Heimdal Security

Product Documentation

Technical whitepaper and implementation guide for corporate environments

Thor Foresight
Thor Vigilance

1. Table of contents

2. Introduction

This document contains an in depth technical walkthrough of Heimdal Security Thor Enterprise products. The document describes the software products, product features, communication, system requirements, implementation recommendation and administration processes.

3. Who is Heimdal Security

Heimdal Security A/S was founded in early 2014 in Copenhagen, Denmark. At present, Heimdal Security A/S works with major corporations, public entities and major banks across the world in fighting against e-crime.

Ever since its inception, the Heimdal Security A/S company has developed new products that have set new standards in malware detection by continuously following IT criminals' footsteps and providing the best security solutions for organizations as well as private individuals.

Find out more about us:

https://heimdalsecurity.com/en/about

https://heimdalsecurity.com/blog/

4. What are the Heimdal Security products

The Heimdal Security product Thor Enterprise line-up includes 2 main product branches: **Thor Foresight** and **Thor Vigilance**. The products complement each other, and they should be combined in order to offer maximum system and network protection for the protected companies and entities. Thor Foresight can be regarded as the product branch which is minimizing threats, closing loopholes in the security of applications and filtering unsafe traffic, while Thor Vigilance can be regarded as the reactive branch that deals with threats that have found their way on the local machines like viruses and malware.

4.1 Thor Foresight

Work-related and private internet usage create challenges for corporations, as it becomes difficult for the average user to defend himself from advanced malware techniques employed by cyber criminals. Since malicious code can be executed even from legitimate websites, through drive-by attacks or through phishing links, checking traffic for applications which are using web technologies is a must for all company endpoints.

Thor Foresight embeds everything a system needs to prevent an infection before it happens. It filters malicious traffic, it updates 3rd party apps thus minimizing exploitation risks and it identifies the computers that may have been compromised by attackers, also reporting this to the centralized management system. The protection is proactive, reliable, scalable and consists of three active modules: DarkLayer Guard, VectorN Detection and X-ploit Resilience.

4.2 Thor Vigilance

Thor Vigilance is the reactive protection side of our product suite. It is the next gen antivirus solution that reacts to infected files found on the system. It complements the Thor Foresight product module to offer all around protection. It offers a centralized management interface across all the devices for easy corporate client management. It is flexible, easy to use and it offers a wide variety of scanning profiles to fit your corporate needs.

5. Minimum System Requirements for Heimdal Security products

You may install Thor Foresight and Thor Vigilance on computers running the following configurations and specs:

OS:

- Windows 7 (32 and 64 bit), Service Pack 1 or higher with the newest updates, hotfixes and service packs installed
- Windows 8 (32 and 64 bit)
- Windows 8.1 (32 and 64 bit)
- Windows 10 (32 and 64 bit)
- Windows Server 2008 R2 with Service Pack 1
- Windows Server 2012/2012 R2.
- Windows Server 2016

Please note that for the best experience we recommend using the latest version of any OS available from an official source.

Processors:

- AMD: Ab Athlon 64/Sempron (Paris Core)/Opteron
- Centaur Technology: starting with VIA C7
- Intel: starting with Pentium 4 (Desktop) or Pentium M (Laptop)
- Transmeta: starting with Efficeon

Memory:

- At least 2GB RAM

Hard disk:

- At least 2GB disk space. The space is required for downloading Virus Definition Files and quarantined files, not for the actual local agents.

Browser:

- The recommended browser for using the Heimdal Security Dashboard is Chrome.

Special requirements:

- Microsoft .NET Framework 4.6.1 must be installed on the operating system prior to the installation
- Internet access with the following ports open to traffic: port 80, port 53, port 443

5.1 PC rights

To install, close or restart the local Thor agent, you must have administrative rights over the relevant machine. With local user rights, the user interface can still be run.

Action:	Required user rights:
Installation of Thor Enterprise	Local/ Domain administrator
Automatic update of Thor Enterprise	Local user
Patching 3rd party software*	Local user
Dark Layer Guard	Local user
Reboot or restart of Thor Enterprise	Local/ Domain administrator
Manual starting of Thor Enterprise	Local/ Domain administrator
Changing locked setting for Thor suite in the Enterprise version	Not Possible

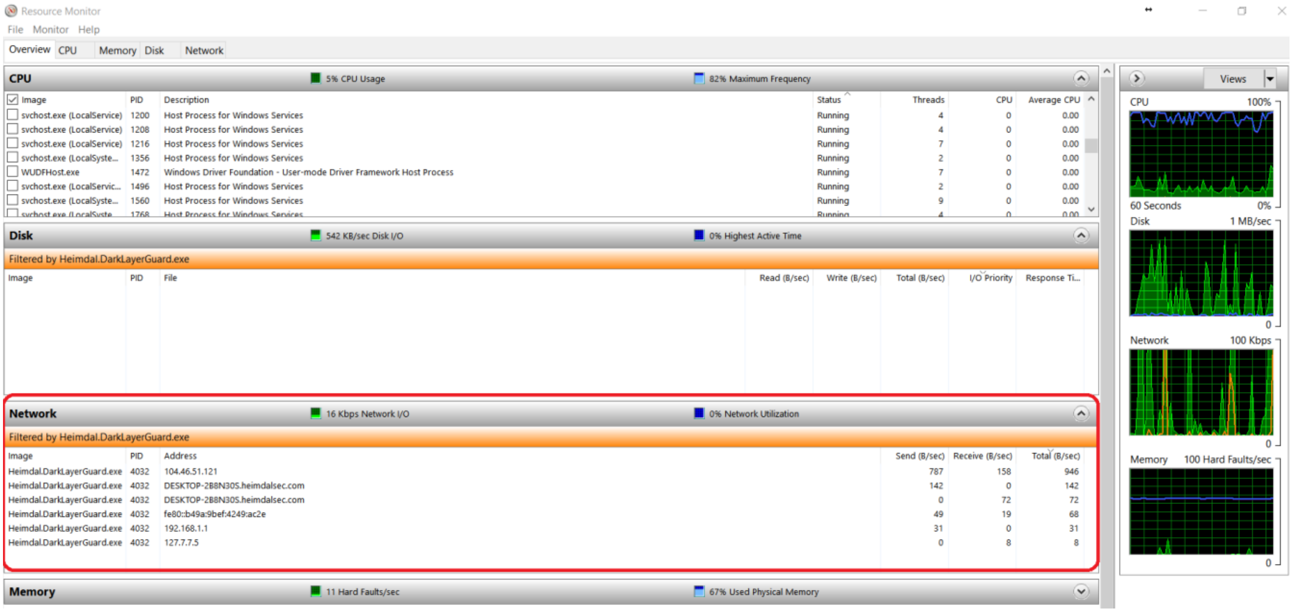
* If the used group policy allows the action to be permitted locally.

