DPM Server and its registered agents exchange sensitive information, the most significant of them being the encryption keys themselves. TLS is also applied to protect each connection to every trusted agent, so only a legitimate party gets access to the required keys.

### 10.2.1 Setting Up the HTTPS Connection

The default installation comes with a self-signed certificate issued to the loopback IP address (127.0.0.1). This certificate (Figure 1) must be used with the sole purpose of allowing an initial setup of the system and must not be trusted as the definite server identity.

To make sure your system holds a unique and strong identity within your network, it will be necessary to replace the certificate used by the web console server. You can perform this operation using either of two methods – generating a new self-signed certificate or importing an existing one, issued by a Certificate Authority of your preference. Please note that self-signed certificate is not trusted by most web browsers. So to have 'trusted' connection you need to import a certificate issued by a Trusted Certificate Authority.

1. Navigate to System Management – TLS – Server tab.




Within the TLS management area, the first tab, named *Server*, contains a list with two certificates employed by DPM easyCipher. The first certificate in the list is used by DPM Web Console to protect browser sessions. The second one refers to the certificate used by DPM easyCipher Server to communicate with registered Agents and its update procedure will be covered in section 4.2.4.

For now, let us focus on the first row of the table, where the certificate details are listed as follows:

- **Alias**: identifies the respective service to which this certificate belongs. *DPMFile_Web* refers to the certificate presented by the DPM Web Console when users access this management interface;
- **Issued to**: corresponds to the field Common Name (CN) of a digital certificate and represents its owner

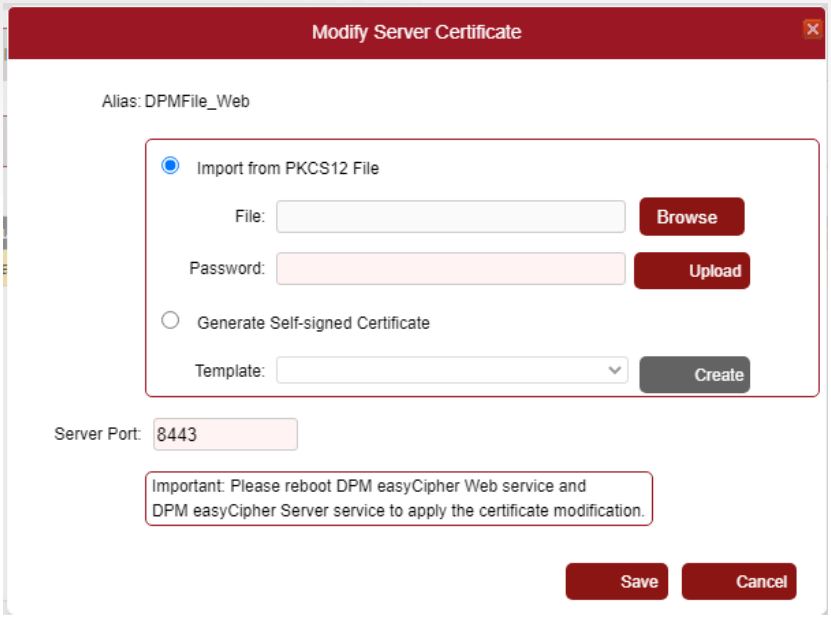
(or holder). In TLS certificates, where the owner is generally an internet host, this field is usually filled with the host IP address or domain name;

- **Issued by**: contains the identification of the issuing authority of the certificate. As the default certificate consists of a self-signed one, this field matches the *Issued to*, meaning the host is at the same time owner of the certificate and the issuing authority. In CA signed certificates, this field will contain the name of the certificate authority responsible for issuing the certificate;
- **Expiry Date**: correspond to the maximum date within which this certificate must be considered valid. For security reasons, digital certificates must be updated from time to time;
- **Bind Port**: denotes the port used by the service. The default port for the web console service is TCP 8443. This value can be changed to a preferred alternative address;
- **View**: this operation allows you to see further details regarding the current configuration and server certificate;
- **Export**: allows you to export the current certificate as a file in a default format (.CER). This file can be easily visualized on Windows and Linux machines by double clicking them;
- **Modify**: finally, the modify functionality is used to update the certificate, regardless of which method has been chosen. This is the operation we will be using to update DPM Web Console certificate.

2. Click on '*Modify*' icon.

Two different options will be presented. The first one refers to the installation of an externally generated certificate, through importing a PKCS#12 file. The second proceeds the generation of a new self-signed certificate.

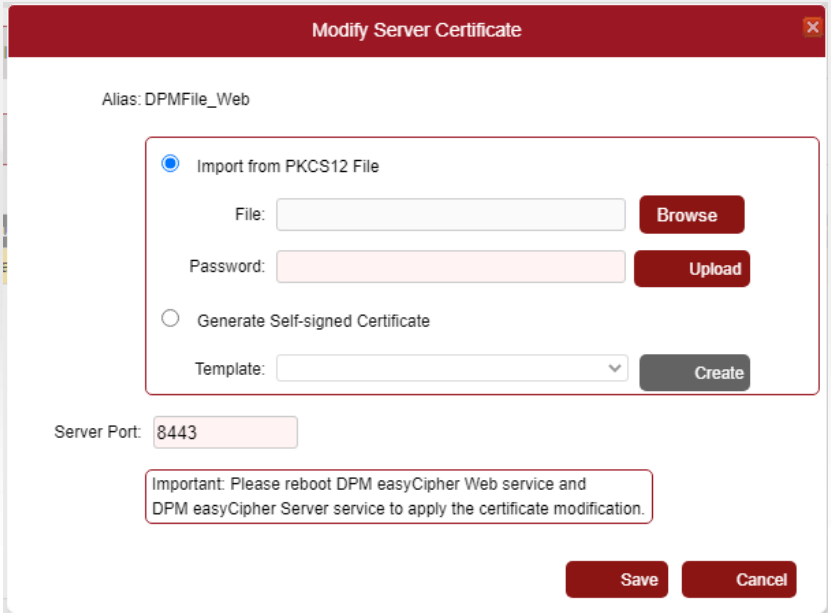
After installing a new certificate, the respective service must be restarted in order for the settings to be reloaded by the server.



**Method 1: Importing an External Certificate**

This is the recommended method for organizations that use internal or third party PKI to provide TLS certificates. This functionality allows you to import a Private Key Exchange file in the format PKCS#12 (also known as PFX file). With the PKCS#12 file at hand, select the option *Import from PKCS#12 File* on the Server Certificate Management Dialog.

***Note on importing the PKCS#12 file***
*Before importing your new server identity, make sure that a Root CA and all Intermediate CAs are imported via 'Trusted CAs' tab.*
*PKCS#12 files are protected by passwords. When you import the PKCS#12 file, the password used to protect the imported file will become the password used to protect your server's credential internally. Hence, make sure to use a strong password protecting your server's identity before importing it.*




Click browse to select the PKCS#12 file from your file system and click *Open.* Enter the password used to protect the PKCS#12 file (see note above on password strength). Click *Upload* to import the PKCS#12 file. If the process succeeds, you will be presented with a message, and details of the new certificate will be updated to the first row of the certificate list.

If using 3rd party certificates, make sure they have extended key usage "Server Authentication" and "Client Authentication"

Method 2: Generating a new Self-signed Certificate

This method is suitable for organizations that do have an existing PKI infrastructure are/or wishing to rely on third party certificates. For such cases, DPM easyCipher offers a simplified way to deploy a trusted TLS connection. Please note that this type of certificate will be reported as "Not trusted" by web browsers.

For your convenience, DPM easyCipher allows you to define a set of Certificate Templates to prevent you from typing all the required fields every time a new certificate needs to be updated. As there are no templates defined yet *(this process is covered in a later section),* simply leave the '*Template'* field blank and click '*Create'.*

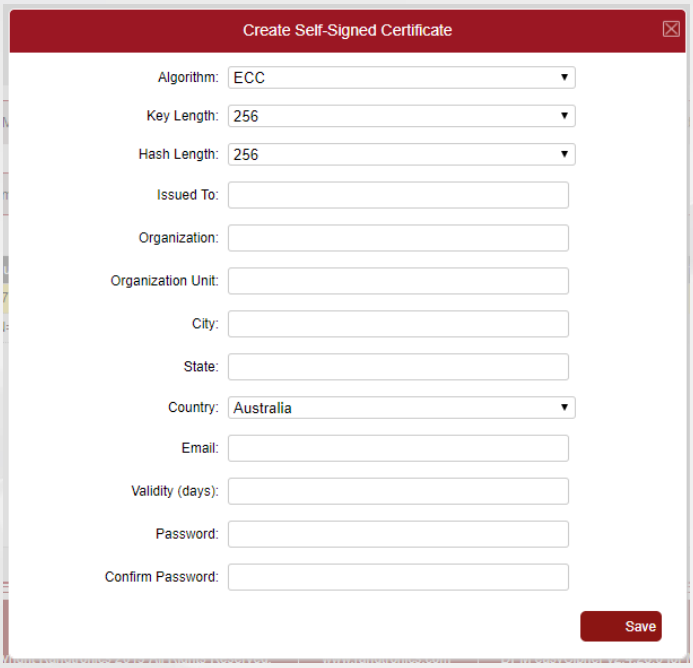



*Figure 1: Certificate request form.*

In the Self-signed Certificate Generation dialog, you can input the details of your certificate. These details will compose a certificate request and will become part of your new certificate.

- **Algorithm**: allows you to select which algorithm should be employed to generate the Key Pair associated with the new certificate. ECDSA (ECC) keys have the benefit of providing high security level with shorter keys, improving the overall communication performance. On the other hand, some legacy browsers and OS do not offer support for this algorithm. If you will be accessing the web console from such system configurations, select RSA signed certificates;
- **Key Length**: defining the key length, you can choose the security grade which best fits according to your security policies;
- **Hash Length**: DPM easyCipher makes use of SHA algorithm family to provide message digesting (hash) operations during the issuance of a certificate. You can define the digest length that best suits your requirements;
- **Issued To**: this is the field that will hold the address of your server. Browsers usually match the information contained in this field to the URL typed by the user on the address bar. Thus, before issuing a new certificate, make sure the server is configured with the definitive domain name and inform it here (e.g. filemanager.mydomain.com if the access is done through https://filemanager.mydomain.com);
- **Organization**: a free choice field that usually holds the name of the organization responsible for the system (e.g. your company name, as Randtronics PTY Limited);
- **Organizational Unit**: another free choice field, frequently used to refer to an internal department of a company, but can hold any text content (e.g. DPM easyCipher Web Console);
- **City**: the city where the organization responsible for this certificate is located;
- **State**: the state or province to where the organization belongs;
- **Country**: A country of the issuing organization – choose from a drop down list;
- **Email**: a contact e-mail of your choice;
- **Validity**: time period for which this certificate should be considered valid;
- **Password**: The generated certificate will be stored in an encrypted store. This password will be used to protect the referred key store;
- **Confirm Password**: confirmation field to assure the intended password will be applied.

With the request form correctly filled click '*Save*' to generate the self-signed certificate. All dialogs will be closed and the respective line will be updated with details from the new certificate.

Having issued your new self-signed certificate, you can utilize the export function to download it and import it into your domain as a Trusted Root Certificate Authority as a way to prevent security alerts on system user's browsers.

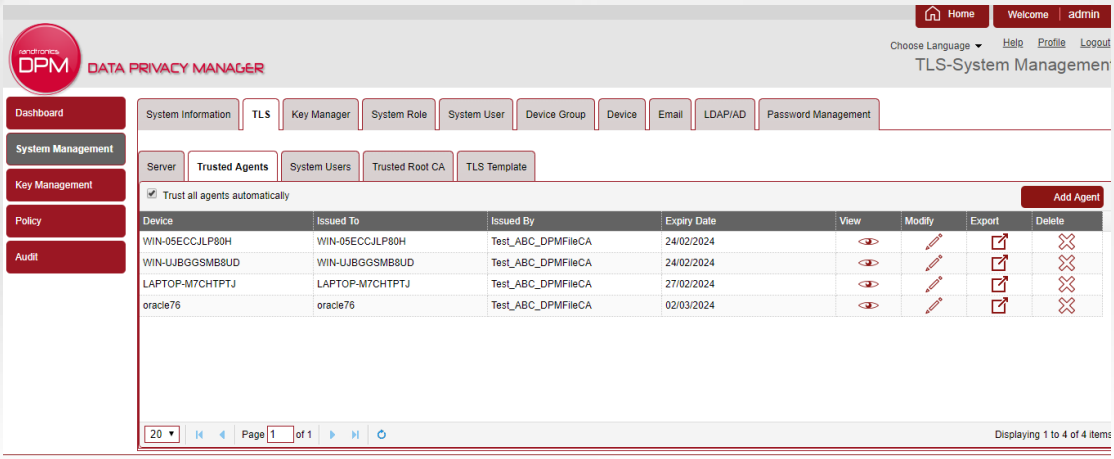
After updating your certificate, close your browser and restart DPM easyCipher services.

Wait for the server to restart. Reopen your browser and access the web console. You will be able to verify the new certificate in the browser.

### 10.2.2 Trusting DPM easyCipher Agents

To manage trust relationships between server and its clients, please access the tab *Trusted Agents* under the TLS area.

If an agent is not in the trusted list it will not be able to receive policies and keys.



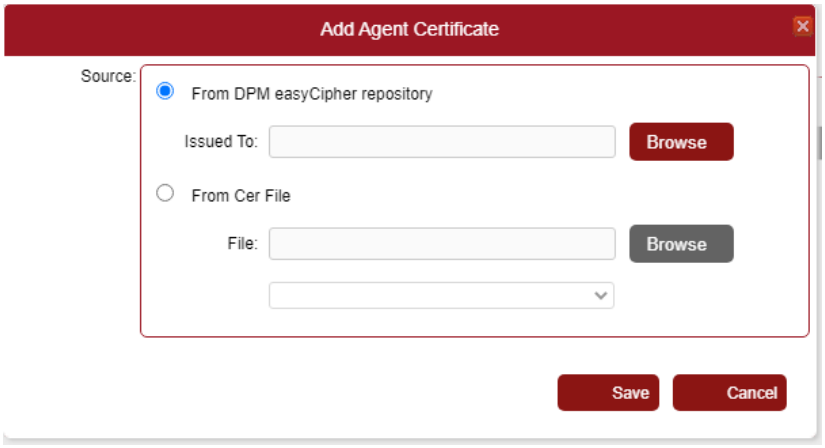

This area shows the list of trusted agents. At the top-left side of this list there is an option named *Trust all agents automatically*, allowing the automatic trust to be switched on or off.

Method 1: Manual inclusion of an Agent to the Trusted Agents List

When the '*Trust all*' option is unchecked, a new Agent must be added to the trusted list manually.

Click '*Add Agent*'.

'Add Agent Certificate' dialog will be presented.




The two options available for manually including an Agent certificate are:

- *Use a certificate from DPM repository:* this option allows you to register an agent using a certificate generated internally;

- *Importing an external certificate to identify the agent:* this option is suitable for organizations wishing to use their own externally managed digital certificates to protect the communication between agents and server;

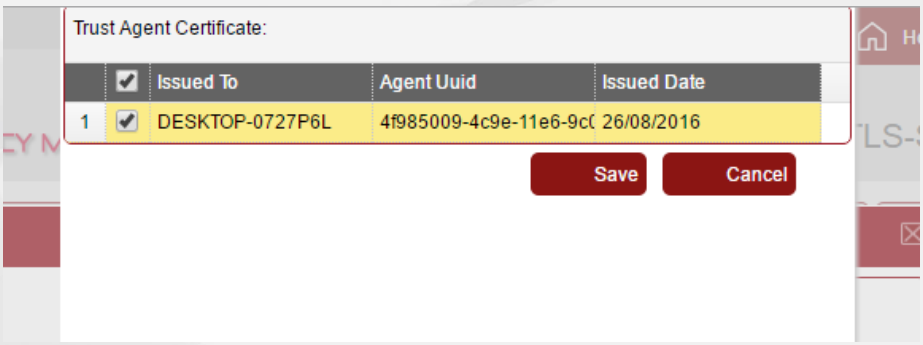
Option 1: Select from DPM easyCipher repository

a. Select 'From DPM easyCipher repository' option

b. Click Browse

c. Select which certificate you want to trust

d. Click Save and Save

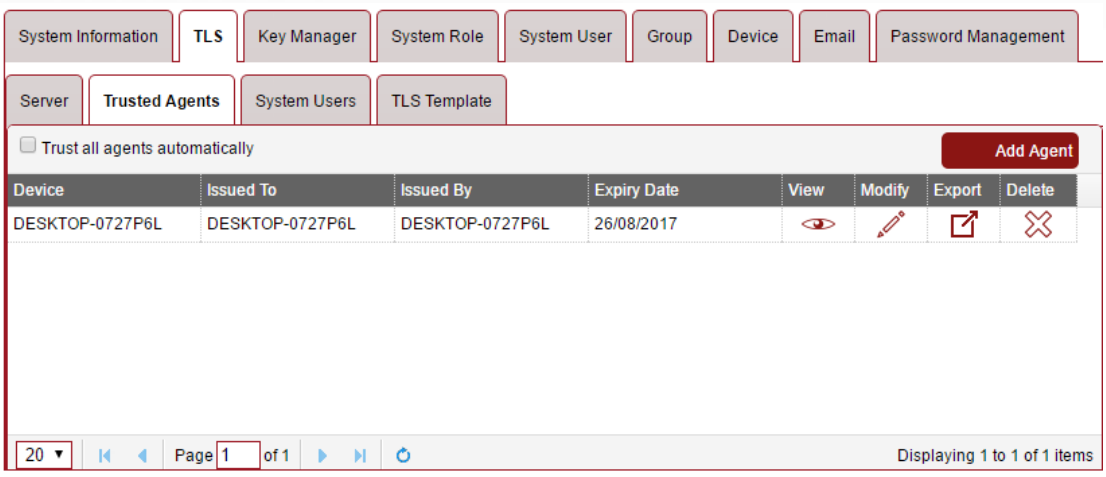



Option 2: From Cer file

a. Select 'From Cer file' option

b. Click Browse and navigate to the public certificate

c. Click 'Open' and Save




***Note on importing an externally managed agent certificate***

***Before importing a 3rd party certificate make sure a CA certificate is uploaded in 'Trusted CA' tab.***

***The import of an externally generated agent certificate is only part of the registration process. The other part happens on the client side, where a PKCS#12 corresponding to the certificate imported on server side should be imported to the DPM easyCipher Agent user interface. Furthermore, it is mandatory that the steps described in this section have been executed prior to the .P12 file import on client side.***

Method 2: Configuring DPM easyCipher Server to automatically trust new Agents

The manual inclusion of agents can turn out to be impractical when working with a large number of devices. In such cases, the administrator can enable the automatic trust on connected agents, which will automatically have their certificates issued and consequently appear in the trusted list. When you select *Trust all agents automatically*, any agent requesting registration will be added as a trusted device and receive a new digital certificate. After having most of your agents registered, you can review the list and we would strongly advise that you deactivate the automatic trust and deal with new registration manually.

## 10.2.3 System User Certificates

### 10.2.3.1 One-way vs. Two-way TLS

TLS protocol offers two different options when establishing a secure connection. The first is often called one-way TLS tunnel and it denotes a connection where only the server presents its credential to the client. From a TLS protocol perspective, any client can connect and further authentication is delegated to the application to handle. In the context of DPM Web Console access, it means the server presents its TLS certificate and is authenticated by the client, while user authentication is limited to the username-and-password sign in form, presented by the server.

Two-way TLS, introduces an additional level of two-factor authentication To establish a two-way TLS connection is established, the server requires its clients to provide a valid certificate in order to establish the secure connection. This process, when allied to the usual password based authentication is often regarded as a two-factor authentication support.

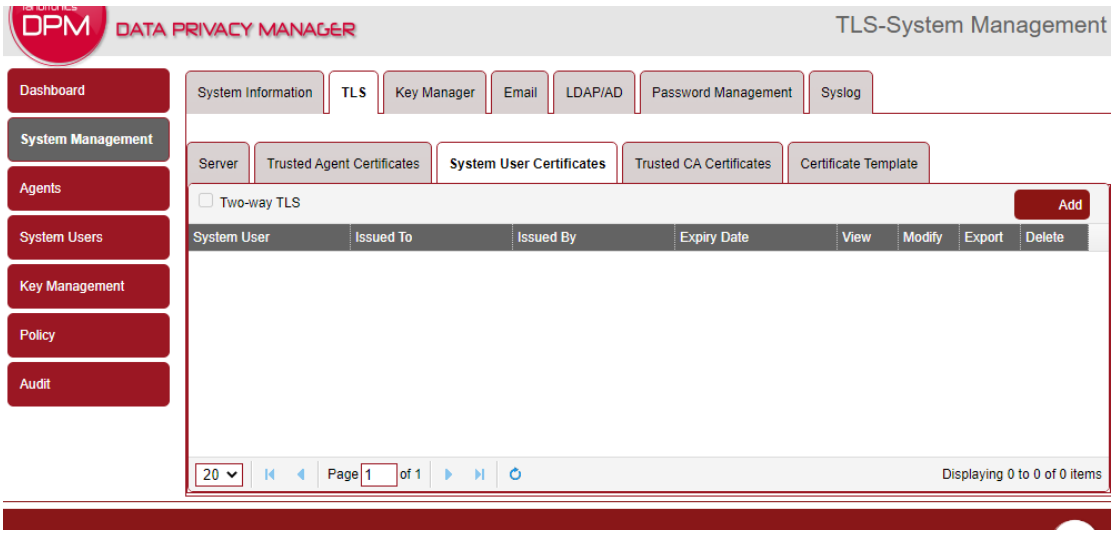
DPM easyCipher allows you to configure which degree of security you want for your web administration console sessions, providing support to single or multifactor authentication. By default, only password based authentication is required, which means the server is configured to operate in One-way TLS mode.

In order to activate Two-way TLS mode, it is paramount that all the users expected to access the management console have their own certificates, which must have been installed on the client operational environment from where connections will be originated.

### 10.2.3.2 Managing System User Certificates

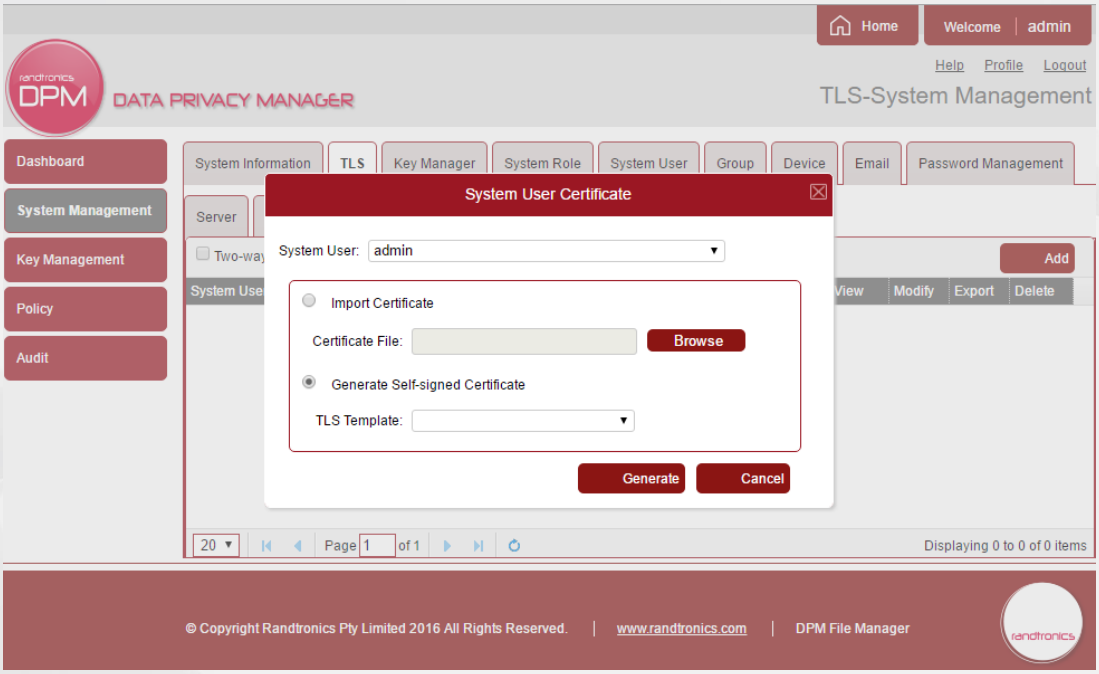
In order to manage system user certificates, you can import an external certificate or generate your own self-signed one.

To add a trusted certificate for a system user, access the tab *System User Certificates* under the *TLS* tab




Note the unchecked option *Two-way TLS* on the top-left side of the *System Users* certificate list. This is the option that activates the Two-way TLS mode. Before doing so, the first step is to add a new trusted certificate to the current user.

Click on '*Add*' button on the right-hand side of the screen to open the System User Certificate Management dialog.

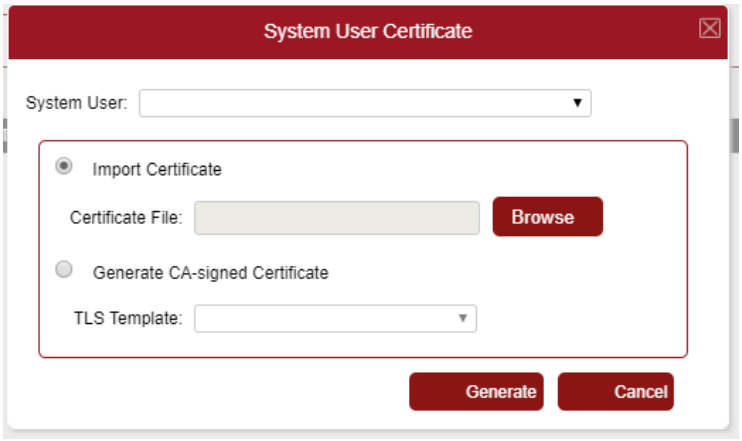



You can import a certificate file or generate a self-signed certificate.

Method 1: Import System User Certificate

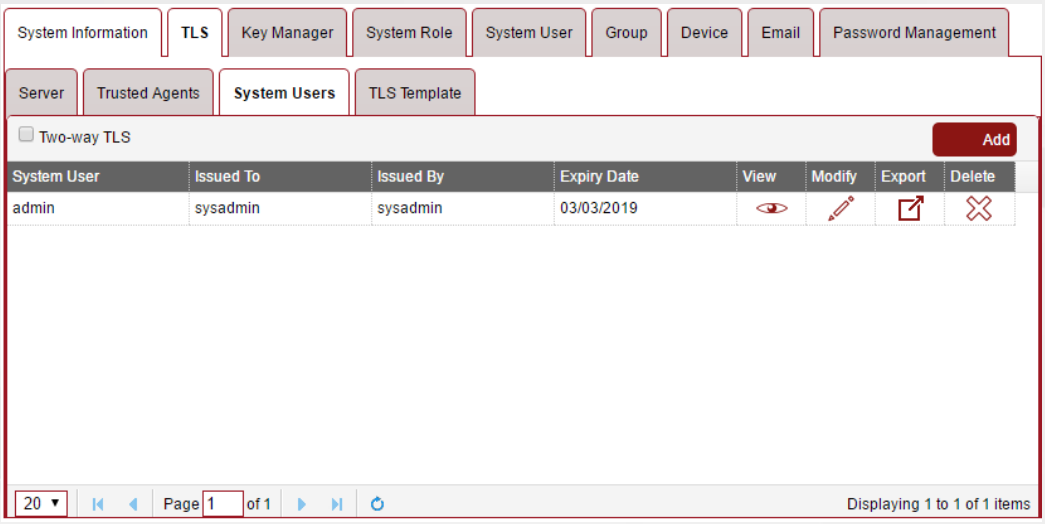
If importing a 3rd party CA signed certificates make sure you import a CA certificate first in 'Trusted CA' tab.

To add a trusted certificate for a *System User*, select the intended user and check *Import Certificate* option. The field *Certificate File* will become enabled, allowing you to select the respective certificate file from your file system. Supported formats are .cer and .crt




Having selected the certificate, click on *Import* button to finish the import process.

The dialog window will be closed and a new entry in the trusted user certificate list will be displayed.




With Two-way-TLS mode enabled, whenever the user will need their certificate in order to log in the web administration console..

Method 2: Generate a new Self-signed Certificate

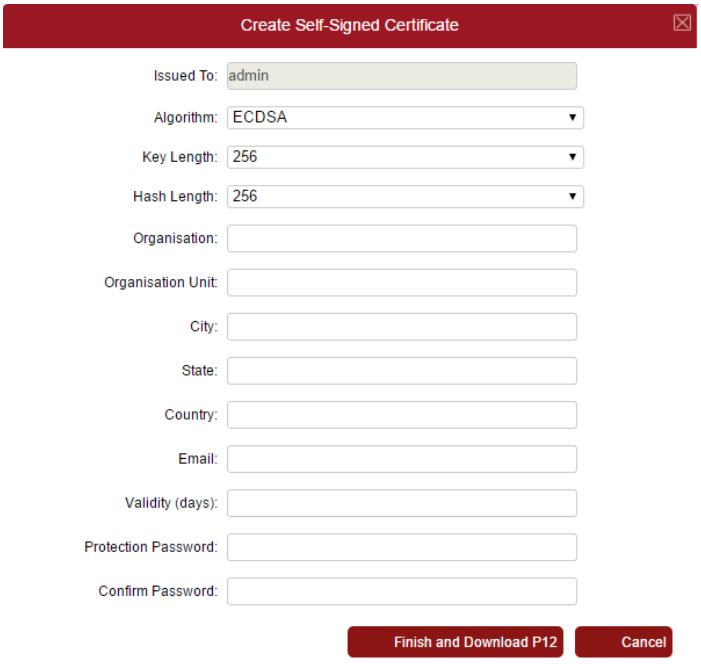
The process of generating a self-signed certificate for DPM Server follows the same steps covered during generation of server certificates.

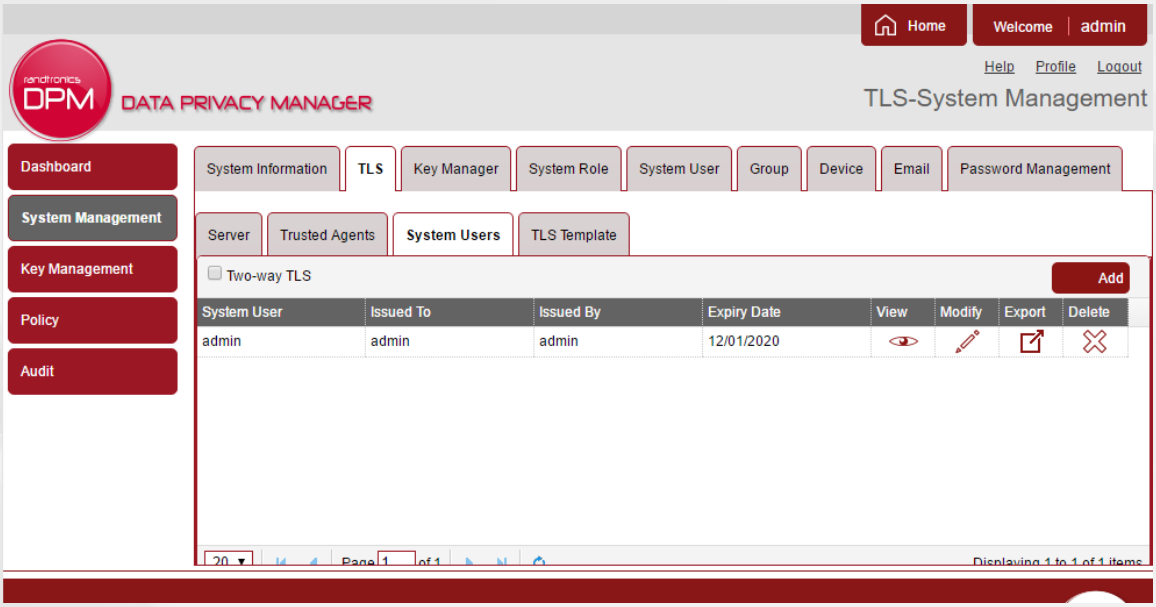
There are two slight differences

The field *Issued to,* will be automatically filled with the name of the selected user to whom the certificate will belong; and

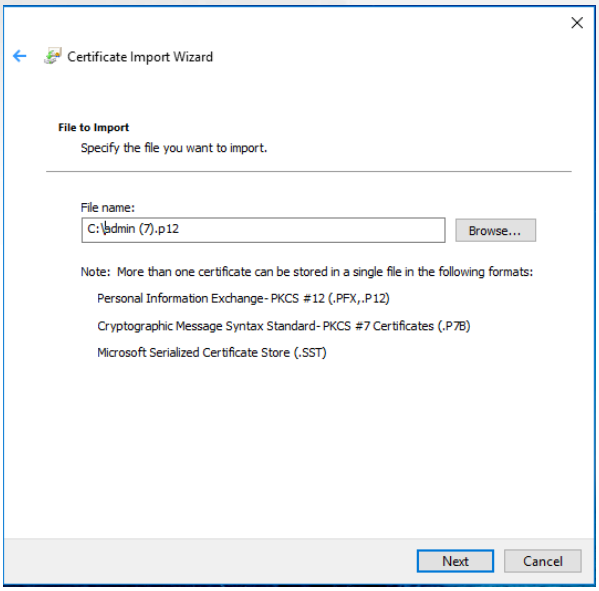
The password entered by the user when requesting the certificate will be used to protect the PKCS#12 file which the user is able todownload at the end of the process.

