

# DEPLOYING AN ENDPOINT CLIENT WITH GROUP POLICY OBJECTS

July 2018

Aaron Rose  
arose@checkpoint.com

<b>OVERVIEW.....</b>	<b>2</b>
<b>ASSUMPTIONS &amp; REQUIREMENTS .....</b>	<b>2</b>
<b>SYSTEM ARCHITECTURE OVERVIEW .....</b>	<b>3</b>
<b>CREATING A PACKAGE FOR EXPORT.....</b>	<b>4</b>
<b>CREATING A DISTRIBUTION POINT. ....</b>	<b>5</b>
<b>CREATING &amp; LINKING A GROUP POLICY OBJECT .....</b>	<b>6</b>
<b>TESTING THE DEPLOYMENT.....</b>	<b>8</b>
<b>ADDITIONAL RESOURCES .....</b>	<b>9</b>

## Overview

Active Directory's Group Policy Objects can be used to deploy Check Point's Endpoint Client to Windows computers. This guide will demonstrate the necessary steps to:

- Create & export an endpoint client installation package using SmartEndpoint
- Create a distribution point for the software package
- Create a Group Policy Object to deploy the package & link the GPO to the appropriate Organizational Unit(s)
- Force a Group Policy update on the client computer to test the deployment

## Assumptions & Requirements

This guide makes the following assumptions:

- You have previously installed and configured an Endpoint Security Management Server, including necessary licenses & client packages.
- You have installed SmartEndpoint on a computer that supports the client installation and have established a connection to the Endpoint Security Management Server
- You have an existing Active Directory infrastructure with defined Organizational Units (OU's)
- Your Windows computers have been previously connected to your domain and are able to receive Group Policy updates
- We will be installing the initial client without software blades; this will facilitate installation of the blades by defining the software deployment rules after the initial client is deployed.

Note: You may find minor variances in the steps required if you use different versions of Windows or SmartConsole, but the process is generally the same.

This guide was developed using the following lab environment:

- Domain Controller: Microsoft Windows Server 2016
- Test Client: Microsoft Windows 10 64bit edition
- Console: SmartConsole/SmartEndpoint for Endpoint Security Server R80.20M2
- Endpoint Client Version: E80.86