5.2 Resource usage

Thor Enterprise consists of one modular application and 4 Windows services:

Component:	Component type:
HeimdalAgent.exe	Application
Heimdal Client Host	Service
Heimdal DarkLayer Guard*	Service
Heimdal Uptime Checker	Service
Heimdal Antivirus	Service
Heimdal Security Service Monitor	Task Scheduler

*The bandwidth needed by the DarkLayer Guard service is quite low. When the DarkLayer Guard is in use and Thor starts to block DNS requests, the average bandwidth needed is around 1,500 bytes per second.



☑ Image	PID	Description	Status	Threads	CPU	Average CPU
□ svchost.exe (LocalService)	1200	Host Process for Windows Services	Running	4	0	0.00
□ svchost.exe (LocalService)	1208	Host Process for Windows Services	Running	4	0	0.00
□ svchost.exe (LocalService)	1216	Host Process for Windows Services	Running	7	0	0.00
□ svchost.exe (LocalSyste...	1356	Host Process for Windows Services	Running	2	0	0.00
□ WUDFHost.exe	1472	Windows Driver Foundation - User-mode Driver Framework Host Process	Running	7	0	0.00
□ svchost.exe (LocalServic...	1496	Host Process for Windows Services	Running	2	0	0.00
□ svchost.exe (LocalSyste...	1560	Host Process for Windows Services	Running	9	0	0.00
□ svchost.exe (LocalSyste	1768	Host Process for Windows Services	Running	4	0	0.00

Filtered by Heimdal.DarkLayerGuard.exe

Image	PID	File	Read (B/sec)	Write (B/sec)	Total (B/sec)	I/O Priority	Response Ti...

Filtered by Heimdal.DarkLayerGuard.exe

Image	PID	Address	Send (B/sec)	Receive (B/sec)	Total (B/sec)
Heimdal.DarkLayerGuard.exe	4032	104.46.51.121	787	158	946
Heimdal.DarkLayerGuard.exe	4032	DESKTOP-2B8N30S.heimdalsec.com	142	0	142
Heimdal.DarkLayerGuard.exe	4032	DESKTOP-2B8N30S.heimdalsec.com	0	72	72
Heimdal.DarkLayerGuard.exe	4032	fe80::b49a:9bef:4249:ac2e	49	19	68
Heimdal.DarkLayerGuard.exe	4032	192.168.1.1	31	0	31
Heimdal.DarkLayerGuard.exe	4032	127.7.7.5	0	8	8

The data from the above picture comes from a resource stress test that was carried out throughout a normal work day as to simulate a normal day at the office for the average user.

5.3 What system changes do apply when installing Thor Enterprise?

The most important change the DLG module does is the modification of the local DNS value. For a full list of these changes you can click the below link:

What Changes Does Thor Apply When Installed?

It's also worth mentioning that in addition to the services that Thor creates on your machines, you may also see new tasks created under Task Scheduler. **Heimdal Security Service Monitor** is a task scheduler that verifies if all services are up and running. If they are not, it will start them.

This scheduler is triggered at system startup, log on of any user and on local connection to any user session. This task scheduler is controlled by the Heimdal.MonitorServices.exe program.

5.4 Software compliance

We constantly whitelist our products with other major AV vendors so that the conflicts between our products can always be kept to a minimum.

Since Thor Vigilance is a fully-grown antivirus solution, incompatibilities may arise between this product and the AV that you are currently using. If you use the **Thor Vigilance** product, you should not have any other AV solution installed on your endpoints.

If you are **only** using the **Thor Foresight** product, you will not have any incompatibility between it and any pre-existing AV solution.

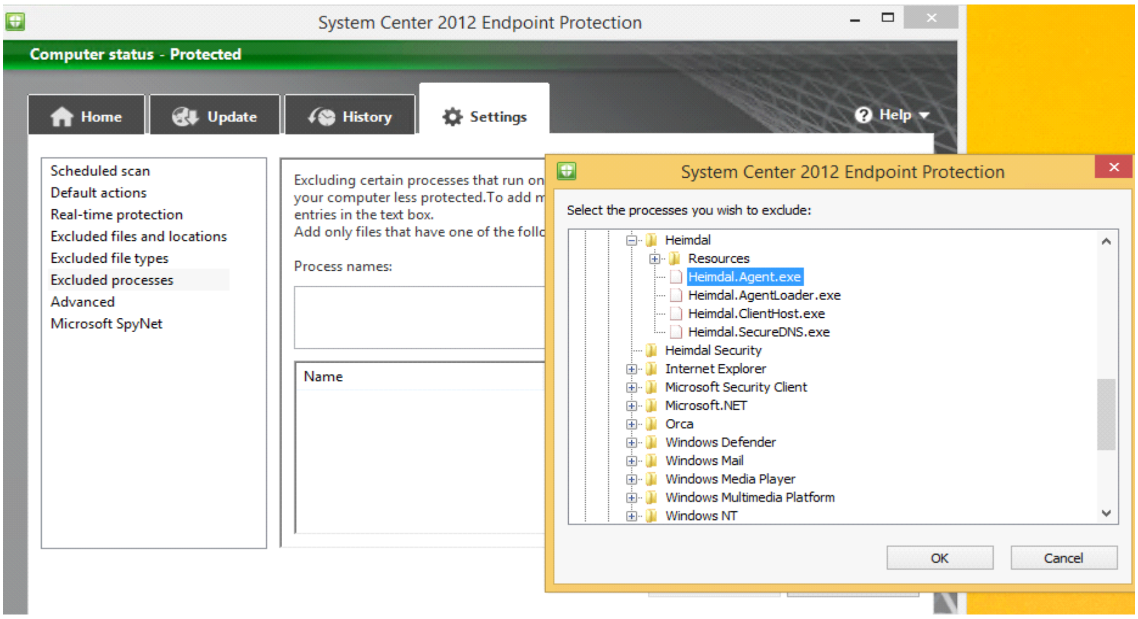
If a **Firewall** or a **Proxy** is installed on the Client, you have to make sure Thor is allowed to communicate with our servers online. To create a rule in your Firewall, Thor needs to be able to access these domains:

