



## WHITEPAPER

### - Deploying NPRO v9 – Sample scenarios -



## GENERAL CONSIDERATIONS

When selecting a computer to be used as an Endpoint Manager server you should consider the following (in prioritized order)

1. Availability (max uptime)
2. Lowest network load

File shares with product updates (alternative shares) may reside on different computers than the computer(s) running Endpoint Manager. Clients may access file shares using standard UNC paths instead the TCP port 2868 as by default, when updating from an Endpoint Manager. These shares could for example be a Linux machine or any type of device as long as it can be accessed using UNC. Accessing to these shares can be set up through the **Policies**.

**NOTE:** Internet Update downloads:

In case of a full upgrade, the download could require 100 MB or more, depending on the amount of platforms and languages you have setup in NEM. On daily basis, an incremental definition files update would require 1~10 MB.

**Remember:** Communication between the clients and the Endpoint Manager server(s) always uses port TCP 2868, so this port must be open on the firewall.

## SCENARIO 1 - SIMPLE LAN NETWORK

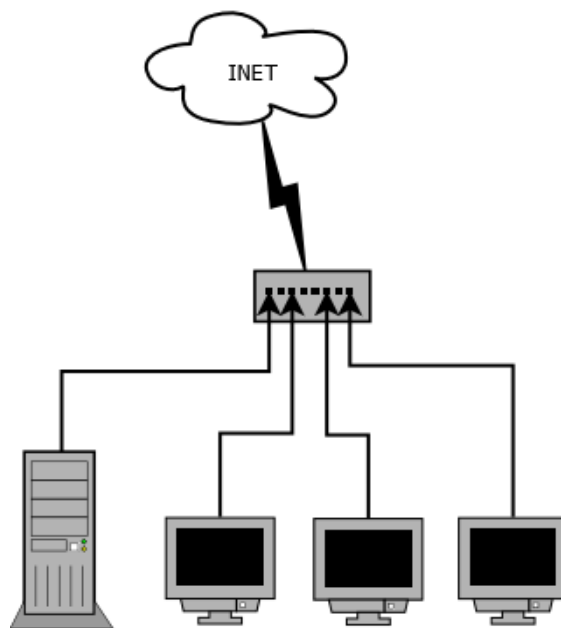
---

A common scenario where a number of clients and/or servers are physically connected on the same network.

In small networks, where there is no Windows server operating system on any of the machines, you can still use a Windows workstation computer. Take care, however, to select the computer best suited according to the criteria above.

**Environment:** A small/medium number of computers (up to 50) on the same physical network segment.

**Example:** One Windows server and 35 Windows clients. Please check the Administrator's Guide for system requirements.



**Description:** In this scenario, a small number of computers are physically connected. The desired deployment will require installing the Endpoint Protection on the Windows server and roll out the MSI installers (created later) to the clients. The purpose is to install the Endpoint client and automatically connect the clients to the server to fetch policies and software updates (including definition files).

### Steps:

1. Install Endpoint Protection with Endpoint Manager on the selected server
2. Open Endpoint Manager console and complete the Install Wizard to create a **Realm**
3. Run Internet Update
4. Create MSI installers from **Settings** and roll them out to the clients

### Behavior:

The Endpoint Manager will download updates from the Internet.

The clients will fetch policies and software updates from the Endpoint Manager and report events (warnings, errors).

**SCENARIO 2 - MULTILEVEL MANAGERS (MEDIUM/LARGE NETWORKS)**

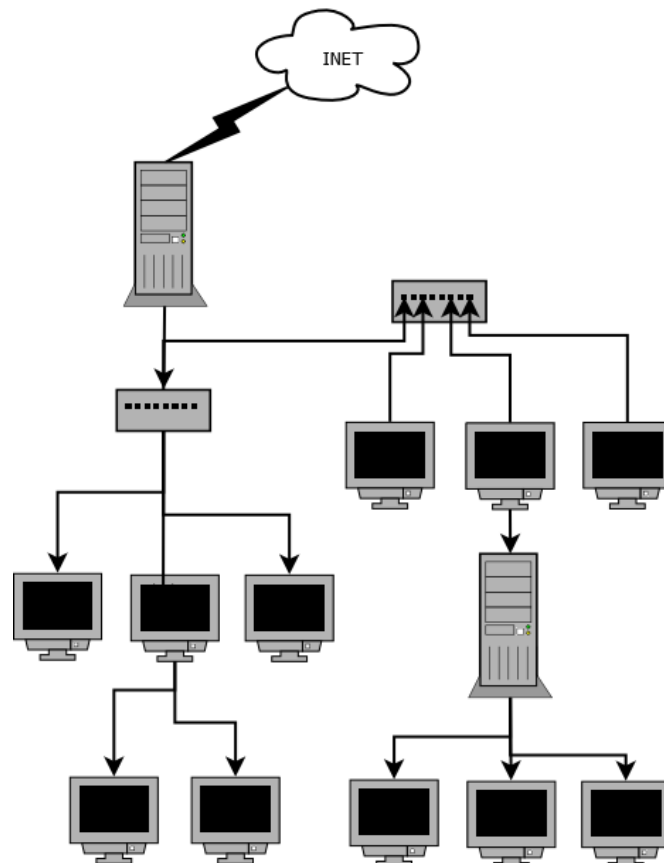
A common scenario where a number of clients and/or servers are physically connected on the same network. Multilevel servers are created in order to distribute the server load.

