COMODO

Creating Trust Online®

Comodo
Dome Data Protection

Software Version 3.1

Installation Guide

Guide Version 3.1.061218

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1.About Dome Data Protection 3
1.1.CDDP Features 3
1.1.1.Protection and Administration with CDDP Network Server 3
1.1.2.Protection & Discovery with CDDP Endpoint 3
2.CDDP Network Server Installation 3
2.1.Using CDDP Appliance CD Image on a Physical or VMware Machine 3
3.CDDP Network Server Initial Configuration 4
3.1.Assigning a Static IP Address to CDDP Network Server 4
3.2.Assigning a Hostname to CDDP Network Server 5
3.3.Firewall TCP Port Configuration for CDDP Network Server 5
3.4.Internet Connection Test 6
3.5.Web Integration 6
3.5.1.Proxy Configuration from Endpoint Machine (Internet Explorer) 6
3.5.2.Proxy Configuration from Endpoint Machine (Mozilla Firefox) 8
3.5.3.Proxy Configuration from Active Directory 9
3.5.4.Transparent Proxy Configuration 10
About Comodo Security Solutions 11

1. About Dome Data Protection

Comodo Dome Data Protection is a fully fledged data loss prevention solution that offers network and endpoint protection and confidential data discovery.

1.1. CDDP Features

You can monitor and control data flow and stored data in your organization with CDDP. You can pass, log, archive and quarantine data using policy actions.

1.1.1. Protection and Administration with CDDP Network Server

Network protection enables you to detect and prevent outgoing data from your organizations network.

CDDP Network Server also functions as the administration center.

1.1.2. Protection & Discovery with CDDP Endpoint

Endpoint protection enables you to detect and prevent any data moved to removable devices such as USB sticks or smart phones from workstations or laptops in your organization.

Endpoint protection also covers any document printed using network and local printers connected to computers.

Endpoint data discovery also enables you to detect and enforce policy on stored data on computers in your network.

2. CDDP Network Server Installation

Comodo Dome Data Protection Network Server is a standalone software which runs on a Ubuntu Server 12.04 LTS edition operating system. Using following installation methods, you can install CDDP and operating system on a dedicated virtual or physical machine.

You can use Comodo Dome Data Protection Network Server using one of the three alternative ways:

- Using CDDP Appliance CD image on a physical or VMware machine.
- Using CDDP Appliance CD image on a Hyper V machine.

2.1. Using CDDP Appliance CD Image on a Physical or VMware Machine

After getting related images from http://www.mydlp.com/getting-started/ you can start CDDP installation. Please follow the steps below.

1. Burn your CDDP Appliance CD image onto a CD.
2. Select CDROM/DVDROM device from boot menu of your machine.
3. Start installation using the installation CD .
4. Select Installation language English.
5. Select Install CDDP Appliance.
6. Select Language English.

7. Select your country.
8. Skip keyboard detection by selecting No.
9. Select keyboard origin USA.
10. Select keyboard layout USA.
11. Check and correct the time zone..
12. Wait for automatic installation steps.
13. Enter OS user name.
14. Enter OS user password
15. Do not select "Encrypt home directory"
16. Wait for automatic installation steps to finish.
17. Default username and passwords are as below:

- SSH - Terminal will user name and password will be as you defined on step 13 and 14.
- Management console

  Default Username: mydlp , Default Password: mydlp

3. CDDP Network Server Initial Configuration

This document contains the following sections:

- **Assigning A Static IP Address To CDDP Network Server**
- **Assigning A Hostname To CDDP Network Server**
- **Firewall TCP Port Configuration For CDDP Network Server**
- **Internet Connection Test**
- **Web Integration**

3.1. Assigning a Static IP Address to CDDP Network Server

1. Find a local IP address dedicated to Comodo Dome Data Protection Network server which is not used for another machine or distributed by your DHCP server.
2. Make sure Comodo Dome Data Protection Network Server is connected to your local area network via a physical or virtual ethernet card.
3. After your Comodo Dome Data Protection Network Server installed, reboot the machine and open the command line terminal on the installed physical or virtual machine.
4. Login by entering your username and password you created during the installation.
5. If you are using virtual image please contact with support@mydlp.com for username and password.
6. To check the network interface status type the following command and press Enter:

   sudo ifconfig -a

7. Check the eth0 (or seth0 if you use a Hyper V Virtual Machine) line in ifconfig output.

   a. If you cannot see a line containing eth0 check the network see if its properly connected and functioning.

   b. If you cannot see the line containing eth0 or seth0, while using a virtual machine check the virtual network interface.

