DPM easyCipher

Installation Guide

Version 8.2

DPM easyCipher

Installation Guide

Version 8.2

Contents

1 Overview

This document covers the installation, uninstallation and upgrade procedure for the DPM easyCipher software.

DPM easyCipher solution consists of :

1. DPM easyCipher Agent – performs the encryption and protection of data installed on user laptops, PCs and servers. DPM easyCipher Agent needs to be installed on each laptop, PC or server that needs data protection.
2. DPM easyCipher manager – installed on a central server (recommended), laptop or PC. The DPM easyCipher acts as a central point to manage policies on user laptops or PCs or servers.

DPM easyCipher requires a backend database to store application information.

This can either be a standalone database that needs to be installed and ready before starting the DPM easyCipher installation, or can be a bundled database that is installed during the DPM easyCipher installation.

Once the software has been successfully installed, it is necessary to import a license before the software can be used.

If using Randtronics easyCloudPlus SaaS offering then DPM easyCipher manager will be preinstalled. Only DPM easyCipher Agent installation will be required.

2 Requirements

2.1 DPM easyCipher

The server hosting the DPM easyCipher will require the following minimum specifications.

CPU	2 cores 2.1 GHz 64 bit
Memory	4 GB or greater
Disk Space	At least 30 GB free disk space
Operating System	64 bit OS required Windows Server 2012 R2 and up RHEL or CentOS 7 and up SUSE Linux Enterprize Server 12 SP2 and up Ubuntu 18.04 or up

2.2 DPM easyCipher Backend Database

The server hosting the DPM easyCipher database will require the following minimum specifications. For more details please check the database vendor's recommended requirements.

CPU	2 cores 2.1 GHz 64 bit
Memory	4 GB or greater
Disk Space	At least 80 GB free disk space
Operating System	Check OS requirements for the chosed database vendor
Database	MySQL 5.7 or 8.0 MS SQL Server 2014 or later All databases must have case sensitivity off

Note that for MySQL backend databases the max connections should be set to 500 if more than one DPM software is using the same MySQL backend database.

Please see the MySQL documentation for setting the max connections value.

2.3 DPM easyCipher Agent

Any laptops, desktops and servers with the DPM easyCipher Agent installed will require the following minimum specifications.

CPU	x86_64 architecture, AES_NI enabled
Memory	1 GB or greater
Disk Space	At least 512M free disk space
Operating System	Windows 8.1 and up, Windows Server 2012 R2 and up RHEL and CentOS with Linux kernel 3.10 Others – for more supported platforms please see “DPM easyCipher Agent - Supported versions.pdf”

2.4 Network access

2.4.1 On-premise

DPM easyCipher console URL	https://<server>:8443/dpmeasycipher
Ports (TCP)	Need to be open in a firewall on DPM easyCipher: 8443 - HTTPS Web console port 10000 – Policy retrieval port 10005 – Agent registration port

	Need to be open in a firewall on DPM easyCipher Agent: 20000 – to browse folders and ping from DPM easyCipher If this port is not opened encryption will still work but policy path will need to be configured manually.
Initial login	Username: admin Password: admin

2.4.2 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. The connection from the manager to the agent requires the following to be configured: 1) public IP address mapped to the agent 2) Port 20000 opened for external connections These are used to browse folders when configuring policies and pinging from the manager. If you 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 Password: admin

3 DPM easyCipher installation process

This section will document the steps to installing and starting the DPM easyCipher on-premise. If using DPM easyCloudPlus then this is not required.

The installation procedure for DPM easyCipher is:

1. Prepare the backend database (only applies if using an existing MS SQL Server or MySQL database)
2. Install the DPM easyCipher application
3. Open the correct firewall ports
4. Access the application and request a license for the software

3.1 Backend database

DPM easyCipher requires a database to store application configuration information.

There are three options:

1. Use an existing Microsoft SQL Server database
2. Use an existing MySQL database
3. Install the MySQL database bundled with the DPM installer – this option is only available for the Windows version of DPM easyCipher

For options 1 and 2, please refer to Microsoft SQL Server or MySQL database installation user manual for database installation.

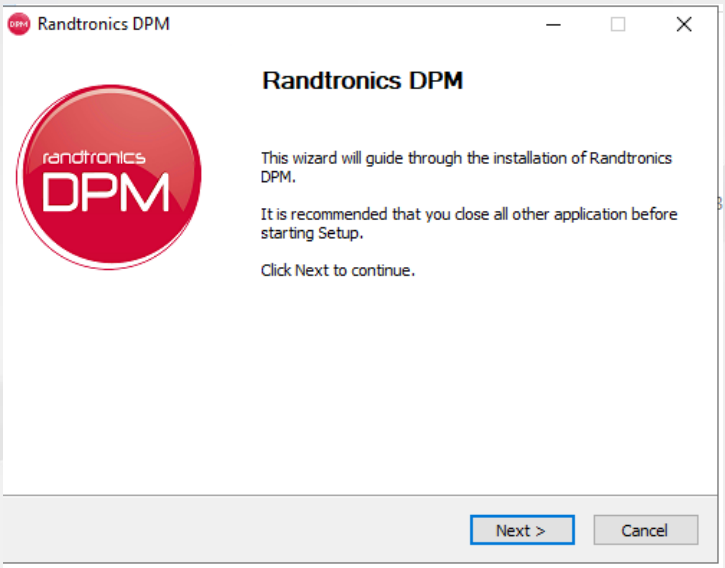
3.1.1 Database initialization - Use existing MySQL database on Windows

MySQL database must be already preinstalled and ready for use. It must be configured to allow remote access for 'root' user. Firewall rules must allow accessing the port that the database is using (default port it 3306).

Database initialization can be performed on its own directly on the database server or as a part of the main installation.

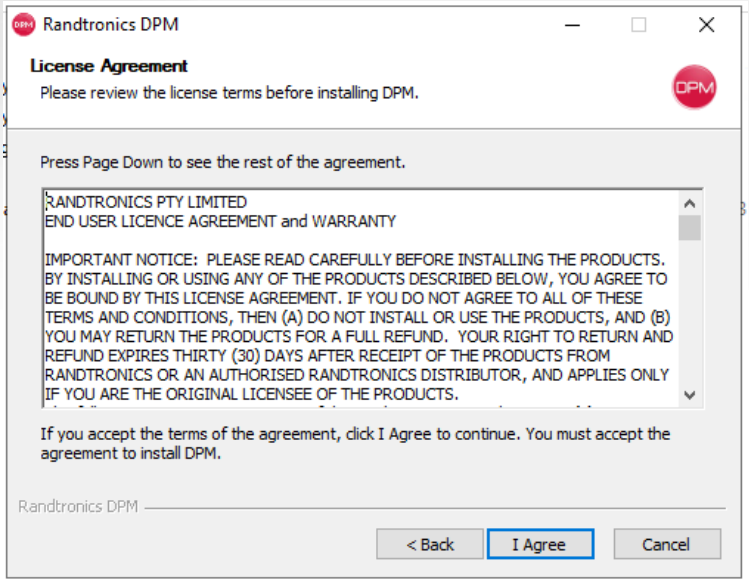
3.1.1.1 Database initialization on the database server – direct option

1. Start the installer



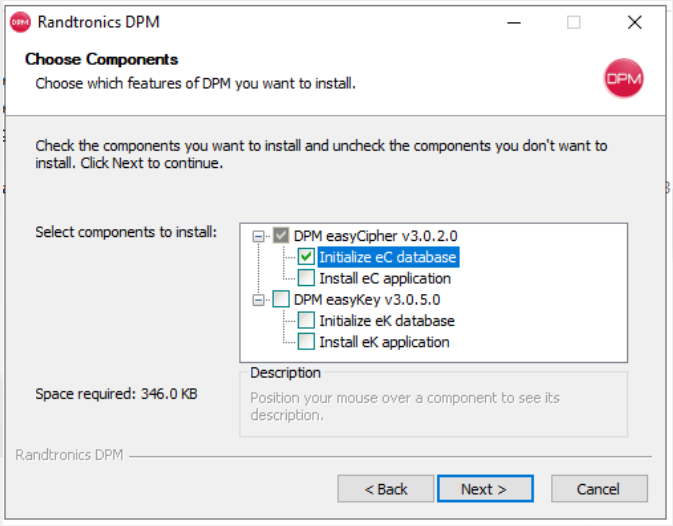
Click on the Next button

2.