- http://heimdalprodstorage.blob.core.windows.net with local port 80;
- https://cloudservice.heimdalsecurity.com with local port 443;
- https://rc-cloudservice.heimdalsecurity.com;
- https://dashboard.heimdalsecurity.com;
- https://rc-dashboard.heimdalsecurity.com;
- prodcdn.heimdalsecurity.com;

Example of firewall and proxy in which you need to add these exclusions:

Websense, Fortigate, SonicWALL, Windows Firewall, Watchguard, Zscaler, Cisco ASA firewalls, Sophos UTM, Untangle, Barracuda, Webtitan, TRITON AP-WEB, Symantec, Trend Micro, Netgear.

For Software Center Endpoint Protection 2012 you need to exclude Thor's processes (Heimdal.Agent .exe, Heimdal.AgentLoader .exe, Heimdal.Antivirus .exe, HeimdalClientHost .exe, HeimdalDarkLayerGuard .exe and Heimdal.UptimeChecker .exe) as shown in the pictures below:



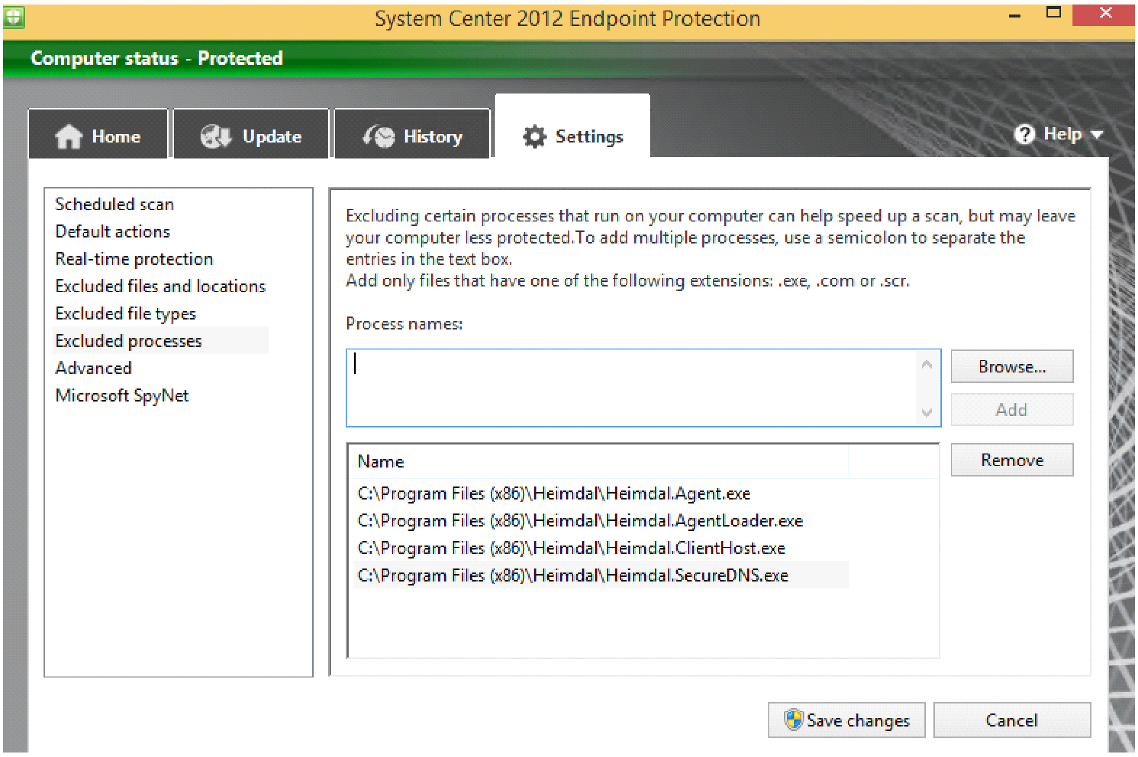
Excluding certain processes that run on your computer less protected.To add m entries in the text box. Add only files that have one of the follo

Process names:

System Center 2012 Endpoint Protection

Select the processes you wish to exclude:

- Heimdal
  - Resources
  - Heimdal.Agent.exe
  - Heimdal.AgentLoader.exe
  - Heimdal.ClientHost.exe
  - Heimdal.SecureDNS.exe
- Heimdal Security
- Internet Explorer
- Microsoft Security Client
- Microsoft.NET
- Orca
- Windows Defender
- Windows Mail
- Windows Media Player
- Windows Multimedia Platform
- Windows NT



Excluding certain processes that run on your computer can help speed up a scan, but may leave your computer less protected.To add multiple processes, use a semicolon to separate the entries in the text box.
Add only files that have one of the following extensions: .exe, .com or .scr.

Process names:

Name
C:\Program Files (x86)\Heimdal\Heimdal.Agent.exe
C:\Program Files (x86)\Heimdal\Heimdal.AgentLoader.exe
C:\Program Files (x86)\Heimdal\Heimdal.ClientHost.exe
C:\Program Files (x86)\Heimdal\Heimdal.SecureDNS.exe

5.5 Web based administration module

Thor Enterprise includes an online management tool, which can be accessed through https://dashboard.heimdalsecurity.com

If you are curious about the latest Thor Enterprise features and technologies, you can always have a look here: https://rc-dashboard.heimdalsecurity.com. Our recommendation is to always allow the enrollment of a few endpoints in the RC (release candidate) program so that you can see what the next new and exciting features inside the Thor products will be.

6. Function description

Thor Enterprise consists of 3 elements: a software client with 2 logical modules, a content delivery network (CDN) and a web-based statistics module.

6.1 Installation of Thor Products

Both Thor products are installed via one unique installation file and can be deployed automatically in corporate environments, using different installation triggers and delivery mechanisms/ techniques.

