COMODO

Creating Trust Online®

Comodo
MyDLP

Software Version 2.0

Installation Guide

Guide Version 2.0.010215

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1. About MyDLP

MyDLP is a fully fledged data loss prevention solution that offers network and endpoint protection and confidential data discovery.

1.1. MyDLP Features

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

1.1.1. Protection and Administration with MyDLP Network Server

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

MyDLP Network Server also functions as the administration center.

1.1.2. Protection & Discovery with MyDLP 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. MyDLP Network Server Installation

MyDLP 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 MyDLP and operating system on a dedicated virtual or physical machine.

You can use MyDLP Network Server using one of the three alternative ways:

- Using MyDLP Appliance CD image on a physical or VMware machine.
- Using MyDLP Appliance CD image on a Hyper V machine.
- Installing on a previously installed Ubuntu Server 12.04 system.

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

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

1. Burn your MyDLP 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 MyDLP 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

2.2. Installing MyDLP on a Ubuntu 12.04 Server Edition

You can install MyDLP Network Server on a previously installed Ubuntu* system. This is not a preferred method. You have to install operating system manually before installing MyDLP.

1. Logon to the Ubuntu server via command line using username and password you set during the installation of the operating system before.
2. open /etc/apt/sources.list with command below:

   sudo pico /etc/apt/sources.list
3. Add line below at the end of /etc/apt/sources.list

   deb ftp://ftp.linux.org.tr/mydlp/ubuntu/ precise main
4. To save the file and exit , use the CTRL+X option, then press Y key.
5. Install mydlp and mydlp-appliance packages using command below (Ignore GPG warning):

   sudo aptitude update

   sudo aptitude install mydlp mydlp-appliance
6. Enter Yes when prompted to install untrusted package**.
7. Reboot when installation finishes

*MyDLP is able to run on any Linux Distributions however as MyDLP Corp. we only provide professional support for Ubuntu 12.04.

** Please do not put any password for MySQL during the installation.

3. MyDLP Network Server Initial Configuration

3.1. Assigning a Static IP Address to MyDLP Network Server

1. Find a local IP address dedicated to MyDLP Network server which is not used for another machine or distributed by your DHCP server.
2. Make sure MyDLP Network Server is connected to your local area network via a physical or virtual ethernet card.
3. After your MyDLP 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 MyDLP 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 MyDLP Network Server

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

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

3.3. Firewall TCP Port Configuration for MyDLP Network Server

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

For using MyDLP 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 MyDLP.

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

If there is a firewall between MyDLP Network Server and your endpoints allow incoming TCP 443 and 80 connections to MyDLP Network server from endpoint to allow MyDLP 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 MyDLP 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 MyDLP Network Server connections.

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

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

    d. Network connection problem.