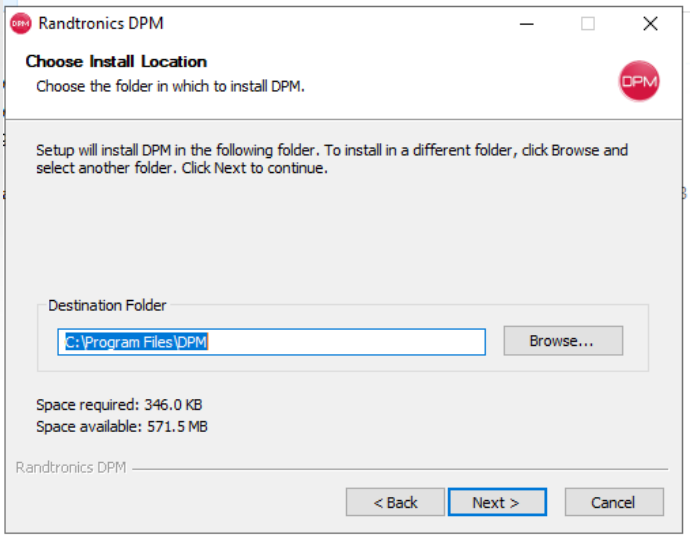
Click ‘I Agree’ to agree with the license agreement

3.



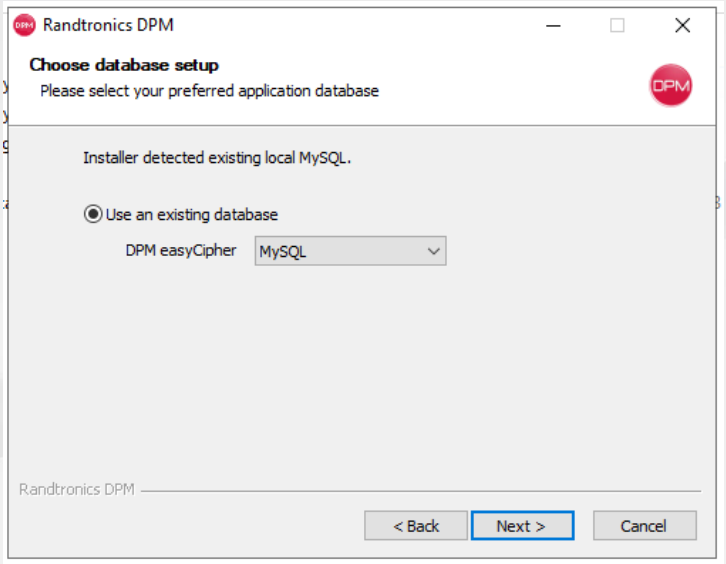
Select 'Initialize eC database'

4.



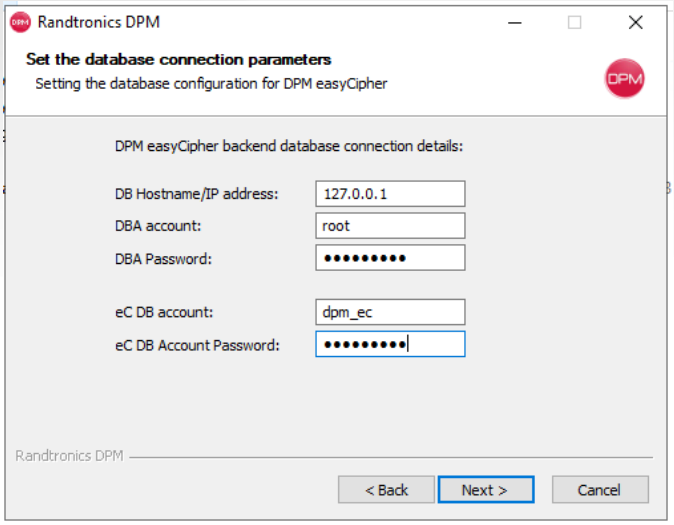
Set the destination installation folder

5.



Select the desired type of database: MySQL or MS SQL Server

6.



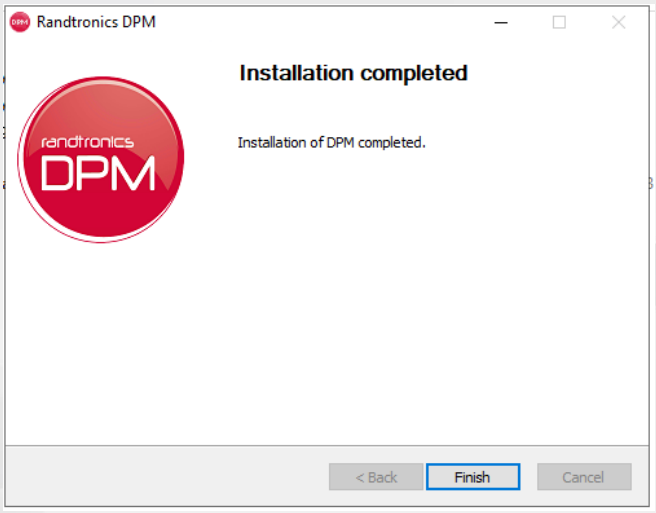
For this step, you will need to have the account details of the root or DBA user of the MySQL database or 'sa' user of MS SQL Server database.

Enter the username and password of the root/DBA user.

Configure a new database user name and password that DPM easyCipher will use to connect to the database. Default is dpm_ec.

Click 'Next' to begin the process of initialization of the backend database. The installer will create a new database 'dpm_ec' in the target database server.

7.



Click Finish to close the installer.

3.1.2 Database initialization – Use existing MySQL database on Linux

MySQL database must be already preinstalled and ready for use. It must be configured to allow remote access for 'root' user. Firewall rules must allow accessing the port that the database is using (default port it 3306).