Please note that for Thor Vigilance installation to take effect, a computer restart is needed.

The right order for AV activation is to firstly activate the module from the interface management under the group policies section. This will trigger the AV installation behind the scenes and will also download the Virus Definition Files (VDF's) from our cloud. After the process is done, the computer will require a restart so that the AV can actually come into effect.

6.1.1 Installation Process and usage environments

Thor can be installed via MSI based installers. For corporate usage we recommend that the msi used for deployment be the one published under the GUIDE section (download and install sub-section) inside the dashboard.

By default, this msi installer file is called **Heimdal_Thor_Launcher.msi** and it is an online installer. The files installed are always downloaded from our cloud and the installer will always push the **latest Thor version** as well as Microsoft .NET Framework 4.6.1 which is a prerequisite. This is of crucial importance when deploying in environments which still rely on Windows 7 OS.

Default behavior when pushing .NET is needed: Thor will push .NET first and then it will wait for a computer restart from the user's side to be able to install the actual Thor agent.

6.1.1.1 Installation via offline MSI file

It is also possible to install Thor via offline MSI. The newest version including detailed documentation can be downloaded below: https://heimdalprodstorage.blob.core.windows.net/setup/Heimdal.msi

*In order to be able to install Thor Enterprise please verify that you have **Microsoft .NET Framework 4.6.1** full profile with all the appropriate updates. If **Microsoft .NET Framework 4.6.1** is not installed onto your computer, please download **it from here:*** https://www.microsoft.com/en-us/download/details.aspx?id=49982

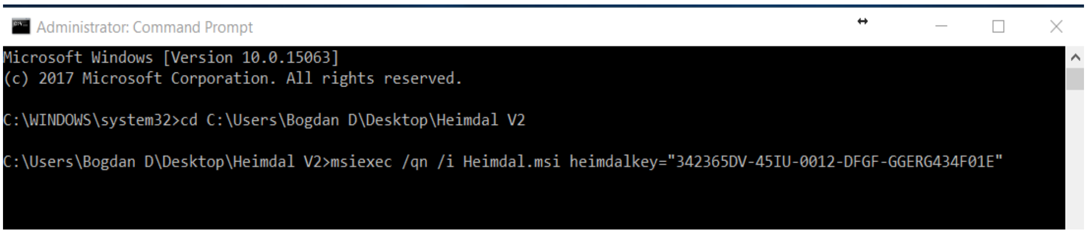
*Each time a new version of Thor is released, we are also releasing an **RC-VERSION** that contains fixes, improvements or other changes that will appear in the next official launch. This is the download link for the beta version:*

https://heimdalprodstorage.blob.core.windows.net/setup/Heimdal-rc.msi

*If you want to install or test the **RC version** of Thor, **we do not recommend** you do it on more than 1 or 2 machines, because this version may have features that have not yet been fully tested.*

Thor can be installed via command line like shown below:

```
msiexec /qn /i Heimdal.msi heimdalkey="key here"
```



```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\Bogdan D\Desktop\Heimdal V2

C:\Users\Bogdan D\Desktop\Heimdal V2>msiexec /qn /i Heimdal.msi heimdalkey="342365DV-45IU-0012-DFGF-GGERG434F01E"
```

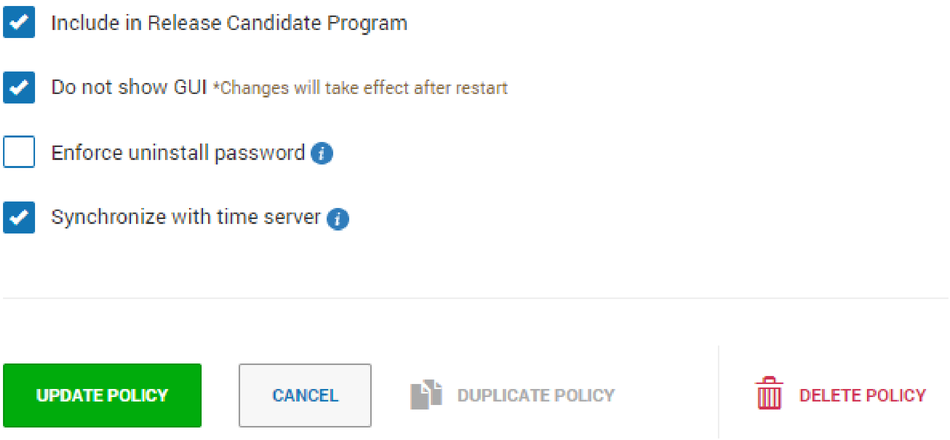
*The silent deployment of Thor does not support changes of the installation path, i.e.: set PATH...

6.1.1.2 Install Thor with no GUI

Thor can be deployed as GUI-less. That means you can choose to deploy the product but hide the interface and the agent presence from the taskbar notification area. Thor's services will still be running in the background (visible in services.msc console) and the installation will still be shown in the programs and features section.

Here is how you do this:

1. Install Thor on your machines (see 5.1.1.1)
2. After the installation is done, open your **web-based administration panel**: Heimdal Security Dashboard
3. Select and create a new **policy** (if you already have a policy set, then you can edit that one if you don't want to create a new one)
4. In the policy you've just created, or you want to edit, go to the "General" section and check the option **"Do not show GUI"**