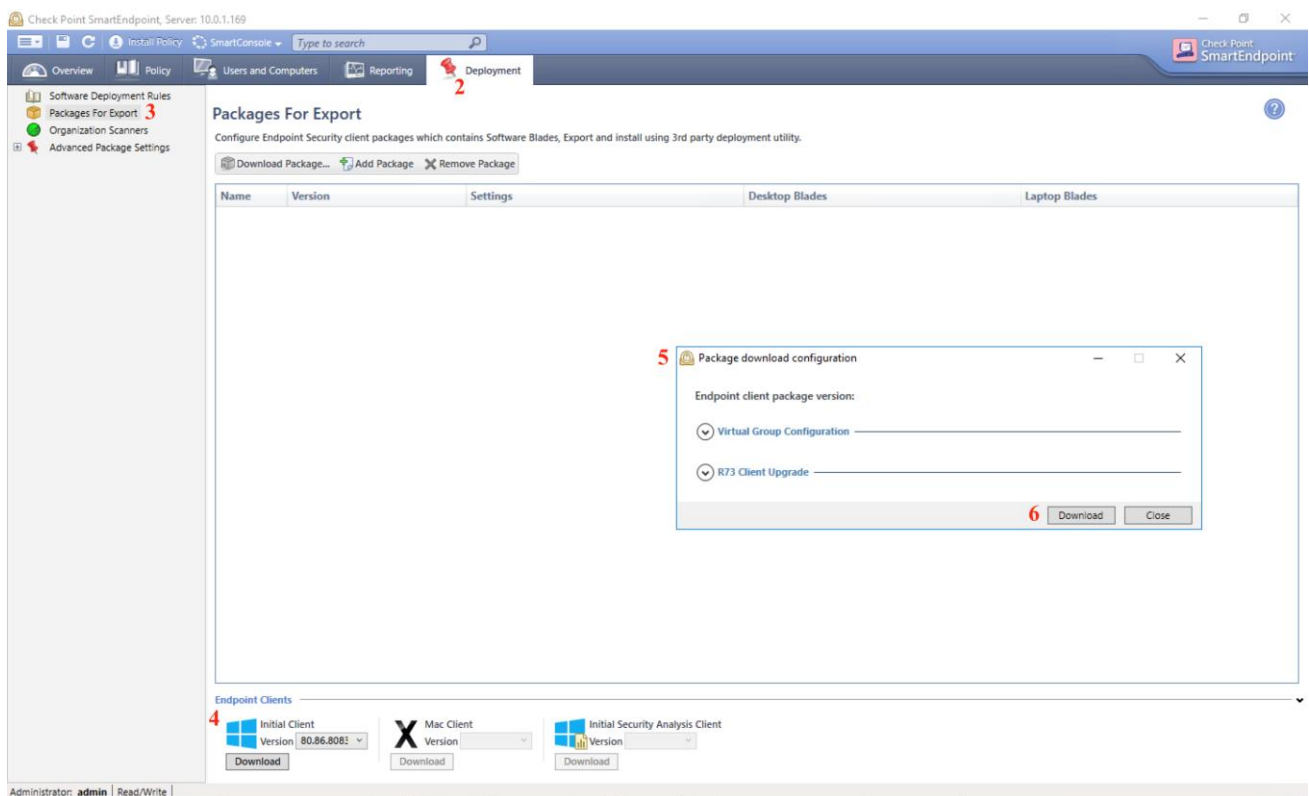
## System Architecture Overview

Component	Description
<b>Endpoint Security Management Server</b>	A standard Check Point Security Management Server with the Endpoint software blade enabled & configured
<b>SmartEndpoint</b>	A Check Point SmartConsole application used to deploy, configure and monitor Endpoint clients & policies.
<b>Endpoint Security Client</b>	The application installed on end-user computers to enforce security polices & monitor the security status of the endpoint.
<b>Domain Controller</b>	A Windows server that provides security authentication & management of Windows computers within a Windows Server domain.

# Creating a Package for Export

Before deploying the Endpoint Client via GPO, you must first export the appropriate initial client package using SmartEndpoint.

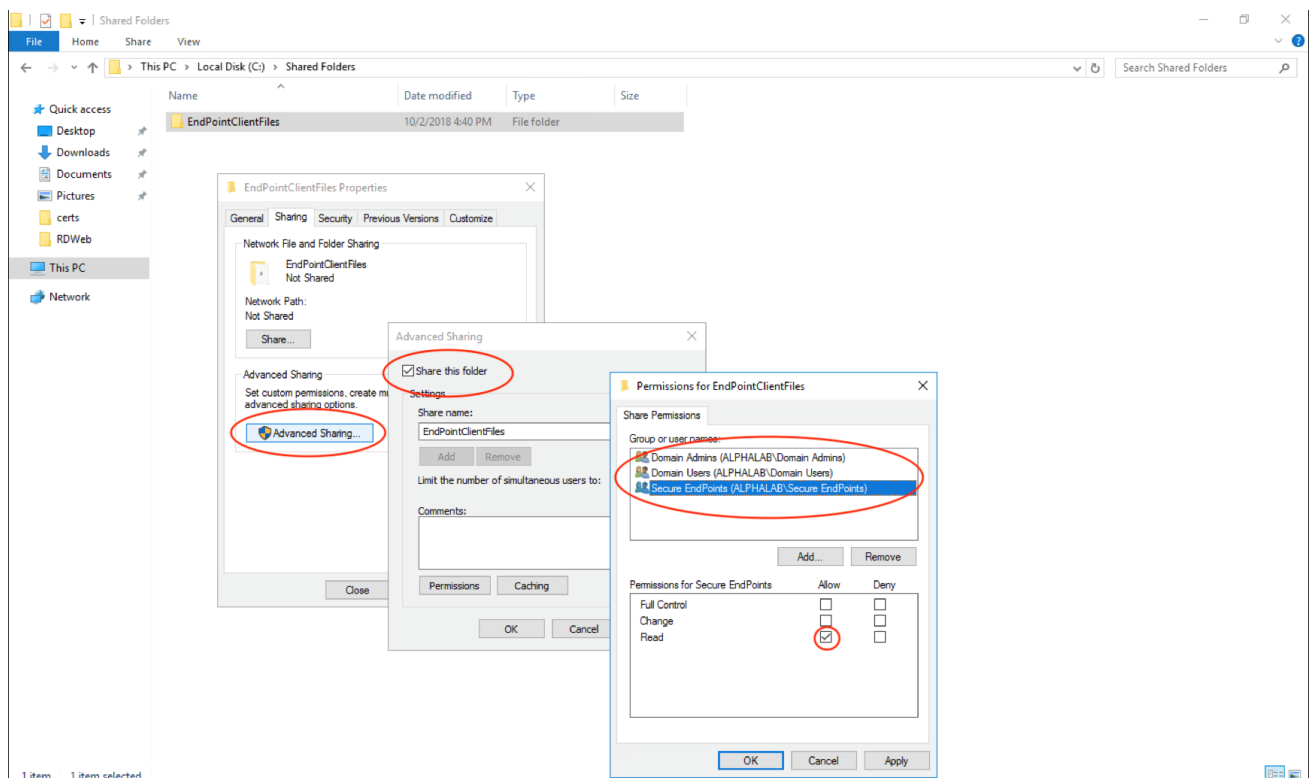
1. Launch SmartEndpoint and login using the appropriate credentials.
2. Select the “Deployment” tab
3. Select “Packages for Export” on the left menu bar
4. Under the “Endpoint Clients” section near the bottom of the window, choose the appropriate Initial Client Version from the dropdown and select “Download”
5. A “Package download configuration” window will appear; here you can choose to assign the Endpoints to a Virtual Group automatically if you wish.
6. Select “Download” and choose a location to save the package.