The DPM easyCipher database script will be run from the command line:

1. Untar the database init file

   ```
   tar xvf DPM_easyCipher_Linux_x.x.x.x_database_init.tar.gz
   ```

2. Change to the DPM easyCipher database init directory

   ```
   cd dpmeasycipher_database_init
   ```

3. Run the database init script and answer the prompts

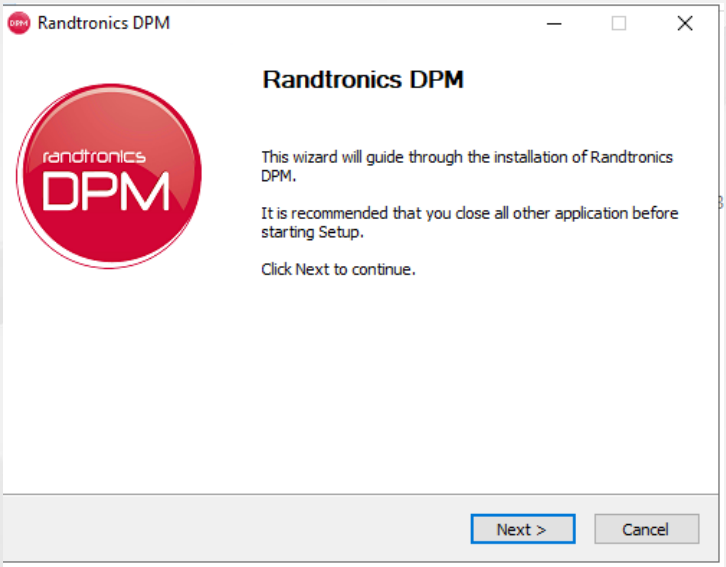
   ```
   ./install.sh

   Please enter the backend MySQL database IP address or
   hostname:[127.0.0.1]:
   Please enter DBA user[root]:
   Please enter DBA password[]:
   The installer will now create a new database user for the DPM
   easyCipher application
   Please enter the new DPM easyCipher database username[dpm_ec]:
   Please enter password[T3str@123!]:
   ```

3.2 DPM easyCipher Installation

3.2.1 Windows Installation

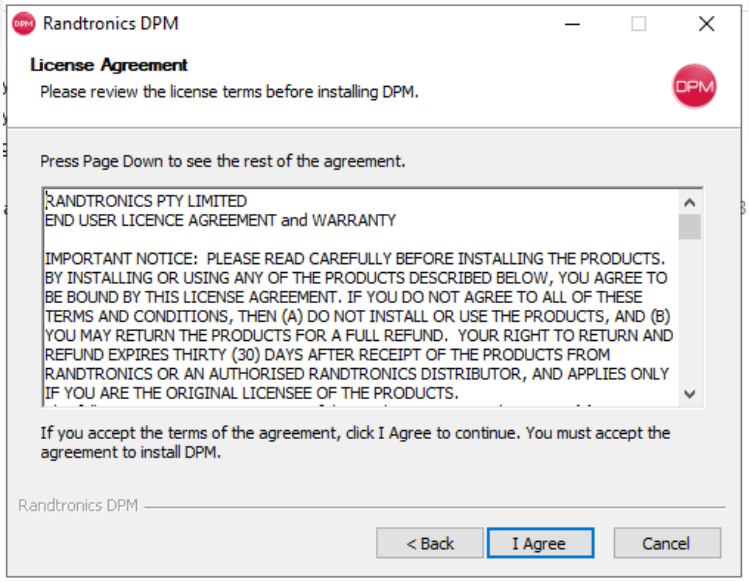
This section will cover installation of the DPM easyCipher in a Windows environment

To start installation of the DPM installer, right click on the DPM_vx.x.x.x.exe file and click the Run As Administrator option.

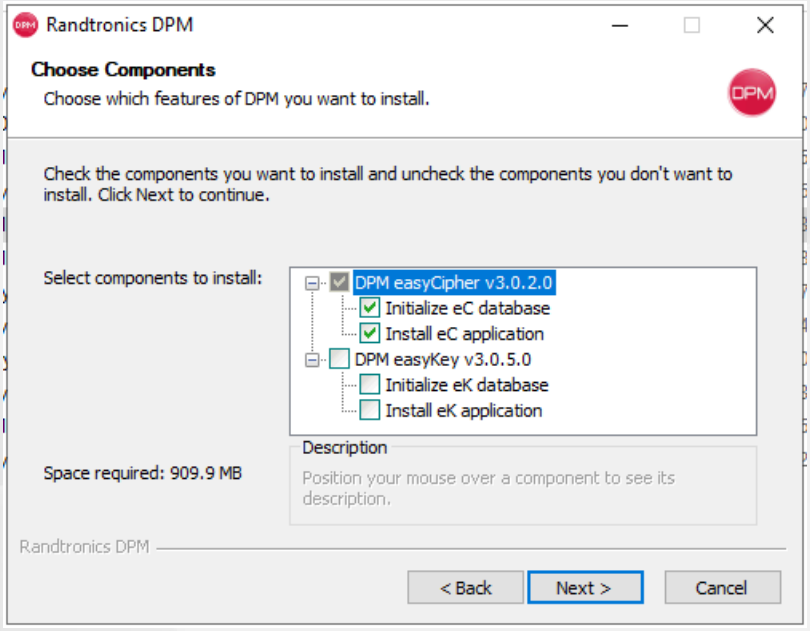


Click on the Next button

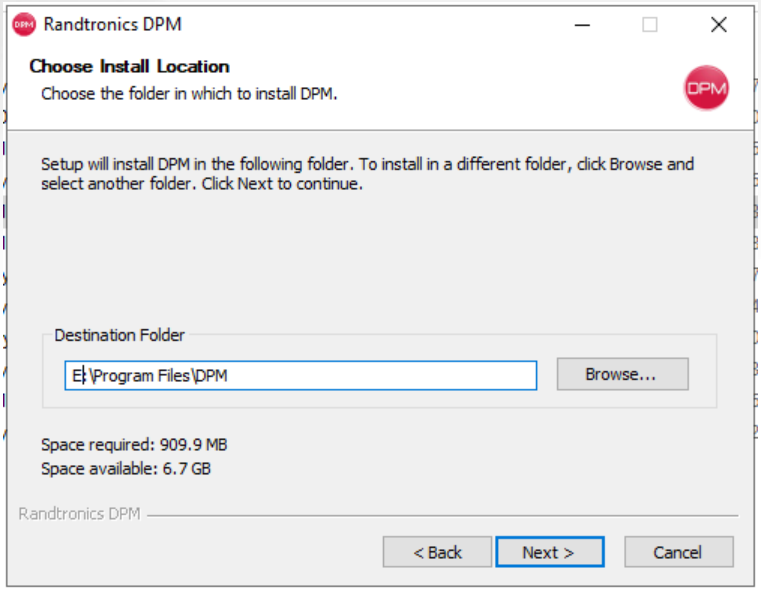
1. Accept the license agreement by clicking 'I Agree'.



2. Select 'DPM easyCipher vx.x.x.x
   Select 'Initialize eC database' if you want to initialize the backend database for easyCipher. Do not select this option if installing the second node in HA configuration as it will delete all existing configurations.
   Select 'Install eC application' if you want to install easyCipher manager on this system.
   Click 'Next'.