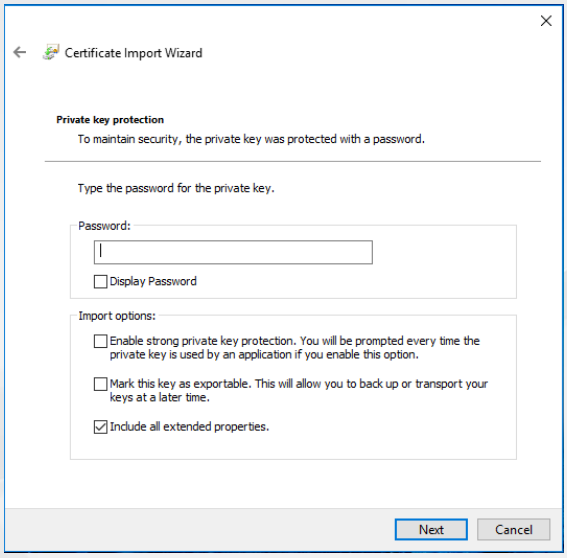
It is important to note that a particular user can only have one trusted certificate registered at a time. If you want to generate or import a different certificate to a user which already has a registered one, you need to delete that certificate from the list and add a new one.






Export the certificate to the client machine (or machines) from where the access will be originated for this particular user and double-click the .P12 file. An import dialog will be prompted and you will be required to enter the password used to protect your credentials.

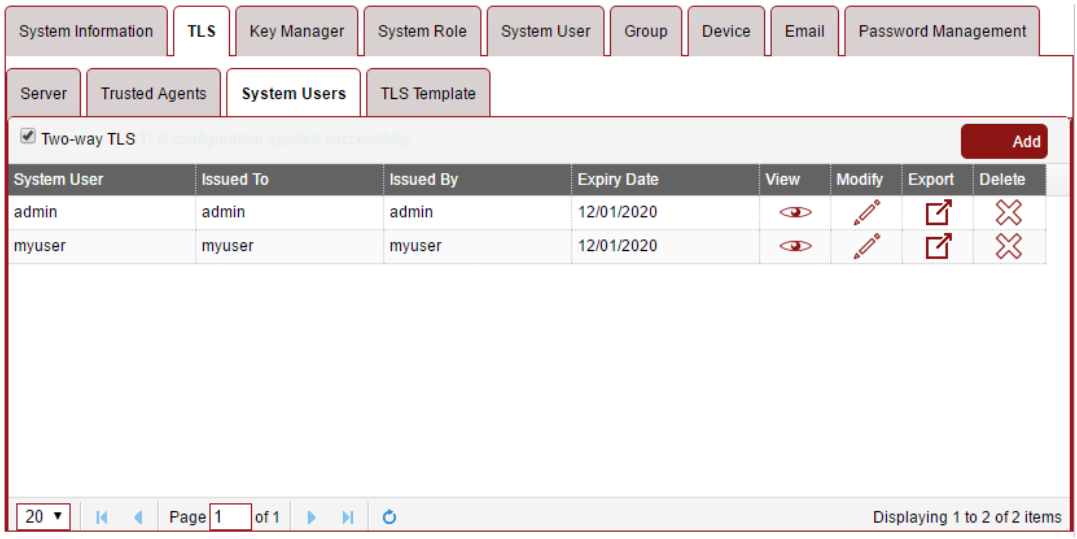




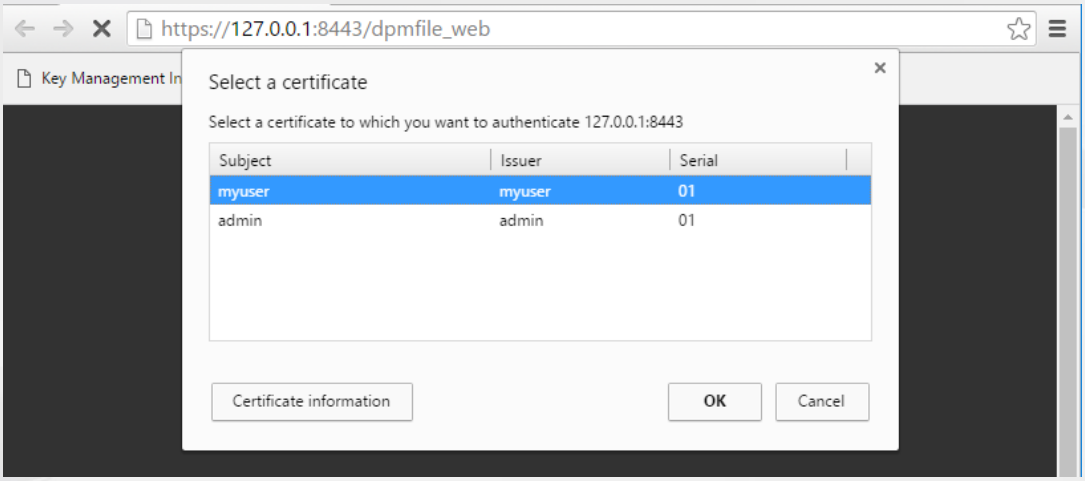

> ***Note for Firefox and Linux users:***
>
> ***Linux users and Firefox on Windows users will need to import the PKCS#12 file directly to the browser certificate store. This is due to the fact that Firefox keeps its own internal certificate storage, which is the default storage for the major browsers running on Linux platform.***

### 10.2.3.3 Activating Two-way TLS mode

With your users properly registered as trusted certificate holders and with their digital certificates imported on their client machines, you can safely turn on the Two-way TLS feature. After activation of the feature, only machines where a trusted certificate has been installed will be allowed access to the system, so prefer using one of these machines when activating this feature. Check the option Two-way TLS on the tab System Users Certificates. A restart of the web console service will be required. Log out the Web Console and restart the service.




After the web console has been restarted, access the web console again and you will be required to provide a digital certificate. If your certificate store contains only the certificate trusted by DPM easyCipher, it will be automatically used and you will see the login window immediately. If you have other certificates installed (belonging to other users, for example), you will have to select one of them to proceed. If that is the case, select which user you want to log in as and click Ok.




You will be prompted for a second factor password based authentication, which will have to match the user associated to the selected certificate. Passing the two-factor authentication steps, you will finally be granted access to the web console.

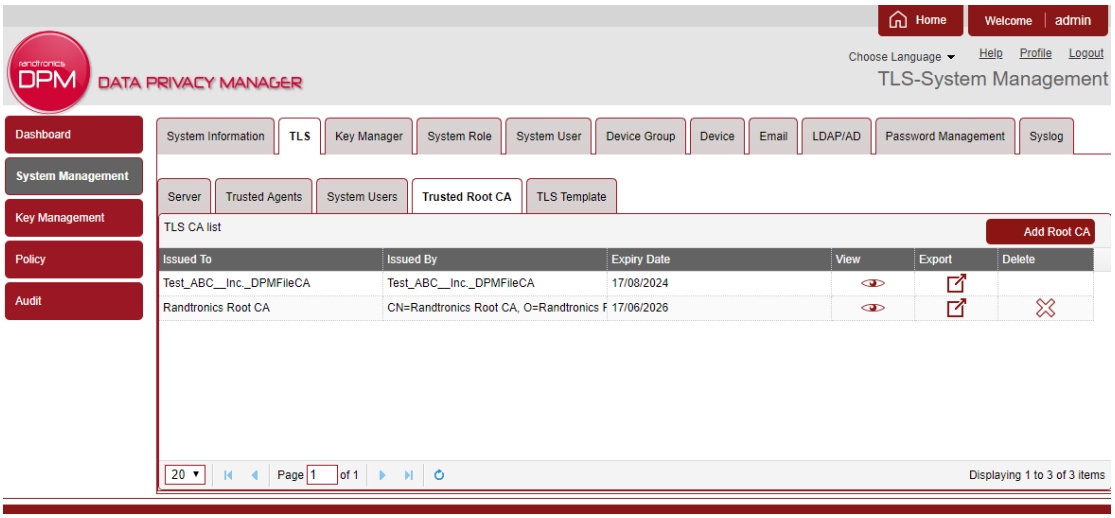
## 10.2.4 Trusted Root CA

If 3rd party certificates are to be used with DPM easyCipher a corresponding CA certificate will need to be imported into the solution so that the trust chain can be verified. If a certificate chain consists of two or more CAs then all CA certificates need to be imported.

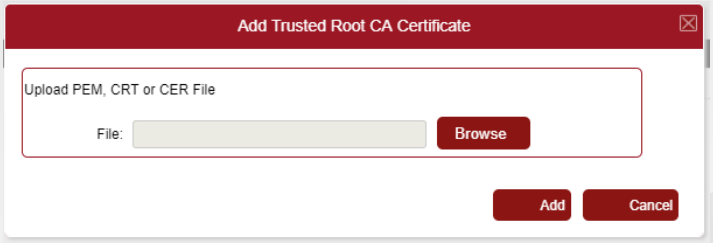
However, if all certificates that are used for agents, server or system users are self-signed then there is no need to import them into 'Trusted Root CA'.

To import a CA certificate:

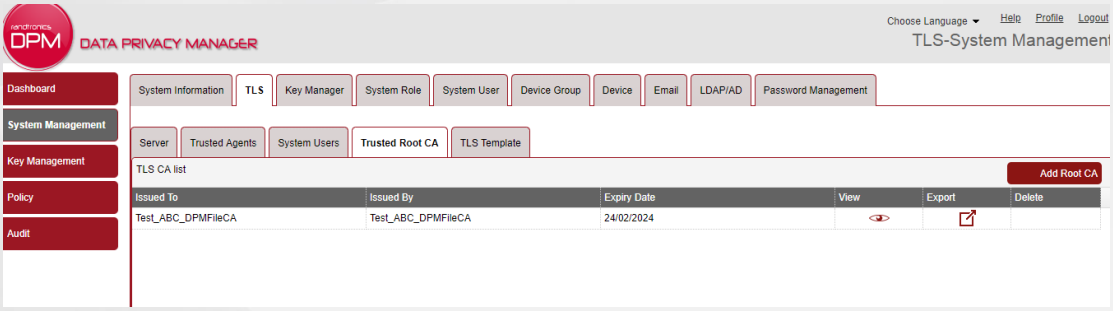
1. Navigate to 'System Management' – 'TLS' – 'Trusted Root CA'




2. Click 'Add Root CA'. 'Add Trusted Root CA Certificate' dialog will appear.




3. Browse to a file with CA certificate by clicking ‘Browse’. Supported formats: .pem, .cer, .crt.
4. Click ‘Add’
5. A CA certificate will appear in the list.

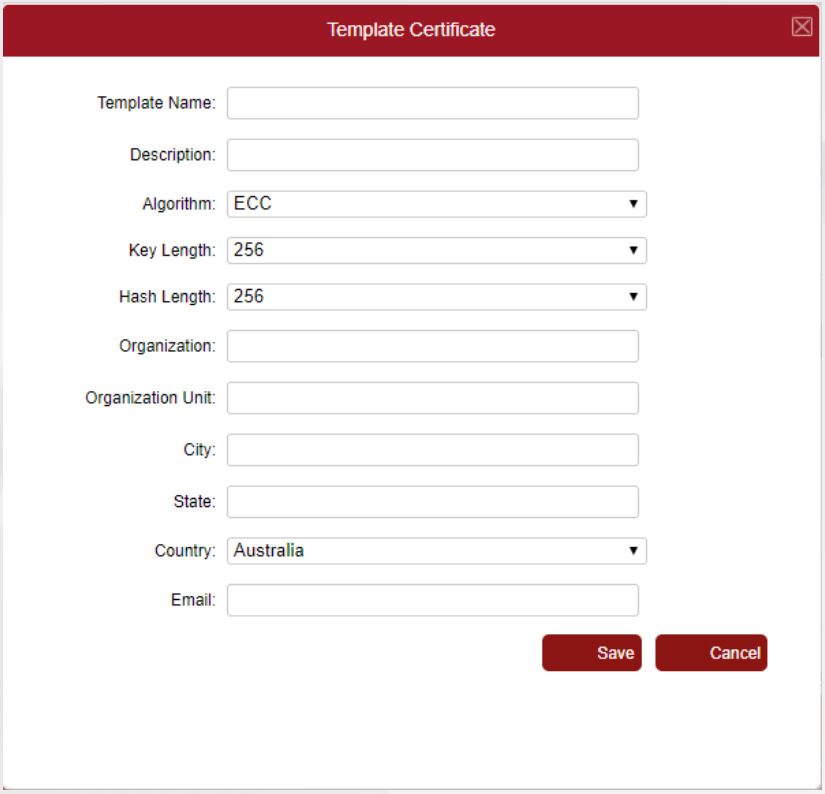



Once CA certificate is uploaded, you can upload agents, system user or server certificates in the corresponding tabs.

## 10.2.5 Certificate template

You can create a template that can be used during creation of self-signed and CA-signed certificates.

1. Login with ‘System Management’ rights and navigate to ‘System Management’-‘TLS’-‘Certificate Template’.
2. Click ‘Add’
3. Provide details for the template:




- Template name - name for this template
- Description – description of this template
- Algorithm – Select RSA or ECC
- Key Length – for RSA: 2048, 3072, 4096; for ECC: 256, 384
- Hash Length – for RSA: 256, 384; for ECC-256: 256; for ECC-384: 384
- Organization – company name
- Organization unit – organization unit of the company
- City – location of the company
- State – name of the state
- Country – Country selected from the list
- Email – email address

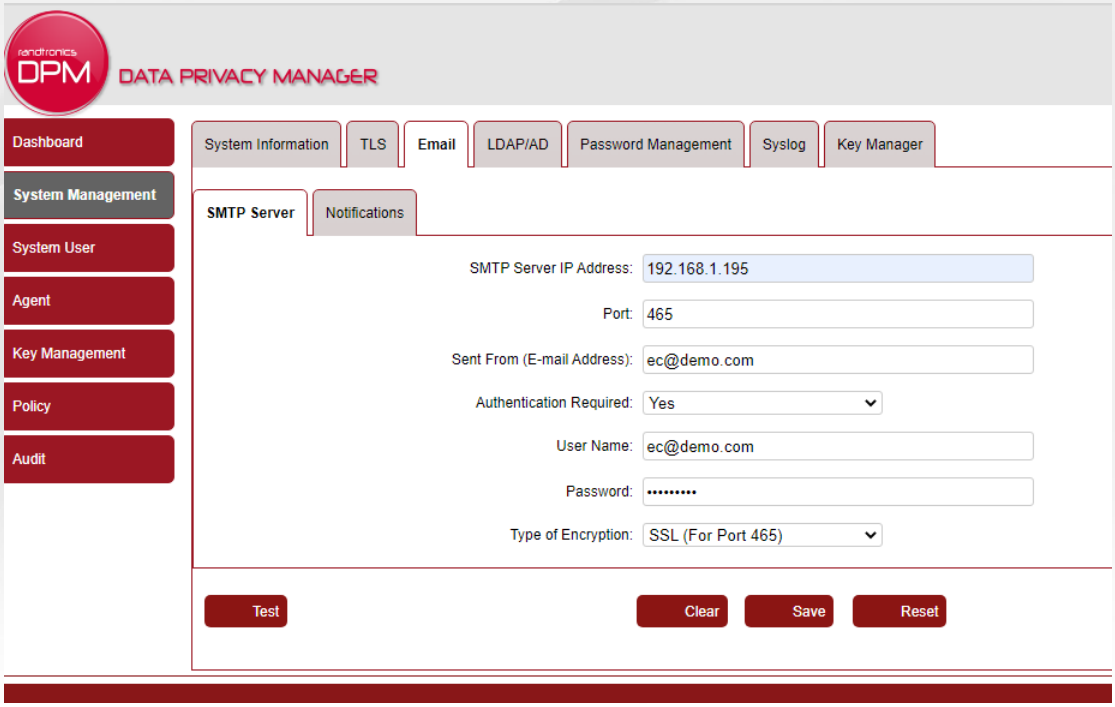
Only ‘Template name’ is mandatory.

## 10.3 Email tab

The Email tab allows the configuration of email SMTP server. This enables the DPM easyCipher software to send emails and notifications.

Emails are also sent when a user has forgotten their password and the password reset instructions are sent to them.

### 10.3.1 SMTP Server



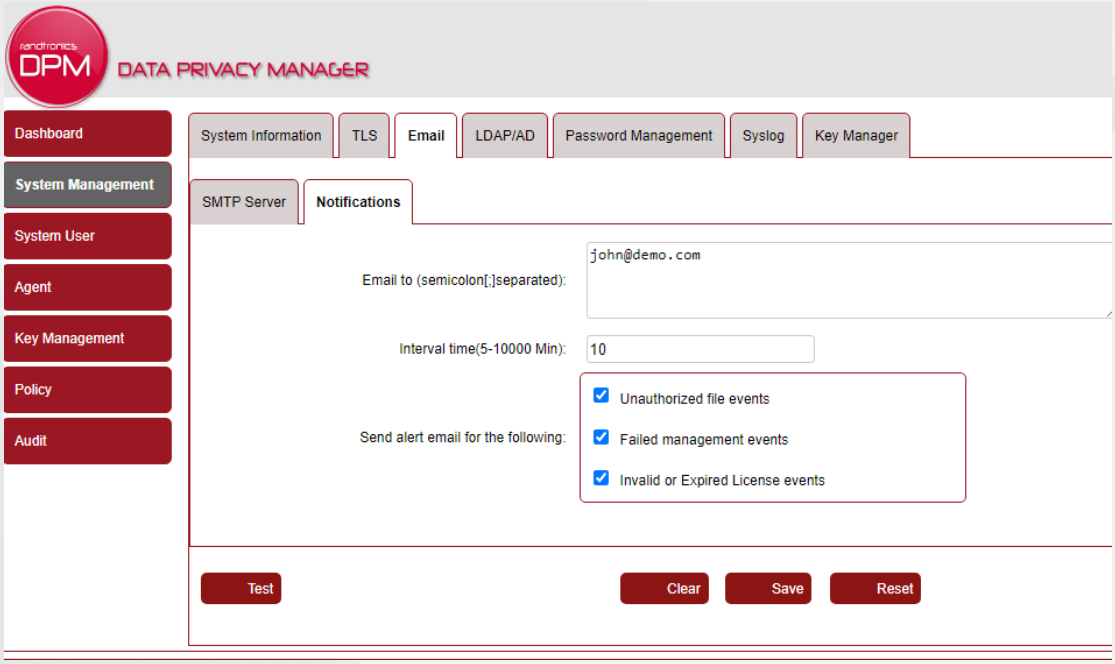

The SMTP Server tab has the following fields:

- **SMTP Server IP Address** – the IP address or hostname of the SMTP email server
- **Port** – the port to access the SMTP port on. The default port for SMTP is 25, 465 (SSL), or 587 (TLS)
- **Send From (Email Address)** – the "from" address to use when sending an email. Some email services require 'Send from' to be the same as the username. Check with your email provider.
- **Authentication required** – whether or not to use username/password authentication when logging into the SMTP server (this depends on SMTP provider)
- **Username** – the username to use if Authentication Required is set to Yes
- **Password** – the password to use if Authentication Required is set to Yes
- **Type of Encryption** – Default (no encryption), TLS, SSL

Click on the 'Save' button to save the changes.

When 'Test' is clicked, easyCipher will send a test email to the email of the currently logged in user. If an email is not set for the user it will send an test email to the account which is configured in 'Send From'.

## 10.3.2 Notifications



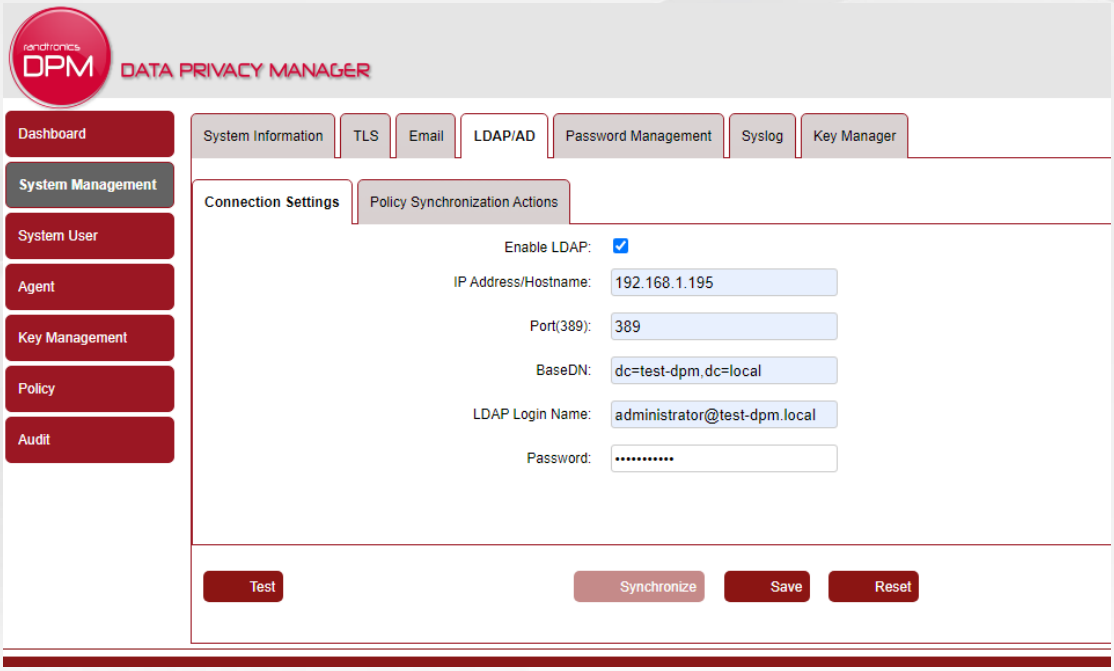

Email notifications can be sent to an email about unauthorised file events, failed management events or license expiry on schedule.

To receive notifications filled in the following details.

- **Email to (semicolon[;]separated):** - email addresses of users to receive notifications. If multiple addresses are entered they should be separated by a semicolon. For example, john@test.com;mary@test.com
- **Interval time(1-10000 Min):** - how often check notifications and send out emails. For example, 60 – every 60 minutes. If there are no notifications in a queue then nothing will be sent out.
- Send alert email for the following:
    - **Unauthorized file events** - tick if want to receive a list of unauthorized file events
    - **Failed management events** – tick if want to receive a list of failed management events from Web Console
    - **Invalid or Expired License events –** tick if you want to receive a license expiry notification or license invalidation notification. A license is checked on startup and at 12am every day. If a license validity period is less than 60 days a notification will be sent out on start up. If a license is invalid on startup a notification will be sent out.

## 10.4 LDAP/AD tab

The LDAP/AD tab allows to configure connection settings to LDAP/AD server for user/role import and synchronization. Currently only Microsoft Active Directory is supported. If using DPM easyCloudPlus the AD must have public IP address to be accessible from the manager.




The LDAP/AD tab has the following fields:

Connection Settings:

**Enable LDAP** – enable or disable use of LDAP/AD.

**IP Address/Hostname**– IP address or a host name for LDAP/AD server

**Port** – connection port. Default port for LDAP – 389. LDAPS is not supported.

**LDAP Login Name** – login user name for connection in a form of user@domain.com

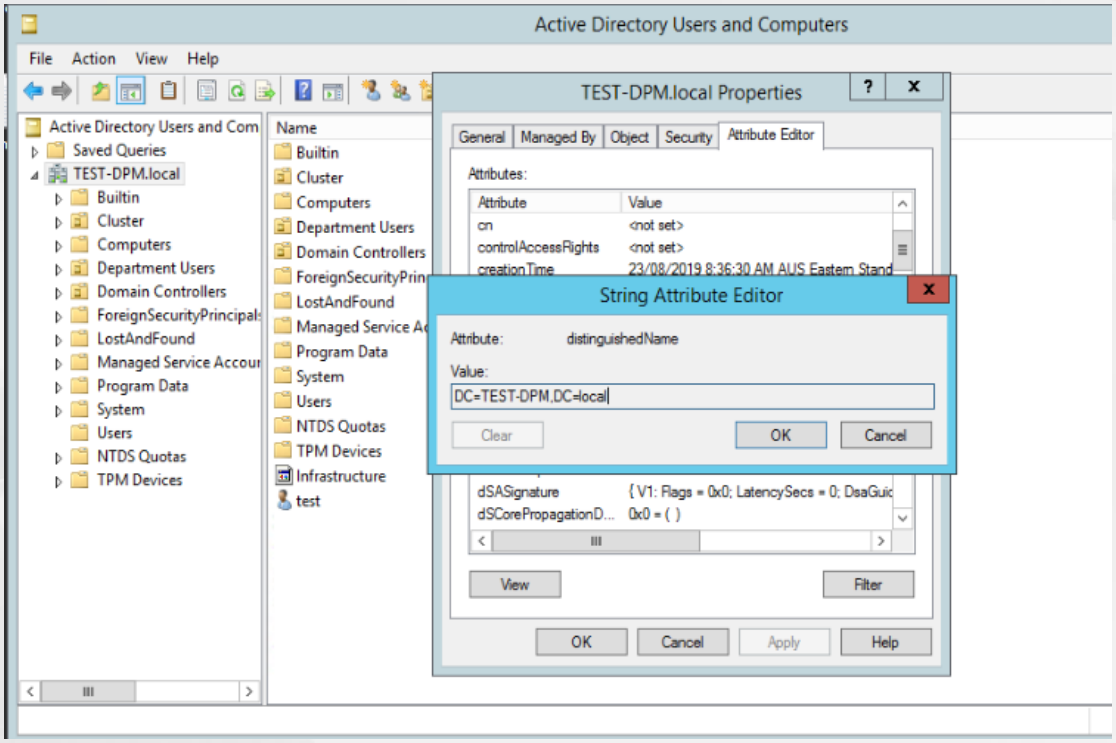
**Password** – password for the above user

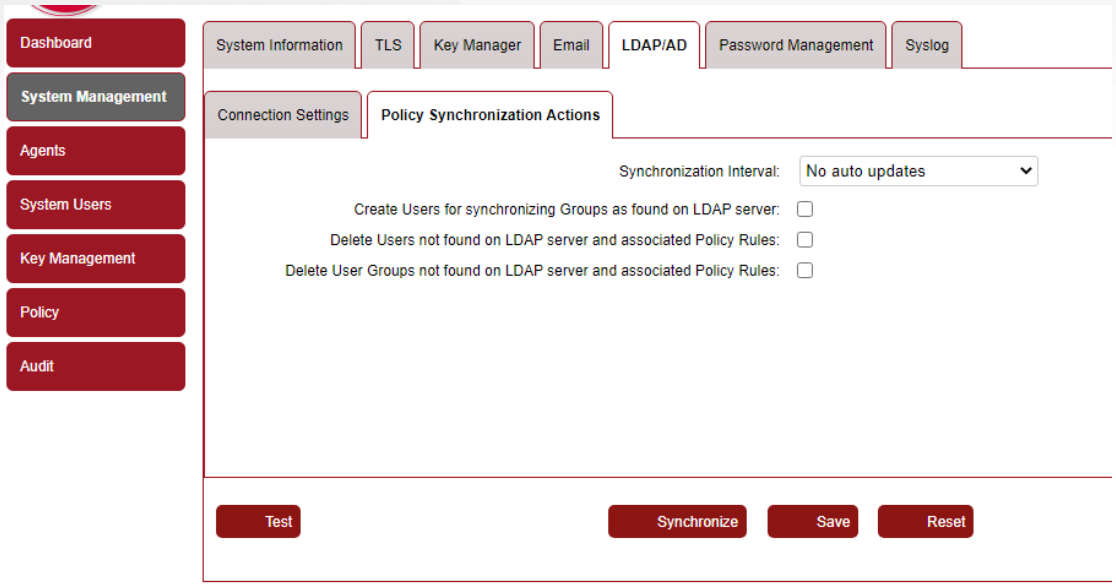
**BaseDN** – base distinguished name for connection. Example: DC=TEST-DPM, DC=local

To find BaseDN of the organisation unit you want to connect to, open 'Active Directory Users and Computers'. Make sure that 'View'-'Advanced Features' is ticked on.

Right-click on the domain name you would like to point, select 'Properties' and open 'Attribute Editor'.

Copy a value from 'distinguishedName' and paste it into 'BaseDN' of the DPM easyCipher LDAP/AD configurations.




Policy Synchronization Actions:

DPM easyCipher can automatically synchronize policy users and roles with Active Directory. If a policy role is imported from Active Directory all users from the role can be added and deleted automatically from DPM if desired. This ensures that the policy which is applied to a protected folder is updated with the correct user list.

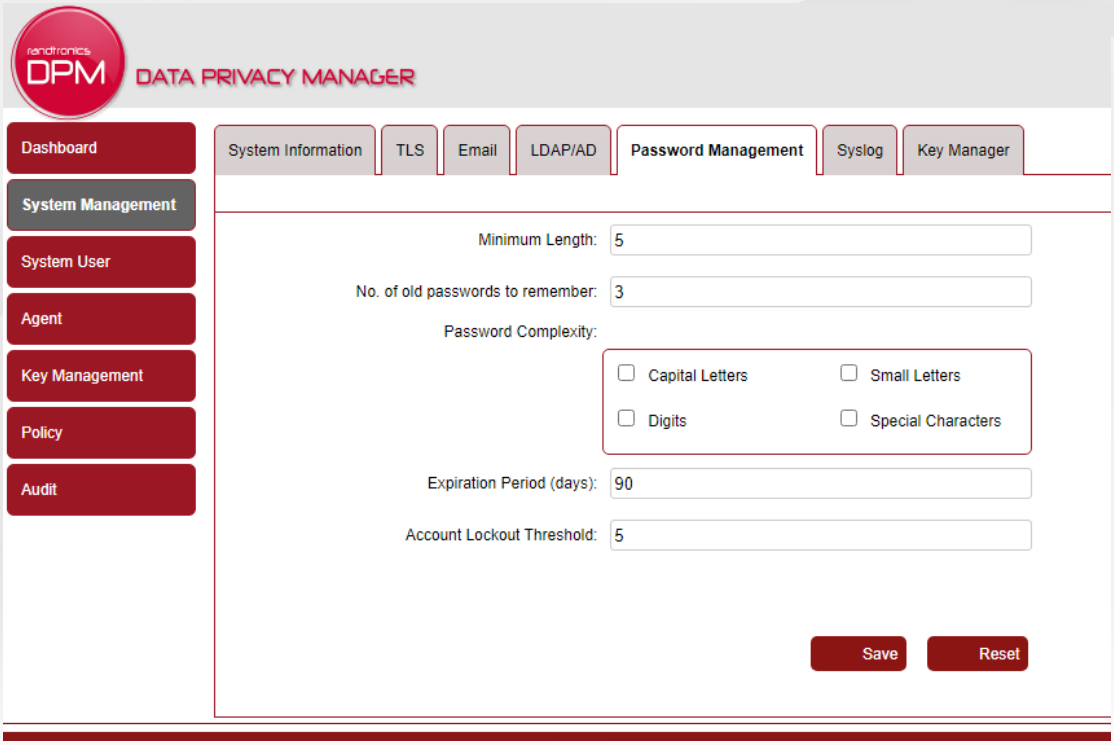
- **Synchronization Interval** – automatic synchronization interval (No auto updates, 15 min, 30 min, 1 hour, 2 hours, 3 hours, 12 hours, 24 hours). Synchronization will be performed based on 'Synchronization Actions' configurations.
- **Create users for synchronizing Groups as found on LDAP server** - If there are any users that have not been imported from LDAP/AD or users that have been created since last synchronization, they will be

automatically imported into the Policy User list. If there is any policy that exists for the imported role, it will be updated with the new users and distributed to the Agents. Only applied to the roles that are already imported to DPM.

- **Delete Users not found on LDAP server and associated Policy Rules** – if imported users have been deleted from LDAP/AD, they will be removed from the Policy user list. If there is any policy that exists for the deleted users, it will be automatically updated (the user policy rule will be deleted) and distributed to the Agents.
- **Delete User Groups not found on LDAP server and associated Policy Rules** – if imported Policy User Group was deleted from the LDAP/AD server, it will be deleted from the DPM easyCipher Policy User Group list. All users from the group will be removed from the user group but they will not be deleted from the User list. If there is any policy that exists for the deleted group, that policy will be modified automatically (the role rule will be deleted) and distributed to the Agents.

## 10.5 Password Management tab

The Password Management tab allows to set the password guidelines. Password guidelines are applied only to local system users.