# Creating a Distribution Point

In order to facilitate the deployment of the initial client MSI package, a distribution point accessible by the relevant computers must be created.

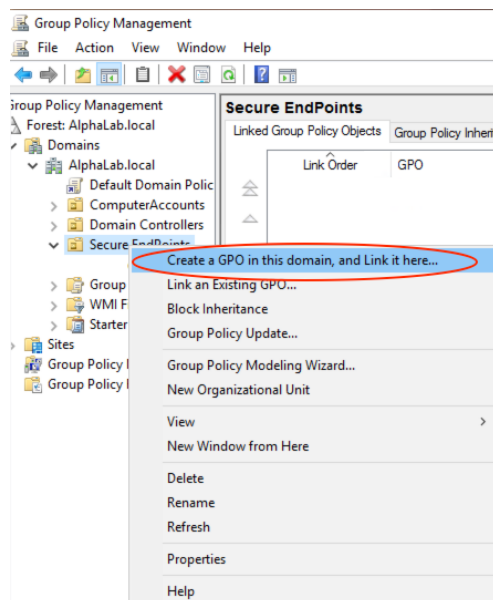
1. Log on to the server that you are using to share the package.  
Note: For the purpose of this guide, we will be using shared folder on the domain controller but any storage server that is accessible on your network can be used as a distribution point.
2. Create a shared network folder, this folder will contain the initial client MSI package
3. Set the appropriate permissions on this folder to allow access to the package
4. Copy the MSI package that was downloaded on page 4 to the shared folder
5. After sharing the folder, reopen the properties window of the shared folder and select the sharing tab. Make note of the network address of the shared folder for use on the next page of this guide.



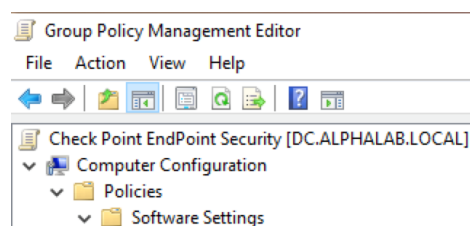
## Creating & Linking a Group Policy Object

MSI Packages can be deployed using Group Policy Objects (GPO) in Active Directory by linking the GPO to the Organizational Unit (OU) containing the target computers.

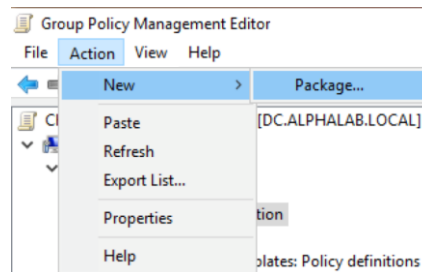
1. Open Server Manager on the domain controller, or the remote computer you are using to manage the domain controller.
2. Use the Tools menu to open Group Policy Management
3. Right click the OU you wish to assign the EndPoint client to and select “Create a GPO in this domain, and link it here...”