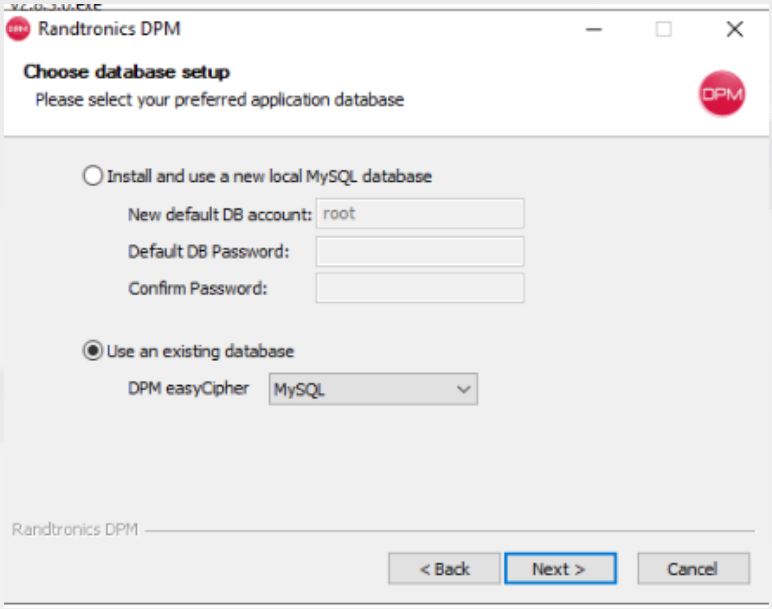


3. Select a destination folder to install the DPM easyCipher software.



Then click Next to continue

4. Choose whether you are using an existing database or want to install a new MySQL database.

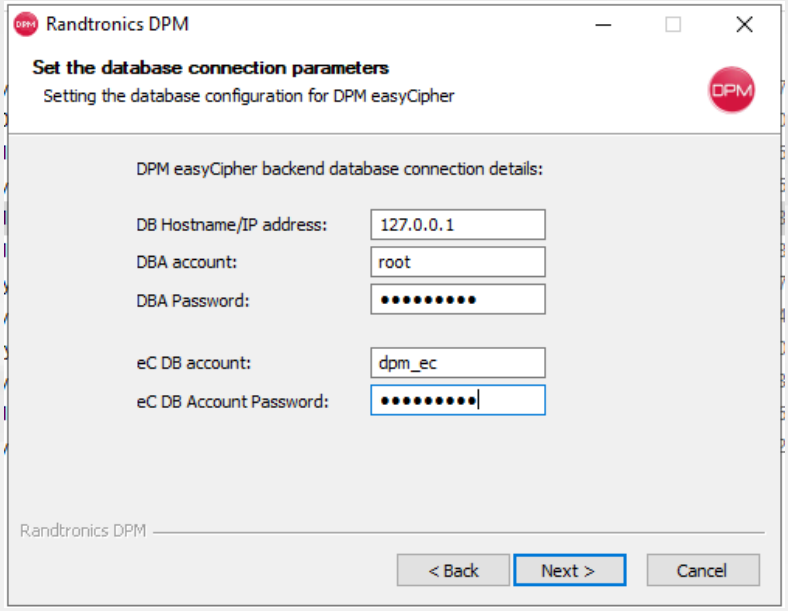


If you don't have an existing MySQL database you can choose option 'Install new local MySQL database' and the installer will install MySQL database.
If MySQL or MS SQL Server database is already installed on this server or a different server then you can use it as a backend database.

Click Next.

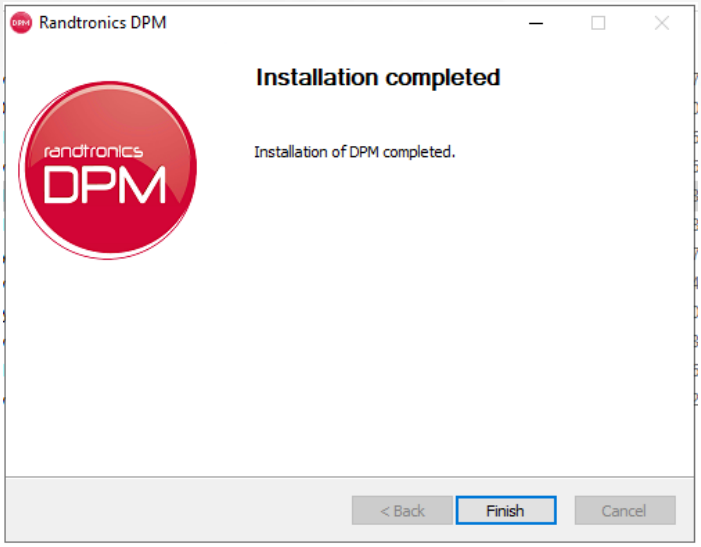
5. Enter the connection details for the database.

DB Hostname/IP Address: 127.0.0.1 for a database on the local system, or the IP address/hostname of the database server.
DBA Account: a 'root' or 'sa' database administrator user. If the new local MySQL database option was selected then the installer will create this user.
DBA Account Password: 'root' or 'sa' database administrator password
eC DB Account: a database user that will be used by DPM easyCipher application. If initializing the database then this user will be created.
eC DB Account Password: a database user password



Click Next.

6. Click 'Finish' to close the installer.



3.2.2 Linux Installation

Before installing DPM easyCipher install the following libraries:

1. fontconfig
    a. On Ubuntu
    sudo apt-get install fontconfig
    b. On CentOS/RHEL

sudo yum install fontconfig

Installation:

1. Create an installation directory. This will be referred to as <installDir>
   `mkdir <installDir>`

2. Copy the installation tar file into the <installDir>
   `cp DPM_easyCipher_x.x.x.x.tar.gz <installDir>`

3. The installation made then be run from the <installDir>
   `cd <installDir>`

4. Unzip the tar file:
   `tar –xvf DPM_easyCipher_x.x.x.x.tar.gz`

5. Run the setup script and follow the prompts:
   `sudo ./DPMFile/setup.sh`

6. Install the DPM easyCipher Manager and DPM easyCipher Server as a service (this must be run as root):

   `sudo ./DPMFile/install_service.sh`

7. Installation complete

Note that MySQL database must be initialized by a separate installer. Please refer to the sections above.

3.3 Firewall Set Up

The following port must be enabled to use DPM easyCipher:

- TCP 8443 (HTTPS) – Web Console access
- TCP 10000, 10005 (TCP) – Access by Agents

The following port must be enabled on DPM easyCipher Agent system to perform a few actions from DPM easyCipher such as ping the agent and browse folders on the agent's system.

- TCP 20000 (TCP) - if this port is not opened, encryption can still be used but policies path will need to be configured manually

These ports must be externally accessible. Firewall rules must be relaxed to allow inbound traffic. However, rules or access can be limited to the IP addresses/ranges from which DPM easyCipher, DPM easyCipher Agents, and DPM easyCipher Administrators are operating.

Please note that Windows installers will create local Windows incoming firewall rules for DPM easyCipher applications.

3.4 Starting DPM easyCipher

3.4.1 Windows

The DPM easyCipher is installed as two Windows services and is set to start automatically.

To manually start it, open the Services screen and click start on the 'DPM easyCipher Web' and 'DPM easyCipher Server' services.

3.4.2 Linux

The Linux version will install two services:

- dpmeasyciphermanager – the web application that system users connect to using a browser
- dpmeasycipherserver – the service responsible for communicating with the DPM easyCipher Agents

Open a command prompt and type:

```
sudo service dpmeasyciphermanager start
sudo service dpmeasycipherserver start

or

sudo systemctl start dpmeasyciphermanager
sudo systemctl start dpmeasycipherserver
```

3.5 Accessing the management console

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

https://ip_address:8443/dpmeasycipher

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.