**NOTE:** Regardless of the place a client occupies within the tree, it will fetch updates from the Toplevel Endpoint Manager until the client is fully installed and has received its policy (then it knows where it belongs). It is therefore critical the DNS name set up on the installation for the Toplevel Endpoint Manager is resolvable in the whole network.

**NOTE:** If the connection is lost between clients and their parent Endpoint Manager (other than Toplevel), after some failed attempts to update, the clients will connect temporarily to the Toplevel Endpoint Manager for fetching policy updates. Their next connection attempt will be to their Midlevel Endpoint Manager unless it is changed at the Toplevel Endpoint Manager.

**Environment:** A medium/large number of computers on the same physical network segment.

**Example:** Two Windows servers and 150 Windows clients. Please check the Administrator’s Guide for system requirements.



**Description:** In this scenario, we have a medium number of computers physically connected. The desired deployment will require installing the Endpoint Manager on one of the Windows servers and roll out the MSI installers (created later) to the clients.

As soon as the clients appear on the Endpoint Manager console, we will “promote” the selected client as Midlevel Endpoint Manager, and subsequently assign clients to it.

**Steps:**

1. Install Endpoint Protection with Endpoint Manager on the selected server
2. Open Endpoint Manager console and complete the Install Wizard to create a **Realm**
3. Run an Internet Update
4. Create MSI installers from **Settings** and roll them out to the clients
5. Promote specific client(s) to Midlevel Endpoint Manager(s)
6. Create groups/subgroups and assign them to the new Endpoint Manager(s) we want they update/report from/to

**Behavior:**

The Toplevel Endpoint Manager will download updates from the Internet.

The clients and Midlevel Endpoint Managers will fetch policies and software updates from the Toplevel Endpoint Manager, and report events (warnings, errors) to the parent Endpoint Manager that will report directly to the Top.

The clients within groups/subgroups assigned to the Midlevel Endpoint Managers will fetch policies and updates, and report events, from/to their Midlevel Endpoint Manager.

### SCENARIO 3 - USING MULTILEVEL MANAGERS (WAN NETWORKS)

---

A common scenario where a number of clients and/or servers are in different physical network segments but connected through WAN.

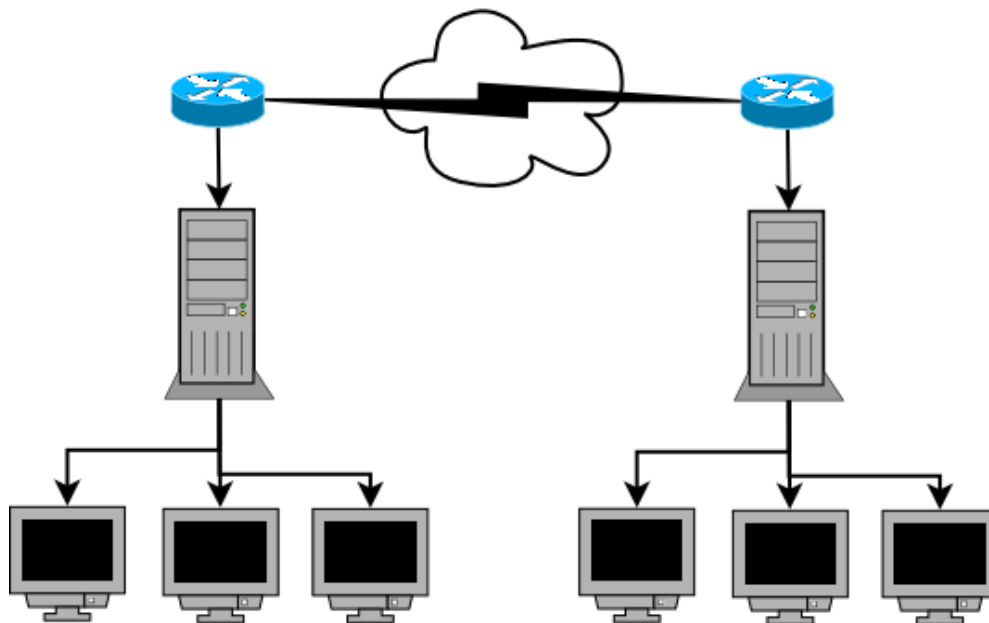
**HINT:** In cases of slow upload speed between networks, we can set up the midlevel manager policy for Midlevel Endpoint Manager(s) so that updates are downloaded directly from the Internet instead of from the Toplevel Endpoint Manager. Policy updates and reporting will still be from/to the Toplevel Endpoint Manager.