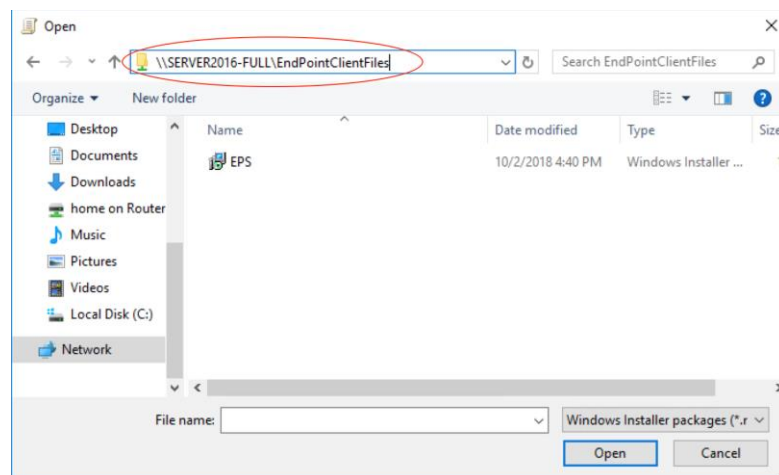
4. Name the GPO, leaving the “Source Starter GPO” dropdown to none & click OK
5. Right click on your new GPO and select edit
6. Select Computer Configuration --> Policies --> Software Settings --> Software installation



7. Under the action tool bar menu, select New --> Package



8. Do not navigate locally to the EPS package, as the local path will not be accessible by client. Instead, use the path bar to type in the network address of the shared folder that we found on step 5 of Creating a Distribution Point. Select the EPS.msi package and click Open.



9. A "Deploy Software" window will open, select "Assigned" and click OK. You have now successfully setup your GPO to deploy the package and it has been linked to the OU you selected.



## Testing the Deployment

1. Launch command prompt on the client computer
2. Run “gpupdate /force” to force a Group Policy Update
3. After the policy updates, you will be prompted to restart the computer, enter Y press enter.

```
C:\Windows\system32>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.

The following warnings were encountered during computer policy processing:

The Group Policy Client Side Extension Software Installation was unable to apply one or more settings because the changes must be processed before system startup or user logon. The system will wait for Group Policy processing to finish completely before the next startup or logon for this user, and this may result in slow startup and boot performance.

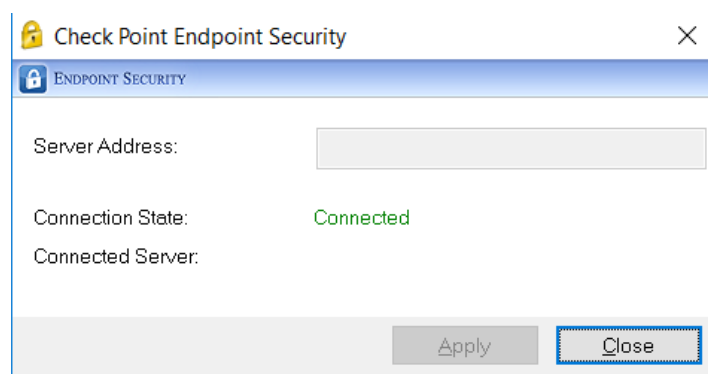
User Policy update has completed successfully.

For more detailed information, review the event log or run GPRESULT /H GPREport.html from the command line to access information about Group Policy results.

Certain Computer policies are enabled that can only run during startup.

OK to restart? (Y/N)
```

4. Wait for the computer to restart & install the package.
5. Once the restart & package install is complete, you should see the client icon in the system tray. Double click the icon to see that the client is successfully connected to the management server. Now you can proceed with defining deployment rules to install the applicable software blades & settings.



## Additional Resources

<b>sk117536</b>	The Endpoint Security Homepage
<b>Endpoint Security Management Server Administration Guide</b>	Access the guide <a href="#">here</a> or retrieve the document from the Endpoint Security Homepage.
<b>R80.20 GAIA Administration Guide</b>	Download the guide <a href="#">here</a>