3.6 Uninstalling the DPM easyCipher

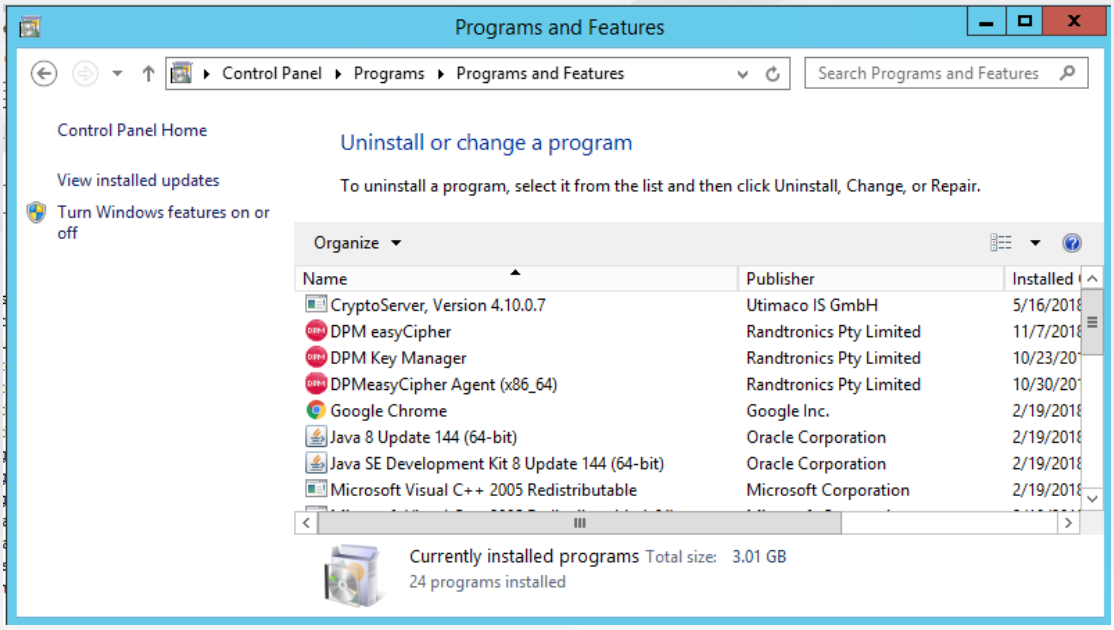
This section is only necessary if the user wishes to remove the DPM easyCipher.

3.6.1 Windows

If you are uninstalling the DPM easyCipher as a part of an upgrade, please make sure you backup the system first. Please refer to the System user manual for the backup procedure.

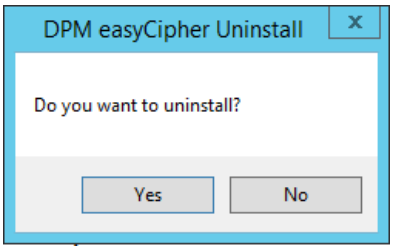
To uninstall the DPM easyCipher, perform the following steps.

1. Navigate to Control Panel – Programs and Features

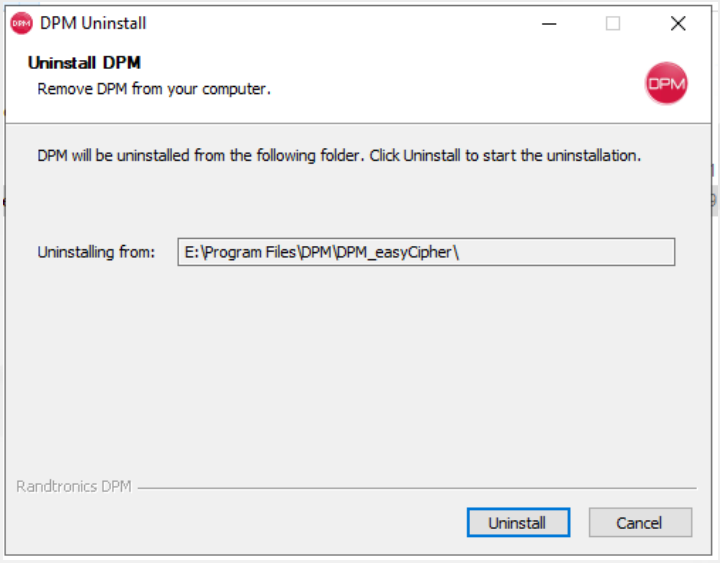


2. Select DPM easyCipher and click 'Uninstall/Change'

3. On the uninstall prompt, click Yes



Click the Uninstall button to commence the removal process



3.6.2 Linux

If you are uninstalling the DPM easyCipher as a part of an upgrade, please make sure you backup the system first. Please refer to the System user manual for the backup procedure.

To uninstall the DPM easyCipher, perform the following steps.

1. Locate the installation directory. This will be referred to as <installDir>. The easiest way to do this is to check the directory that the dpmeasyciphermanager process is running from:

   ```
   ps –elf | grep dpm
   ```

   This will return the location of the dpmeasyciphermanager. The installation directory is two directory levels up from this, for example, if the PS command return /home/rand/DPMFile/tomcat/bin/dpmeasyciphermanager, then the <installDir> is /home/rand/DPMFile

2. The installation made then be run from the <installDir>
   ```
   cd <installDir>
   ```

3. Uninstall the DPM easyCipher Manager and DPM easyCipher Server services (this must be run as root):
   ```
   sudo ./uninstall_service.sh
   ```

4. Delete the <installDir> directory
   cd ..
   sudo rm <installDir> -R -f

5. Uninstallation complete

3.7 Upgrading DPM easyCipher

Upgrade of DPM easyCipher may be required as a part of a maintenance. Randtronics regularly releases new versions of DPM easyCipher with various fixes and new features.

Before performing an upgrade of DPM easyCipher make sure to take a backup of the database and DPM easyCipher as outlined in a System User guide.

To perform upgrade of DPM easyCipher follow upgrade instructions and scripts from Randtronics.

4 DPM easyCipher Agent

The DPM easyCipher Agent needs to be installed on each computer that requires protection. The Agent receives security policies from the DPM easyCipher and enforces those policies on the computer and performs encryption and access control.

4.1 Firewall Set Up

Both the Windows and Linux version of the DPM easyCipher Agent require the following port to be enabled to use DPM easyCipher Agent:

• TCP 20000 (TCP)

The DPM easyCipher accesses this port in the agent to ping the agent and also to retrieve a folder structure.

Please note that Windows installer will create Windows internal incoming firewall rules for DPM easyCipher Agent application.

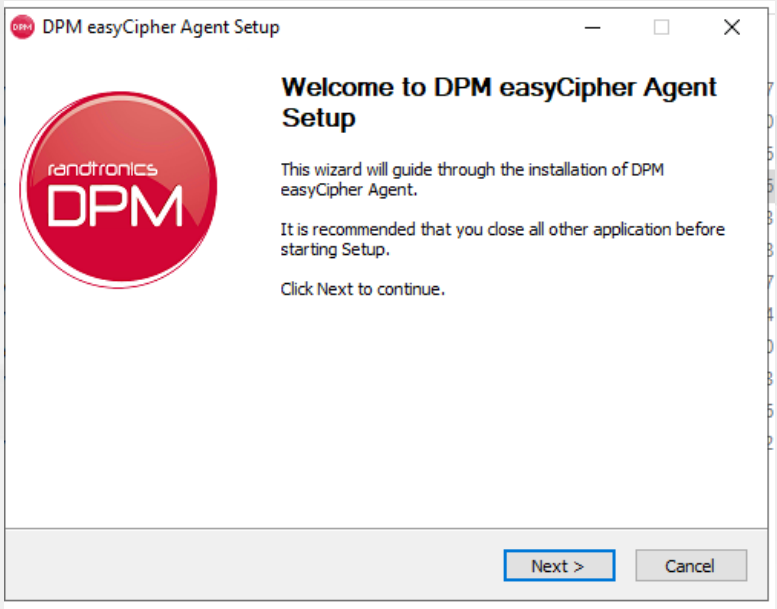
If using DPM easyCloudPlus, in addition to the local firewall rules, the system where agent is installed must have a public IP address and port 20000 so it can be accessed from the easyCloudPlus manager. This connection is required for browsing a path when creating a policy. If this connection is not available then the path needs to be entered manually.