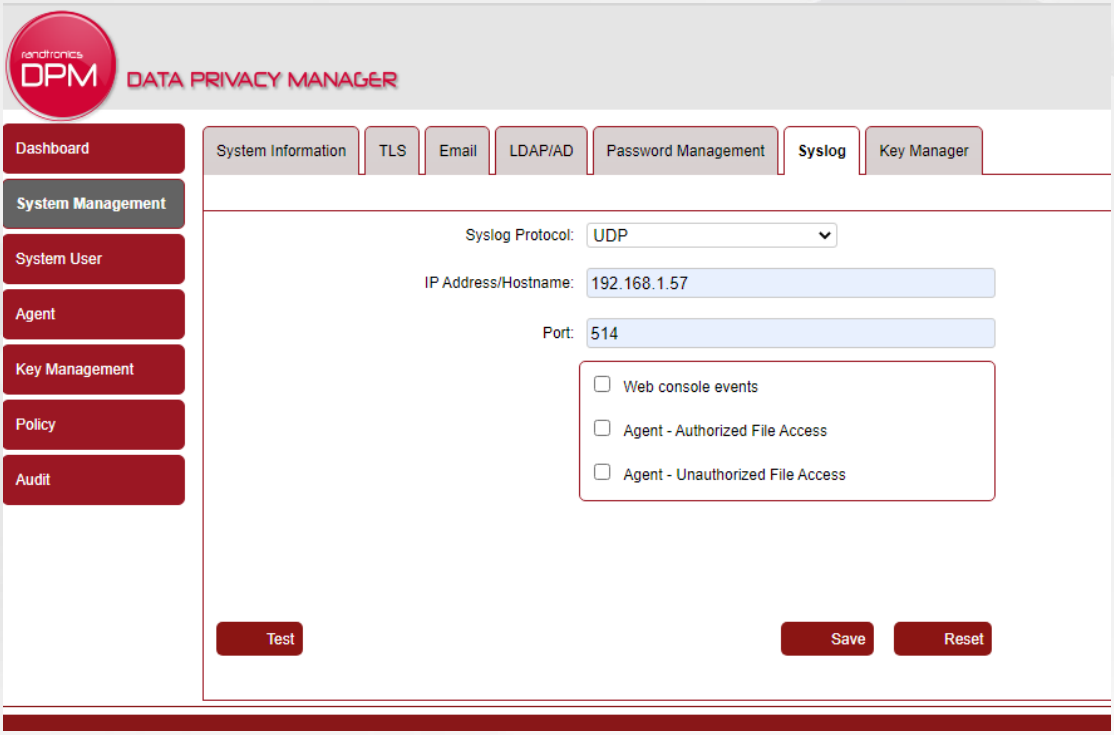

The Password Management tab has the following fields:

- **Minimum Length** – the minimum number of characters of the password
- **No of old passwords to remember** – the maximum number of old passwords to remember. When the user changes their password, they may not reuse an old password that has been remembered
- **Password complexity** – the mix of letters, digits and special characters must use in their passwords
- **Expiration Period (days) -** The number of days for the password changes to be required
- **Account Lockout Threshold** – the maximum number of attempts to login before the account will be locked for 1 hour

Click on the 'Save' button to save the changes

## 10.6 Syslog Tab

The Syslog tab allows to configure DPM easyCipher to send all audit events to a syslog server (SIEM) using SYSLOG protocol.




The Syslog tab has the following fields:

- Syslog Protocol – TCP or UDP
- **IP address/Hostname** – IP address or hostname of a syslog server
- **Port** – syslog server port. Default port for UDP is 514
- **Web console events** - Tick if want to forward all system management events from Web Console
- **Agent – Authorized File Access** – Tick if want to forward all authorized file access events reported by agents
- **Agent – Unauthorized File Access** – Tick if want to forward all unauthorized file access events reported by agents

Click on the 'Save' button to save the changes

## 10.7 Key Manager tab

Key Manager tab allows to select whether to use an internal Key Manager module within the DPM easyCipher or an External DPM easyKey for key generation and protection. By default, an internal Key Manager module is used.

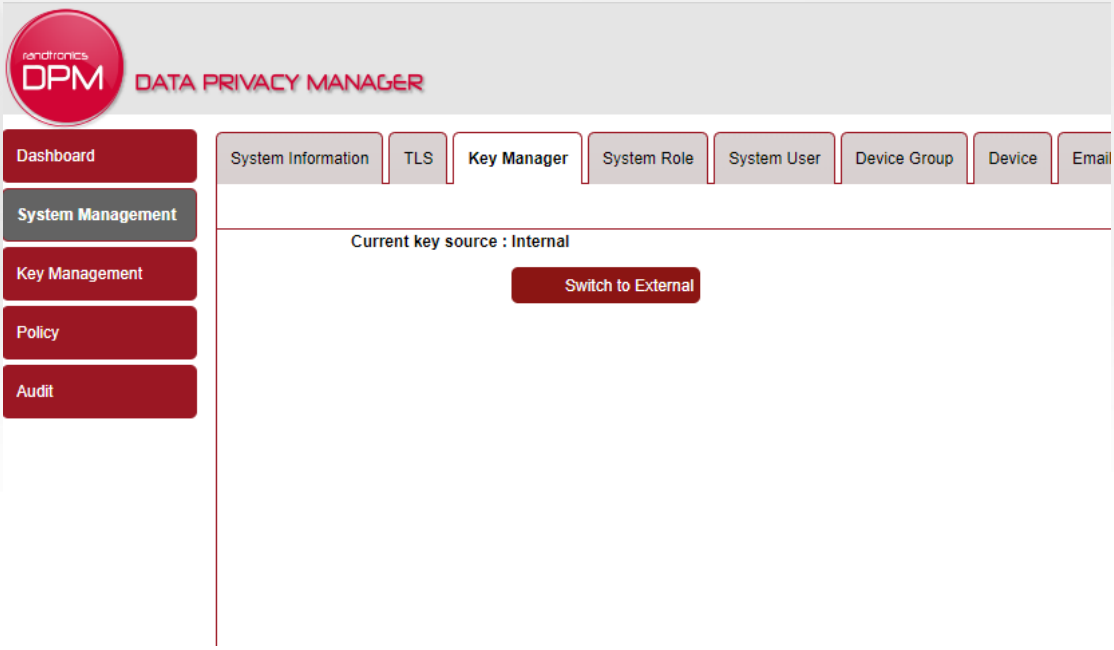
### 10.7.1 Use External Key Manager

DPM easyCipher can use an external DPM easyKey for key generation.

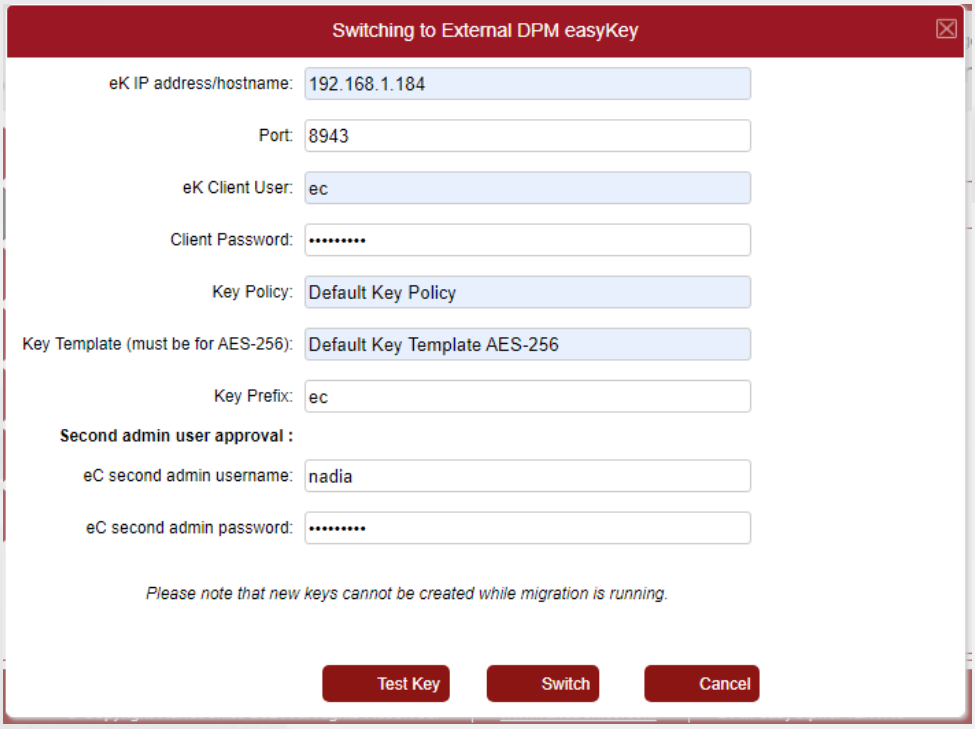
To switch from an internal Key Manager to an external DPM easyKey a second system user with system management permissions is required to enter their login and password.

Before switching to use an external DPM easyKey, you need to configure a client username/password in DPM easyKey, and assign the client to an existing policy in DPM easyKey. AES-256 key template must exist in the key policy.

1. Navigate to 'System Management->Key Manager' .




2. Click 'Switch to External"




3. Enter the following details

- **IP address/hostname** – IP address or hostname of DPM easyKey. DPM easyCloudPlus details are as provided by Randtronics.
- **Port** – KMIP connection port of DPM easyKey (default is 8943). If using DPM easyCloudPlus then use port provided by Randtronics
- **Username** – client name configured in DPM easyKey
- **Password** – client password configured in DPM easyKey
- **Policy Name** – Key policy name configured in DPM easyKey
- **Template Name** – Key template name configured in DPM easyKey (must be for AES-256)
- **Key prefix** – this is to differentiate keys created by this easyCipher system. Key prefix is appended to the key name when the key is created in DPM easyKey. A key prefix must be unique within a given DPM easyKey. If switching to and from external DPM easyKey several times, the same key prefix cannot be used again. Do not use '-' in the key prefix.
- **Second Admin User name:** user name of another easyCipher system user with System Management permissions
- **Second Admin password:** password of the second user

4. Click 'Test Key' to test creation of a dummy key in the DPM easyKey to verify provided configurations.
5. Click 'Switch' to switch to use an external easyKey.

After switching all existing keys will be registered within DPM easyKey and local keys will re-encrypted using the newly created External Key Encrypting Key.

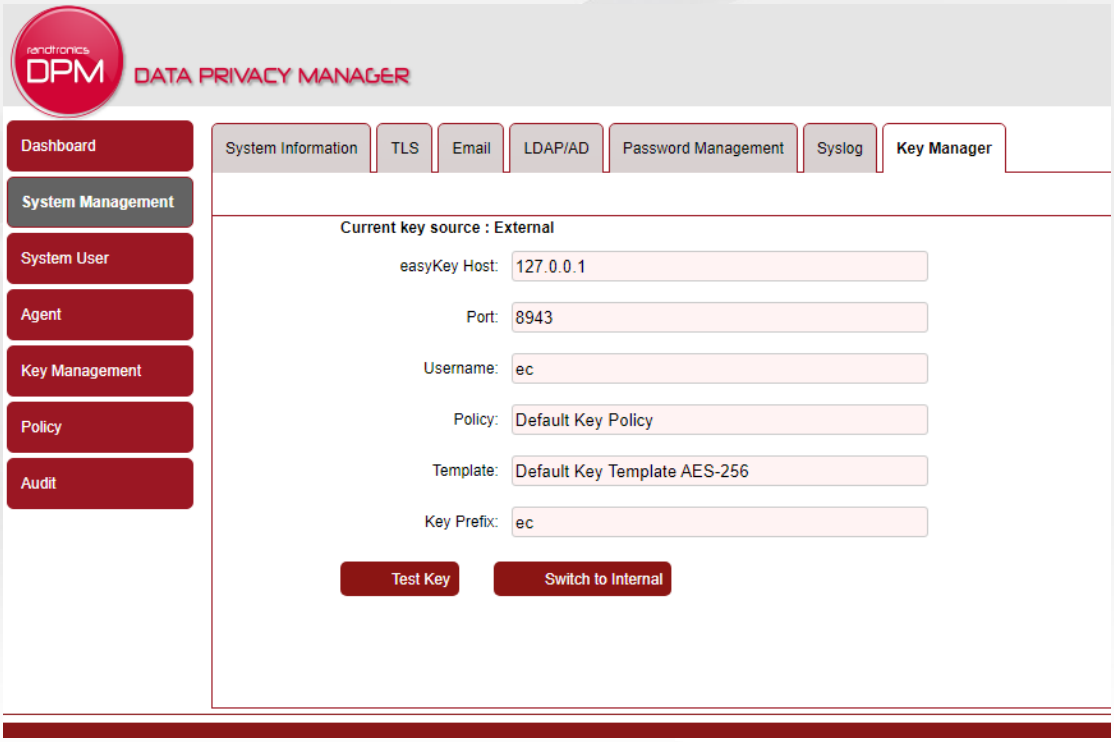
All new keys will be generated by the external easyKey (by software or HSM) based on the policy.

## 10.7.2 Use Internal Key Manager

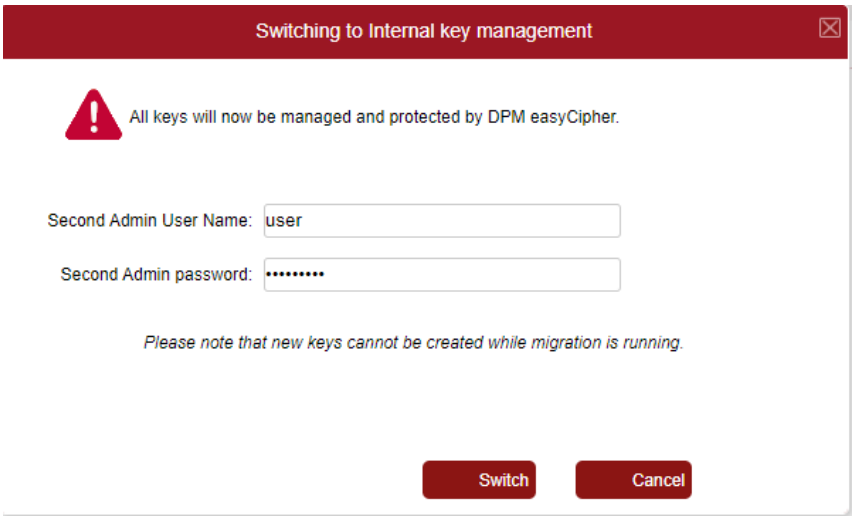
Internal Key Manager is used by default.

However, if it is already switched to use an external Key Manager and you would like to switch from an external Key Manager to an internal it can be done in 'System Management – Key Manager screen'. A second system user with system management permissions is required to enter their login and password as well.

1. Navigate to 'System Management->Key Manager'




2. Click 'Switch to Internal'




3. Another easyCipher system user with 'System Management' permissions needs to provide their credentials.

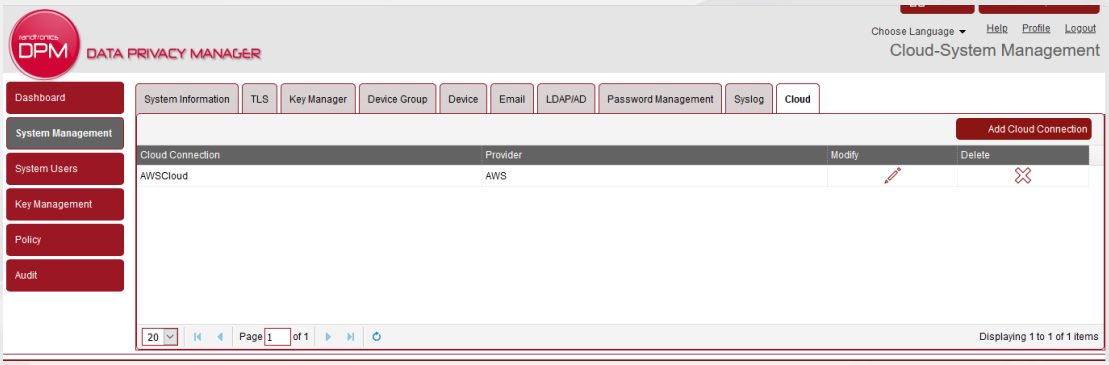
Click 'Switch'.

After switching all existing keys will be re-encrypted using the Internal Key Encrypting Key.

All new keys will be generated by the internal key management module.

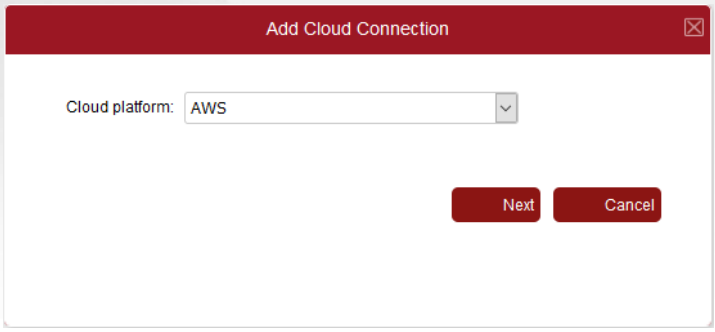
## 10.8 Cloud Tab (Cloud license only)

The Cloud tab allows to configure DPM easyCipher to connect to various cloud providers to fetch information about target AWS instances. Currently only AWS is supported.

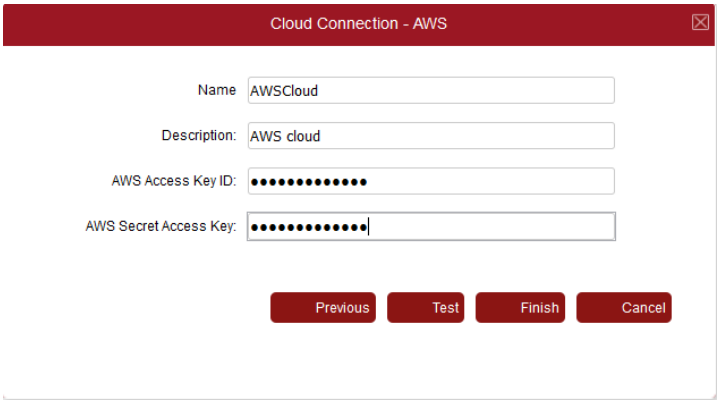



### 10.8.1 Add Cloud Connection

To add Cloud Connection, clicking button “Add Cloud Connection”




Select cloud type “AWS” from drop list “Cloud platform” list, then click “Next” button to input connection parameters for AWS cloud platform.




Click “Previous” button will go back previous config windows;

Click “Test” button will test if the parameters are correct;

Click “Finish” button will save one Cloud Connection object with provided parameters;

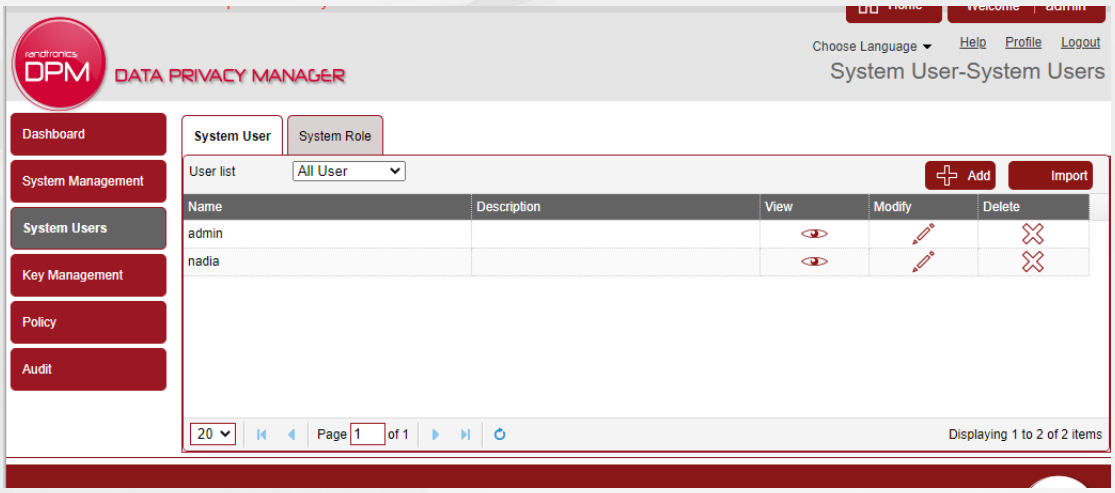
Click “Cancel” button will destroy all parameters and exit.

# 11. System Users

## 11.1 System User tab

System Users are users who are able to log into the DPM easyCipher and administer the DPM easyCipher system.

The System User tab allows new system users to be created, viewed, modified and deleted. To get to the page, click on the 'System Users' menu, then click on the 'System User' tab.

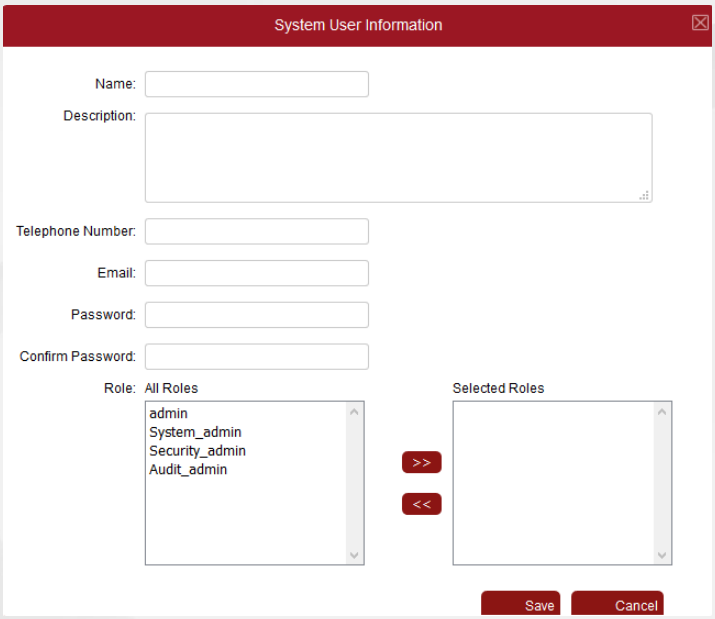



There are two ways of adding new System Users:

- Local Users – users created by the DPM easyCipher.
- AD/LDAP Users – users that have been imported from Active Directory or LDAP.

### 11.1.1 Add a new System User

Add a new User by pressing 'Add' button. This process will create a new local user.




Enter the new system user information:

- **Name** – the name of the system user (this is the username they will use to log into the DPM easyCipher)
- **Description** – a brief description of the user (optional)
- **Telephone number** – the users phone contact details (optional)
- **Email** – the users email contact details. Email is used when a user has forgotten their password and the password reset details are sent to them. (optional)
- **Password** – the user password to login to the Manager
- **Confirm Password** – re-enter the user password
- **Role** – the roles that the user will be part of. If user does not have role, they will not be able to login to the system.

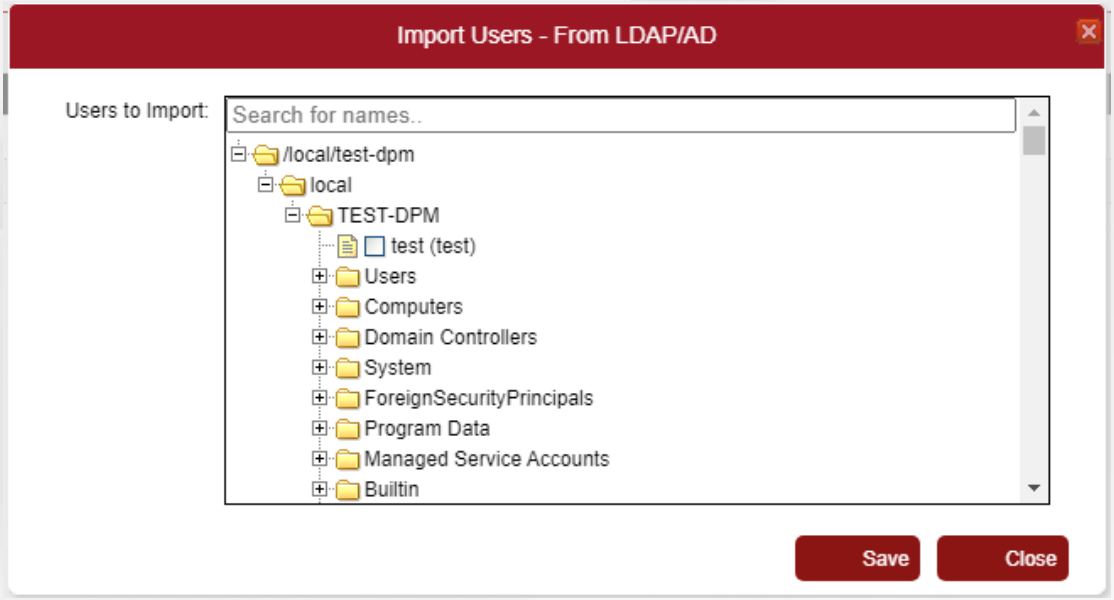
Click 'Save' to create the new user

### 11.1.2 Import new System Users from Active Directory

It is possible to import system users from Active Directory.

To be able to import from AD, LDAP/AD server configurations must be preconfigured in 'System Management – LDAP/AD'. Please refer to the sections above about configurations.

To start the import process, click the 'Import' button.




Tick the boxes next to the usernames to import into DPM easyCipher, then click on the '**OK'** button.

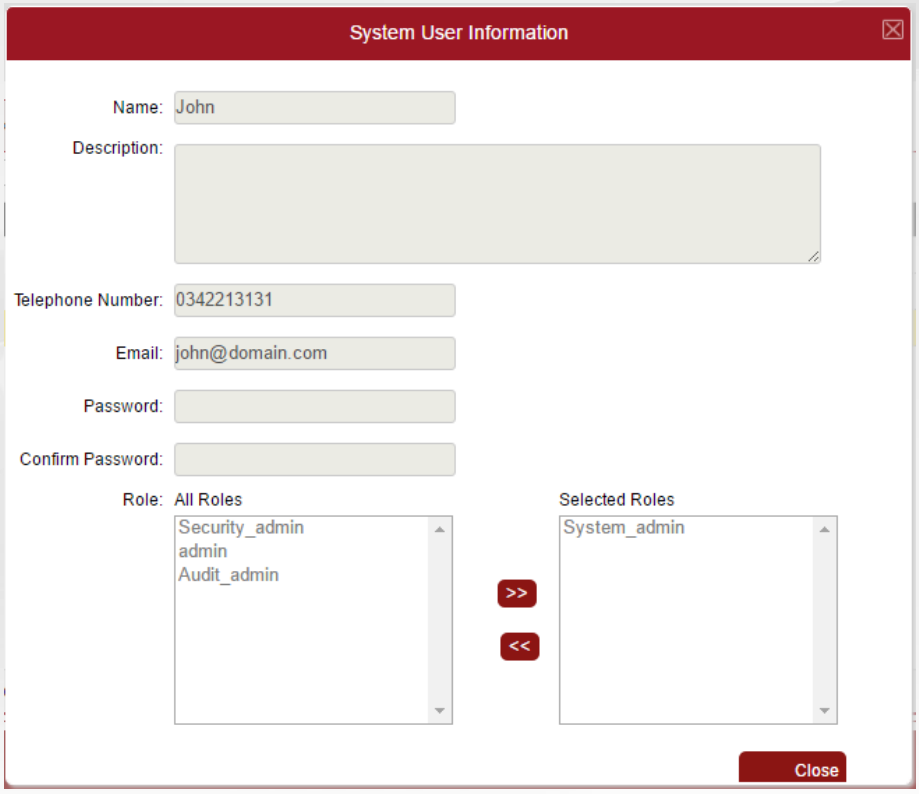
You can search for a user by entering 3 or more characters in 'Search or names…' field.

After importing system users, a system role needs to be assigned to the user so that the user can managed DPM easyCipher. A user can login to the management console using their AD/LDAP password.

Please note that already imported users will not be displayed in the list.

### 11.1.3 View existing System User

To view properties of an existing System User, click on 'View' icon of the target user.




### 11.1.4 Modify existing System User

To modify properties of an existing System User, click on 'Modify' icon of the target user.

You can modify all properties of the System User except Name. If you need to change the user name then delete the user and create a new one.

You can modify membership of the user (a role) by moving them from the right Selected Roles list to the left or from the left All Roles to the right.

### 11.1.5 Delete an existing System User

To delete an existing System User, click on 'Delete' icon of the target user. You cannot delete your own user or the last user with a System User permission.

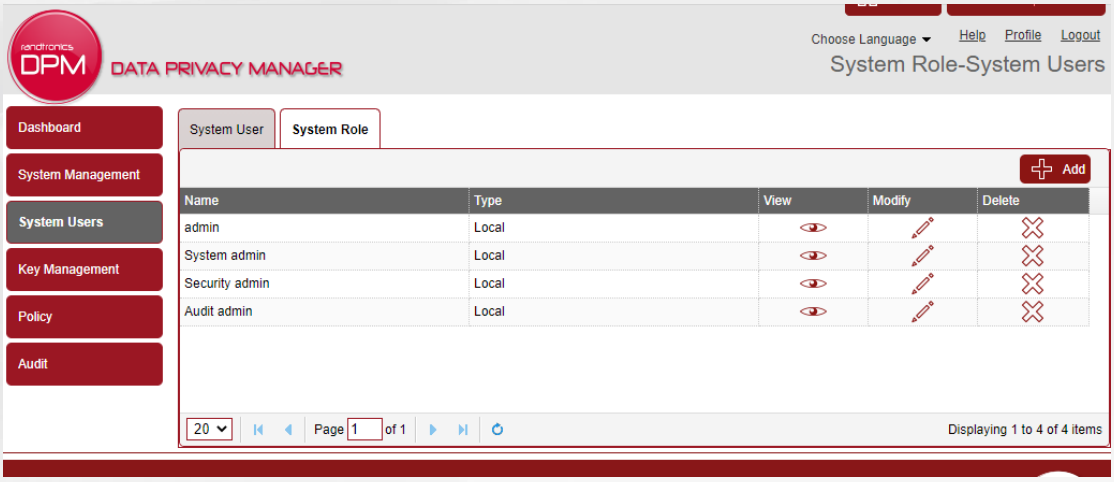
## 11.2 System Role

System Role offers a way to group system users into groups to implement separation of duties within the management system. System users are users who are able to login into the DPM easyCipher to administer the DPM easyCipher software.

The System Role tab allows System Roles to be created, viewed, modified and deleted.

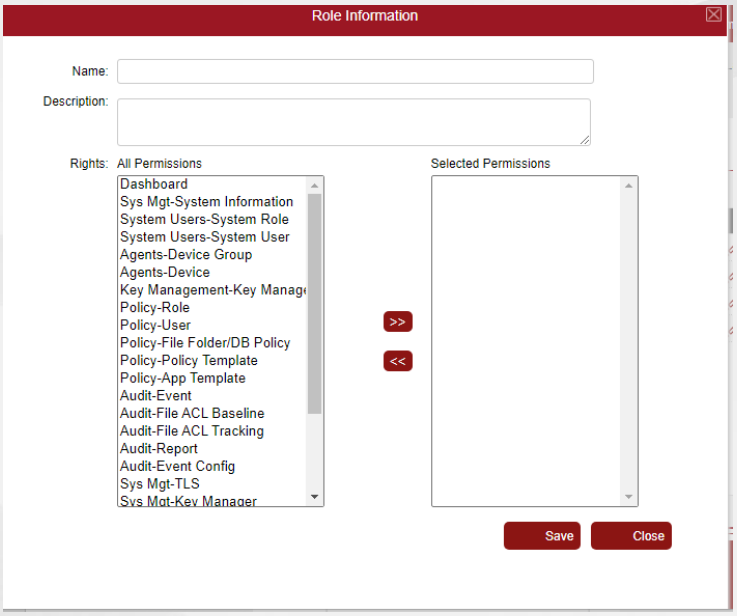
System Role defines permissions for accessing various areas of Web console.

To view the System Roles, click on the 'System Management' button in the left hand menu, then click the 'System Role' tab.



### 11.2.1 Add a new System Role

Add a system role by pressing the “Add” button:



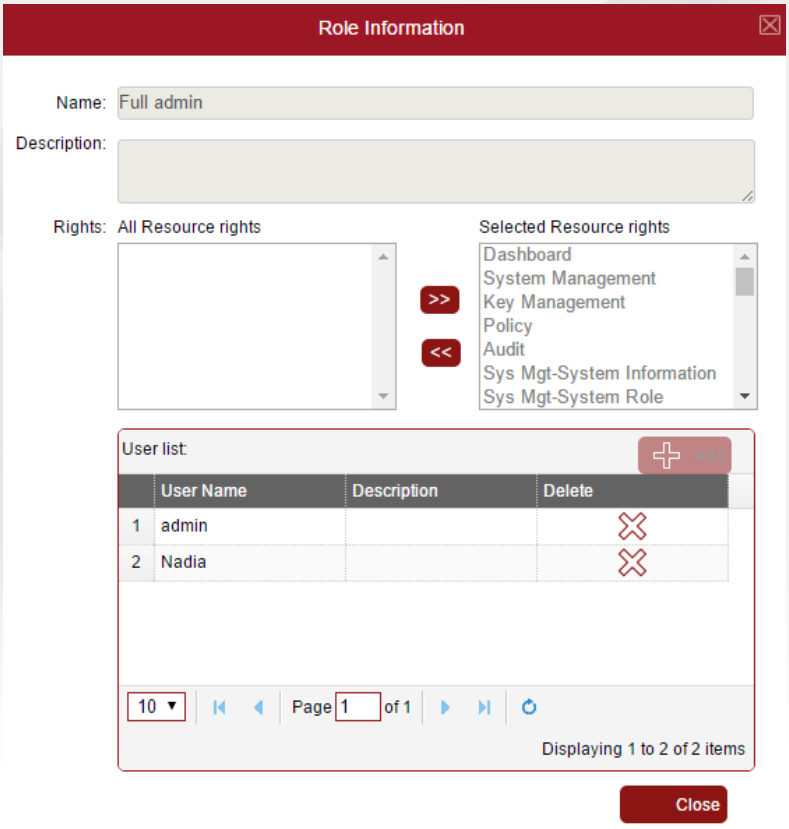

Enter the following information:

- **Name** - name of the system role
- **Description** - a brief statement about the purpose of the role
- **Rights** - the system resource that this system role is allowed to access. All users who belong to the role can access these resources. Rights generally map to a tab or page in the Manager screens. Thus it is possible to give certain System Roles access to only part of the DPM easyCipher.