☑ Include in Release Candidate Program

☑ Do not show GUI *Changes will take effect after restart

□ Enforce uninstall password

☑ Synchronize with time server

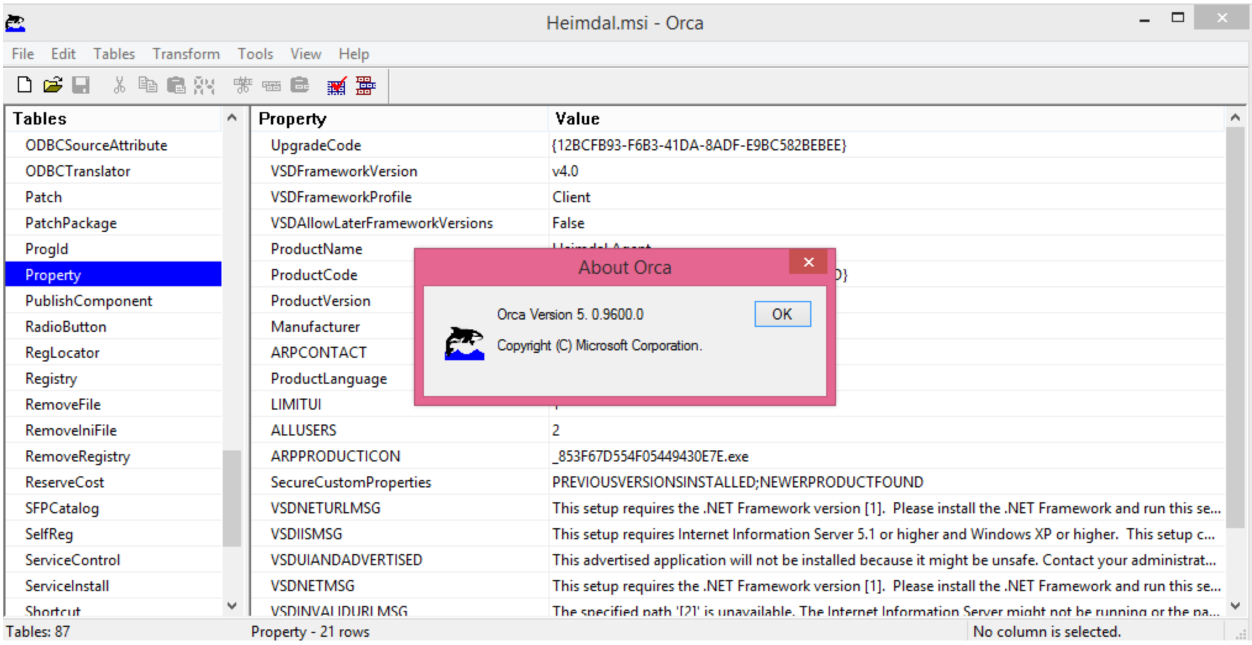
5. Press the green 'Update Policy' button and save your changes

These policy changes will be applied after the machines on which Thor is installed and that respond to the relevant policy will receive a reboot. Please note that the reboot is mandatory for proper GUI-less functionality.

6.1.2 Creating adapted MSI installation files

It is possible to install Thor Enterprise in non-command accepting environments such as Active Directory Group Policy Management and similar systems.

The activation key can be inserted directly into the MSI, as a row with the property "HEIMDALKEY" and Value "[activationkey/serialkey]". The following section shows the approach to be used when inserting the activation key using Orca Version 5.0.9600.0.



Property	Value
UpgradeCode	{12BCFB93-F6B3-41DA-8ADF-E9BC582BEBEE}
VSDFrameworkVersion	v4.0
VSDFrameworkProfile	Client
VSDAllowLaterFrameworkVersions	False
ProductName	
ProductCode	
ProductVersion	
Manufacturer	
ARPCONTACT	
ProductLanguage	
LIMITUI	
ALLUSERS	2
ARPPRODUCTICON	_853F67D554F05449430E7E.exe
SecureCustomProperties	PREVIOUSVERSIONSINSTALLED;NEWERPRODUCTFOUND
VSDNETURLMSG	This setup requires the .NET Framework version [1]. Please install the .NET Framework and run this se...
VSDIISMSG	This setup requires Internet Information Server 5.1 or higher and Windows XP or higher. This setup c...
VSDUIANDADVERTISED	This advertised application will not be installed because it might be unsafe. Contact your administrat...
VSDNETMSG	This setup requires the .NET Framework version [1]. Please install the .NET Framework and run this se...
VSDINVALIDURLMSG	The specified path '[2]' is unavailable. The Internet Information Server might not be running or the pa...

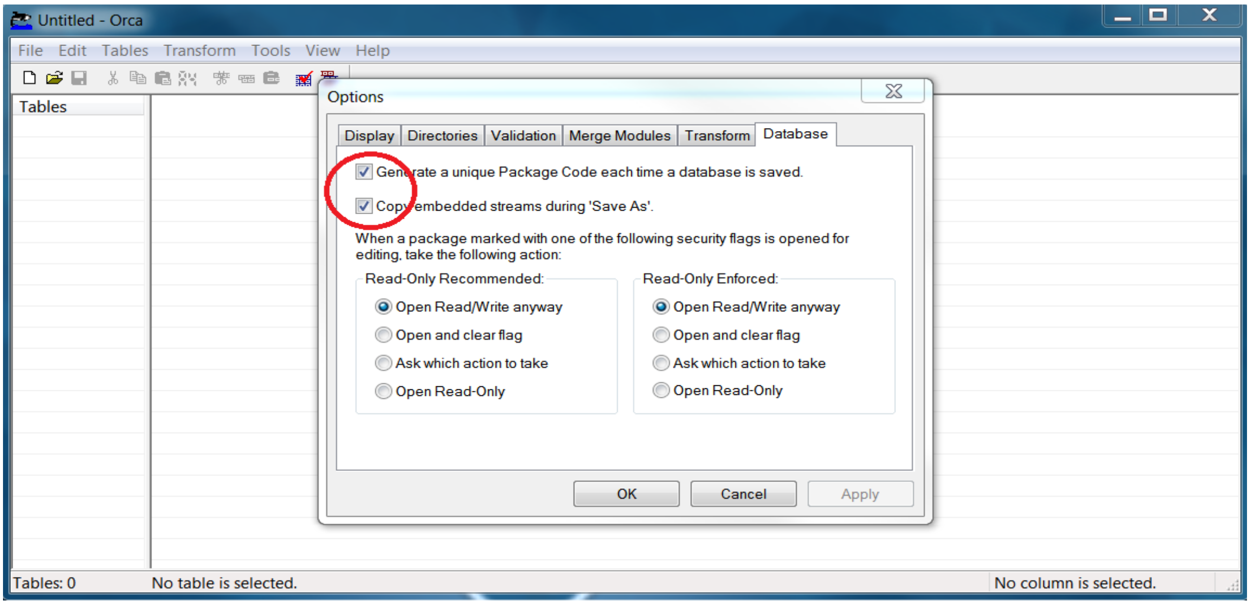
Orca Version 5. 0.9600.0

Copyright (C) Microsoft Corporation.