4.2 Windows Agent

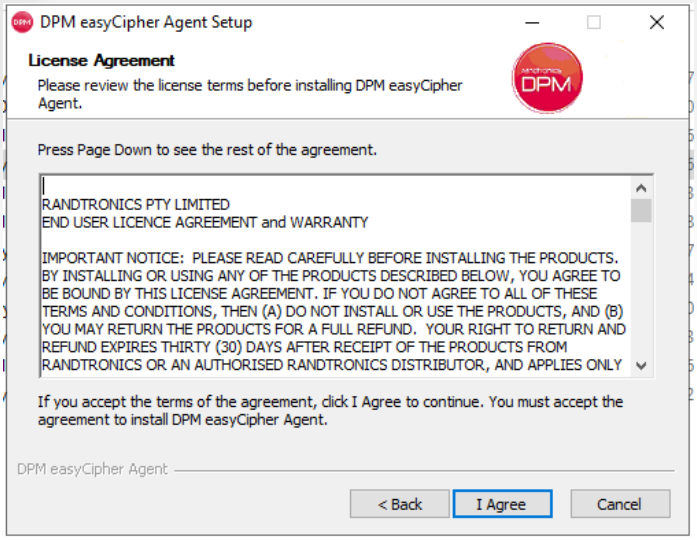
DPM easyCipher Agent can be installed in an interactive or in silent mode.

4.2.1 Installing the Agent in interactive mode

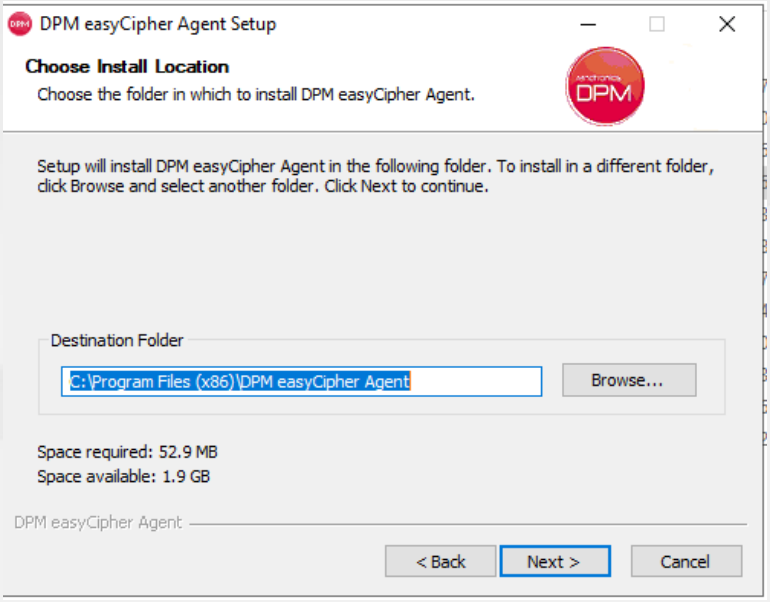
1. To start installation of the Agent, right click on the DPMeasyCipher_Agent_vx.x.x.xx.exe installer file and click the Run as Administrator.



2. Click Next to continue

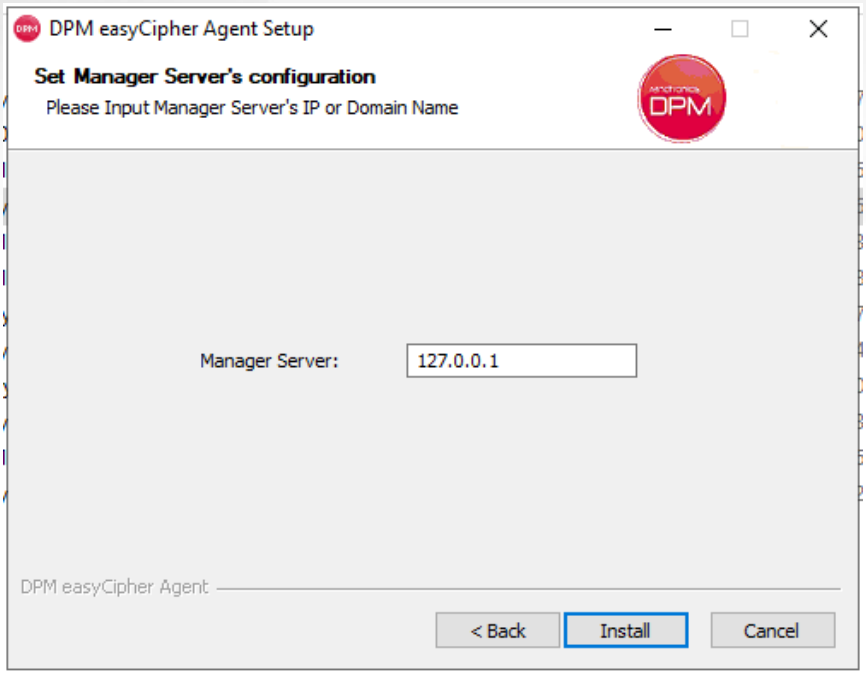


3. Click ‘I Agree’ to agree with the license agreement



4. Select a destination folder to install the DPM easyCipher Agent software to.

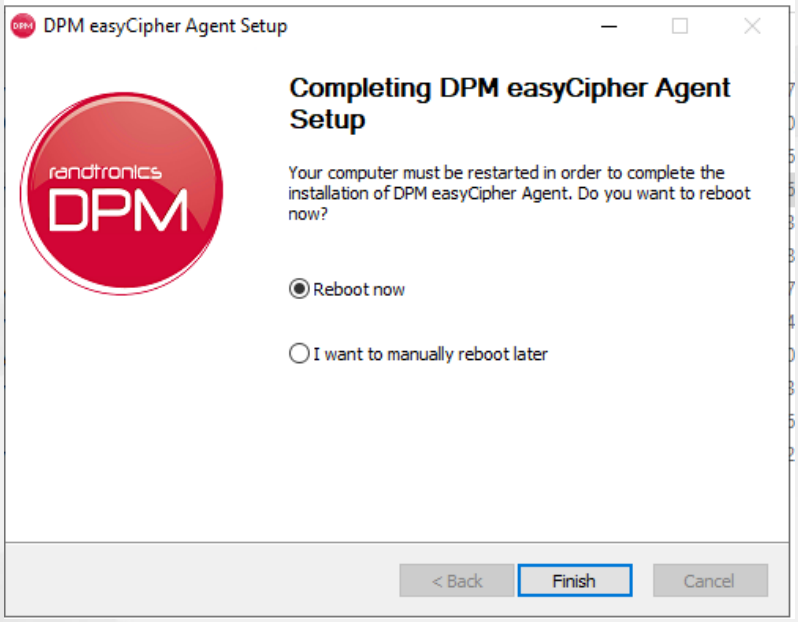
5. Click the Next button



6. Enter the IP address or a hostname of the DPM easyCipher server.
   For easyCloudPlus enter hostname of the registration port details. You will need to update Manager hostname and ports after installation in DPM easyCipher Agent Tray screen. Please see details in further sections.