Users can be added to the system role by modifying the role.

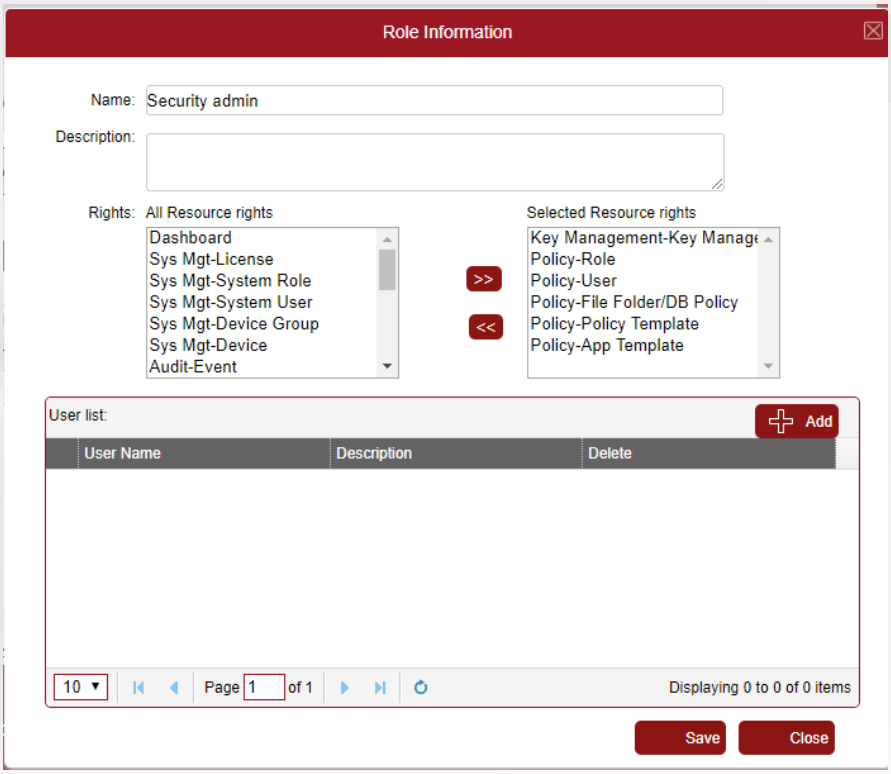
### 11.2.2 View existing System Role

To view properties of an existing System Role, click on 'View' icon of the target role.



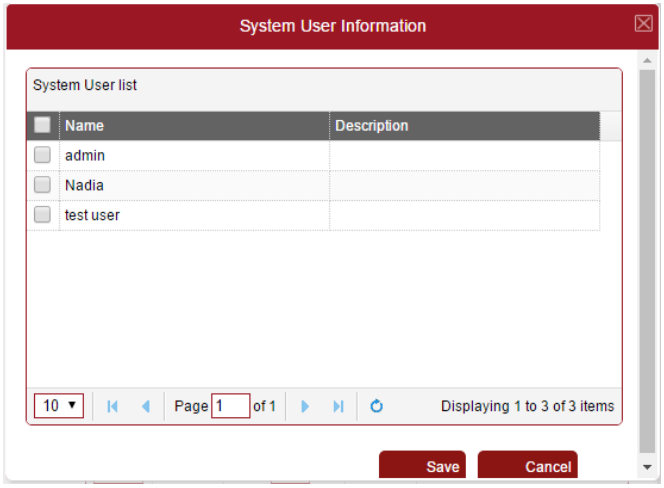
### 11.2.3 Modify existing System Role

To modify properties of an existing System Role, click on 'Modify' icon of the target role.




You can modify resource rights (permissions) by moving them from the right Rights list to the left or from the left to the right.

You can also add system users to this system role by clicking 'Add' button, selecting a user and clicking 'Save'.




### 11.2.4 Delete existing System Role

To delete an existing System Role, click on 'Delete' icon of the target role. You cannot delete a role which has system users assigned to it.

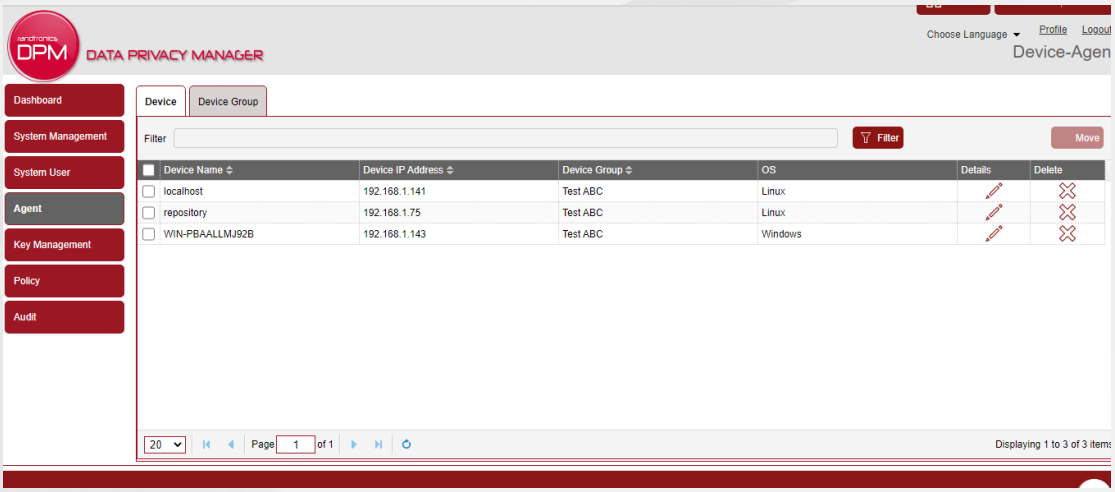
# 12. Agent

## 12.1 Device tab

The Device tab lists all of the Agent devices registered with the easyCipher Manager. As the Agent software is installed on devices, the Agent automatically registers with the Manager.

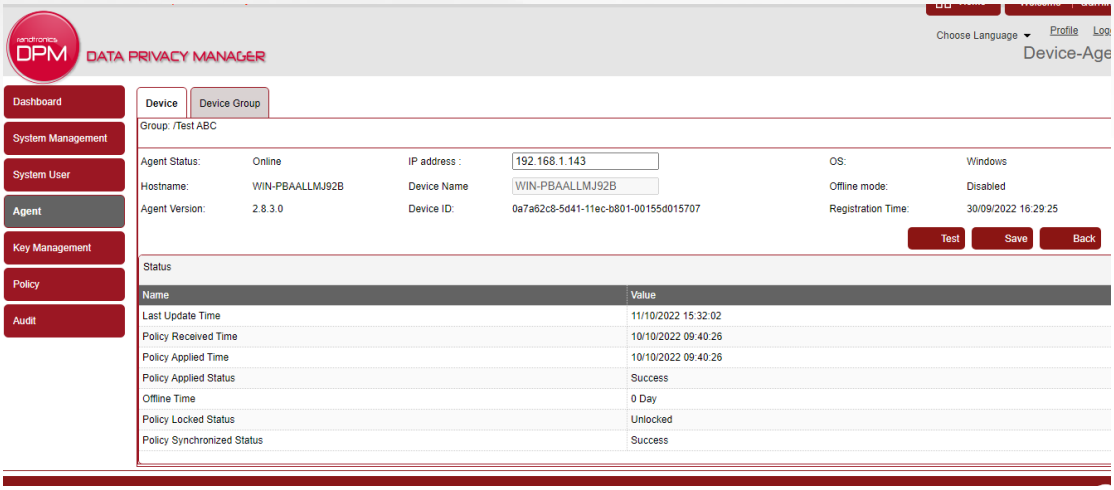
To access the Device page, click the 'Agent' button on the left hand menu, then click the 'Device' tab.

A list of all registered agents will appear.




### 12.1.1 View device information

To view detailed information click on the 'Details' button next to that device.




Device Information

Along the top of the Device tab, information about the device will be displayed:

- **Agent Status** – what the agent is currently reporting as the status: Online (agent has connected to the Manager in the last 3 minutes), Offline (agent has not sent any status within last 3 minutes) or Unknown
- **Hostname name** – the name of the device on which the Agent is installed
- **Agent version** – the version number of the Agent on the device
- **IP address** – the device IP address. Sometimes a client device may have multiple network adapters with multiple IP addresses. As a result, an IP address shown in this field may show an IP address from a different network adapter. You can update an IP address to configure a correct IP address for the agent so it can be reached from the manager. If using DPM easyCloudPlus then all agents will display the DPM network gateway address which will require to be changed to its respective public address off the agent.

- **Device name** – the name of the device
- **Device ID** – UID of the device
- **OS** – what operating system the device is using
- **Offline mode** – whether the device is running in offline mode

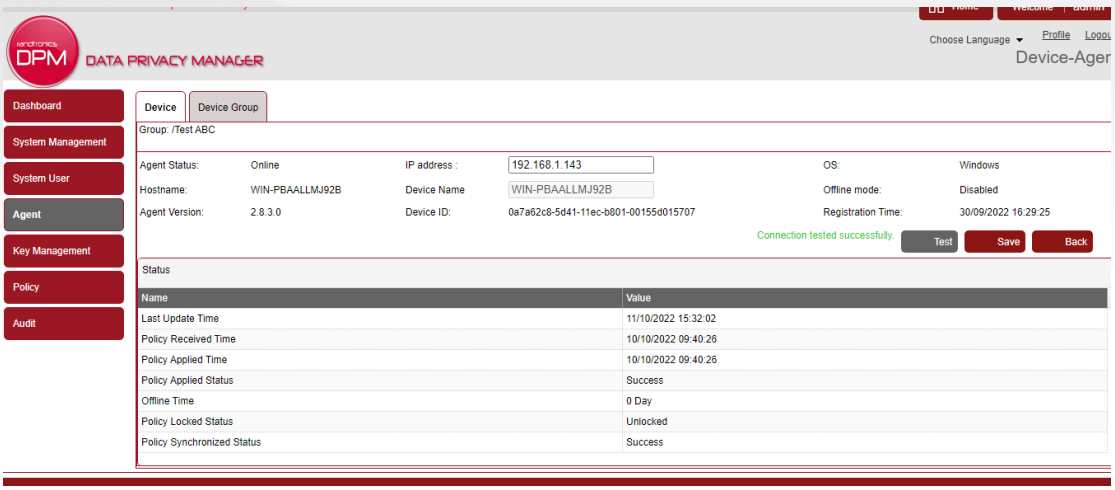
This page shows the status of the Agent on the device and can be useful when troubleshooting. Information about the last update from the Agent, along with the policy received and update times.

### 12.1.2 Test connection to device

To test whether DPM easyCipher can reach the agent navigate to Agent->Device page and click on 'Details' column for a target device. For the Manager to be able to connect to the agent, the agent's IP address must be reachable and port 2000 must be open on the Agent side. In some cases when the agent is in a different network/subnet, the agent's IP address will be displayed incorrectly. In this case you will need to modify the IP address field before testing the connection.

Click on 'Test'.

If connection is successful it will display 'Connection tested successfully' in green.




If it displays an error, check whether IP address in 'IP address' field is correct and also whether port 20000 on the Agent device is open. It may also indicate a problem with TLS certificate. Check 'TLS'-'Trusted Agents' tab and also certificate related errors in the agent log.

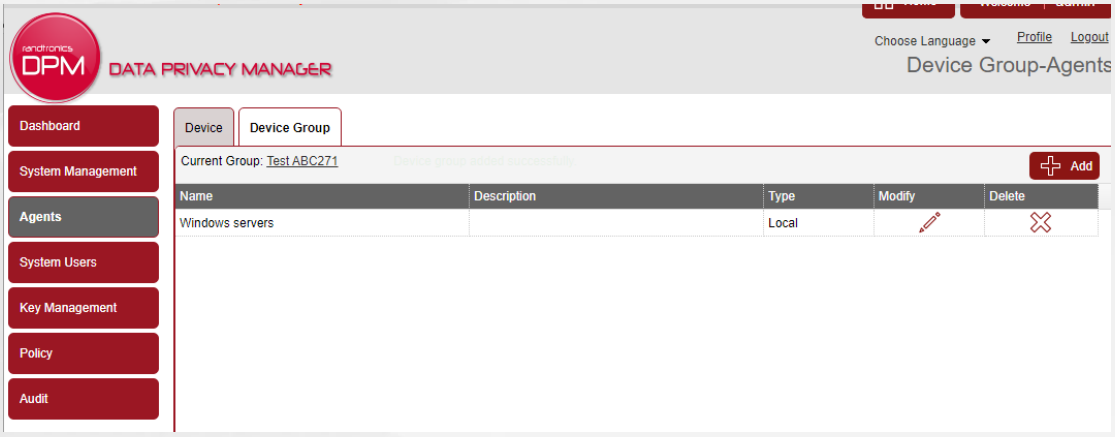
## 12.2 Device Group tab

A device group is a logical way to group all Agent devices. Usually this is done per department of an organization.

Device groups are a convenient way to view large numbers of devices by breaking them down into smaller sub groups. A policy can later be created for the device group.

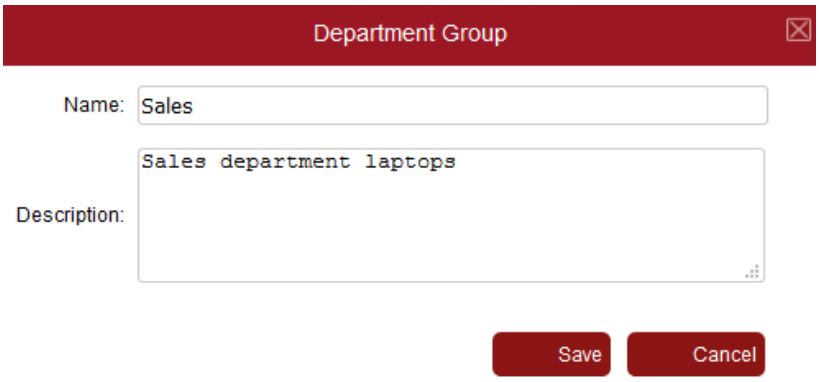
To access the Group tab, click the 'System Management' button on the left hand menu, then click on the 'Group' tab.

Autoscaling groups from AWS can be imported. All devices from the same autoscaling group will be assigned to the group during registration.




### 12.2.1 Create a new device group

To add a device group manually, press the 'Add' button



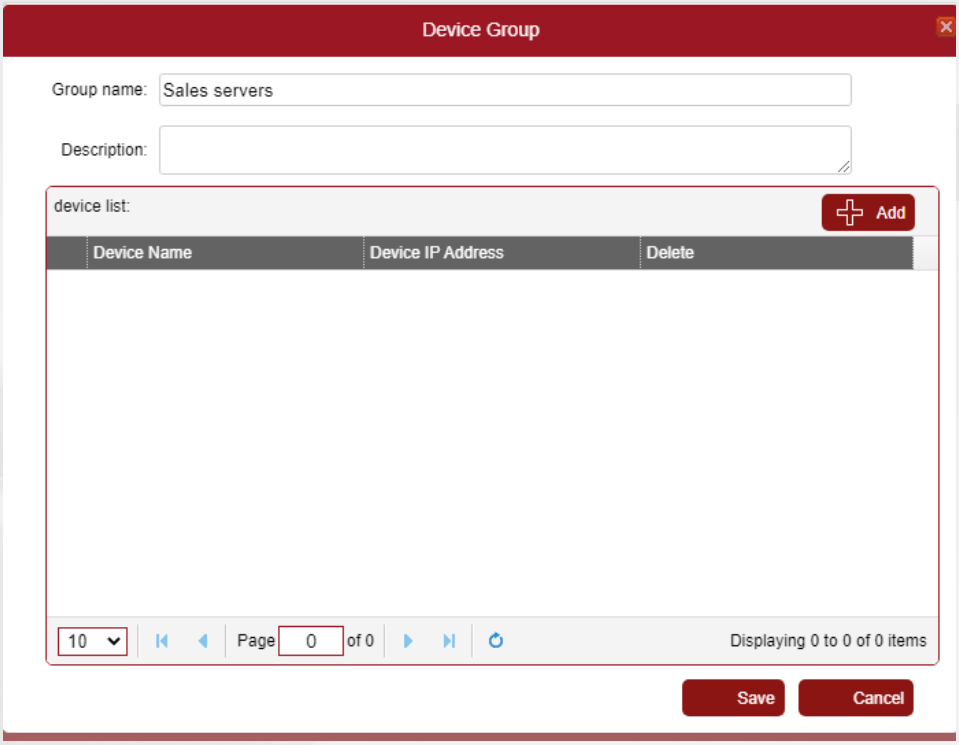

Fill out the device group information:

- **Name** – the name of this device group
- **Description** – a brief description of this device group

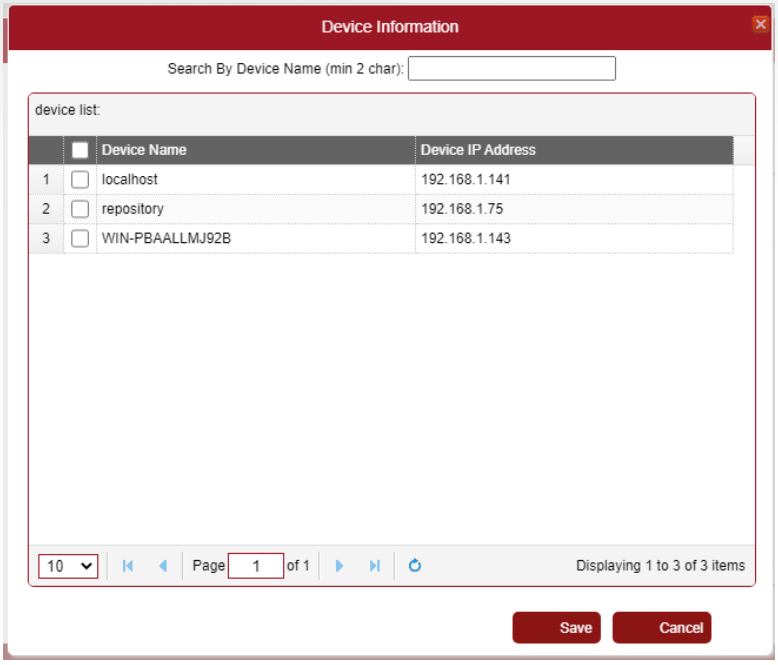
Click the 'Save' button to save the Device group

### 12.2.2 Add agents to a device group

To add agents to a device group, navigate to 'Agent' – 'Device group' and click 'Modify' button.




Click ‘Add’ in ‘Device list’. You will see a list of devices that don’t belong to any group.

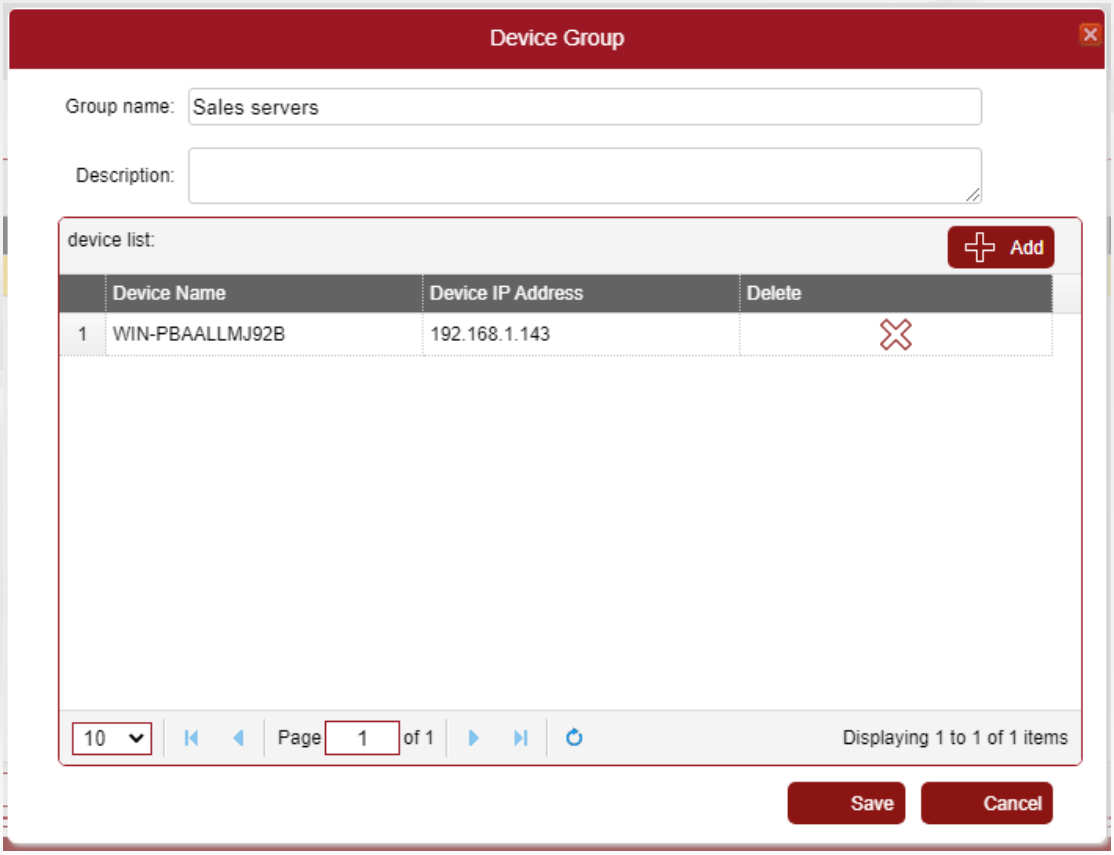



Select a checkbox next to the target device and click ‘Save’. Click ‘Save’ again.

If you have many devices, you can perform a device search using the top field.

## 12.2.3 Remove agents from device group

To remove agents from a device group, navigate to 'Agent' – 'Device group' and click 'Modify' button.




Click on 'Delete' next to the device that you want to remove from the group.

Click 'Save'

## 12.2.4 Cloud group (Cloud license only)

### 12.2.4.1 SNS notifications

In AWS SNS service allows to receive notifications when an instance in an autoscaling group is launched or terminated. DPM easyCipher can listen to these notifications to remove the agent from the system and to free a license allocation.

Using SNS notification is optional. If SNS is not used then DPM easyCipher will monitor status of the group agent and it will delete the agent from the list if it has not reported its status for 2 minutes.

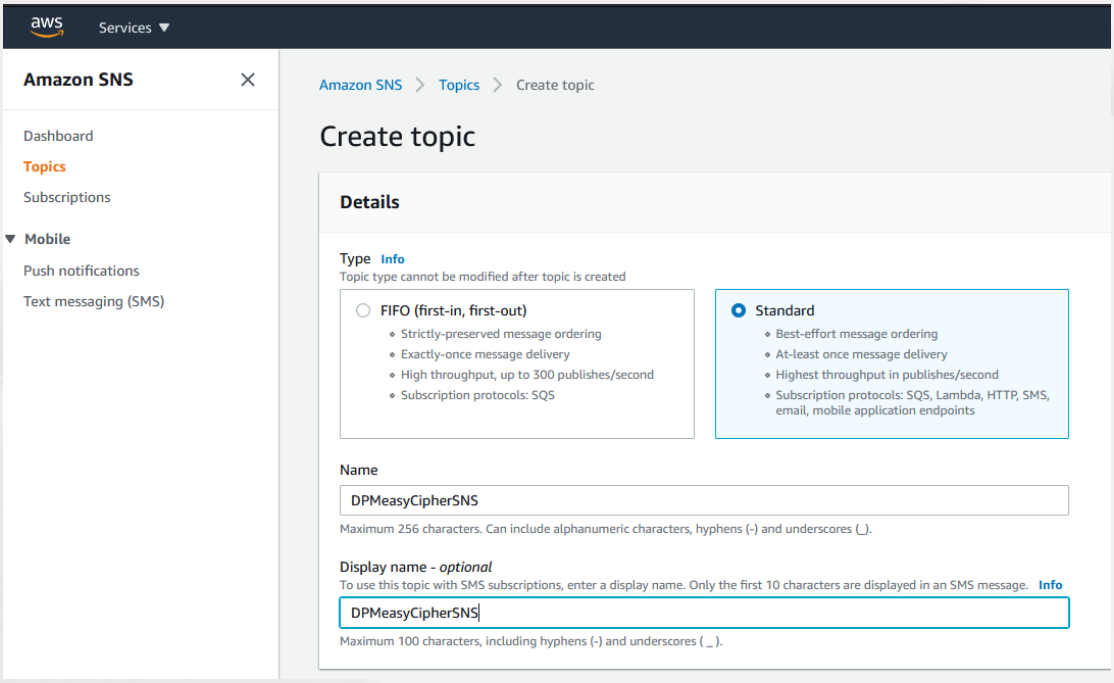
To use SNS notifications, the following steps need to be performed in AWS console:

1. Create a AWS SNS topic for DPM easyCipher

Open the Amazon SNS console

On the Amazon SNS dashboard, under Common actions, choose Create Topic

In the Create new topic dialog box, select “Standard” type and input topic name “DPMeasyCipherSNS”. This is a static name; a different topic name will not work.




2. Create notification for AWS auto scaling group

DPM easy Cipher agent will be installed in VM instances of AWS auto scaling group. To monitor the VM instance lifecycle and automatically apply license , it is necessary to create notification for auto scaling group.

d. Open Amazon Auto Scaling Group console

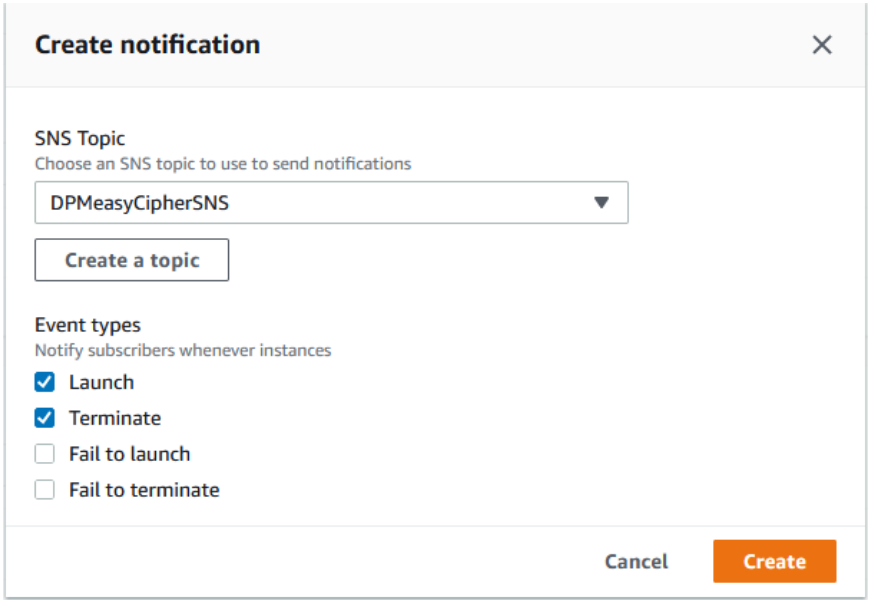
e. Open the auto scaling group that will install DPM easy Cipher agent

f. Click “Activity” tab

g. Click “Create notification”

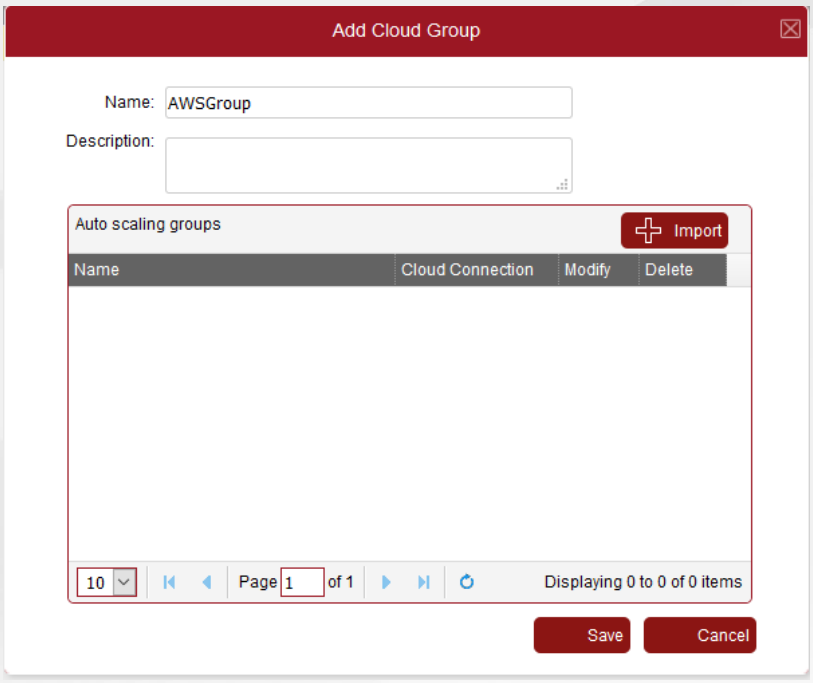
h. Select the SNS Topic named “DPMeasyCipherSNS” that is created for DPM easyCipher

i. Select Event Type “Launch” and “Terminate” and click “Create”



### 12.2.4.2 Add Cloud group

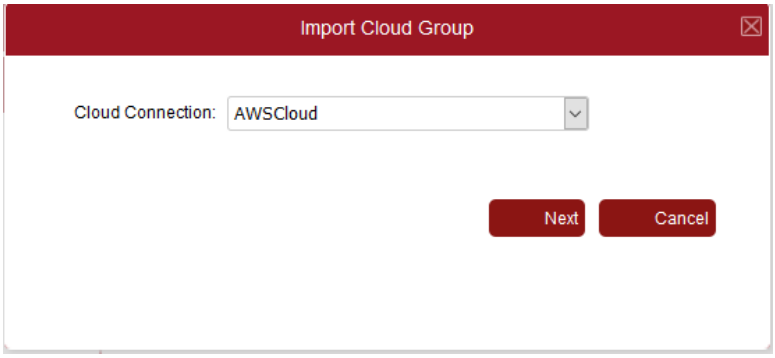
To add a cloud group, press “Add Cloud Group”



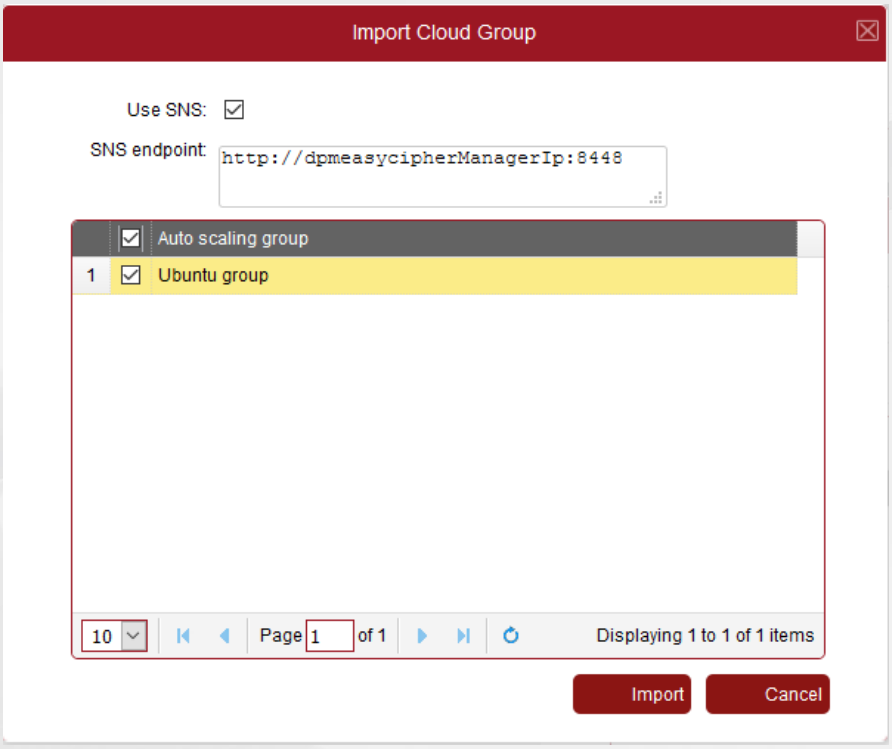

Fill out the cloud group information:

- **Name** – the name of this cloud group
- **Description** – a brief description of this cloud group

Click the “Import” button to get auto scaling group from cloud provider



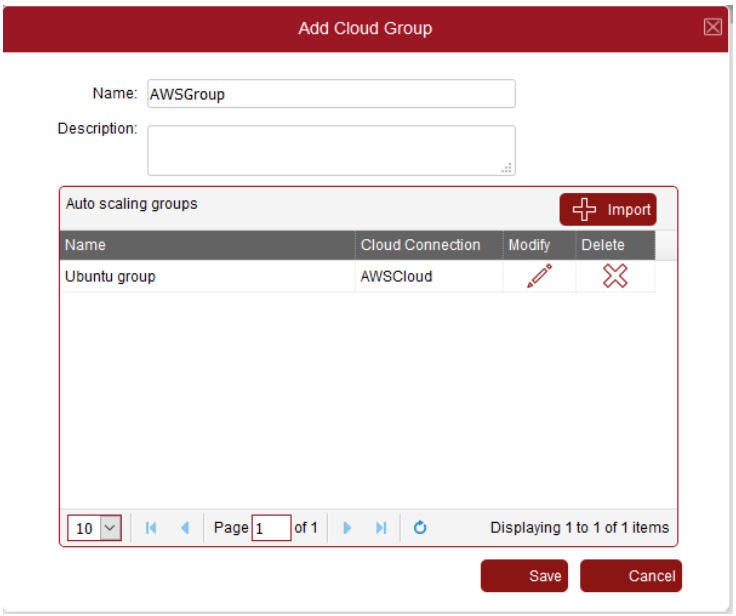

Select the existed Cloud Connection and click “Next”




Fill out the parameters for Cloud auto scaling group:

- **Use SNS:** – use SNS topic to get VM instance notification. This is optional. On how to create SNS topic please refer to the previous section.
- **SNS endpoint** – DPM easy Cipher service that receives and process VM instance nofification, it will use this URL: http://dpmeasycipherManagerIp:8448. "dpmeasycipherManagerIp" shall be your DPM easy Cipher server's public IP address or reachable DNS name.

