Comodo

IT and Security Manager

Software Version 5.4

On-Premise Installation Guide

Guide Version 5.4.062918

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1. Comodo IT and Security Manager: On-Premise Deployment Instructions

Comodo IT and Security Manager (ITSM) is a centralized device management system that allows network administrators to manage, monitor and secure mobile devices which connect to enterprise networks. ITSM is available in two models - Software as a Service (SaaS) and on-premise installation. Refer to the ITSM quick start and admin guides for details about how to use the application:

- Quick start guide - **https://help.comodo.com/topic-399-1-787-10248-Comodo-IT-and-Security-Manager---Quick-Start.html**
- Admin guide - **https://help.comodo.com/topic-399-1-786-10078-Introduction-to-Comodo-IT-and-Security-Manager.html**

This guide explains how to install ITSM on your server.

- **Minimum Hardware Requirements**
- **New Installation**
- **Interaction during Installation**
- **Updating Existing Installation**
- **Configuring 3rd Party Applications / Services**
    - **Setting up the Domain**
    - **Installing SSL Certificates and Configuring Nginx**
    - **SMTP Settings**
    - **Setting up Incoming Connection Ports**
    - **Setting up Outgoing Connection Ports**

2. Minimum Hardware Requirements

1. Hardware requirement for hosting all services in one VM

	Up to 250 managed devices	Up to 2000 managed devices
Host OS	Linux 64-bit, modern kernel Ubuntu server 14.04 LTS 64-bit	
VA Network Mode	Bridge	
RAM	8 GB	32 GB
CPUs	2 Core	8 Core
Storage Min Size	127 GB	1 TB RAID5

2. Hardware requirement for services distributed among VM host farm servers

	Up to 250 managed devices	Up to 2000 managed devices
Web Server		

Host OS	Linux 64-bit, modern kernel Ubuntu server 14.04 LTS 64-bit	
VA Network Mode	Bridge	
RAM	2 GB	8 GB
CPUs	2 Core	4 Core
Storage Min Size	32 GB	32 GB
Application Server		
Host OS	Linux 64-bit, modern kernel Ubuntu server 14.04 LTS 64-bit	
VA Network Mode	Bridge	
RAM	8 GB	16 GB
CPUs	2 Core	8 Core
Storage Min Size	64 GB	127 GB
DB Server		
Host OS	Linux 64-bit, modern kernel Ubuntu server 14.04 LTS 64-bit	
VA Network Mode	Bridge	
RAM	8 GB	32 GB
CPUs	4 Core	8 Core
Storage Min Size	127 GB	1 TB RAID5

CPU core means one of physical core of Intel Xeon E3/E5 on VM host server.

3. New Installation

Please note the following:

- All instructions apply only to Ubuntu server 14.04 LTS 64-bit version.
- Testing with other Linux distributions has not been made yet.
- All commands should be run as root.

Ubuntu Server Installation *(instructions for those new to Ubuntu)*

Select the following parameters during Ubuntu server installation:

- Language: English
- Country: US
- Detect Keyboard Layout: No
- Country Origin: English (US)
- Keyboard Layout: English (US)

- Hostname: <anything meaningful, for example, ITSM Server>
- Fullname for the new user: <anything meaningful, for example: devops1>
- Username for your account: <anything meaningful, for example: devops1>
- Password: <some passwd>
- Is this timezone correct? <depending on proposal, typically - yes>
- Partitioning method: Guided - use entire disk
- Select Disk to partition: <usually one item only, so select it or any you suppose to use>
- Write the changes to disk?: Yes
- HTTP proxy information: <set URL as explained in the current dialog if proxy is mandatory>
- How do you want to manage upgrades on this system?: Install security updates automatically
- Choose software to install: Select "OpenSSH server", all the rest will be configured later

After the message 'Installation is completed' is displayed, press continue. In the black console enter your user name and password as you set up during the installation. After login is completed you need to rise your privileges:

- In the console, after ~$, type *sudo bash*

System requests your password, the same as on login stage.

After successful verification, you can see super user invitation: ~#

Next, you can proceed to install **ITSM**.

ITSM Installation procedure:

Select

Add a repo for fresh php :

```
apt-add-repository ppa:ondrej/php
```

Add a repo with CDM server and environment:

```
sudo bash -c "echo -n | openssl s_client -showcerts -connect dmdemo.comodo.com:443 2>/dev/null |
sed -ne '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
>> /etc/ssl/certs/ca-certificates.crt"
wget --no-check https://dmdemo.comodo.com/deb/keyFile
apt-key add keyFile
echo "deb https://dmdemo.comodo.com/deb/ trusty main" >> /etc/apt/sources.list.d/dmdemo.list
```

Refresh packages list:

```
apt-get update
```

Install postfix mailer
(Rem: applies to local DB and mailer)

```
apt-get install postfix
```

Posfix SMTP server installer:

- General type of mail configuration: Internet site
- System mail name:<default is ok>

Install postgresql DB server

```
apt-get install postgresql-9.3
```

During the installation CDM server and verdict server will initialize their databases.
(Note: Make sure postgresql server is tuned for this and you have credentials to access the DB).