7. Click on the Install button to install the software.

8. Once the DPM Agent installer has finished installing the software, the computer will need to be rebooted.



4.2.2 Installing the Agent in silent mode

When installing DPM easyCipher Agent in a silent mode it will automatically detect if it is a brand new install or un upgrade. If the current version can be upgraded in-place then it will proceed with the upgrade. If the current version is too old and cannot be upgraded then the install will be aborted.

To install DPM easyCipher Agent in a silent mode from a command line or script you need to pass the following parameters:

/S - silent mode
/MANAGER=manager_ip|name - manager address. If not set then 127.0.0.1 is used. Not needed for upgrade and will be ignored.
/REBOOT=y|n - reboot or do not reboot the OS. Default is 'n'. You will need to reboot manually. If 'y' then the system will be automatically rebooted after installation.
/D=folder_name - target installation folder. Must be the last parameter in the command line and must not contain quotes even if the path contains blank spaces. Default is "C:\Program Files(x86)\DPM easyCipher Agent". Not needed for upgrade and will be ignored.

For example,
DPM easyCipher_Agent_vX.X.X.X.exe /S /REBOOT=n
DPM easyCipher_Agent_ vX.X.X.X.exe /S /MANAGER=192.168.1.133 /REBOOT=y /D=C:\Program Files(x86)\DPM easyCipher Agent

4.2.3 Updating IP address/hostname of the manager

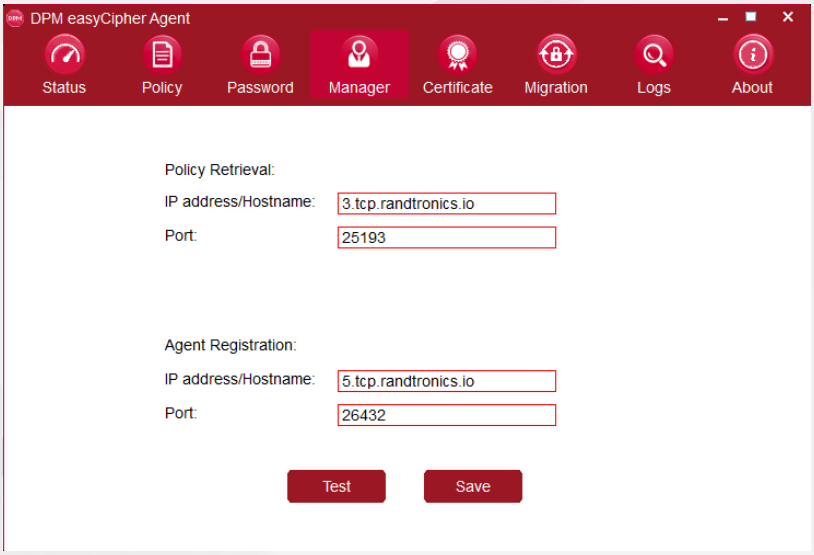
DPM easyCloudPlus manager is using non-standard ports and hostname which are different from on-prem installation. So, if using easyCloudPlus service then you will need to change

Manager's hostnames and ports in DPM easyCipher Agent.

To update hostname of the manager, open DPM easyCipher Agent tray by right-clicking on DPM icon in system tray and clicking 'Open DPM easyCipher Agent'.

Open 'Manager' menu and type hosname and ports with policy port and registration port details received from Randtronics.

Click Save and restart DPM easyCipher Agent service.

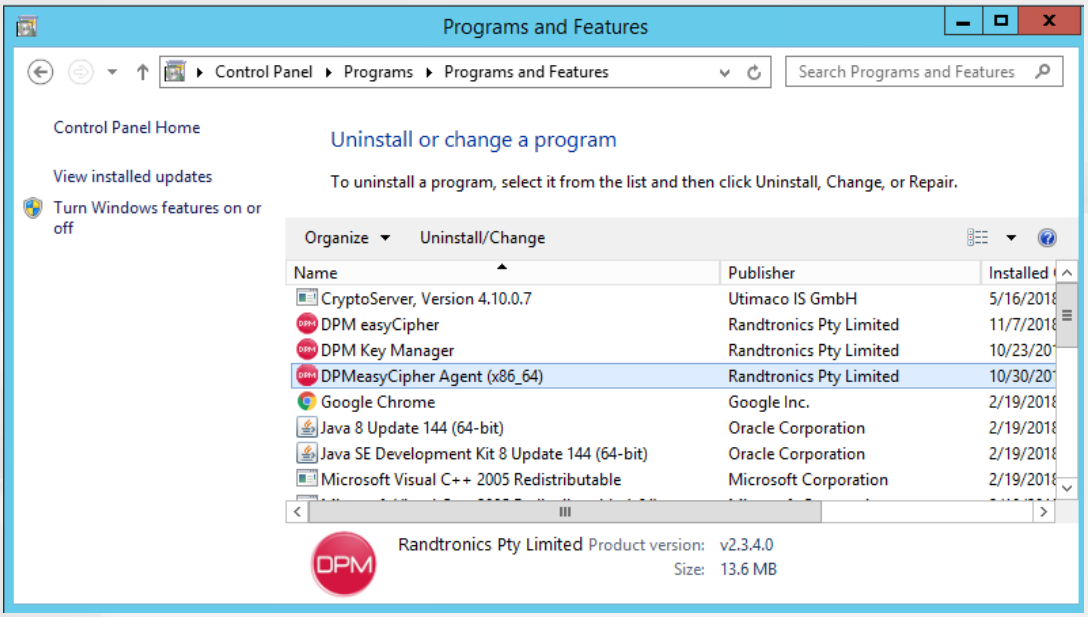


4.2.4 Uninstalling the Agent

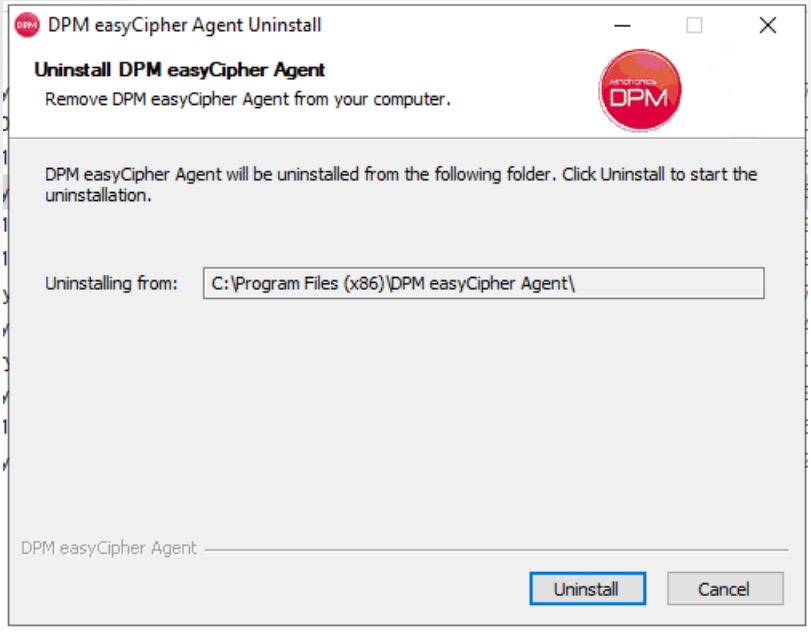
Uninstallation may be required during software upgrade.

To uninstall the DPM easyCipher Agent, perform the following steps.