**NOTE:** Regardless of the place a client occupies within the tree, it will fetch updates from the Toplevel Endpoint Manager until the client is fully installed and has received its policy (then it knows where it belongs). It is therefore critical the DNS name set up on the installation for the Toplevel Endpoint Manager is resolvable in the whole network (WAN).

This is also relevant with respect to speed, as all clients will use the WAN connection to fetch updates/policies from the Toplevel Endpoint Manager the first time.

**Environment:** Any number of computers placed on different physical network segments.

**Example:** Two Windows Servers and 35 Windows clients. Please check the Administrator's Guide for system requirements. There are two groups of clients in different locations, connected using VPN over the Internet.



**Description:** In this scenario, we have a small group of computers separated in two different physical networks, connected through VPN. The desired deployment will require installing the Endpoint Protection on one of the Windows servers and roll out the MSI installers (created later) to the clients and the other server. As soon as the remote server appears on the Endpoint Manager console, we will “promote” it as Midlevel Endpoint Manager, and then assign groups of clients from that location to it.

**Steps:**

1. Install Endpoint Protection with Endpoint Manager on the selected server
2. Open Endpoint Manager console and complete the Install Wizard to create a **Realm**
3. Run an Internet Update
4. Create MSI installers from **Settings** and roll them out to the clients
5. Promote a specific client as the Midlevel Endpoint Manager in the remote location
6. Create groups/subgroups with clients on the remote location and assign them to the new remote Midlevel Endpoint Manager they should update/report from/to.

**Behavior:**

The Toplevel Endpoint Manager will download updates from the Internet.

The clients and Midlevel Endpoint Managers will fetch policies and software updates from the Toplevel Endpoint Manager, and report events (warnings, errors).

The clients within groups/subgroups assigned to the Midlevel Endpoint Manager will fetch policies and updates, and report events, from/to their Midlevel Endpoint Manager.

**SCENARIO 4 - DEPLOYING ON CLIENTS OUTSIDE THE NETWORK**

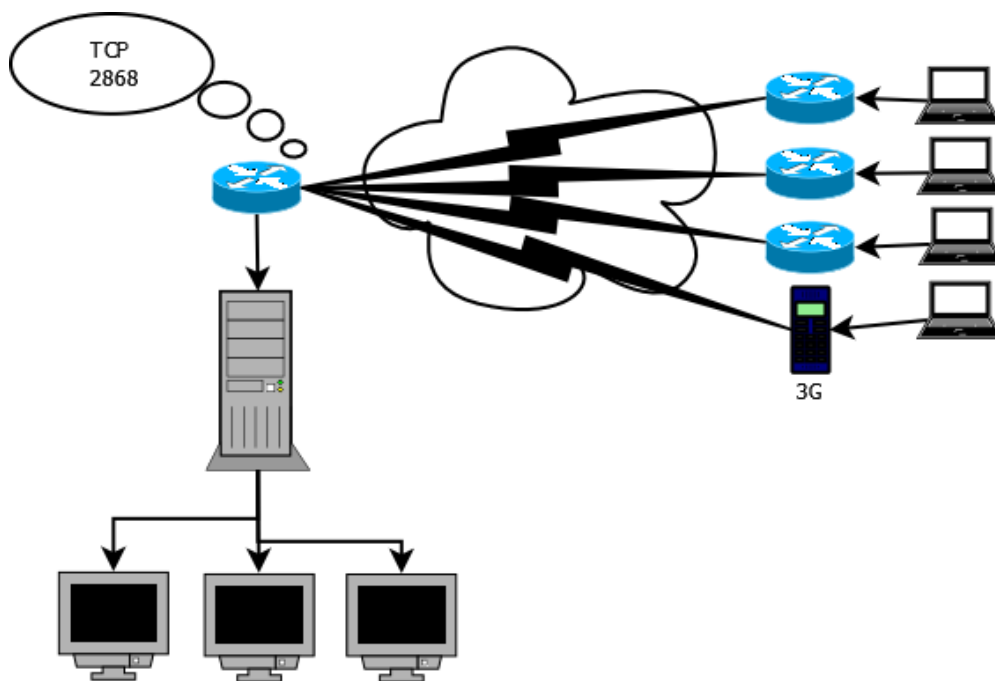
A common scenario where a number of clients are located separately in remote locations with no access to the main office except through of the public IP address.