Configuring PostgreSQL

PostgreSQL must be pre-configured so that it can be used from ITSM, this needs to be done before ITSM installation.

The simplest way to do it is to change the below line in

/etc/postgresql/9.3/main/pg_hba.conf

Original line:

```
host    all         all         127.0.0.1/32         md5
```

Changed line:

```
host    all         all         127.0.0.1/32         trust
```

Once it is changed, restart PostgreSQL running the below command:

```
service postgresql restart
```

The complete guide on how to tune up access in PostgreSQL is available at https://www.postgresql.org/docs/9.3/static/auth-pg-hba-conf.html

Installing ITSM

Install main CDM package and mdm-verdict-server:

```
apt-get install mdm-web mdm-verdict-server
```

ITSM server installer

- This PPA has been deprecated! : Ok

4. Interaction during ITSM Installation

During ITSM installation a number of questions will be asked. Some examples are given below:

```
This PPA has been deprecated! : Ok
Enter the address of the database server [] : localhost
Enter the database name [] : itsm
Enter username to access the database "itsm" [] : postgres
Enter password for user:"postgres" to access the database "itsm" [] : postgres
Do you want to initialize Database [y/N] : y
Enter domain for Comodo CMDM mdm-web [] : itsm.example.com
Enter the address of the database server [] : localhost
Enter the database name [] : itsm
Enter username to access the database "itsm" [] : postgres
Enter password for user:"postgres" to access the database "itsm" [] : postgres
Do you want to initialize Database [y/N] : y
Enter domain for Comodo CMDM mdm-web [] : itsm.example.com
```

Don’t forget to extend 127.0.0.1 line in your /etc/hosts file with your service name, for example:

```
127.0.0.1 localhost itsm.example.com
```

ITSM installation video tutorial is also available at: https://www.youtube.com/watch?v=byS0hVNOiu8

5. Updating Existing Installation

Run the following commands to update the installation:

```
apt-get update
apt-get dist-upgrade
```

All changes in the code and database will be performed automatically.

6. Configuring 3rd Party Applications / Services

In order for the product to work correctly, you have to configure various parameters correctly. Refer to the following for more details:

- **Setting up the Domain**
- **Installing SSL Certificates and Configuring Nginx**
- **SMTP Settings**
- **Setting up Incoming Connection Ports**
- **Setting up Outgoing Connection Ports**

Setting up the Domain

For the product to work correctly, you should make a record for it in the domain. The record should point to the IP address of the server where the product is deployed.

For example, if 10.0.0.10 is the address of the endpoint with the product installed and we want the product to be accessible at https://example.com.

To do it, DNS zone should be changed so that example.com points to 10.0.0.10

For all the devices to work correctly, you should obtain certificates for the necessary domain name.

The certificates can be obtained at https://ssl.comodo.com/

The received certificates have to be installed on the server 10.0.0.10

Installing SSL Certificates and Configuring Nginx

Place the certificate, intermediate certificate and the key to /etc/nginx/certs dir
(Note: run the commands as root:)

```
cd /etc/nginx/certs

cat YourDomainCert.cer > cmdm_comodo_com.bundle

echo >> cmdm_comodo_com.bundle

cat YourDomainCert_interm.cer >> cmdm_comodo_com.bundle

cat YourDomainCert.key > cmdm_comodo_com.key

service nginx configtest
```

If it prints [OK], run the following:

```
service nginx restart
```

SMTP Settings

By default, local e-mail sender (postfix) is configured for direct e-mail access.

If you use any kind(s) of mail filtering or relay hosts for sending e-mails, it needs to be configured in /etc/postfix/main.cf

Add below string to /etc/postfix/main.cf :

```
relayhost = mail.example.com
```

Where mail.example.com is a relay host for your organization.

Setting up Incoming Connection Ports

ITSM uses the following TCP ports for incoming connections:

443 - main access

444 - local verdict server access

5222 - Windows push service (optional i.e.if the service is configured)

Access to these ports must be configured in company’s firewall as a usual operation.

Setting up Outgoing Connection Ports

ITSM uses the following ports for external connections:

25 - connection to the configured SMTP server for e-mail sending

389 - connection to LDAP server (if configured)

443 - connection to https://accounts.comodo.com for license verification

443 - connection to Google Cloud Messaging Server

2195, 2196, 80, 443 - connection to Apple Push Notification Server Outbound

If you require more details about the installation, please contact mdmsupport@comodo.com.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

Comodo Security Solutions, Inc

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.888.266.6361

Tel : +1.703.581.6361

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**