8. Enter following command and press enter:

   sudo pico –t /etc/network/interfaces

9. Modify the last line iface ethX inet dhcp as below (if you are using a Hyper V Virtual Machine change ethX to sethX) (X is the number of ethernet card such as in eth1or eth2): iface ethX inet static

10. Then add the following lines as shown below and modify it according to your network configuration using the instructions below:

    address 192.168.1.100

    netmask 255.255.255.0

    network 192.168.1.0

    broadcast 192.168.1.255

    gateway 192.168.1.1

    a. Replace address with the IP address you reserved for Comodo Dome Data Protection Network Server as explained on step 1.

    ex: 192.168.1.100

    b. Replace netmask with your local area network's netmask. ex: 255.255.255.0

    c. Replace network with your local area network's address part. ex: 192.168.1.0

    d. Replace broadcast with your local area network's broadcast address. ex: 192.168.1.255

    e. Replace gateway with your local area network's gateway. ex: 192.168.1.1

    11. Save the changes and exit the editor by clicking Ctrl + X and press Enter.

    12. Restart the networking service to make changes effective using following command :

    s*udo /etc/init.d/networking restart*

3.2. Assigning a Hostname to CDDP Network Server

If you have a local DNS server you can assign a hostname for the static IP address of your Comodo Dome Data Protection Network Server.

After this you can log on to Comodo Dome Data Protection Management Console using hostname (see CDDP Administration Guide). You can also use this hostname as management_server for CDDP Endpoints (see CDDP Endpoint Installation Guide).

3.3. Firewall TCP Port Configuration for CDDP Network Server

To use CDDP as a direct proxy using bundled Squid 3.X allow outgoing TCP ports 80 and 443 from CDDP to Internet and allow incoming TCP port 3128 from clients to CDDP.

For using CDDP as a direct FTP proxy allow outgoing TCP port 21 and allow passive FTP option in your firewall.

To use ICAP integration allow incoming TCP port 1344 from web gateway to CDDP.

To use CDDP as an SMTP gateway allow incoming and outgoing TCP port 25.

If there is a firewall between Comodo Dome Data Protection Network Server and your endpoints allow incoming TCP 443 and 80 connections to Comodo Dome Data Protection Network server from endpoint to allow CDDP Endpoint Agent to sync with

server.

For other configuration scenarios consult support@mydlp.com

3.4. Internet Connection Test

After the installation is completed and assigned a valid IP address , you can check whether internet connection is established

1. Connect to CDDP Enterprise using console.

2. Type username and password.

3. Type in the command line following command:

mydlp@mydlp01:~$ ping 4.2.2.2

4. The output will be as below:

```
PING 4.2.2.2 (4.2.2.2) 56(84) bytes of data.
64 bytes from 4.2.2.2: icmp_seq=1 ttl=241 time=76.8 ms
64 bytes from 4.2.2.2: icmp_seq=2 ttl=241 time=68.3 ms
64 bytes from 4.2.2.2: icmp_seq=3 ttl=241 time=70.4 ms
64 bytes from 4.2.2.2: icmp_seq=4 ttl=241 time=66.6 ms
```

5. If you do not get any reply from remote server (4.2.2.2 is a public DNS server) due to one of the following cases:

   a. Your firewall blocks connection: Change your firewall policy to accept CDDP Network Server connections.

   b. Mac-filter blocks your connection: Add MAC of the CDDP Network Server to allowed list of MACs in filter.

   c. Port based authentication blocks your connection: Disable port authentication for switch port connected to CDDP Network Server.

   d. Network connection problem.