6.1.2.1 Orca pre-configuration

Before doing the adapted MSI file, check the following settings from ORCA:

a. Open Orca
b. Click on Tools
c. Choose Options
d. Go to the Database tab
e. Check the first two options
f. Click Apply



☑ Generate a unique Package Code each time a database is saved.

☑ Copy embedded streams during 'Save As'.

When a package marked with one of the following security flags is opened for editing, take the following action:

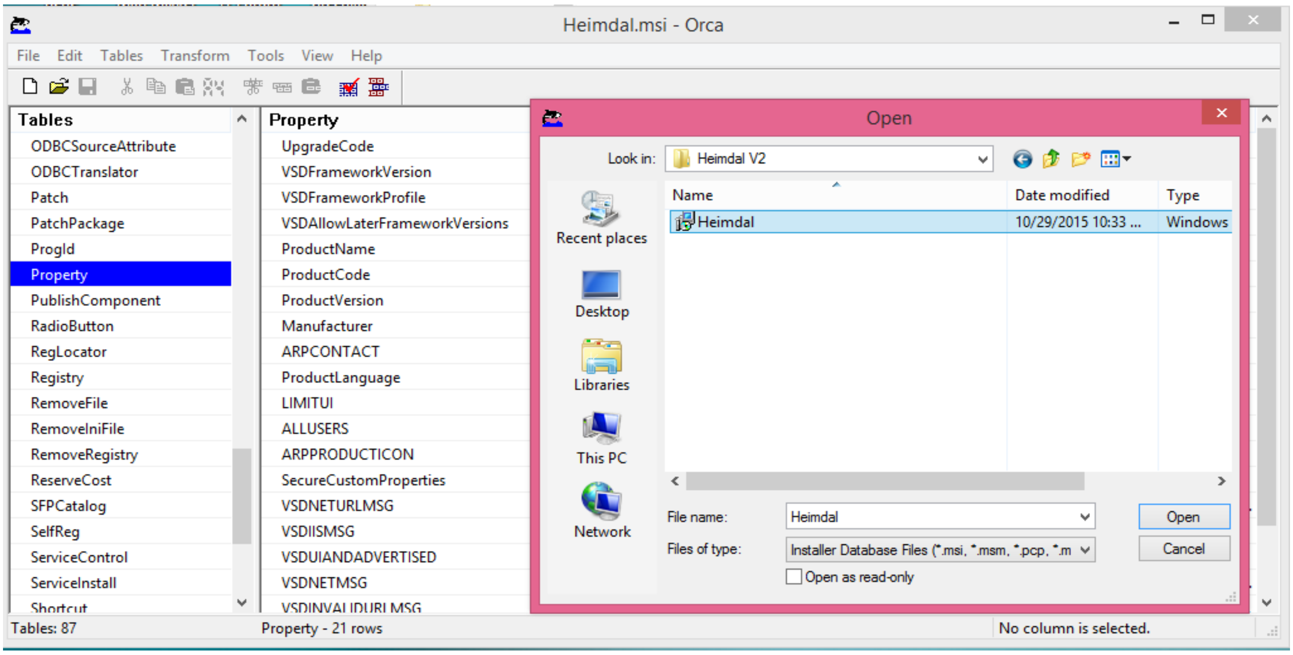
Read-Only Recommended:
- ● Open Read/Write anyway
- ○ Open and clear flag
- ○ Ask which action to take
- ○ Open Read-Only

Read-Only Enforced:
- ● Open Read/Write anyway
- ○ Open and clear flag
- ○ Ask which action to take
- ○ Open Read-Only

6.1.2.2 The MSI editing process

The msi editing process can be broken down into the following steps:

1. Install Orca and open Heimdal.msi:



Look in: Heimdal V2

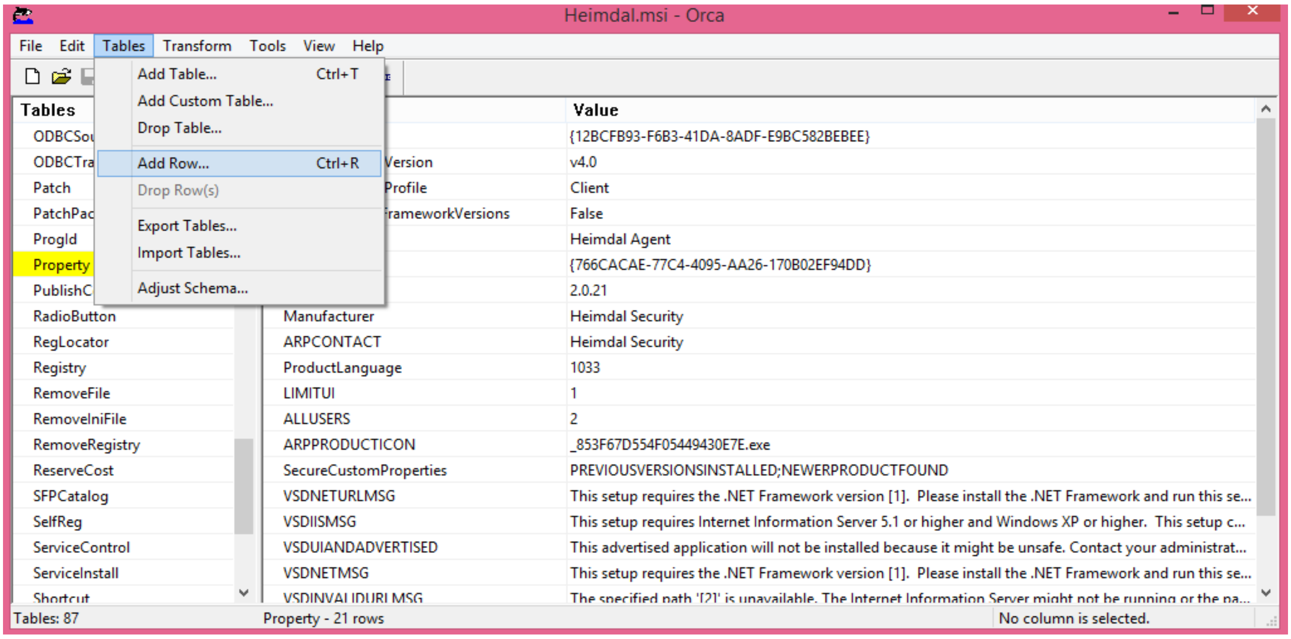
Name	Date modified	Type
Heimdal	10/29/2015 10:33 ...	Windows