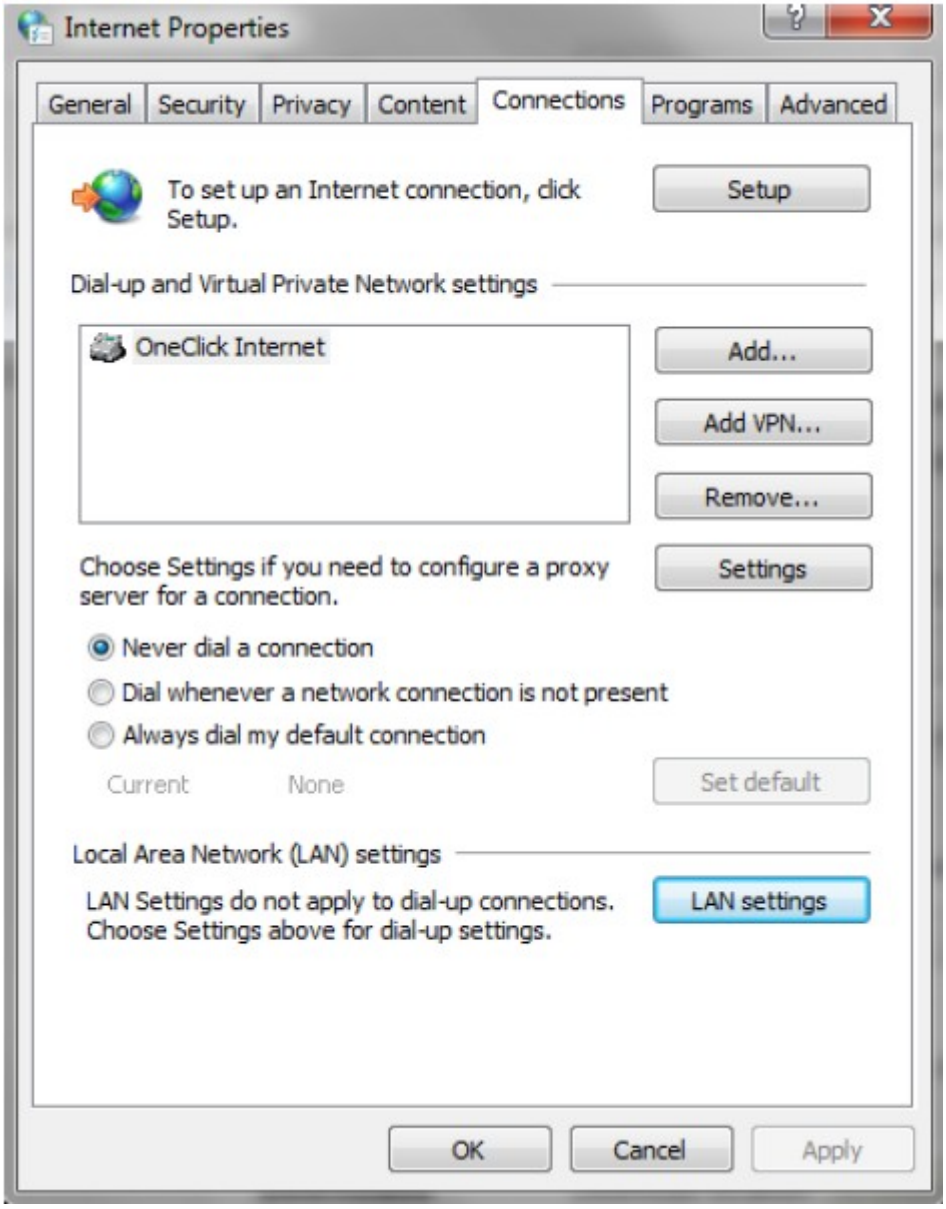
3.5. Web Integration

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

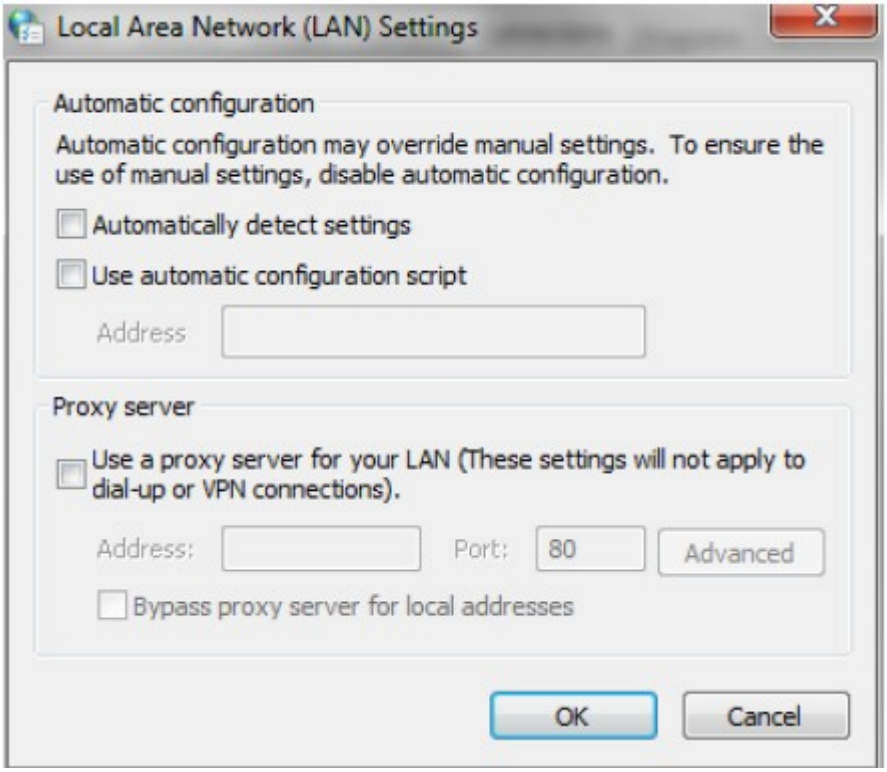
3.5.1. Proxy Configuration from Endpoint Machine (Internet Explorer)

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 donwload MYDLP certificate from MyDLP 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.