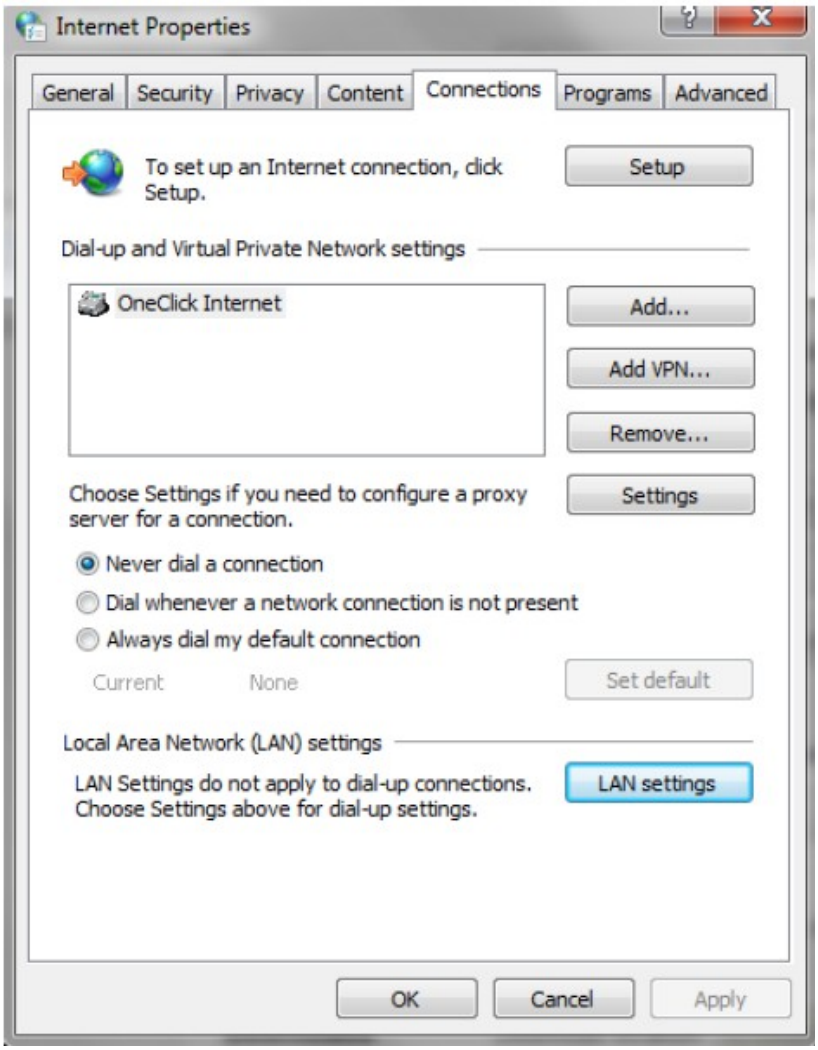
3.5. Web Integration

Web related rules can only work when they are processed on Comodo Dome Data Protection Network Server. To do this you need to use one of the methods below or follow CDDP ICAP Integration document if you have an ICAP web proxy.

3.5.1. Proxy Configuration from Endpoint Machine (Internet Explorer)

This method will handle both HTTP and HTTPS there is no need for configuring different ports for secure connection. However you need to configure them for each of your endpoint machine. The screenshots below is for Internet Explorer.

1. Open Internet Properties, Connection tab.



2. Click and open LAN settings

3. Check Use a proxy server for your LAN checkbox.

4. Set proxy server address to network server address

5. Set proxy port for all protocols to 3128

6. Click 'OK'.

7. (Optional) To prevent HTTPS certificate warnings download CDDP certificate from Comodo Dome Data Protection Management Console - Options - Protocols tab. Add it for each endpoint following steps:

a. Log in to PC with using administrator account.

b. Click 'Start', click Start Search, type mmc, and then press enter.

c. On the File menu, click Add/Remove Snap-in.

d. Under Available snap-ins, click Certificates, and then click 'Add'.

e. Under This snap-in will always manage certificates for, click Computer account, and then click Next.

f. Click Local computer, and click 'Finish'.

g. Click 'OK'.

h. In the console tree, double-click Certificates.