**NOTE:** Regardless of the place a client occupies within the tree, it will fetch updates from the Toplevel Endpoint Manager until the client is fully installed and has received its policy (then it knows where it belongs). It is therefore critical the DNS name set up on the installation for the Toplevel Endpoint Manager is resolvable in the whole network (WAN).

This is also relevant with respect to speed, as all clients on remote locations will use bandwidth available on the Internet connection to fetch updates/policies from the Toplevel Endpoint Manager the first time.

**Environment:** Any sized group of computers not belonging to the local network.

**Example:** One Windows server and 250 Windows clients. Please check the Administrator’s Guide for system requirements.



**Description:** In this scenario, there is a medium group of computers, separated in two groups. One group belongs to the same physical network as the server. The other group is comprised of standalone laptops in different locations, with no other access to the main office than the public IP address. The desired deployment will require installing the Endpoint Protection on the Windows server and roll out the MSI installers (created later) to the clients.

We will configure the remote clients to update from the Internet but check with the Endpoint manager for policy and messaging.

**Steps:**

There are two parts on this deployment. The first one is fixed; the second one will vary depending on your situation.

## FIXED PART

1. Install Endpoint Protection with Endpoint Manager on the selected server
2. Open Endpoint Manager console and complete the Install Wizard to create a **Realm**
3. Run an Internet Update
4. Create a policy for the remote clients group and specify to update from the Internet
5. Forward incoming connections to port TCP 2868 to the Endpoint Manager in your network
6. On the remote clients: Add an entry in the HOSTS file resolving the DNS name address set up for the Endpoint Manager during installation, to the public IP for the main office, for example:  
SERVER.domain.local 80.92.175.8
7. Create MSI installers from **Settings** and roll them out to the local clients.
8. Move the remote clients as they appear in the Endpoint Manager console to the group created for remote locations.

## VARIABLE PART

**CASE A: *The laptops will be located remotely, but we will have them locally on the network at the beginning.***

Run the MSI installers on the clients for installation and update. After that, you can move them to the remote locations. They will fetch downloads from Internet but policy and messaging will be from/to the Endpoint Manager.

**NOTE:** You need to comment out / delete temporarily the line added to the HOSTS file on the clients to allow first installation/update, and re-enable this line when the clients are removed from the network.

**CASE B: *The laptops are and will be located remotely only. The network administrator will setup the installation (with physical or remote access to the laptops).***

Run the latest Endpoint Protection standalone installer from the Norman's website. After installation and update from the Internet, copy the file MIG2NSS7.NTS (residing in the same folder where you created the MSI installers) into the folder \Norman\Config.

After a short period of time the client will connect to the Endpoint Manager for policy updates and messaging information.

**CASE C: *The laptops are and will be located remotely only. The network administrator has no access to them, so the user will do the set up.***

Run the MSI installers on the clients for installation and update. Please note they will fetch all files from the Endpoint Manager the first time, so consider the bandwidth from your main office. After this first update, including policy, the clients will fetch downloads from the Internet. Policy and messaging however will still be from/to the Endpoint Manager.

**Behavior:**

The Endpoint Manager will download updates from the Internet.

The **local clients** will fetch policies and program updates from the local Endpoint Manager, and report events (warnings, errors) to this Endpoint Manager.

The **remote clients** will fetch updates directly from the Internet and policies/messages from/to the Endpoint Manager.

### *OTHER POSSIBLE SCENARIOS*

There are several ways to configure and set up networks, and consequently many ways to set up a Norman Endpoint Protection installation. You can combine the scenarios described on this document, and invent many others.

Please, contact your local Norman subsidiary or distributor to request help about planning in any specific environment.