Click "Import" to add auto scaling group to cloud group




Click the 'Save' button to save the cloud group. A new cloud group will appear inside the parent group.

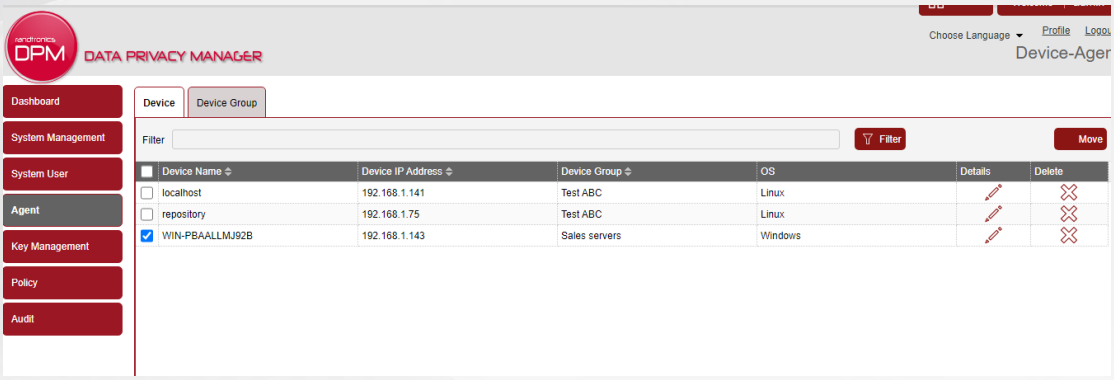
## 12.2.5 Delete an existing Device Group

To delete an existing Device Group, click on 'Delete' icon of the target group. All devices associated with this group will be assigned to a root group.

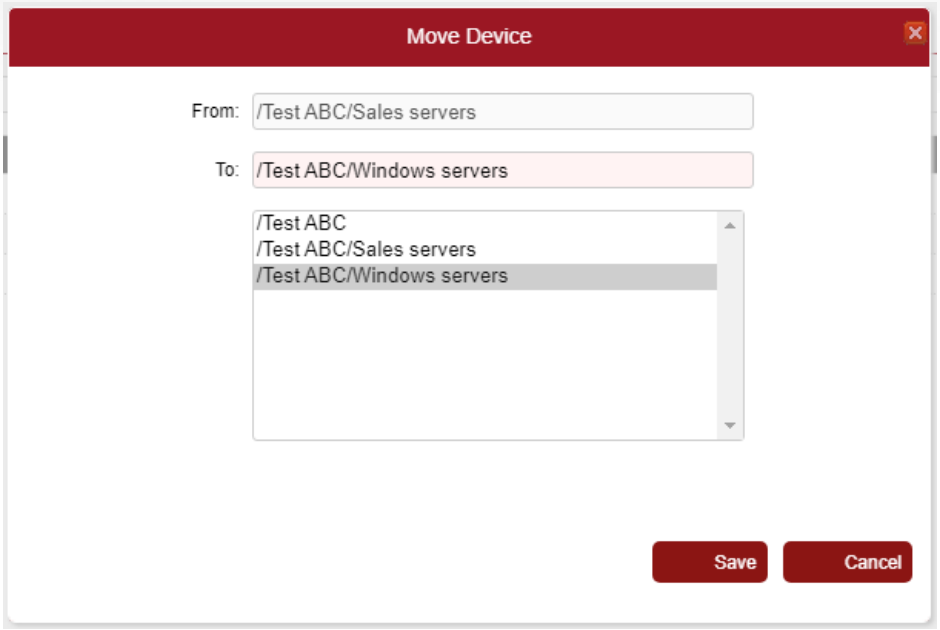
## 12.2.6 Move device to a different Device Group

To move an existing Device Group to a different device group, navigate to Agent – Device.

Select one or multiple devices and then click 'Move'.




Select a target device group from the list and click 'Save'.




**Important note**: If the new target group has a group policy, then the device agent will receive the new group policy (assuming that there is no individual device policy for that device which takes precedence). This may affect encryption/decryption of data on the target device.

# 13. Key Management

## 13.1 Types of keys

The DPM easyCipher software manages three types of Keys:

File Key

File keys are used to encrypt files stored in protected directories. When an encryption policy for a folder is created, a file key is assigned to the folder.

File keys are AES-256 symmetric keys.

If DPM easyCipher is configured to use an external DPM easyKey the keys are generated by DPM easyKey. Otherwise, keys are generated by an internal key management module.

Key Encrypting Key (KEK)

Key Encrypting Key is a symmetric key used to protect all file keys. Before all other keys are stored, they will be encrypted with Key Encrypting key.

The key encrypting key can either be internally generated, or externally generated:

- Internal key encryption key – the DPM easyCipher generates the key encrypting key during the initialization process
- External encryption key – the DPM easyCipher software can be configured to communicate with the DPM easyKey for key generation. In this case the DPM easyKey generates the key encrypting key during switching process.

Master Key

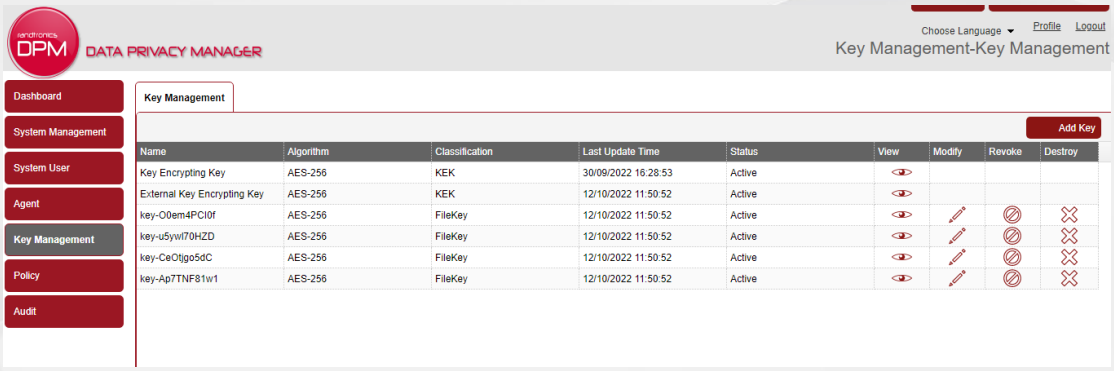
The master key is used to encrypt the internal key encrypting key and an internal CA private key. It is generated during the initialization process based on a master key password provided by user.

IMPORTANT!!!

Please record your master password and keep it in a safe place. It is required to re-enter a master password in case of reinstallation or when an extra node is deployed for high availability. If the master password is entered incorrectly no keys can be decrypted and data cannot be decrypted.

## 13.2 Key list

To view key information, press the Key Management button on the left hand menu.




If using an external DPM easyKey, the corresponding keys can be found in DPM easyKey key list as well. However, in DPM easyKey key names will appear in the following format: 'key prefix – key name'.

## 13.3 File Key

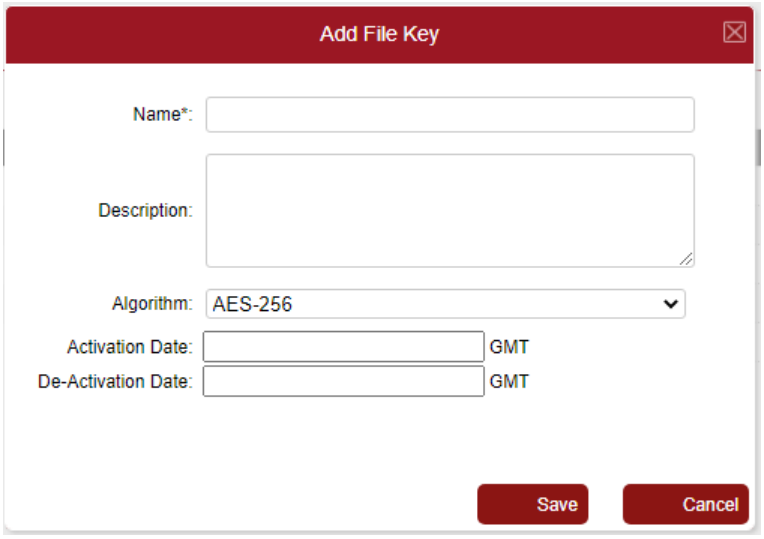
The File Keys are used to encrypt/decrypt files as part of Encryption policy which will be transmitted to the Agents and to encrypt/decrypt files.

Keys can be generated on demand by a system user from Key Management menu or during encryption policy creation.

If DPM easyCipher is configured to use an external DPM easyKey the keys are generated by DPM easyKey. Otherwise, keys are generated by an internal key management module.

To create an encryption key from 'Key Management':

1. Navigate to 'Key Management' and click 'Add' button.




2. Enter the details:

**Name** – unique label of the key

**Description** – optional description of the key

**Algorithm** – the encryption algorithm that the key will be used for. AES-256 is recommended.

**Activation date** – a start date when the key can be used for encryption. By default, it is set to the current date. Not used in the current version.

**De-activation date** – a date after which the key can only be used for decryption and not for encryption. Not used in the current version.

3. Click 'Save'.

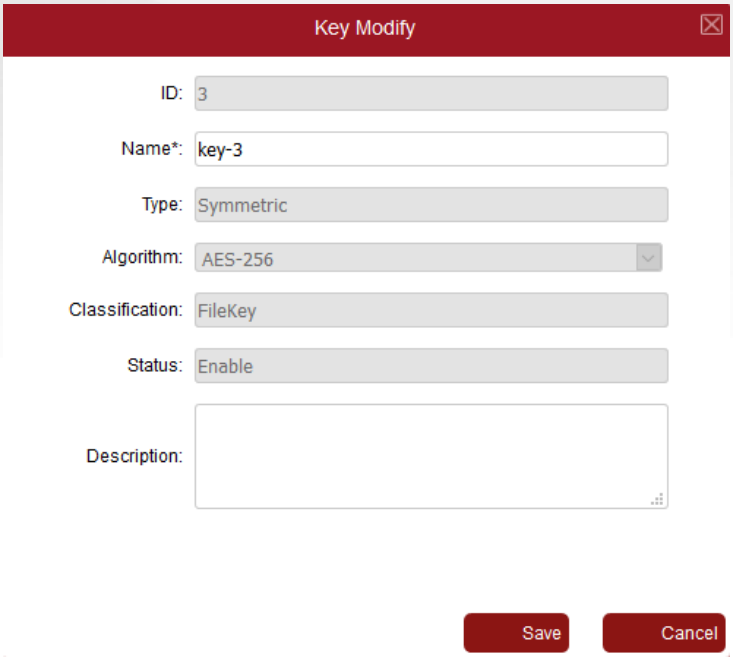
This key can be selected when creating an encryption policy.

## 13.4 Key Modify

Modifying a key allows the System user to change the key name and description. No other values of the key are allowed to be changed. This is useful if you want to change the name of the key that was generation in the encryption policy.

To modify a key:

1. Click on the Key Management button in the left hand menu
2. Click on the Modify icon next to the key to modify
3. Modify the name and description of the key
4. Click the Save button




Only the following fields may be modified:

- **Name** – the name of the key
- **Description** – a description of the key

No other values can be changed.

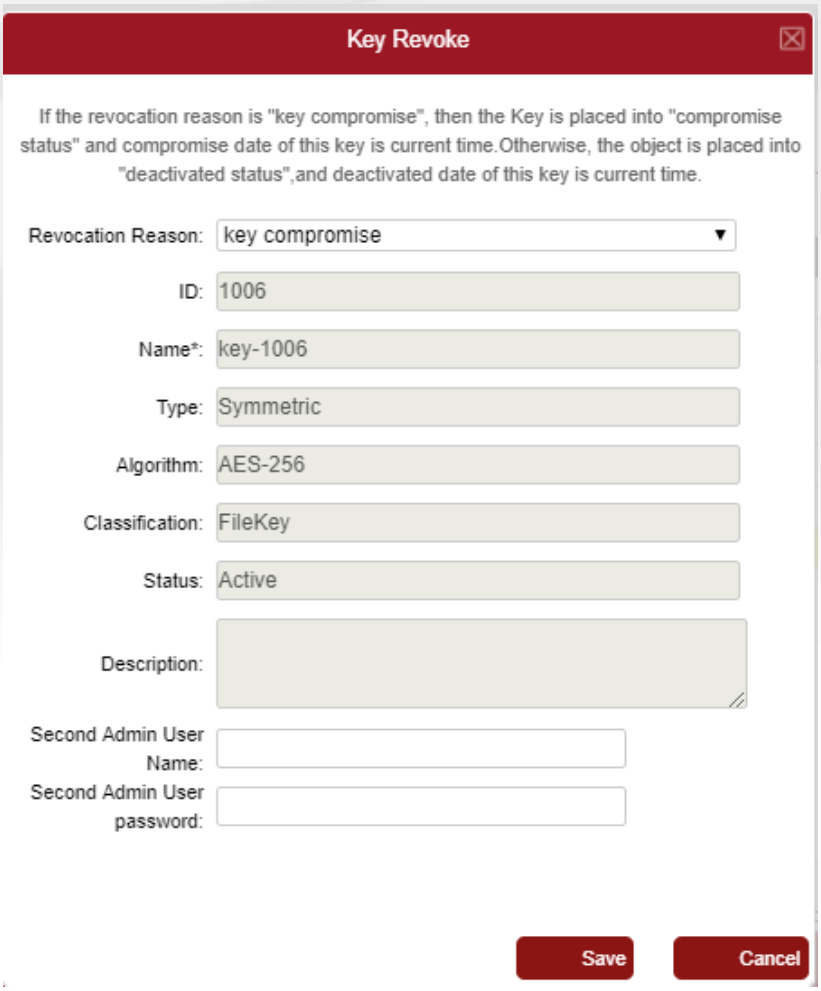
## 13.5 Key Revoke

Revoking a key means that the key can no longer be used to encrypt, but can still be used to decrypt. This means that any policies that are using a key that has been revoked will be able to decrypt existing files, but will not be able to encrypt new files so new files will be created in clear.

A second admin with Key Management permissions is required to perform key revocation operation.

To revoke a key:

1. Click on the ‘Key Management’ button in the left hand menu
2. Click on the ‘Revoke’ icon next to the key to revoke
3. Choose the revoke reason. Currently can only be set to “key compromise”
4. Second admin enters their User Name and Password
5. Click the Save button



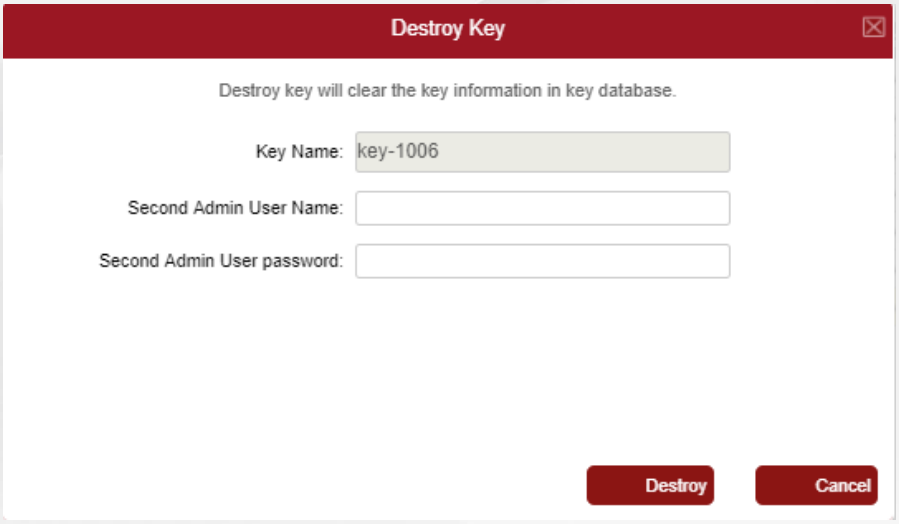
## 13.6 Key Destroy

Destroying a key will remove its key value from storage, but the key meta data (such as key type and algorithm) will be kept for auditing purposes.

Keys that have been destroyed cannot be used for encryption or decryption.

Only keys that are in Revoked status can be destroyed.

A second admin with Key Management permissions is required to perform key revocation operation.



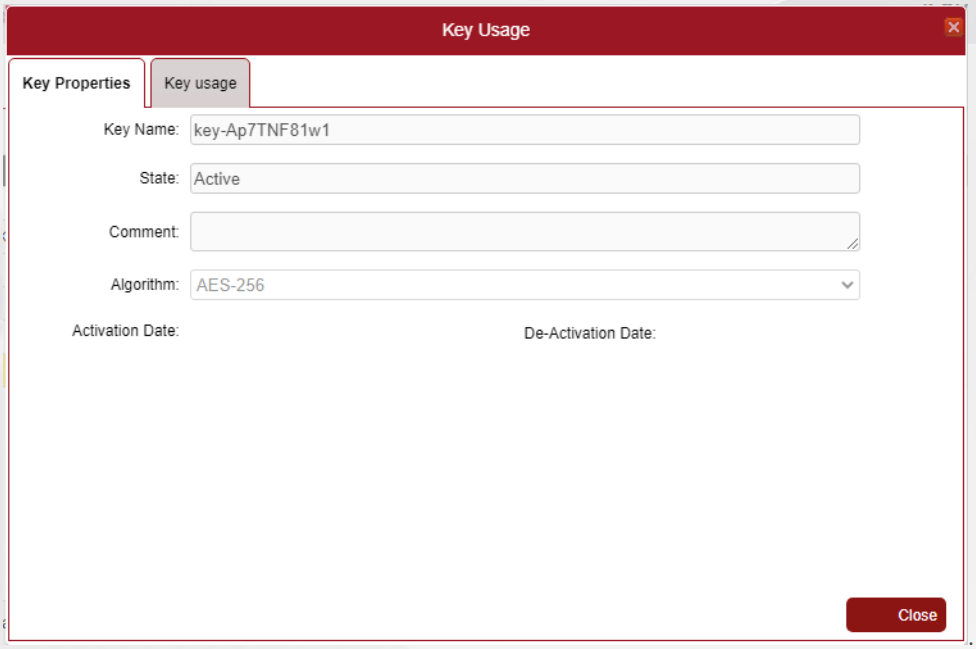

To destroy a key:

1. Click on the 'Key Management' button in the left hand menu
2. Click on the 'Destroy' icon next to the key to destroy (note that the key revoked status)
3. Second admin enters their User Name and Password
4. Click Destroy

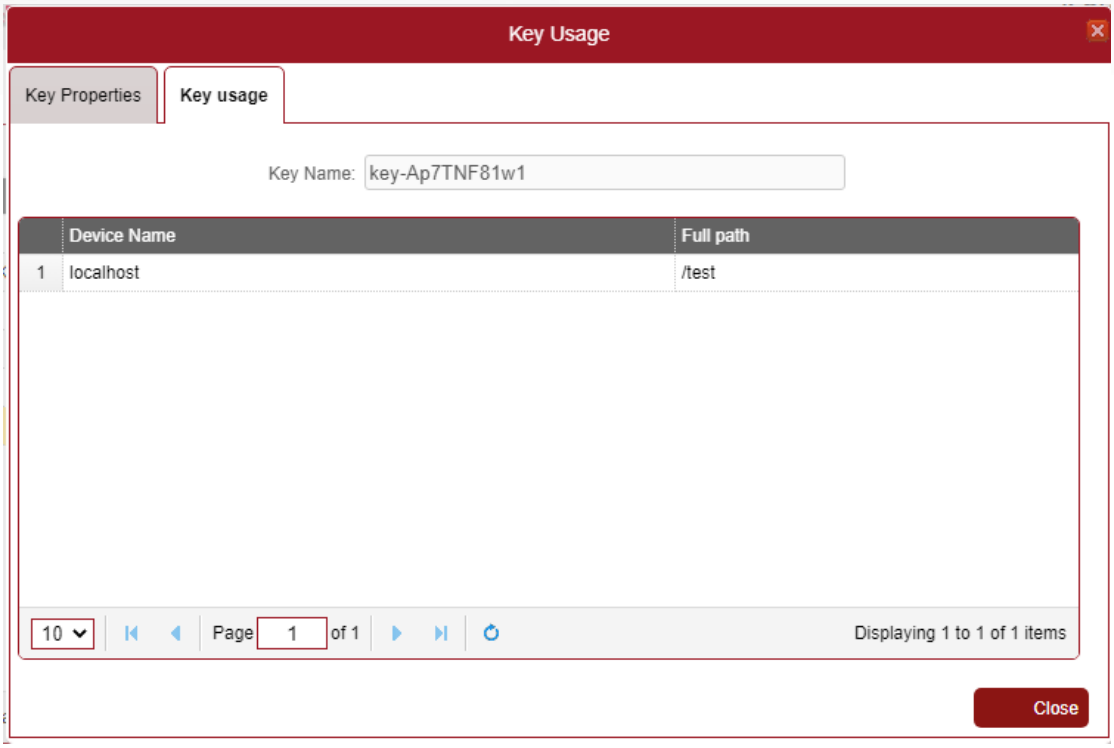
## 13.7 Key Properties

To view the key properties and usage of a key, click on 'View' icon next to the key in the key table.

'Key Properties' tab will display the key name, state of the key and algorithm.




'Key Usage' tab will display all devices, along with the folders that are being protected using the key.

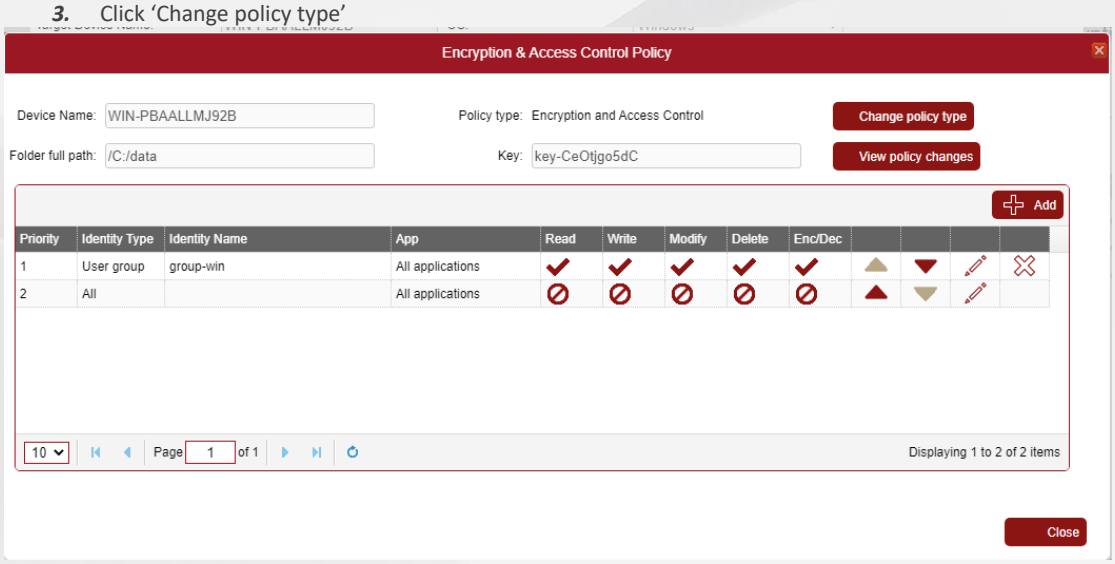


## 13.1 Key Rotation

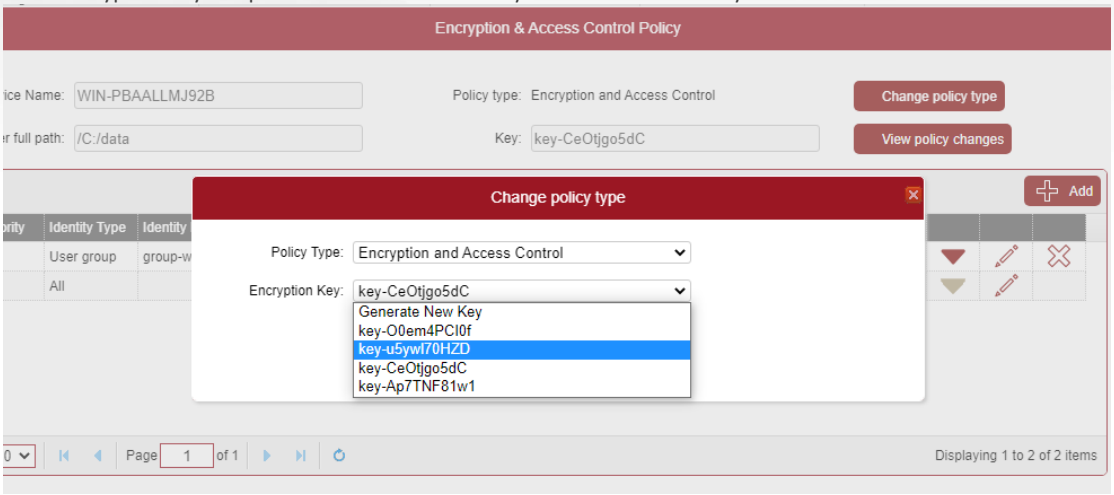
Key rotation of file keys is performed by creating a new key and reencrypting data with the new key.

To rotate a file key for a encryption policy:

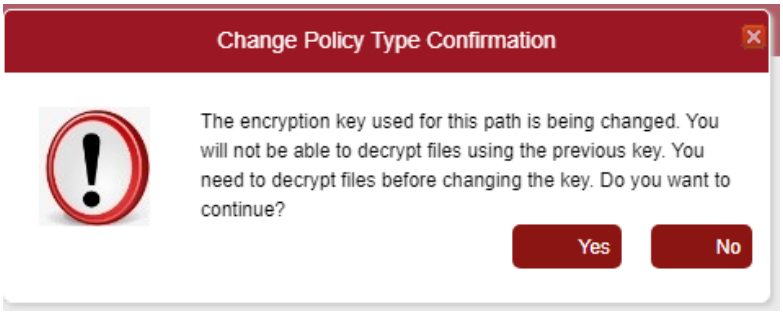
1. Decrypt data by moving the data out of the target folder or using migration tool. Please see further sections about migration.
2. Open the target Encryption or 'Encryption and Access Control' policy for the target folder.
3. Click 'Change policy type'




4. Click 'Encryption key' dropdown and select a new key or 'Generate New Key'. Click 'Save'




5. It will present a confirmation message that the old data needs to be decrypted. Click 'Yes'.




6. Click 'Save' in the main policy dialog.
7. Encrypt target data by moving the target data back to the target folder or using migration tool.

# 14. Policy Management

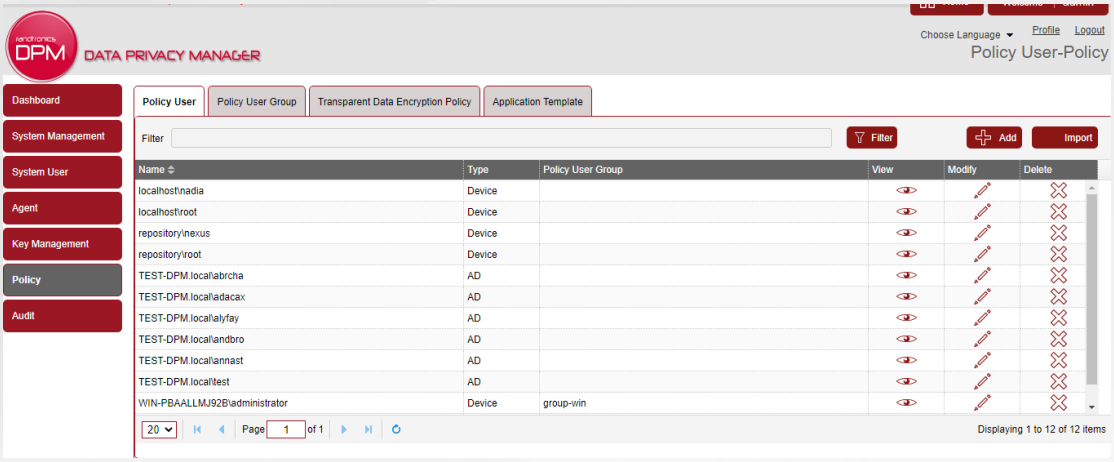
The Policy section allows the user to create new polices, and view, edit and delete existing polices, import end user identities and group them into user groups, configure application templates.

All Policy management is accessed by clicking on the 'Policy' button in the left hand menu.

## 14.1 Policy User

Policy users are logins to devices on which the Agents are installed. These are Operating System end-users or AD/LDAP users that are used to login to laptops, desktops and servers where the agents are installed.

To manage Policy Users, click on the 'Policy' button on the left hand menu, then click on the 'Policy User' tab.

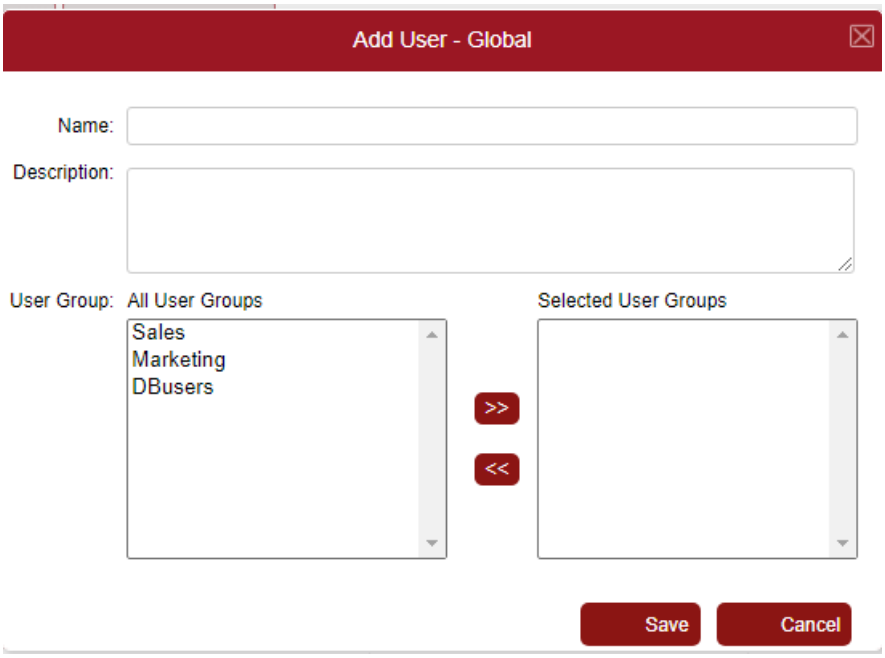



Policy users can be manually added to the list, imported from devices or from AD/LDAP.

### 14.1.1 Create a new Policy User

If a user cannot be imported from a device or AD, you can manually add the user name to the list. These users will become 'Global' users and can be used an any device and group policy.

To manually create a new Policy User, click on the 'Add' tab.



Enter the new user information:

- **Name** – the name of the user. This must exactly match the user on the device that is being protected. It can be prefixed with the device name (eg. LAPTOP\john)
- **Description** – an optional description of the user
- **User Group** – a list of all user groups that the user belongs to

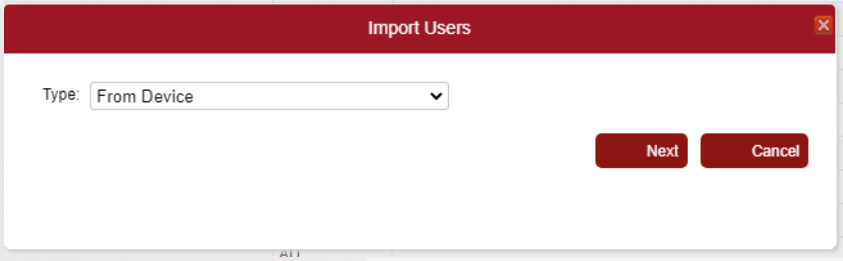
Press the Save button to save the new user.