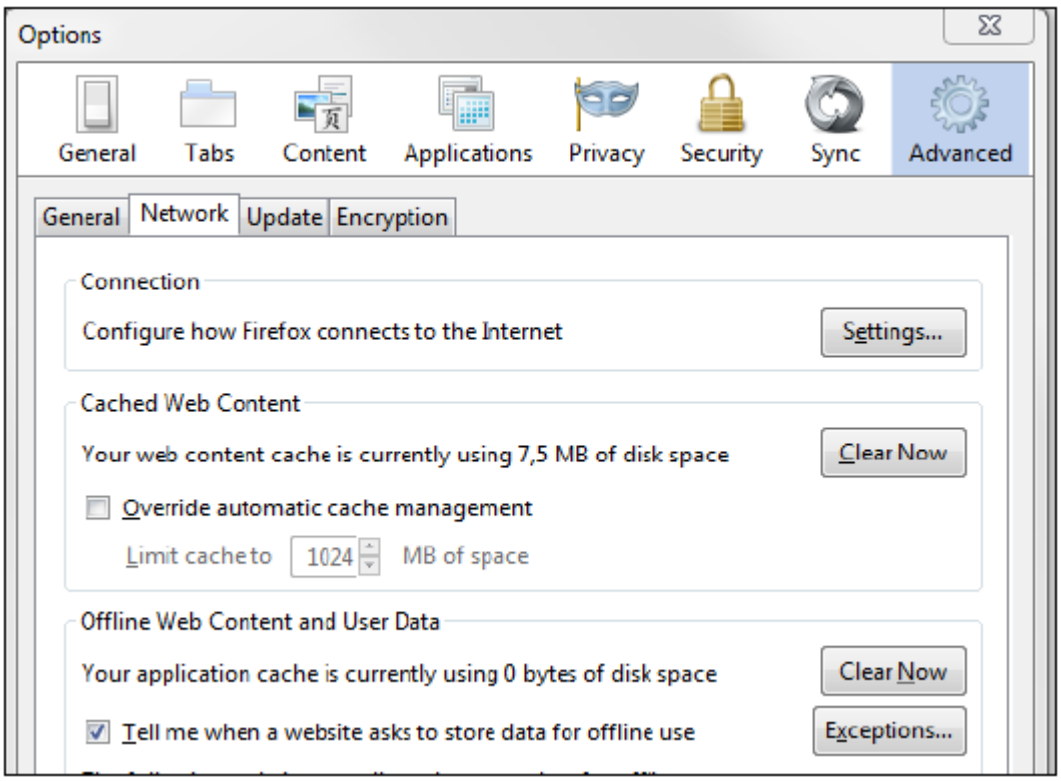
i. Right-click the Trusted Root Certification Authorities store.

j. Click All Tasks → Import to import the certificates and follow the steps in the Certificate Import Wizard.

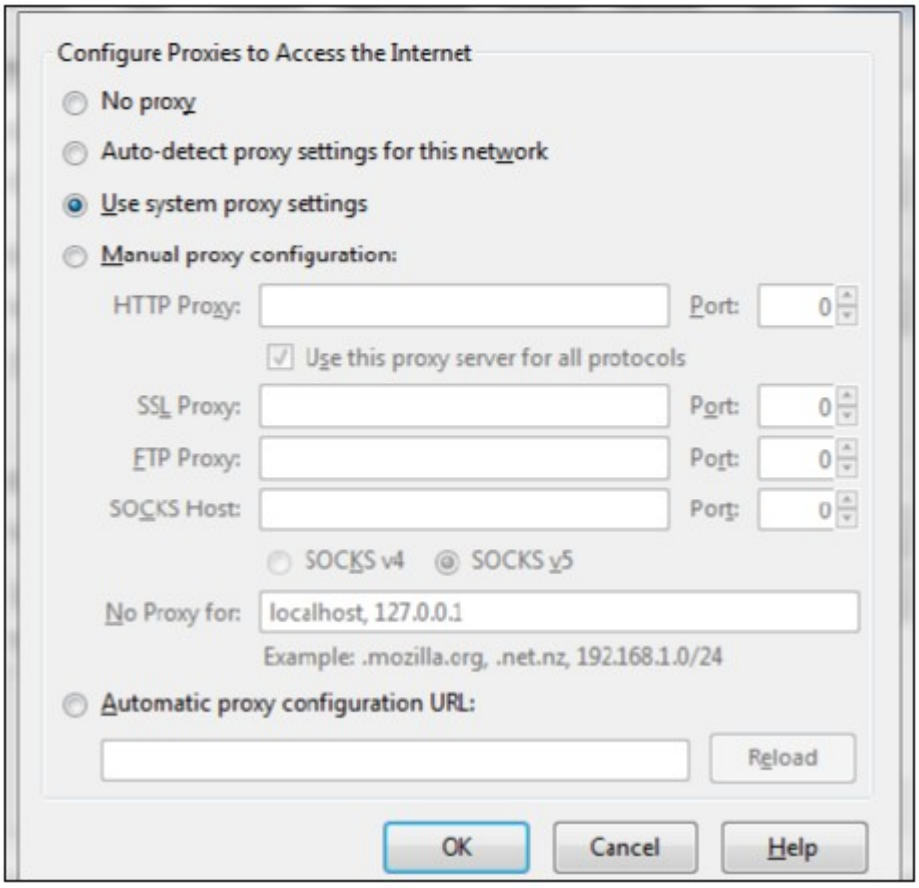
3.5.2. Proxy Configuration from Endpoint Machine (Mozilla Firefox)