1. Navigate to 'Control Panel' - 'Programs and Features'

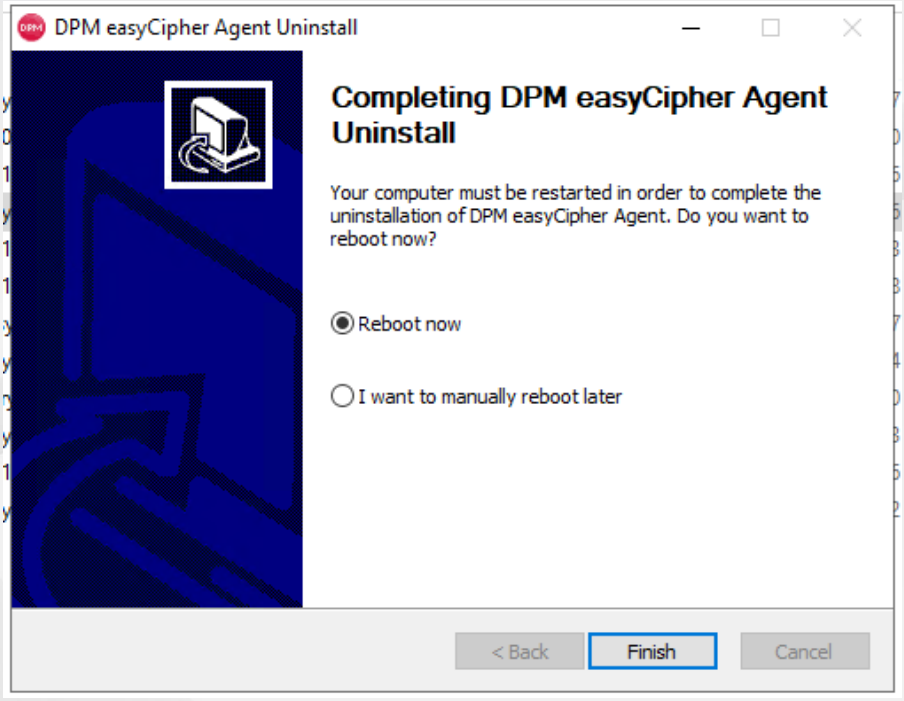


2. Select DPM easyCipher Agent and click ‘Uninstall/Change’



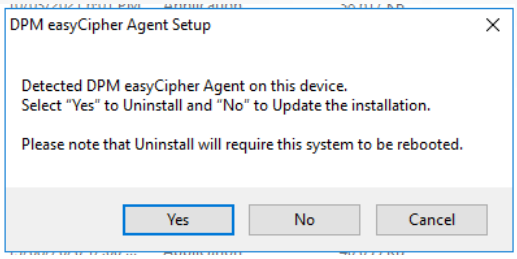
3. Click the Uninstall button to start the uninstall process

4. The computer will need to be rebooted once the uninstall is complete



4.2.5 Upgrading the Agent in interactive mode

To upgrade the agent software run the installer and choose “No” to upgrade the agent.



Sometimes it may require to uninstall the current version and install the new one. In this case the installer will provide such instructions.

Before starting upgrade make sure that applications that are accessing the target protected files are fully stopped and automatic startup of the services is disabled.

4.2.6 Upgrading the Agent in silent mode

When executing DPM easyCipher Agent installer in a silent mode it will automatically detect if it is a brand new install or un upgrade. If the current version can be upgraded in-place then it will proceed with the upgrade. If the current version is too old and cannot be upgraded then the upgrade will be aborted.

To upgrade DPM easyCipher Agent in a silent mode from a command line or script you need to pass the following parameters:

/S - silent mode

/REBOOT=y|n - reboot or do not reboot the OS. Default is 'n'. You will need to reboot manually. If 'y' then the system will be automatically rebooted after installation.

For example,
DPM easyCipher_Agent_vX.X.X.X.exe /S /REBOOT=n

4.3 Linux Agent

4.3.1 Installing the Agent on RHEL/CentOS

There are two steps to installing the Agent on a Linux machine. First the DPM kernel module must be installed, then the Agent application is installed. DPM software is installed using RPM and must be run as the root user.

Install the DPM kernel module:

a. Determine the current running kernel version:

```
uname -r
```

b. The version of kernel module to install will depend on the kernel version returned by the uname command. The RPM files contain the Linux kernel version in the filename

```
sudo rpm –i dpm-x.x-x.x.x86_64.rpm
```

1. Install the DPM easyCipher Agent:

a. Run the RPM install command:

```
sudo rpm –i dpmfile-x.x.x.x86_64.rpm
```

b. Run the DPM easyCipher configure command to configure the IP address of the Manager.

```
sudo dpmfile_config
```

If using easyCloudPlus, please enter 127.0.0.1 as IP address and ignore the message that the server is not accessible. You will change the address in the configuration file later. Please refer to the next section on how to update the IP address of the manager.

The DPM easyCipher Agent service can be started by running the following command:

```
sudo service dpmfile start
or
sudo systemctl start dpmfile
```

The DPM easyCipher Agent service can be stopped by running the following command:

```
sudo service dpmfile stop
or
sudo systemctl stop dpmfile
```

4.3.2 Installing the Agent on Ubuntu

There are two steps to installing the Agent on a Ubuntu machine. First the DPM kernel module must be installed, then the Agent application is installed. DPM software is installed using DEB package and must be run as the root user.

1. Install the DPM kernel module:

a. Determine the current running kernel version:

```
uname -r
```

b. The version of kernel module to install will depend on the kernel version returned by the uname command. The DEB files contain the Linux kernel version in the filename

```
sudo dpkg -i dpm-kernel-x.x-x.x.deb
```

2. Install the DPM easyCipher Agent:

a. Run the DEB install command:

```
sudo dpkg -i dpmfile-x.x.x.x86_64.deb
```

b. Run the DPM easyCipher configure command to configure the IP address of the Manager.

```
sudo dpmfile_config
```

DPM easyCipher Agent can be started during configuration.

3. The Linux machine may require a reboot once the software is installed

If using easyCloudPlus, please enter 127.0.0.1 as IP address and ignore the message that the server is not accessible. You will change the address in the configuration file later. Please refer to the next section on how to update the IP address of the manager.

The DPM easyCipher Agent service can be started by running the following command:

```
sudo service dpmfile start
or
sudo systemctl start dpmfile
```

The DPM easyCipher Agent service can be stopped by running the following command:

```
sudo service dpmfile stop
or
sudo systemctl stop dpmfile
```

4.3.3 Uninstalling the Agent on RHEL/CentOS

To uninstall the DPM easyCipher Agent:

1. Uninstall the DPM easyCipher Agent application:

```
sudo rpm –e dpmfile
```

2. Uninstall the DPM kernel module:

```
sudo rpm –e dpm
```

3. Restart the Linux system to complete the uninstall process

4.3.4 Uninstalling the Agent on Ubuntu

To uninstall the DPM easyCipher Agent:

Uninstall the DPM easyCipher Agent application:

```
sudo dpkg -r dpmfile
```

Uninstall the DPM kernel module:

```
sudo dpkg -r dpm-kernel
```

Restart the Linux system to complete the uninstall process

4.3.5 Upgrading the Agent

To upgrade the agent software, it is required to uninstall the current version and install the new one. Please refer to other sections for each process.

Before starting the upgrade make sure that applications that are accessing the target protected files are fully stopped.

Credits

DPM easyCipher is a product 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: support@randtronics.com

www.randtronics.com

Copyright Information

support@randtronics.com

Randtronics Pty Limited
ABN: 99 101 584 329

Suite 1, Level 1, 64 Talavera Rd NorthRyde, NSW 2113,
Australia

Email: support@randtronics.com

www.randtronics.com