### 14.1.2 Import Policy User from Device

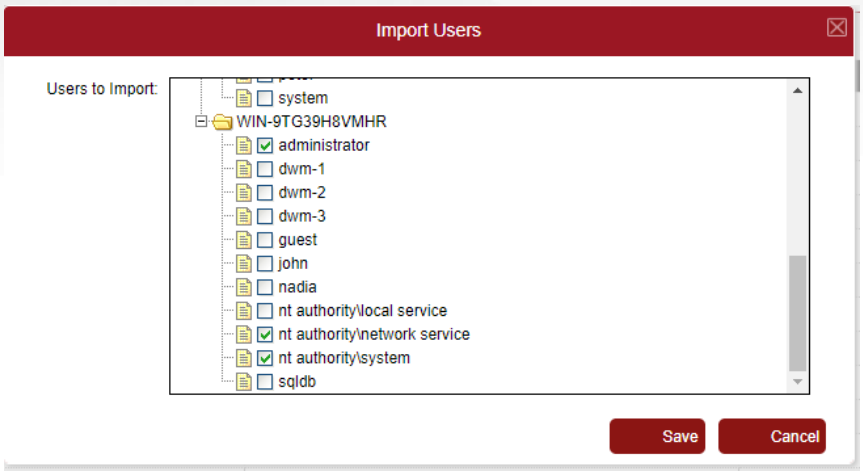
If it is required to protect from a local OS user, the user identity can be imported from the device.

To import users from devices:

1. Click the Import button
2. Under the Import Users dialog box, change the type to From Device and click Next




3. Tick the box next to the users to import and click 'Save'

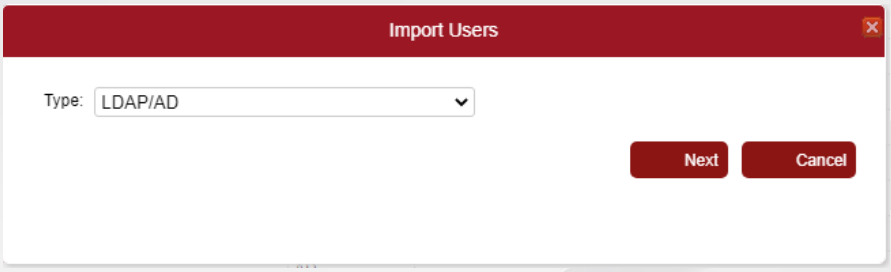



### 14.1.3 Import User from LDAP/AD

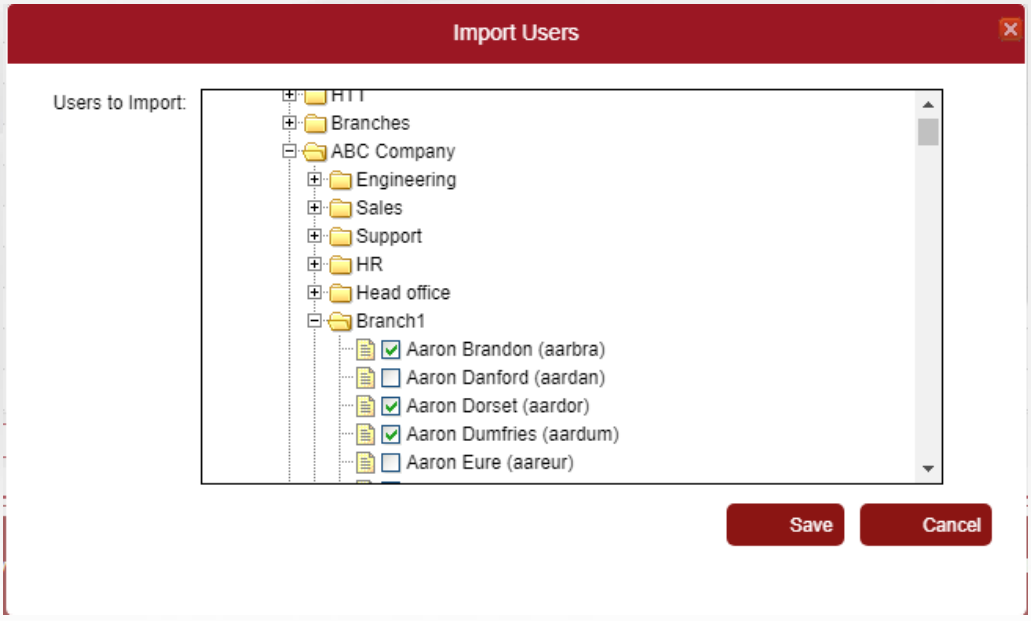
To import users from LDAP/AD it is required to configure LDAP/AD destination in 'System Management'-'LDAP/AD'. Once it is configured 'Import from LDAP/AD' option will be available. Currently only one Microsoft Active Directory is supported.

To import users from LDAP/AD:

1. Click the 'Import' button
2. Under the Import Users dialog box, change the type to LDAP/AD and click 'Next'

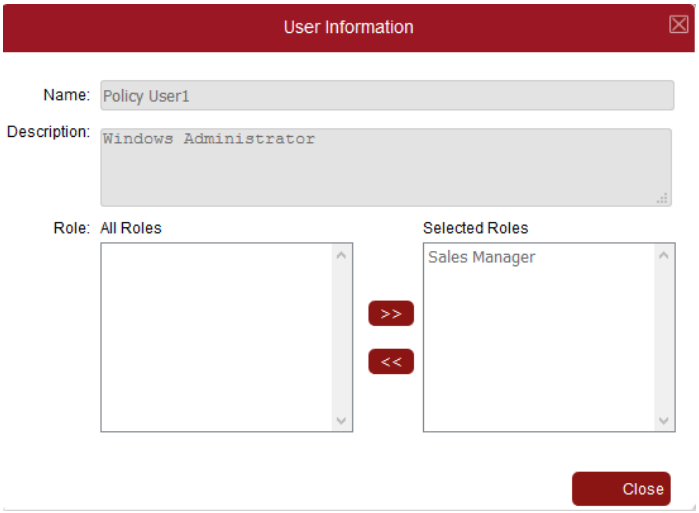



3. Tick the box next to the users to import and click 'Save'




## 14.1.4 View Policy Users

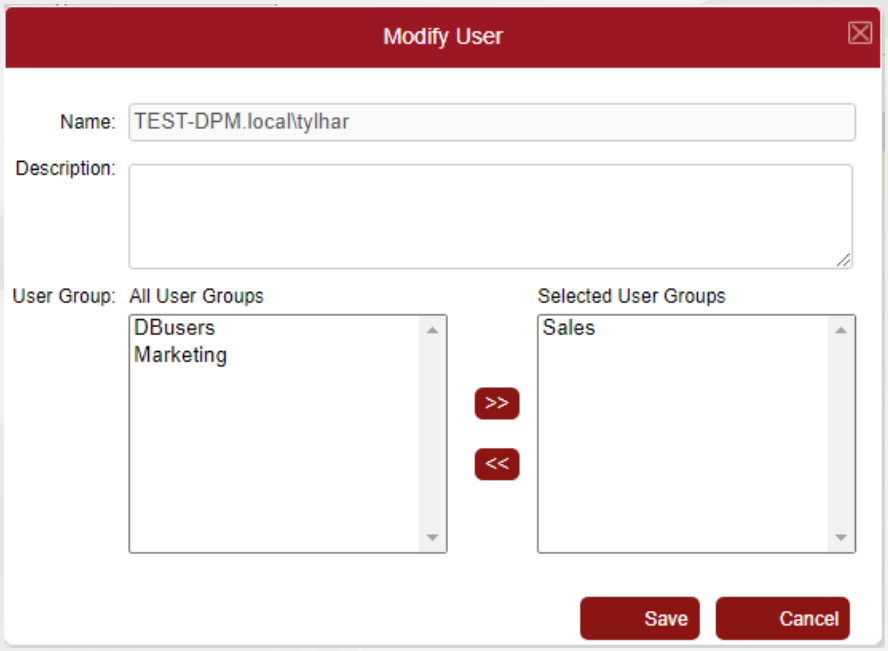
To view a user, click on the 'View' icon on the user to view.




No values can be changed on the view user popup. To modify users, see the Modify Users section.

### 14.1.5 Modify Policy Users

To modify a user, click on the 'Modify' next to the user to modify. Modifying allows the description and user group values of a user to be changed.




The following values can be changed:

- **Description** – the user description can be changed. Description is used for display purposes and changing it will change what is displayed in the view, modify and user list screens
- **User Group** – the user can be added and removed from selected user groups

### 14.1.6 Delete Policy Users

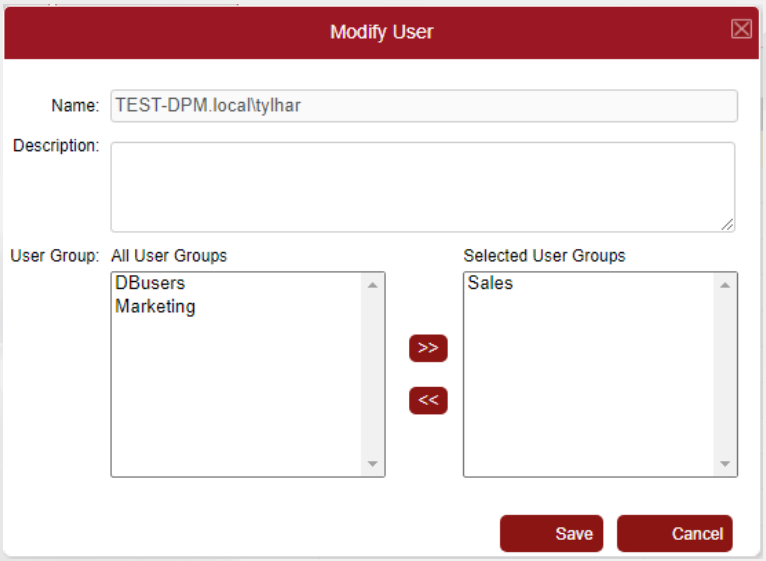
To delete a user, click on the 'Delete' icon next to the user, then click 'Yes' on the delete confirmation popup.

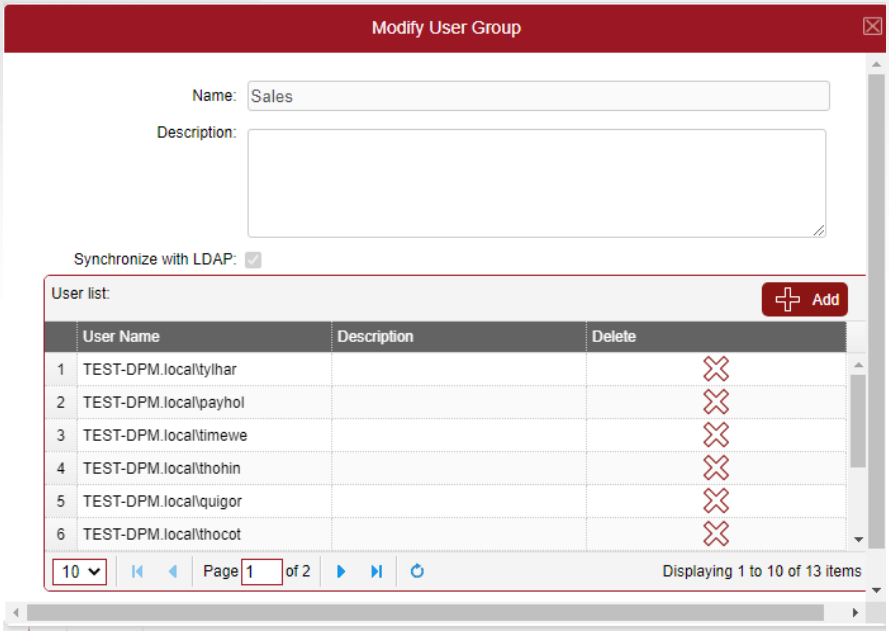
Deleting a user will have the following affect:

- The user will no longer appear in any dropdown when creating or modifying policies
- Any policy rules already created for the user will be deleted and the user will not be able to access files.

## 14.1.7 Add Policy users to a user group

Users can be added and removed from user group on the Add User and Modify User popups or via Modify User group dialog.



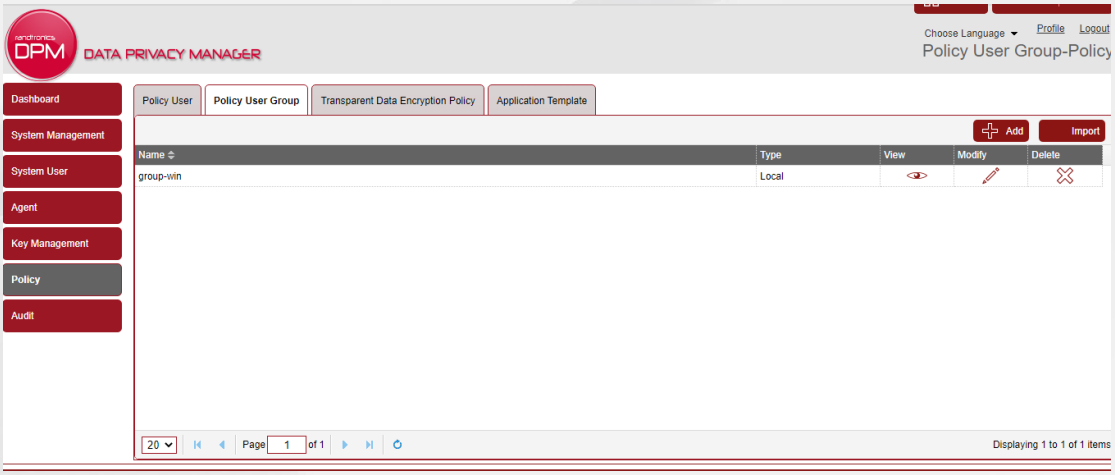

When users are added or removed from user groups, the manager will communicate the permissions changes to the Agents and the new user permissions will be applied.

## 14.2 Policy User Group

A User group is a logical way of grouping end users. It is especially useful if the same folder needs to be accessed by multiple users.

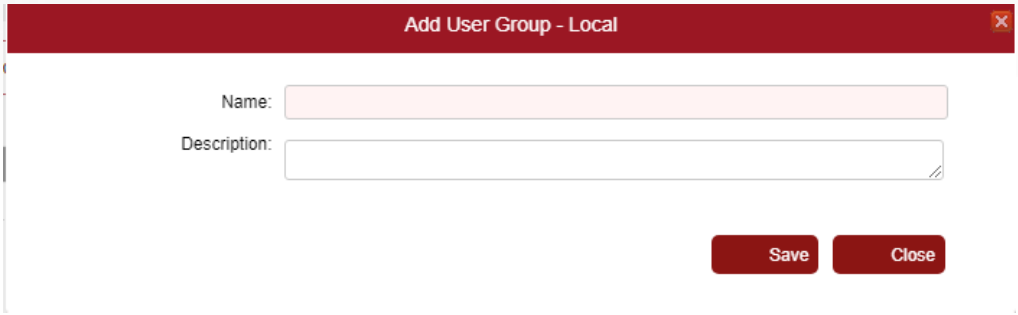
To configure a user group for policy, click on the 'Policy' button in the left hand menu, then click on the 'Policy User Group' tab.

Policy Roles can be imported and synchronized with Active Directory.




### 14.2.1 Create a new Policy User Group

To create a new local user group, click 'Add' button




Enter the group information:

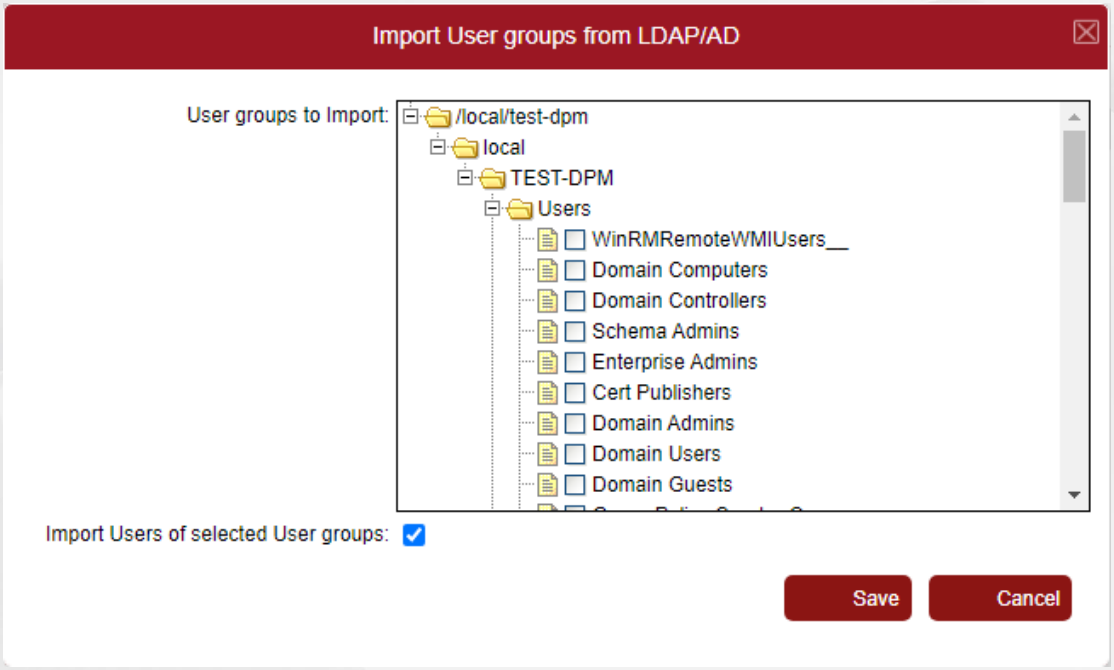
- **Name** – the name of the group
- **Description** – the description of the group

Click on the 'Save' button to save the new group.

Users can be added by modifying the group

### 14.2.2 Import a Policy User group from LDAP/AD

To import a group from LDAP/AD, click 'Import' button



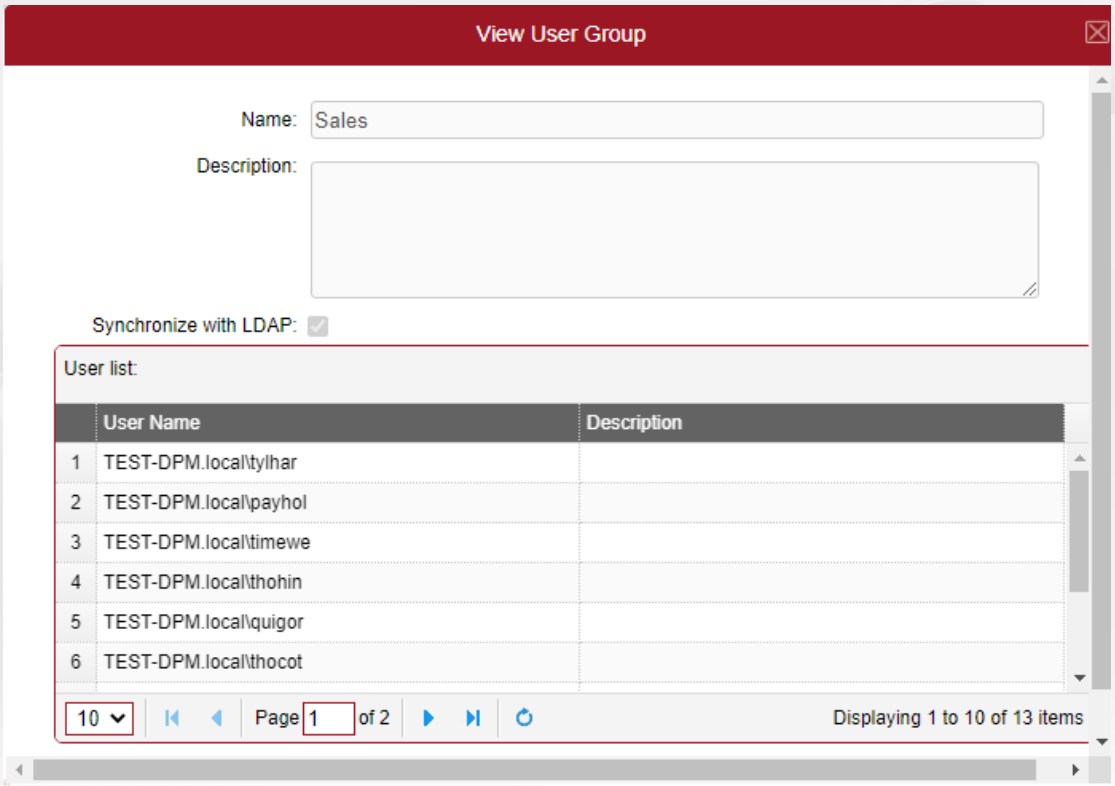

Select group that you would like to import.

Select 'Import Users of selected Roles' if you would like to import all users for those user groups.

Click 'Save'.

### 14.2.3 View Policy User Group

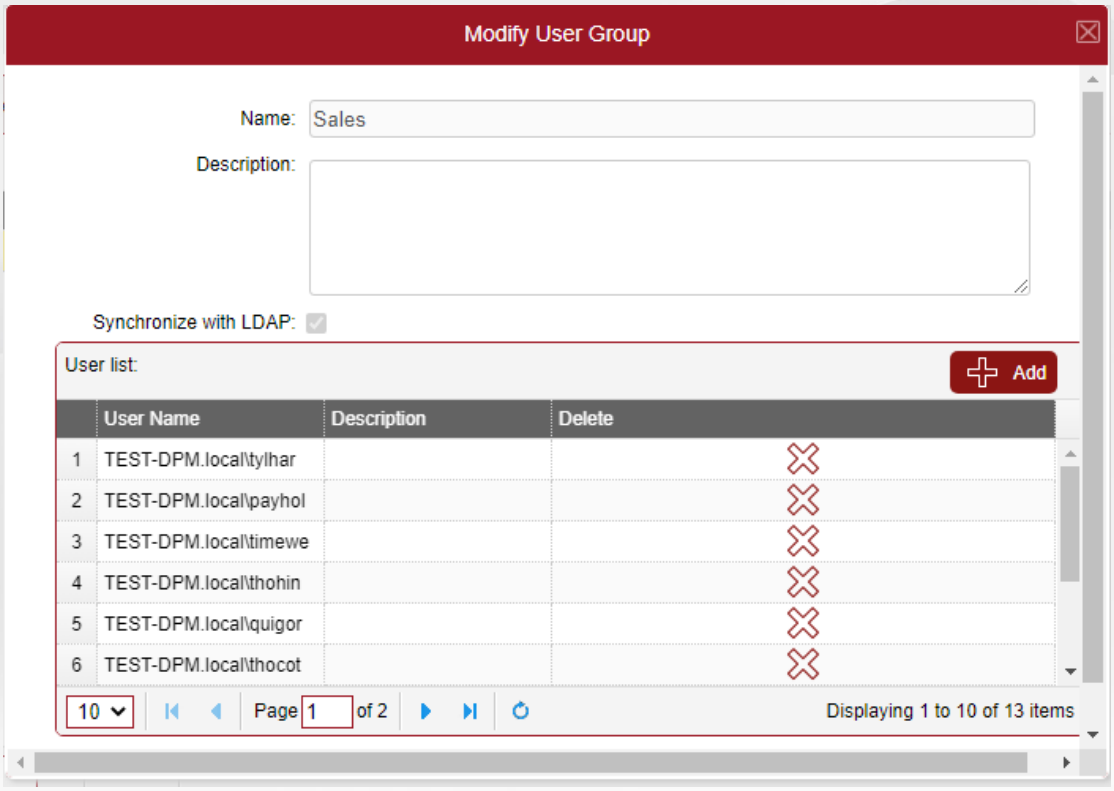
To view a policy user group, click on the 'View' icon on the group to view.




No values can be changed on the view group popup. To modify a group, see the Modify User Group section.

## 14.2.4 Modify User group

To modify a user group, click on the 'Modify' button next to the group to modify. It will allow to modify a group description and user membership.




The following values can be changed:

- **Name** (only for local groups) – group name is only used for display purposes, and changing the group name will change what is displayed on the policy dropdowns, lists and group screens.
- **Description** – description is used for display purposes and changing it will change what is displayed in the view, modify and user list screens.
- **User List** – List of all users that are currently part of the group. New users can be added to the list or existing users deleted from the list

Modifying a user group will affect existing policy where that group is used.

If a group is imported from LDAP/AD it will be changed at the next synchronization point according to the LDAP/AD membership configuration. The users that are added to an imported role manually will be deleted.

## 14.2.5 Delete User group

To delete a user group, click on the 'Delete' icon next to the group, then click 'Yes' on the delete confirmation popup.

Deleting a user group will have the following affect:

- The group will no longer appear in any dropdown when creating or modifying policies
- Any policy rules already created for the group will be deleted. All users that previously belonged to the role will lose access to the files. However, the users of the group are not deleted from the Users list.

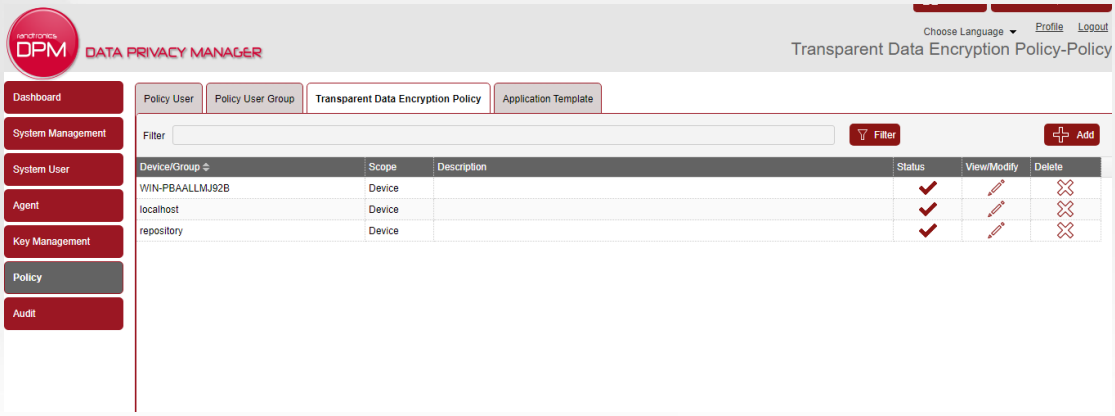
## 14.3 Transparent Data Encryption Policy

The 'Transparent Data Encryption Policy' tab allows the administrator to protect devices by creating and applying security policies. It also allows existing policies to be viewed, updated and deleted.

There are three type of policies that can be applied.

1. **Encryption**– this will encrypt all files created under the target directory with a file encryption key. Authorized and unauthorized users and applications can be configured for encryption/decryption.
2. **Access Control**– This will allow to configure permissions for users and application to perform file/folder operations such as to read, write, modify or delete in the secure folder
3. **Encryption and Access Control**– combination for encryption and access control types.

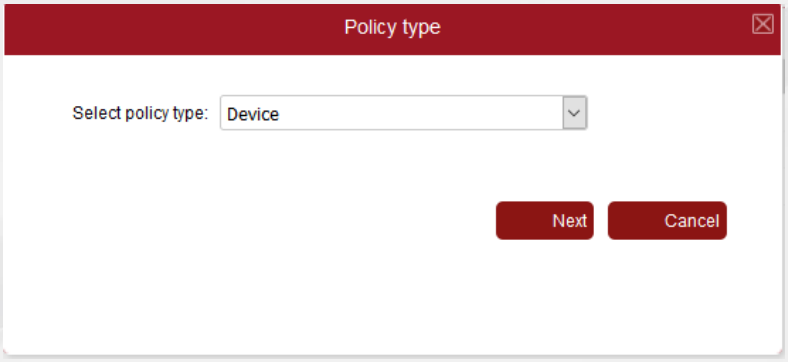
The 'File Folder/DB Policy' tab displays a list of all devices that has a Policy applied to them.



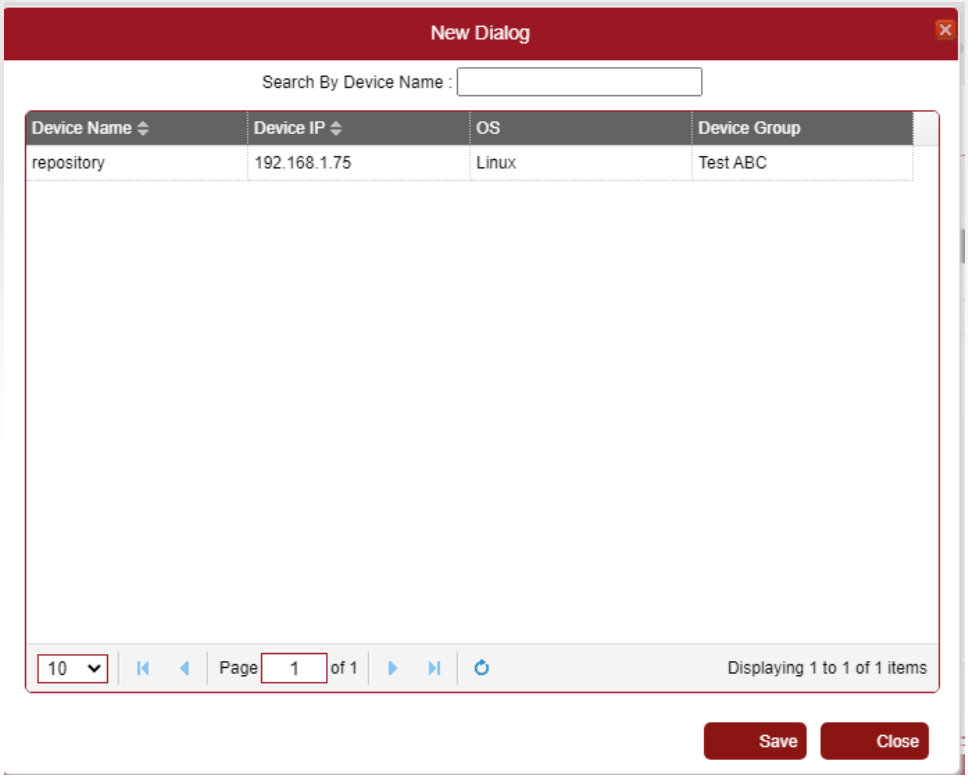
## 14.3.1 Create a new Policy

### 14.3.1.1 Create a new Policy for a device

To create a brand-new Policy for a device that does not already have a policy, click on the 'Add' button.




Select "Device" policy type, click "Next" button



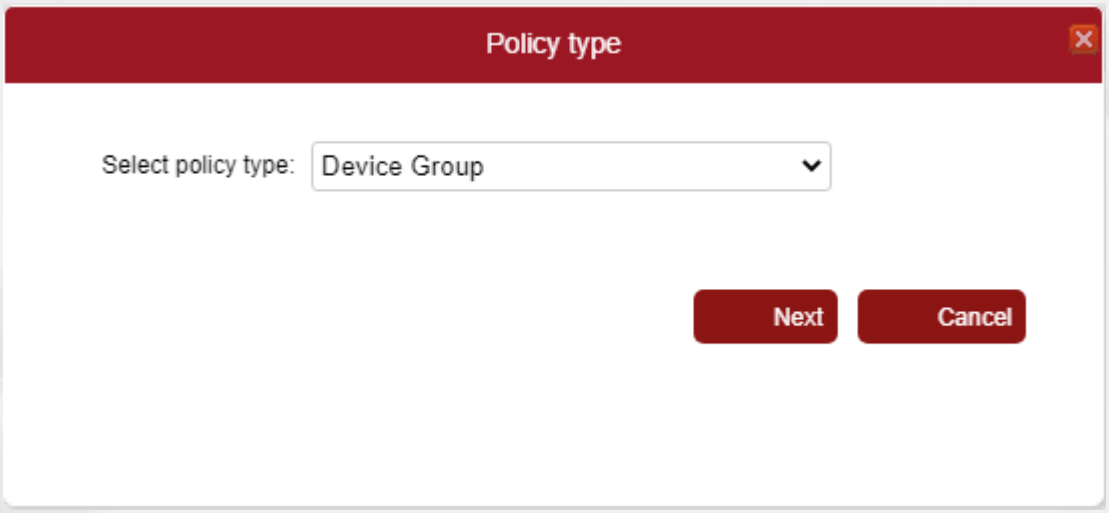

A list of Devices will be displayed.

Select a Device you wish to create the policy for and click 'Save'. It will create an empty policy.