This method will handle both HTTP and HTTPS there is no need for configuring different ports for secure connection. However you need to configure them for each of your endpoint machine. The screenshots below is for Mozilla Firefox.

1. Open Options, Network tab under Advanced tab.



2. Click and open Settings.



3. Check Manual proxy configuration.

4. Check Use this proxy server for all protocols.

5. Set proxy server address to HTTP Proxy and set port to the port field.

6. Click 'OK'.

7. (Optional) To prevent HTTPS certificate warnings download CDDP certificate from CDDP Management Console - Options - Protocols tab. Add it for each endpoint following steps:

a. Click Encryption tab Under Advanced tab.

b. Click View Certificates.

c. Click Import under Authorities tab.

d. Add CDDP User Certificate.

e. Check Trust this CA to identify websites in opened dialog.

f. Click 'OK'.

3.5.3. Proxy Configuration from Active Directory

This method will handle both HTTP and HTTPS there is no need for configuring different ports for secure connection. With this method you do not need configure endpoints one by one.

1. On the Windows Active server start a Microsoft Management Console and add the Group Policy snap-in.

2. Select default domain policy or the appropriate policy if you already have a previously configured policy as the group policy object.

3. Open to the User Configuration - Windows Settings - Internet Explorer Maintenance - Connection

4. Several options are available configure them according to your environment to make each endpoint has the configuration defined in previous manual method.

5. (Optional) To prevent HTTPS certificate warnings download CDDP certificate from CDDP Management Console - Options -

Protocols tab. Add it for all endpoints via Micrososoft Active Directory using following steps:

a. Open Server Manager, and under Features Summary, click Add Features. Select the Group Policy Management check box, click Next, and then click Install.

b. After the Installation Results page shows that the installation of the GPMC was successful, click Close.

c. Click Start, point to Administrative Tools, and then click Group Policy Management.

d. In the console tree, double-click Group Policy Objects in the forest and domain containing the Default Domain Policy GPO that you want to edit.

e. Right-click the Default Domain Policy GPO, and then click Edit.

f. In the GPMC, go to Computer Configuration, Windows Settings, Security Settings, and then click Public Key Policies.

g. Right-click the Trusted Root Certification Authorities store.

h. Click Import and follow the steps in the Certificate Import Wizard to import the certificates.

3.5.4. Transparent Proxy Configuration

This is the transparent method. It can be configured from firewall on user site. No configuration is need on active directory or on workstations.

1. Forward port 80 traffic coming to firewall to port 8080 of CDDP Network server
2. Forward port 443 traffic coming to firewall to port 8443 of CDDP Network server

FTP transparent proxy is not possible so you should set proxy configuration as in browser proxy configuration for each ftp client.

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**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.888.266.636

Tel : +1.703.581.6361

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**