File name: Heimdal

Files of type: Installer Database Files (*.msi, *.msm, *.pcp, *.m

□ Open as read-only

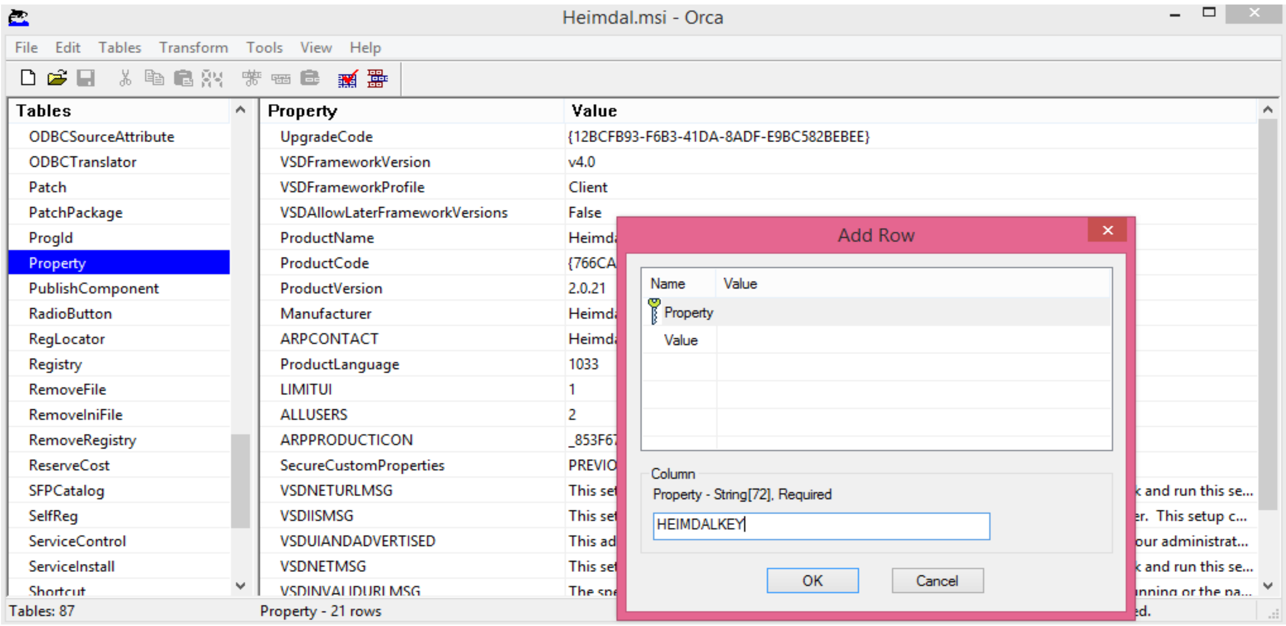
2. Find and mark the table “Property” and select ‘Tables’ and click ‘Add Row…’.



	Value
	{12BCFB93-F6B3-41DA-8ADF-E9BC582BEBEE}
Version	v4.0
Profile	Client
rameworkVersions	False
	Heimdal Agent
	{766CACAE-77C4-4095-AA26-170B02EF94DD}
	2.0.21
Manufacturer	Heimdal Security
ARPCONTACT	Heimdal Security
ProductLanguage	1033
LIMITUI	1
ALLUSERS	2
ARPPRODUCTICON	_853F67D554F05449430E7E.exe
SecureCustomProperties	PREVIOUSVERSIONSINSTALLED;NEWERPRODUCTFOUND
VSDNETURLMSG	This setup requires the .NET Framework version [1]. Please install the .NET Framework and run this se...
VSDIISMSG	This setup requires Internet Information Server 5.1 or higher and Windows XP or higher. This setup c...
VSDUIANDADVERTISED	This advertised application will not be installed because it might be unsafe. Contact your administrat...
VSDNETMSG	This setup requires the .NET Framework version [1]. Please install the .NET Framework and run this se...
VSDINVALIDURLMSG	The specified path '[2]' is unavailable. The Internet Information Server might not be running or the pa...

Tables: 87 Property - 21 rows No column is selected.