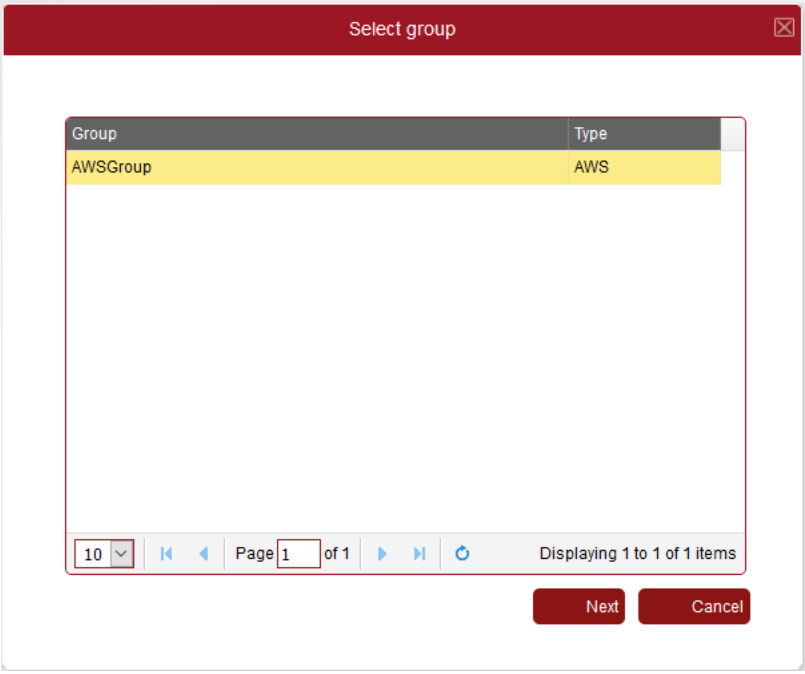
A specific device can be search based on a device name (min 2 characters) in the search field at the top.

### 14.3.1.2 Create a new Policy for device group

To create a brand new Policy for a device group, click on the 'Add' button.

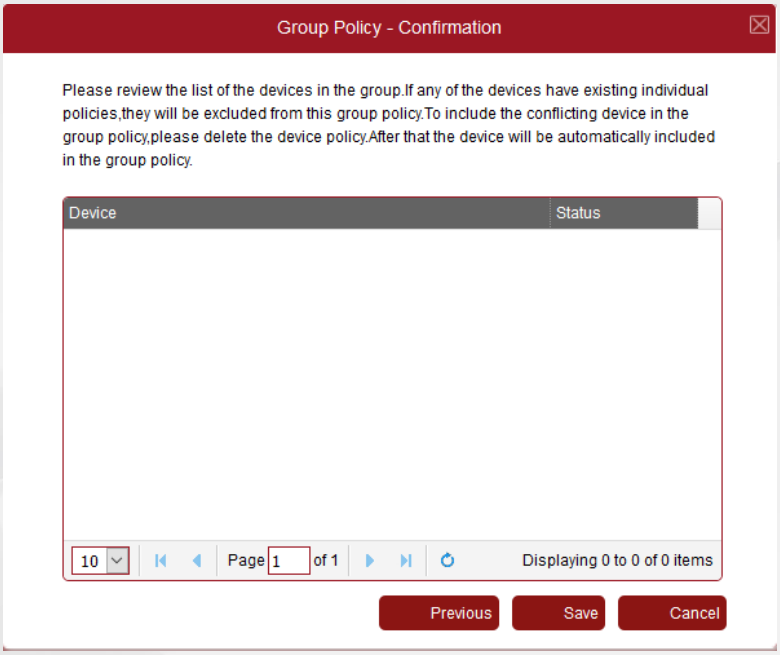



Select "Device group" policy type, click "Next" button




A list of Group will be displayed.

Select a Group you wish to create the policy for and click 'Next'.




If a device already has a device policy, the group policy will not be applied to it. If you want the device to receive the group policy you need to delete the device policy. After deletion of the device policy, the device will automatically receive the group policy.

Confirm the devices with conflicting device policies in this group and Click “Save” button.

To add encryption and access control policy click on ‘Modify’ for the newly created group policy

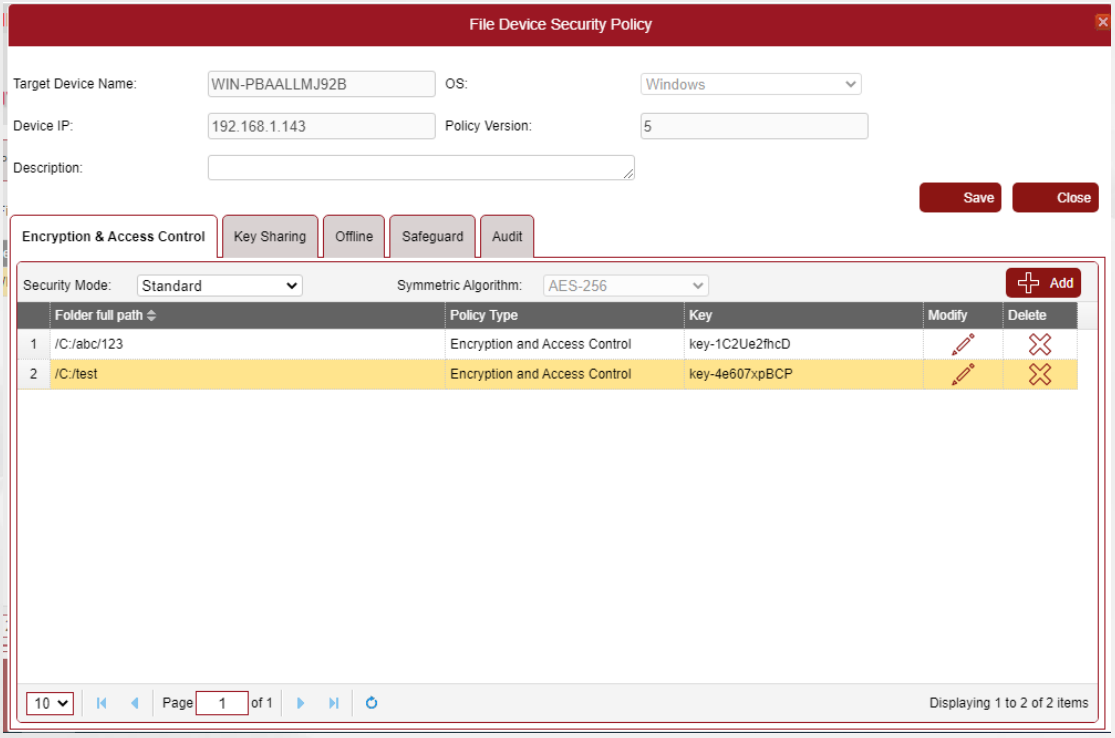
### 14.3.2 Encryption and Access Control policy

Transparent data encryption policy provide protection for files and folders using encryption, access control of both security methods.

If Encryption or “Encryption and Access Control” policy is applied to a folder, all new files created in the target folder will be encrypted with a File Key. Please note that existing files in the directory will not be encrypted automatically. To encrypt existing files, you will need to migrate them. Please refer to ‘Migration of files’ section.

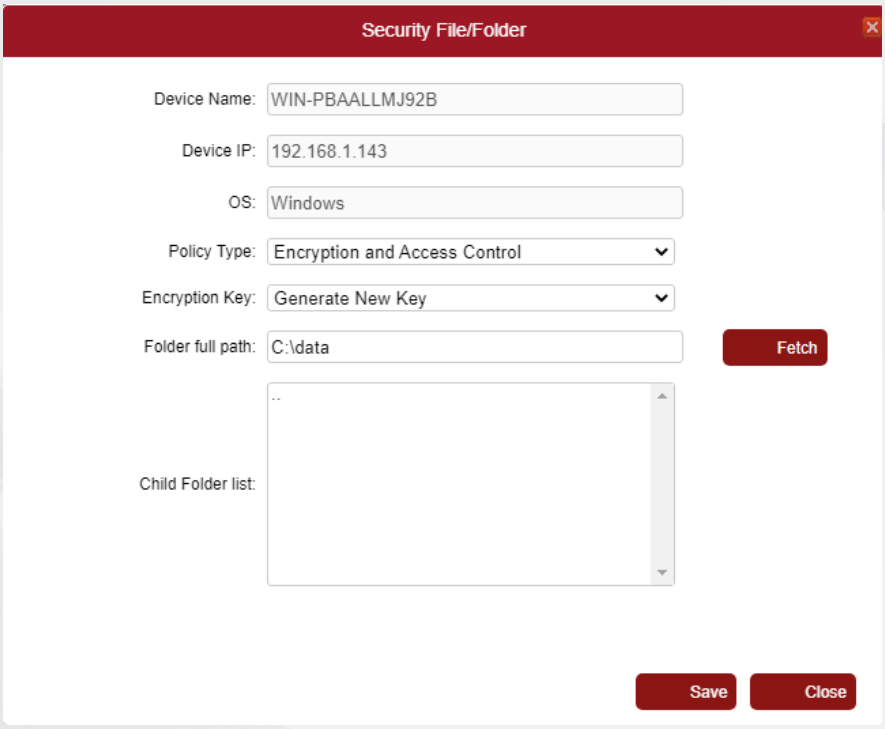
Each security policy also allows the following to be configured:

- **Symmetric Algorithm** - algorithm for encryption and decryption of files on the target Device. This algorithm can only be changed if there is no encryption rule and keys in ‘Key sharing’.

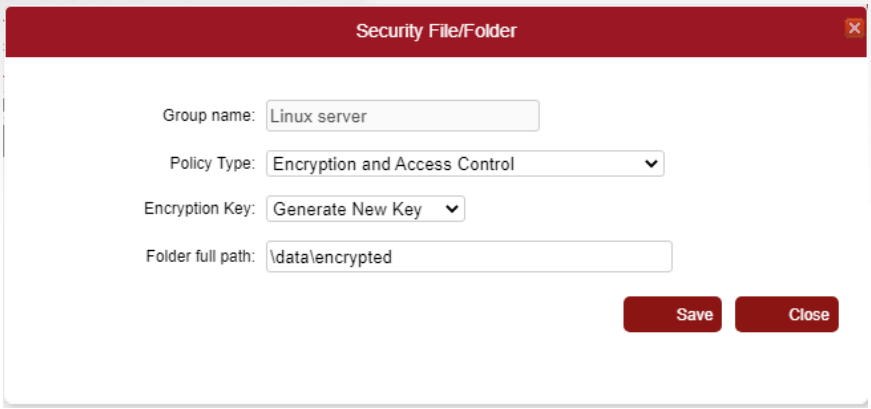



### 14.3.2.1 Add new Encryption & Access Control policy for folder

1. Click on the 'Policy' button on the left hand menu, then click on the 'Transparent Data Encryption Policy' tab.
2. Click on the 'Modify' icon next to the device or group to modify the policy
3. Now create the new folder policy
    a. Click the 'Encryption & Access Control' tab
    b. Click the 'Add' button
        i. Select 'Policy Type': either "Encryption and Access Control", "Encryption only" or "Access Control only".
        ii. (For 'Encryption only" or "Encryption and Access Control") In the 'Encryption Key', select either 'Generate New Key' to generate a new encryption key for this folder. or select an existing encryption key from the list
        iii. (For device) Click the 'Fetch' button, then use the Child File/Folder list to navigate to the folder to be secured. If 'Fetch' button does not retrieve a folder list and giving errors, please check the IP address of the agent and whether firewall for port 20000 is open on the agent side. If using DPM easyCloudPlus then use the public IP address of the agent.



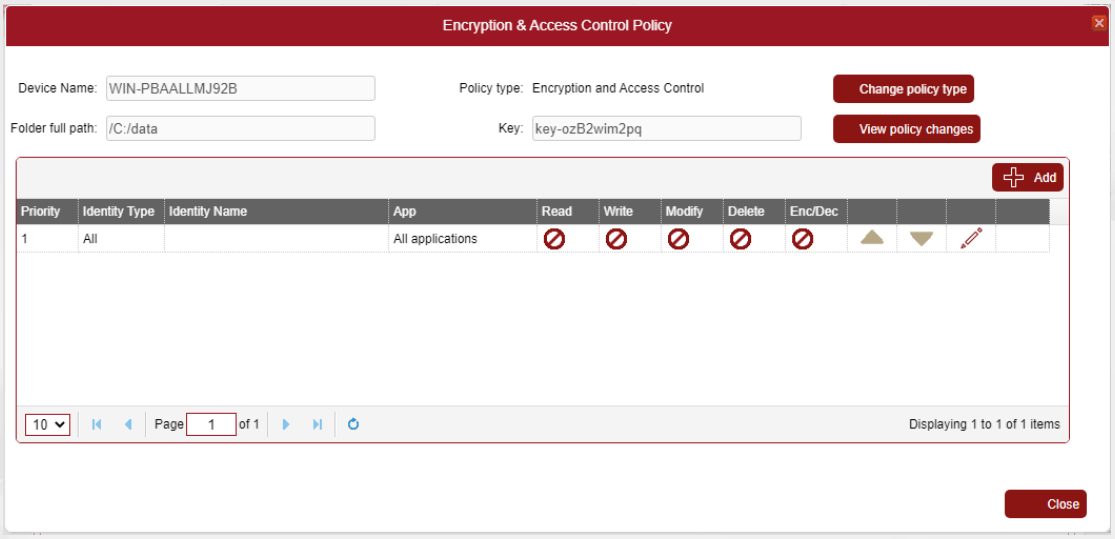

(For group) Type 'Folder full path'.




iv. Make sure that your target folder is displayed in 'Folder full path' field. Click 'Save'

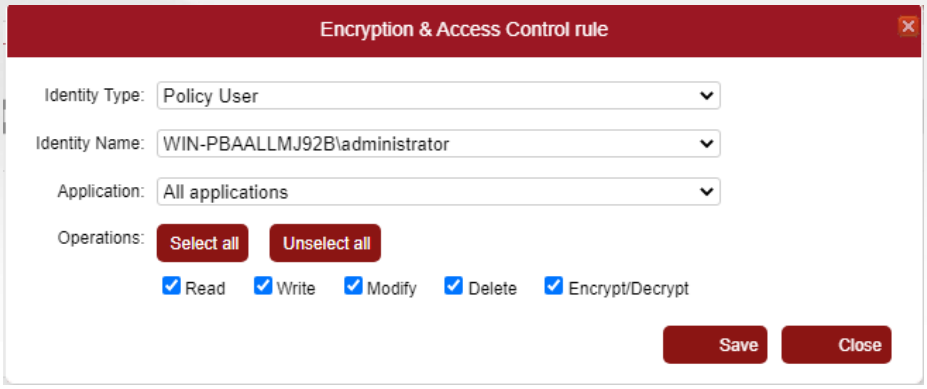
v. A new folder policy will be created. By default all users will have no access permissions. Next you need to modify the policy and assign permissions to relevant users and applications

vi. Click 'Modify' for the newly created folder policy




vii. Depending on the policy type you will see columns with Read, Write, Modify, Delete, Enc/Dec permissions configurations.

viii. Click “Add”




**Identity Type** - select either ‘All’, ‘Policy user group’ or ‘Policy user’. This is selecting the type of Users who will be allowed or disallowed access to use files.

**Identity Name** - select either the role name or user name of the user or user group

**Application** – select an application from the list or ‘All applications’ to apply the rule for all applications on the system. You can define a new application in ‘Policy’ - ‘Application Template’.

**Operations** – select or unselect operations to allow or disallow for this user/application: Read, Write, Modify, Delete, Encrypt/Decrypt. Depending on the policy type some selections will not be available. For example, for ‘Access control only’ type you will not see ‘Encrypt/Decrypt’ operation.

Read – permission to read and open the file in the protected directory

Write – permission to change the contents of a file in the protected directory

Modify – permission to create or renames files in the protected directory

Delete – permission to delete files in the protected directory. To actually delete files a user must have ‘Modify’ permissions as well as delete operation is considered to be a rename operation in Windows.

Encrypt/Decrypt – permission to encrypt and decrypt content of the file.

ix. Click “Save”

x. Continue adding more user/application rules if needed for the folder.

4. Done – new policy will be applied to the device or a group

All user/application rules have priorities which you can see in the left column. The highest priority rule has #1 and it will applied first by the agent. If the rule does not match the user/application accessing the file then the next priority rule will be applied until it finds a match. You can change priorities of rules by clicking Up and Down arrows.

Note that creating an encryption policy does not automatically encrypt existing files in the folder. Only files created in the folder or moved/copied into the folder will be encrypted.

To encrypt existing file, they need to migrate them. Please refer to section 'Migration of files'.

## 14.3.3 Migration of files

When applying an encryption policy to a folder with existing files it does not automatically encrypt existing files. Only newly created files will be automatically encrypted and decrypted.

There are two methods to encrypt existing files:

1. Using move out/move back
2. Using DPM migration tools

### 14.3.3.1 Move out/move back method

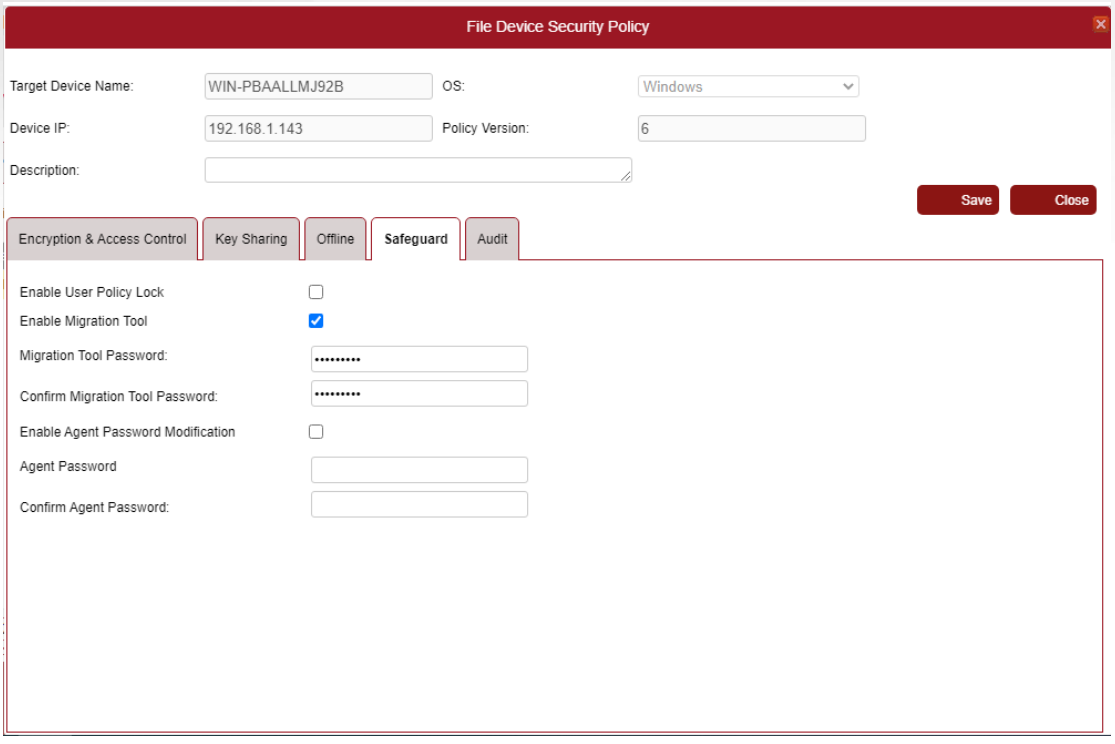
An authorized user needs to move all files out of the protected folder to a different clear folder. Then after applying a policy the files needs to be moved back.

Before moving files out record OS security permissions for the files. After moving files back assign the same OS permissions to the files.

### 14.3.3.2 Enable migration tool in Manager

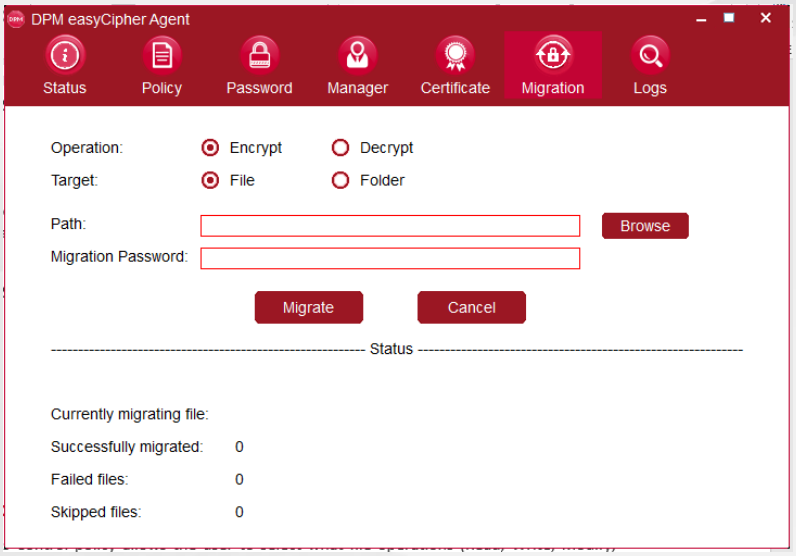
To use Migration tool in Windows Agent or dpmctl tool in Linux, a system user needs to allow it in DPM easyCipher – Policy – Safeguard tab for that agent.

Place a tick in 'Enable Migration Tool' ad set a migration password in 'Migration Tool Password' and 'Confirm Migration Tool Password'.



### 14.3.3.3 Using Migration tool in Windows

After migration tool is enabled in Manager, a migration of file on a Windows platform can be done via DPM easyCipher Agent Tray's 'Migration' menu. Only end users with Encrypt/Decrypt permissions for the folder can perform migration. The user must have Windows write permission for the folder as well.



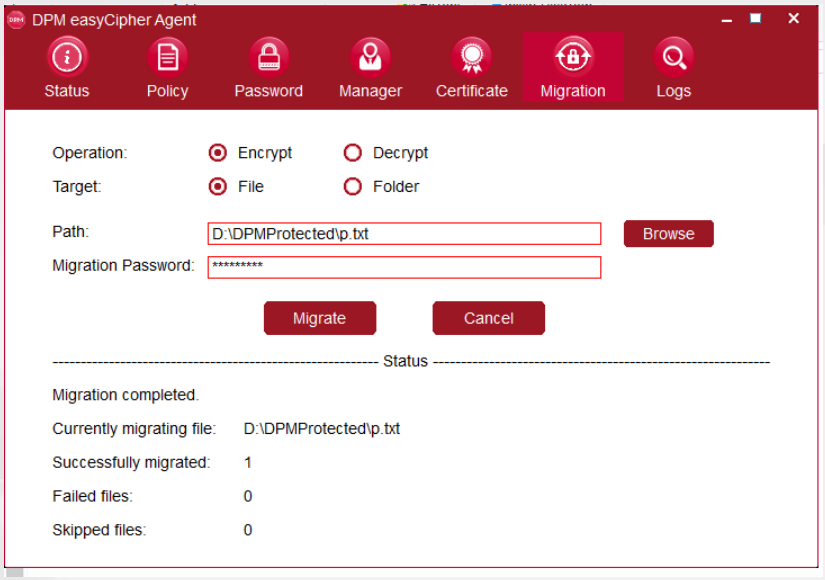

Migration can be performed for individual files of for all files in a folder.

To us the migration feature of the agent it must be enabled in the policy.

To migrate a single file:

1. Click 'Encrypt' for 'Operation' and 'File' for 'Target'.
2. Click 'Browse' and select a file that you want to migrate. The file must be inside the protected folder.
3. Type 'Migration Password' as set in the DPM easyCipher manager
4. Click 'Migrate'

When migration finishes the status will change to 'Migration completed'. If migration was successful you will see the count increased in 'Successfully migrated' line.




If migration did not succeed, then you will see an increased count in 'Failed files'. Check AgentTray.log for errors.

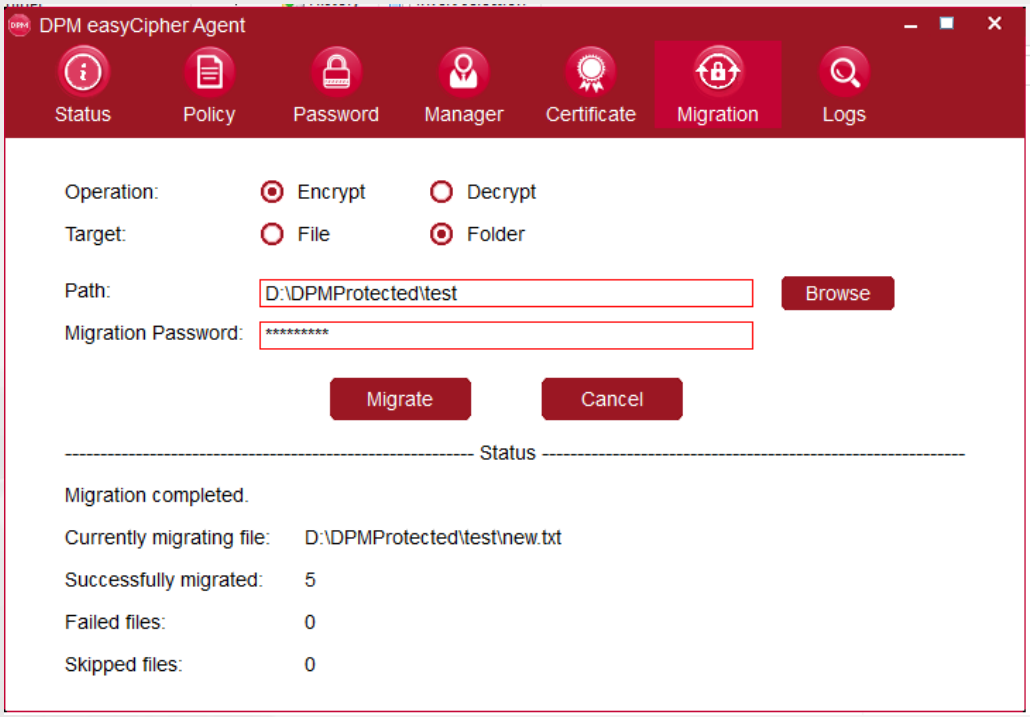
If the file was encrypted already then it will be skipped and you will see an increased count in 'Skipped files' line.

You can migrate the entire protected folder or subfolder at once.

To migrate a folder:

1. Click 'Encrypt' for 'Operation' and 'Folder' for 'Target'.
2. Click 'Browse' and select a folder that you want to migrate. The file must be the protected folder itself or inside the protected folder.
3. Type 'Migration Password' as set in the DPM easyCipher manager
4. Click 'Migrate'

When migration finishes, the status will change to 'Migration completed'. If migration was successful, you will see the count increased in 'Successfully migrated' line.




If migration did not succeed then you will see an increased count in 'Failed files'. Check AgentTray.log for errors.

If there are encrypted file in the folder then they will be skipped and you will see an increased count in 'Skipped files' line.

If you need to demigrate (decrypt) files then select 'Decrypt' option.

#### 14.3.3.4 Using dpmctl tool in Linux

After migration tool is enabled in Manager, a migration of file on a Linux platform can be done using dpmctl utility. Only end users with Encrypt/Decrypt permissions for the folder can perform migration. The user must have Linux read/write permission for the folder as well.

Migration can be perform for individual files of for all files in a folder.

To encrypt one file:

/opt/dpmfile/dpmctl -encrypt -f file_path -p

For example, /opt/dpmfile/dpmctl -encrypt -f /data/file1 -p

To encrypt all files in one directory

/opt/dpmfile/dpmctl -encrypt -d directory_path -p

For example, opt/dpmfile/dpmctl -encrypt -d /data/protected -p

To decrypt one file:

/opt/dpmfile/dpmctl -decrypt -f file_path -p

For example, /opt/dpmfile/dpmctl -decrypt -f /data/file1 -p

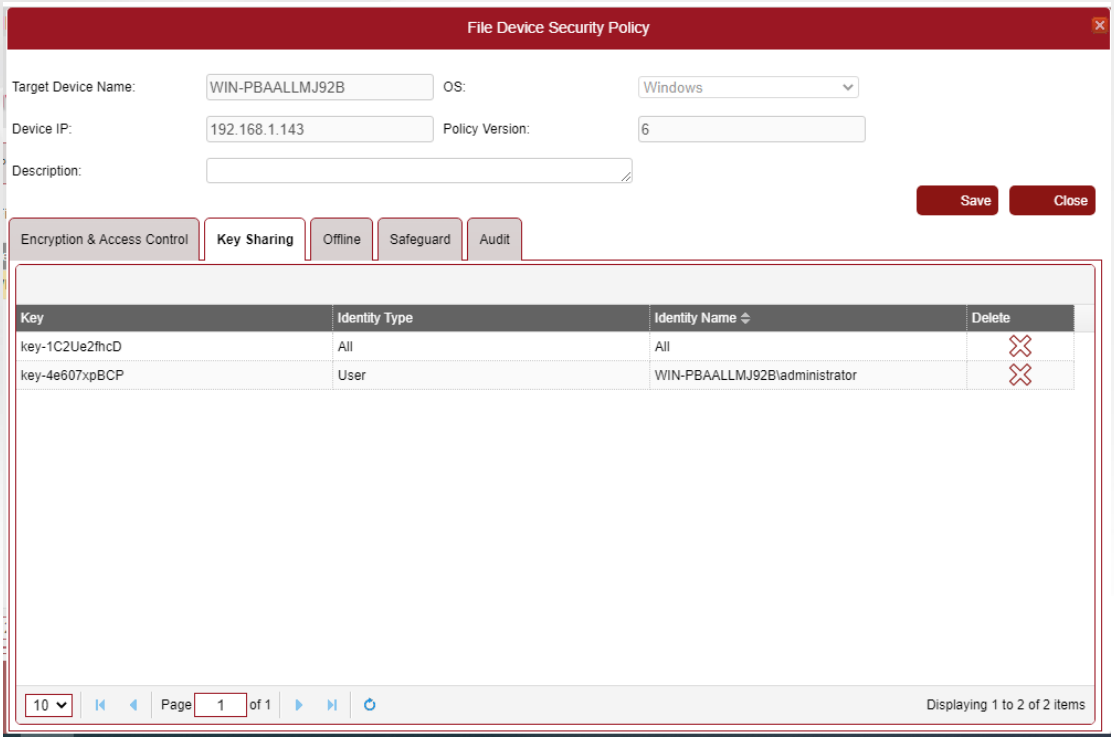
To decrypt all files in one directory

/opt/dpmfile/dpmctl -decrypt -d directory_path -p

For example, opt/dpmfile/dpmctl -decrypt -d /data/protected -p

### 14.3.4 Key Sharing

'Key Sharing' tab display current key permissions for users on the device.




It allows to quickly delete permissions for keys for users if needed.

If you need to add permissions for other users you need to do so via modifying a target folder policy and adding 'Encrypt/Decrypt' permission for that user. Please note that if you share keys between folder on the device, the user will be able to decrypt files encrypted with that key in all folders.

### 14.3.5 Offline Configurations

There are 3 modes of operation for the agent: Strict online, default (non-strict online), and offline mode.

- **Strict online mode** (Windows only) - an agent is required to be connected to the easyCipher server to be able to decrypt and encrypt. If it is disconnected it deletes all keys and policies from the memory and cannot decrypt data.
- **Default mode** – an agent is required to be connected to the easyCipher server initially during startup to receive keys and policies. Once the agent receives them it caches those in memory and continue using cached values while it is running. Even if an agent is disconnected from the manager it still can decrypt and encrypt data. However, if an agent is restarted or a system is rebooted, it requires to be connected to the manager again to receive keys and policies. This is the default mode.

- **Offline mode** – an agent downloads keys and policies locally and stores them as a file protected by an agent password. If an agent is disconnected from the manager it still continues encryption and encryption. When an agent is restarted or OS is rebooted a user needs to enter an agent password to unlock local keys.

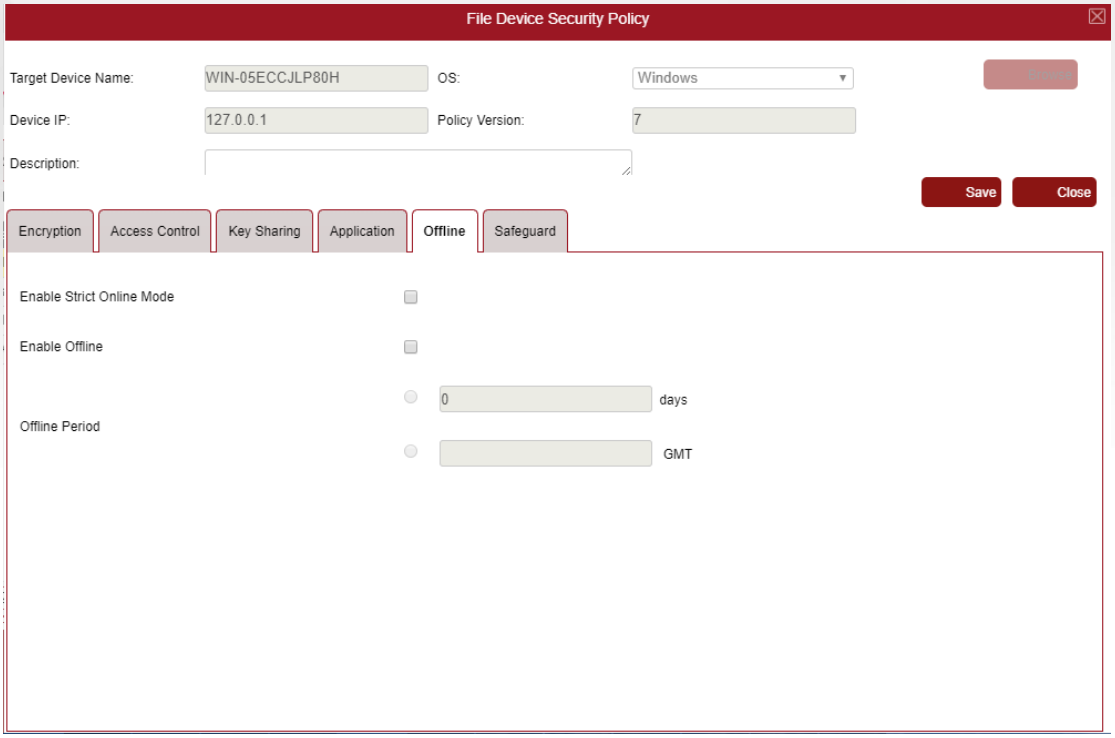
The Offline configurations tab allows the System user to setup the offline mode for an Agent.