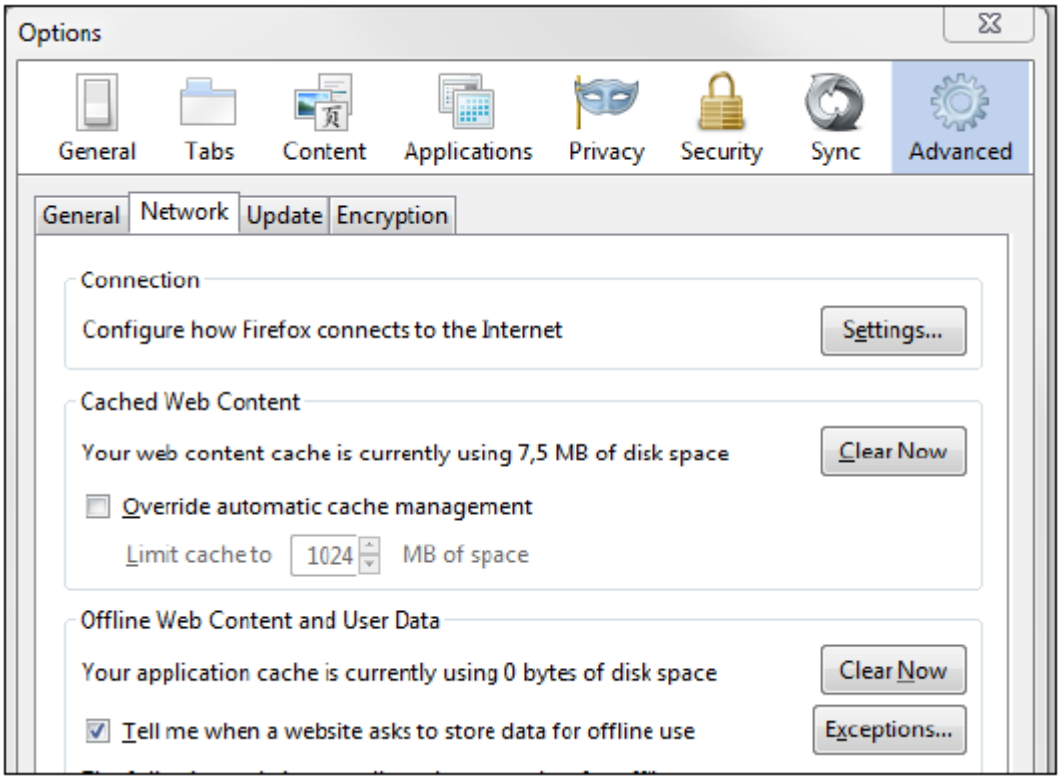
i. Right-click the Trusted Root Certification Authorities store.

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

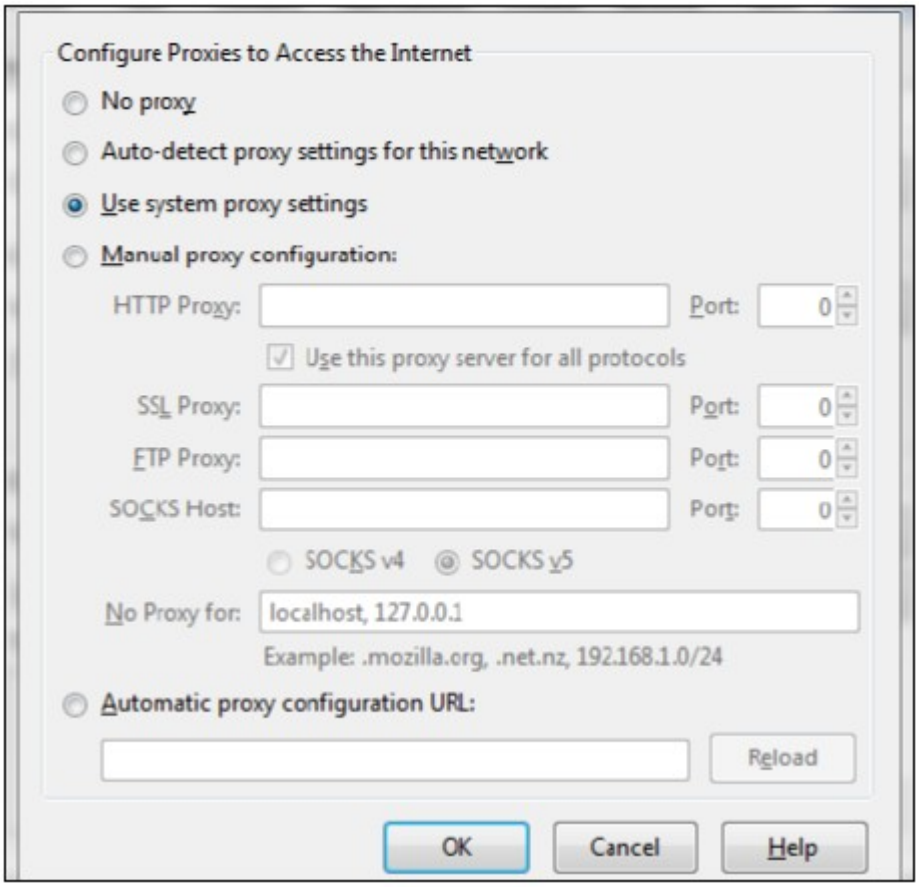
3.5.2. Proxy Configuration from Endpoint Machine (Mozilla Firefox)

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 donwload MYDLP certificate from MyDLP 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 MyDLP 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 donwload MYDLP certificate from MyDLP 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 MyDLP Network server
2. Forward port 443 traffic coming to firewall to port 8443 of MyDLP 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

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Email: **EnterpriseSolutions@Comodo.com**

For additional information on Comodo - visit **http://www.comodo.com**.