Offline allows an Agent to go "offline" for a period of time. This means the Agent is allowed to function even if it is not connected to DPM easyCipher.

Offline mode allows users to take protected devices away from the DPM easyCipher and still be able to encrypt and decrypt the files to which they have access.

There are two steps to setting offline mode for a policy:

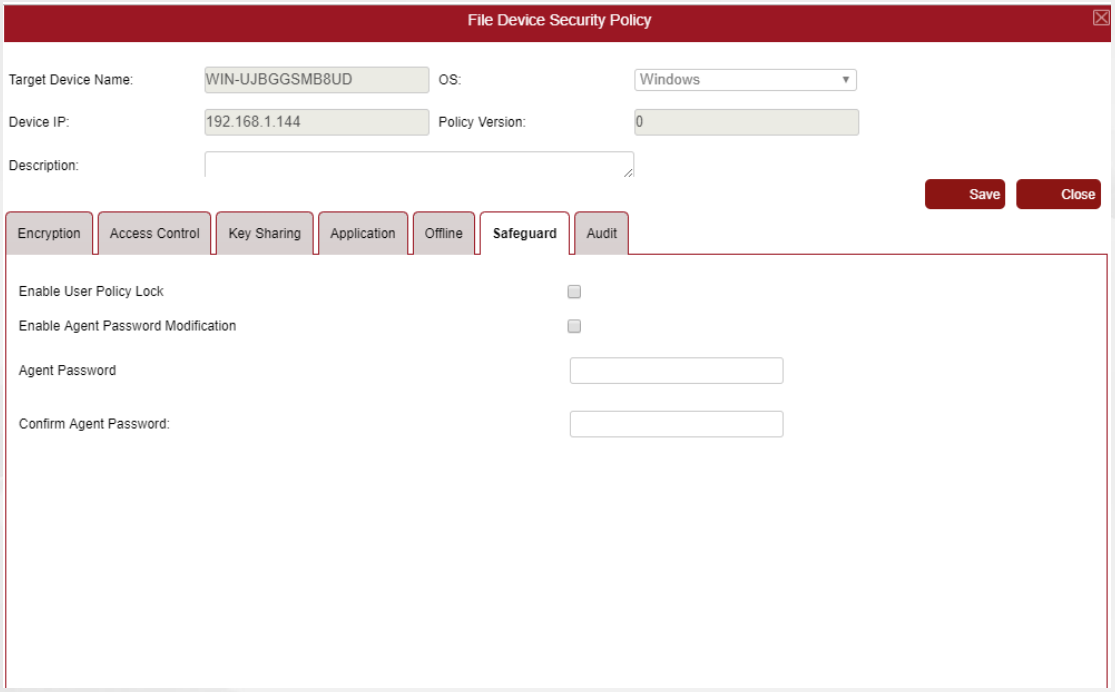
1. The Agent must be configured to allow offline mode
2. The User on the Agent must manually switch to work in offline mode. When an agent is switched offline all necessary keys and policy are downloaded to the agent and stored locally.




To configure offline mode, click on the 'Offline' tab. The tab will have the following fields:

- **Enable Strict Online mode** – forces an agent to work in the Strict online mode
- **Enable Offline** – whether or not this device is allowed to switch to offline mode
- **Offline period** – the number of days that the Offline period is valid for or the last valid date of the offline period. The offline period countdown starts when a user switches to offline mode at the agent side. If a user switches back to online mode and then to offline mode again, the offline period countdown starts again.

It is mandatory to conigure an agent password so that a user can switch to an offline mode. To configure it click on the Safeguard tab.




The tab will have the following fields:

- **Enable Agent Password Modification** – whether or not the offline password is allowed to be changed on the Agent side
- **Agent Password** – the password the user will need to enter on the Agent to switch to offline mode. If the 'Enable Agent Password Modification' setting is ticked, the user may change the password on the Agent device.
- **Confirm Agent Password** – confirmation of the Agent Password

### *14.3.6 Policy Lock Configuration (Windows agents only)*

The Safeguard tab allows the System User to configure whether an Agent is allowed to set the Policy Lock.

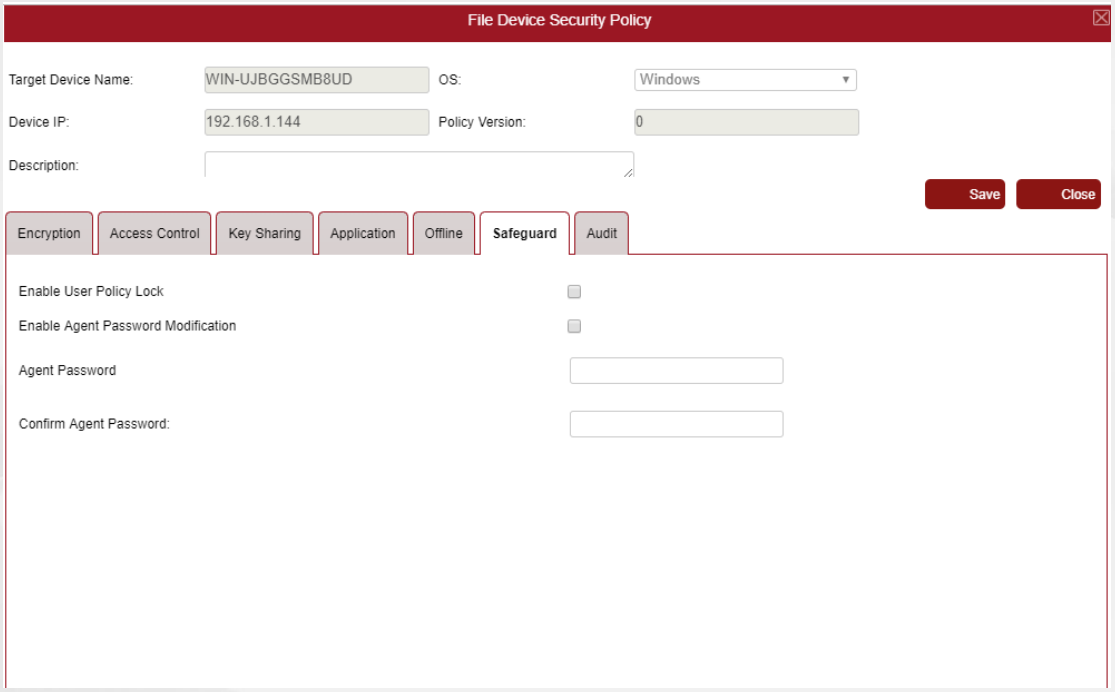
The Policy Lock, if enabled, allows a user on a Device to set a "Lock" on all polices applied to that Device. This sets the Device to "lockdown" mode, where no decryption of protected files is allowed. This mode is handy where a guest user might be accessing a machine and the device user wants to make sure that protected files remain secure.

There are two steps to setting lock mode for a policy:

1. The Agent must be configured to allow policy lock
2. The User on the Agent must manually set the policy lock when they wish to deny any access to their sensitive files

Once the User wishes to switch back, they must unlock the policy in the agent

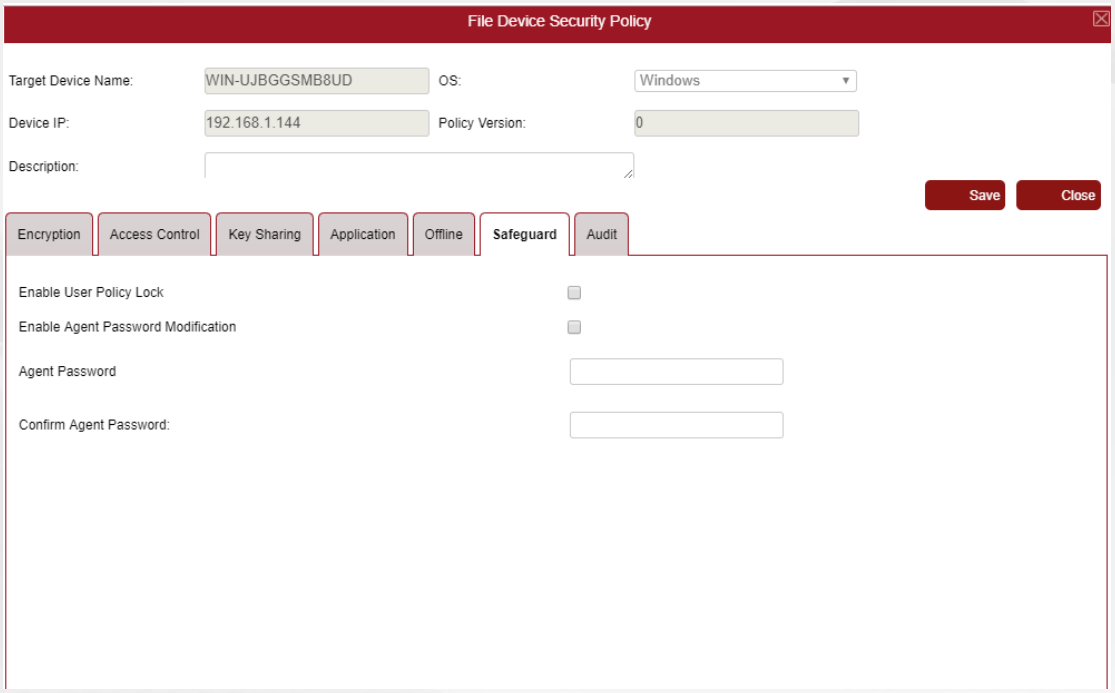
To enable a user to set Policy Lock on a Device:




1. Click on the ‘Safeguard’ tab
2. Tick the checkbox on the ‘Enable User Policy Lock’ setting
3. Configure ‘Agent Password’ and ‘Confirm Agent Password’
4. Click ‘Save’ on the Policy

## 14.3.7 Change Agent Password (Windows agents only)

Agent passwords are controlled from the DPM easyCipher. They can optionally be modified from the Agent, if the Agent policy allows the user to change the Agent password.




To change an Agent password:

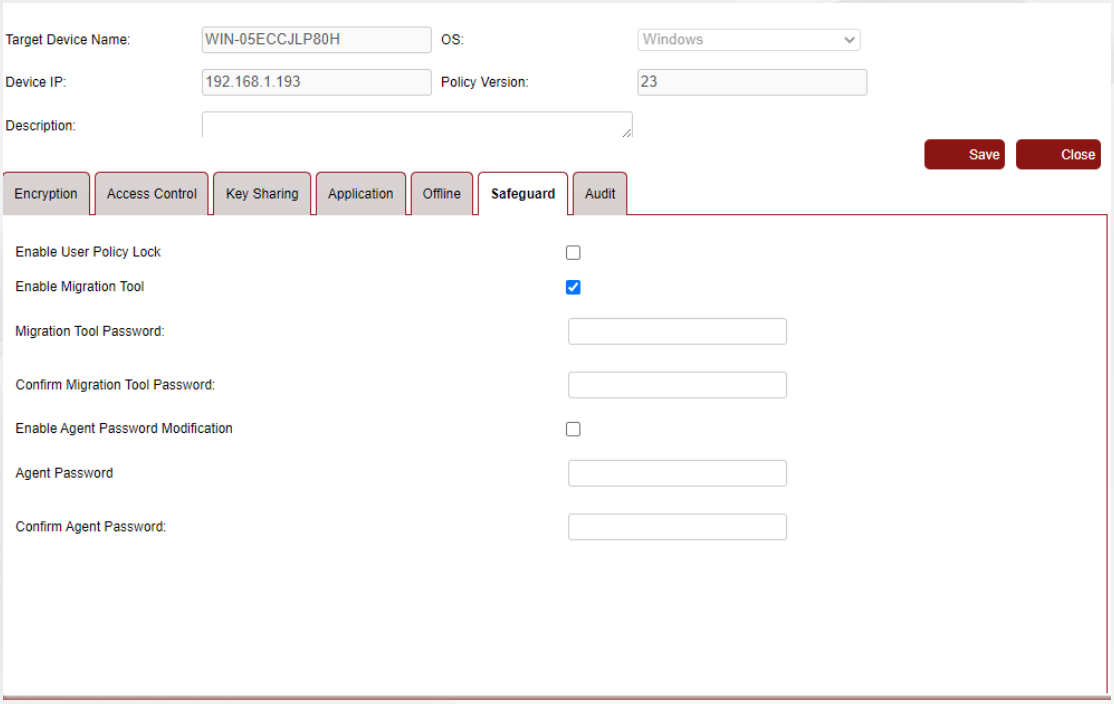
1. Click on the 'Safeguard' tab
2. Enter the new Agent password in the 'Agent Password' and 'Confirm Agent Password' text boxes
3. Click on the 'Save' button
4. Now the user of the protected device must use this password for offline mode or policy lock.

To enable or disable Agent Password changes from the Device side:

1. Click on the 'Safeguard' tab
2. Either tick the 'Enable Agent Password Modification' checkbox, or untick to stop Agent Password changes from the Device side
3. Click on the 'Save' button

### 14.3.8 Migration tool

To be able to use Migration tool on the agent to migrate files, the migration tool needs to be enabled in the manager.




To enable migration tool:

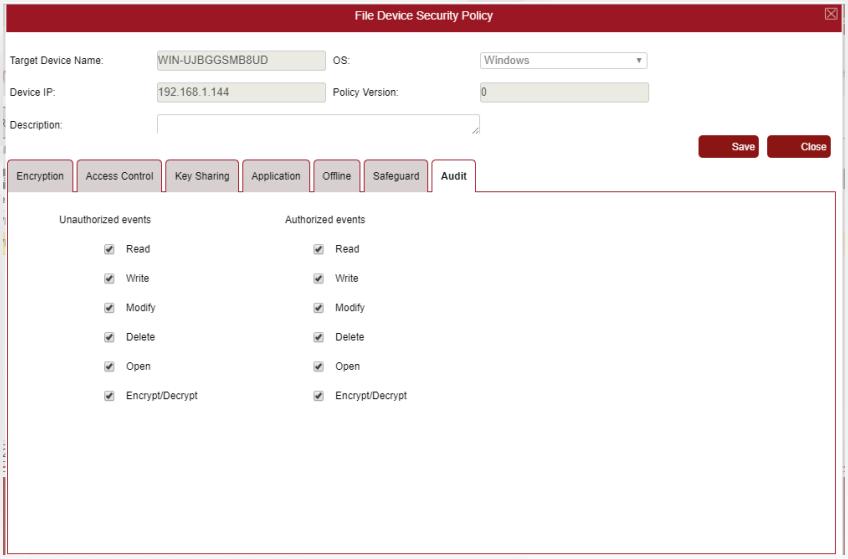
1. Click on the 'Safeguard' tab
2. Tick 'Enable Migration Tool'
3. Enter 'Migration Tool Password'. This password will be used when migrating files.
4. Retype the migration password in 'Confirm Migration Tool Password'.
5. Save the policy.

## 14.3.9 Audit policy

By default, all file events are recorded for authorized and unauthorized users. In some cases, it is only required to audit unauthorized access. In other cases, for example, when protecting databases, a database will access the protected files so frequently that it can generate thousands of events overflooding the network and system. So it is desirable to limit a number of events generated.

In that case auditing of some file events can be disabled in 'Audit' tab of the policy.

Click 'Audit' tab and tick or untick desired events.




## 14.3.10 Modify Transparent Encryption Policy

Existing policies can be modified by clicking on the 'Modify' icon next to the Device containing the policy to modify.

See the Add Policy section for more information about configuring policies.

It is possible to remove individual folder policies by clicking on the modify button next to the policy to modify.

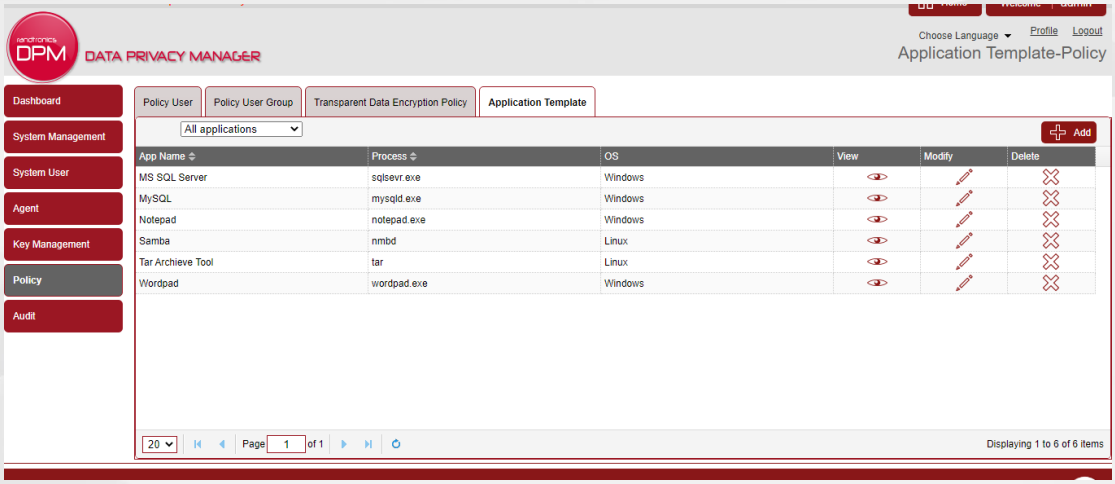
## 14.3.11 Delete Transparent Encryption Policy

To delete an entire policy, click on the 'Delete' icon next to the Device. This will remove all policies on the device.

To delete an individual folder policy, modify the policy then click on the 'Delete' icon next to the folder policy to delete.

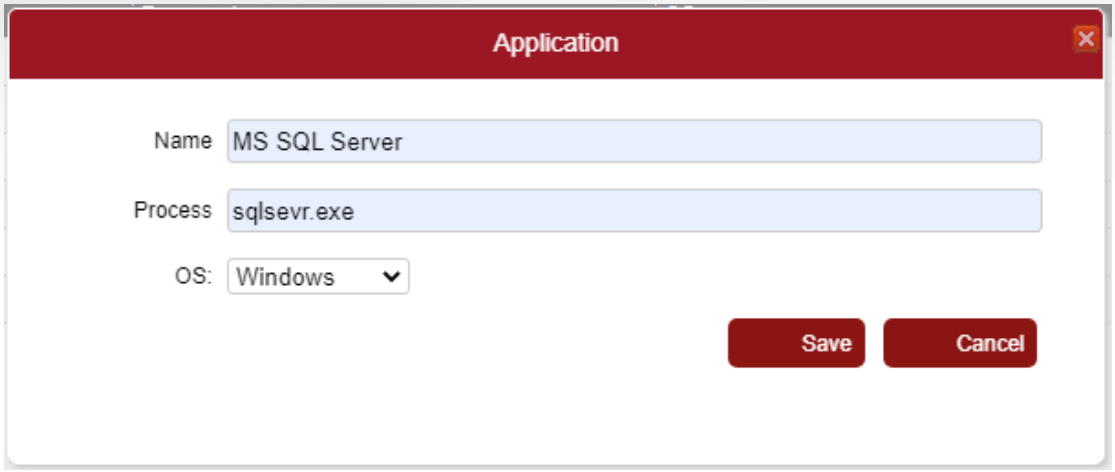
## 14.4 Application Template

To configure a policy for a specific application you need to create an application template first.




### 14.4.1 Add an Application Template

To add an application template click 'Add'




The Application popup includes:

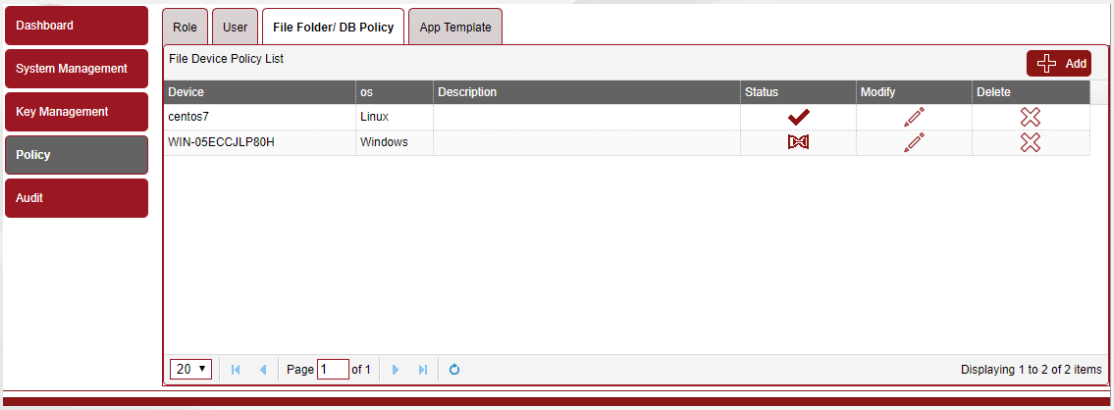
- **Name** – the user friendly name of the application. This is used for display purposes on the DPM easyCipher
- **Process** – the name of the process in Windows (eg. winword.exe) or a full path of the application Linux (eg. /usr/bin/vi)
- **OS** – the type of operating system this application runs on. Can be either Windows or Linux

Once an application template is created, it can be used in a folder policy.

## 14.5 Policy status

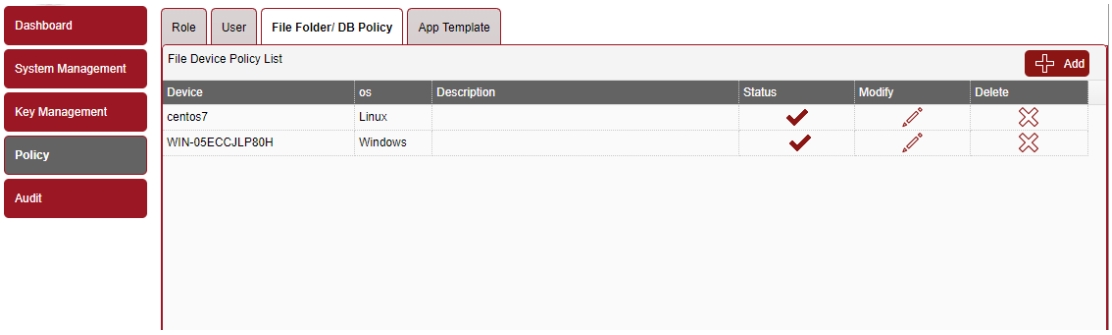
When modifying and saving a Transparent Data Encryption Policy it is saved to the backend database and then distributed to the agents.

It may take up to a minute to distribute an updated policy. During that time a policy status will show a rotating hour glass icon.




To refresh a status of the policy click on the circle arrow at the bottom of the list.


Once the policy is applied the status will show a tick icon.



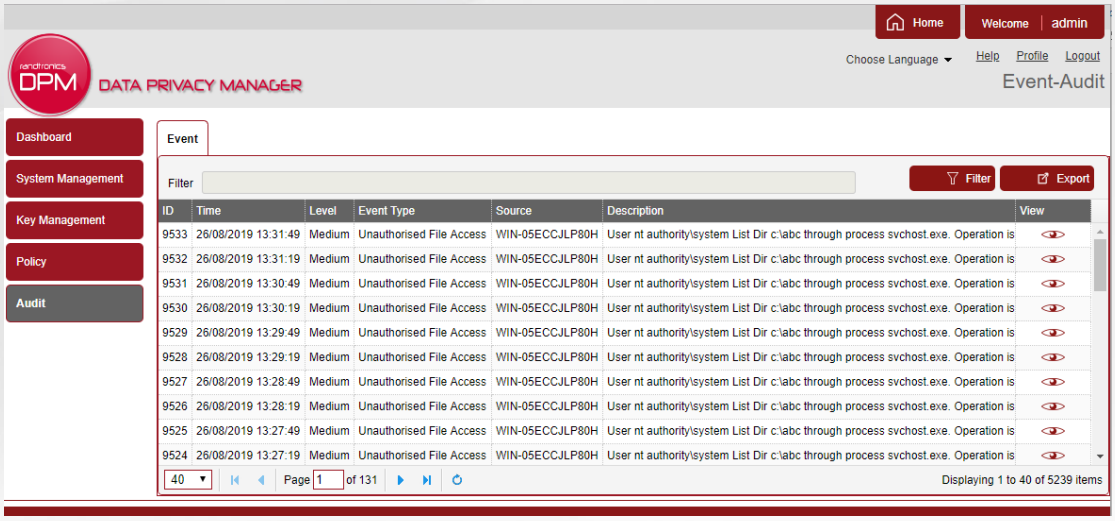
# 15. Audit Management

The Audit screen lists all activities that have been performed on the DPM easyCipher software. It is possible to help troubleshoot problems and track abnormal behaviour with these log records.

## 15.1 Event

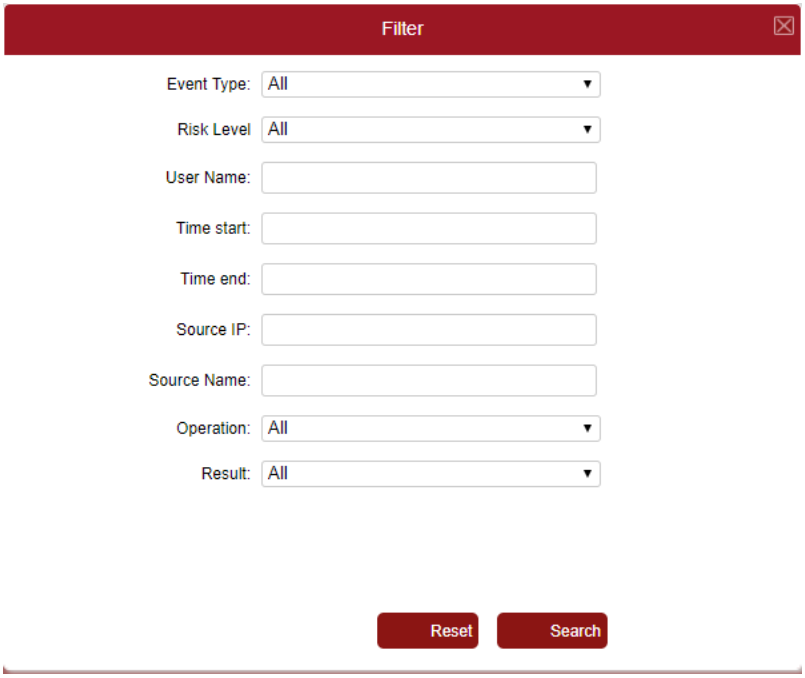
The Event tab displays all logging events.

To view the Events, click on the 'Audit' button in the left hand menu.




## 15.2 Filter Audit events

To filter audit event click 'Filter' button.



Configure a filter to search specific events based on:

- **Event Type –** event type such as 'Authorized file access', 'System management' etc.
- **Risk Level –** Low, Medium, High, All
- **User Name –** the name of the system user or end user
- **Time start –** date to search from
- **Time end –** date to search to
- **Source IP –** IP address of a target device or system user working system
- **Source Name –** Hostname of a target device or system user working system
- **Operation –** Operation such as 'Read', 'Write', 'Login' etc.
- **Result –** Success or failure

Click 'Search' to remember the filter and search audit event.

Click 'Reset' to clear the filter.

## 15.3 Exporting audit data

DPM easyCipher allows audit data to be exported. Data is exported in comma separated format (CSV) which allows the data to be imported into other tools for analysis, such as Microsoft Excel. Maximum 100,000 latest records are exported based on a filter.

To export audit data:

1. Navigate to 'Audit'-'Event' tab
2. To export a subset of the event data, enter the filter options either in the Event Search Result tab settings, or the Event Type tree. If no filtering options are given all event data will be exported
3. Click the Export button. Depending on the amount of data, the DPM easyCipher will retrieve the audit events and create a zipped CSV file that will download to the browser downloads folder
4. Done – the audit data zip can be unzipped and opened

# 16. Troubleshooting

## 16.1 Agent and Manager connection problems

The following is a troubleshooting checklist designed to help users resolve problems with the Agent and Manager connecting.

1. Login into the DPM easyCipher, click on the System Management button, then click the Devices tab. Find the device in the list, click on the Details icon then click the Test button. The Manager will attempt to ping the Agent and will display the result
2. If the Agent is not displayed in the device list, then it has not been able to connect to the Manager to register. By default, it will attempt to connect over port 10000 and 10005:
    a. Check that the firewall on the Manager server will allow an inbound TCP connection over port 10000 and 10005
    b. Use telnet from the Agent server to confirm it is able to connect to the Manager server on port 10000 and 10005
    c. Check that the DPM easyCipher Agent service is running
    d. Check that the Agent has the correct IP address for the DPM easyCipher. In Windows this can be done by clicking on the tray icon and selecting the Manager button. On Linux this can be done by viewing the /opt/dpmfile/config/AgentICETLS.ice file and looking for the IP address in the Manager.ConfigManager.Proxy value
    e. Try restarting the DPM easyCipher Agent service
    f. Check the Manager logs for Agent connection issues. In Windows this can be done by clicking on the tray icon and selecting the Logs button. In Linux this can be done by view the /opt/dpmfile/log/AgentServer.log file. Look for errors in this file to indicate what is not working
    g. Check the DPM easyCipher Server logs for errors. This file will be under the <DpmInstallDir>/DPMFileServer/logs directory.
3. If the Manager is not able to Ping the Agent:
    a. Check that that the firewall on the Agent server allows connections on port 20000 (the default port for Manager to Agent communications)
    b. Try a telnet from the Manager server to the Agent server over port 20000
    c. Check whether the Agent has a certificate. Click on the System Management button, then click on the TLS tab, then click on the Trusted Agents tab.
        i. If “Trust All Agents” has been ticked, then the system will automatically generate a certificate for the Agent and it should be displayed in the list
        ii. Otherwise, if “Trust All Agents” is not ticked it is necessary to generate or upload a certificate and assign it to the Agent
    d. Check that the DPM easyCipher Agent service is running
    e. Check time zone and time on both Manager and Agent system. They must match. Otherwise, a TLS certificate will be accepted and the connection cannot be established. If time had to be adjusted on any of the system then delete the agent from ‘Trusted Agents’ list and let it re-register again.

## 16.2 Manager problems

The following is a troubleshooting checklist designed to help non easyCloudPlus SaaS users resolve problems with the Manager. DPM easyCloudPlus SaaS users should contact Randtronics support.

1. Check that the DPM easyCipher Web and DPM easyCipher Server services are running
2. Restarting the service can often fix problems, if the service is not running or does not appear to be responding, try restarting it
3. Check that the MySQL or SQL Server database backend is running and accessible from the DPM easyCipher
4. Check that the credentials to the backend database are correct. These are stored in the <installDir>/tomcat/conf/n8_jdbc.properties files
5. DPM easyCipher logs are in two places. These logs will log errors and exceptions that can indicate what is going wrong.
    a. <installDir>/tomcat/bin/dpmfilemanager.log
    b. <installDir>/tomcat/logs/*
6. Check that the DPM easyCipher and DPM easyCipher Server are listening on the correct ports. In linux, run the following as the root user on the Manager server:

netstat -tnlp | grep DPM

By default, DPM easyCipher Web should be listening on 8443 and 8448 , and DPM easyCipher Server should be listening on 10000 and 10005

7. The DPM easyCipher Server logs to the <installDir>/DPMFileServer/logs/ directory

## 16.3 Agent problems

The following is a troubleshooting checklist designed to help users resolve problems with the Agent

1. Check that the DPM easyCipher Agent is running and restart it
2. Check that the Manager can connect to the Agent by logging into the DPM easyCipher and click on the Test button in the System Management->Device screen. Follow the steps in section 9.1 if the test fails
3. Check that the DPM easyCipher Agent is listening on the correct ports. In Linux, run the following as the root user on the Manager server:

netstat -tnlp | grep linuxagent

By default, linuxagent should be listening on 20000

4. Check the agent logs. In Windows this can be done by clicking on the tray icon and selecting the Logs button. In Linux this can be done by view the /opt/dpmfile/log/AgentServer.log file. Look for errors in this file to indicate what is not working

## Credits

DPM easyKey, DPM easyCipher and DPM easyCipher Agent are products of Randtronics Pty Limited.

All other product and company names mentioned are the trademarks of their respective owners.

## Contact

Randtronics Pty Limited

ABN: 99 101 584 329

Suite 1, Level 1, 64 Talavera Rd North Ryde, NSW 2113, Australia

Email: enquiry@randtronics.com

www.randtronics.com

support@randtronics.com

## Copyright Information

Contact Randtronics to arrange an evaluation download - **enquiry@randtronics.com**

**Randtronics**

America: Milpitals, CA. Ph: +1 650 241 2671
Australia: North Ryde, NSW. Ph: +614 1822 6234

**www.randtronics.com**