3. In the Property field, write **HEIMDALKEY** and in the Value field paste your activation key

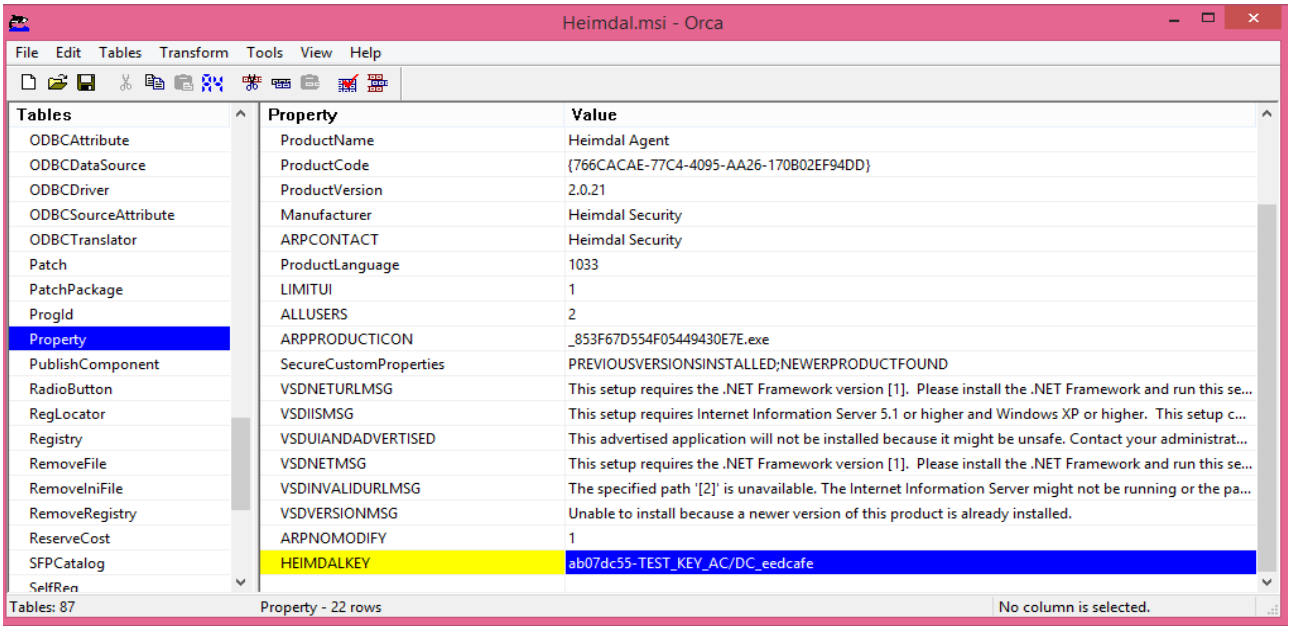


Property	Value
UpgradeCode	{12BCFB93-F6B3-41DA-8ADF-E9BC582BEBEE}
VSDFrameworkVersion	v4.0
VSDFrameworkProfile	Client
VSDAllowLaterFrameworkVersions	False
ProductName	Heimda
ProductCode	{766CA
ProductVersion	2.0.21
Manufacturer	Heimda
ARPCONTACT	Heimda
ProductLanguage	1033
LIMITUI	1
ALLUSERS	2
ARPPRODUCTICON	_853F67
SecureCustomProperties	PREVIO
VSDNETURLMSG	This se ... and run this se...
VSDIISMSG	This se ... r. This setup c...
VSDUIANDADVERTISED	This ad ... our administrat...
VSDNETMSG	This se ... and run this se...
VSDINVALIDURLMSG	The spe ... nning or the pa...

Name	Value
Property	
Value	

Column
Property - String[72], Required
HEIMDALKEY

Tables: 87 Property - 21 rows

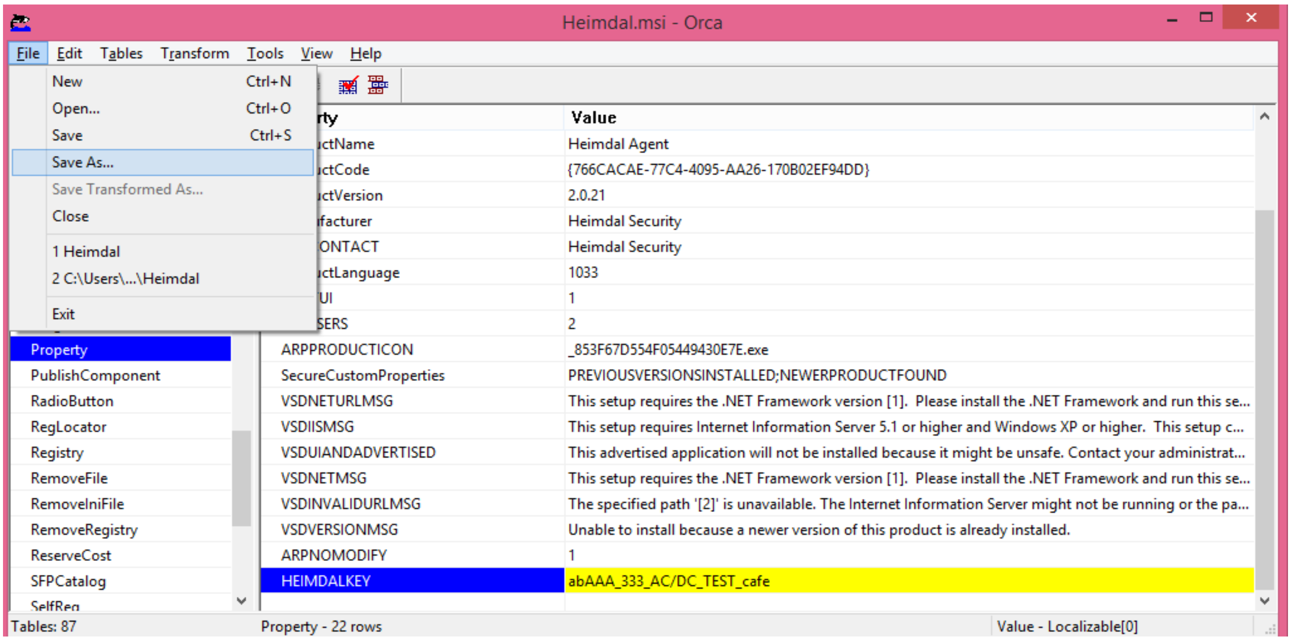


Tables
ODBCAttribute
ODBCDataSource
ODBCDriver
ODBCSourceAttribute
ODBCTranslator
Patch
PatchPackage
ProgId
Property
PublishComponent
RadioButton
RegLocator
Registry
RemoveFile
RemoveIniFile
RemoveRegistry
ReserveCost
SFPCatalog
SelfReg

Property	Value
ProductName	Heimdal Agent
ProductCode	{766CACAE-77C4-4095-AA26-170B02EF94DD}
ProductVersion	2.0.21
Manufacturer	Heimdal Security
ARPCONTACT	Heimdal Security
ProductLanguage	1033
LIMITUI	1
ALLUSERS	2
ARPPRODUCTICON	_853F67D554F05449430E7E.exe
SecureCustomProperties	PREVIOUSVERSIONSINSTALLED;NEWERPRODUCTFOUND
VSDNETURLMSG	This setup requires the .NET Framework version [1]. Please install the .NET Framework and run this se...
VSDIISMSG	This setup requires Internet Information Server 5.1 or higher and Windows XP or higher. This setup c...
VSDUIANDADVERTISED	This advertised application will not be installed because it might be unsafe. Contact your administrat...
VSDNETMSG	This setup requires the .NET Framework version [1]. Please install the .NET Framework and run this se...
VSDINVALIDURLMSG	The specified path '[2]' is unavailable. The Internet Information Server might not be running or the pa...
VSDVERSIONMSG	Unable to install because a newer version of this product is already installed.
ARPNOMODIFY	1
HEIMDALKEY	ab07dc55-TEST_KEY_AC/DC_eedcafe

Tables: 87 Property - 22 rows No column is selected.

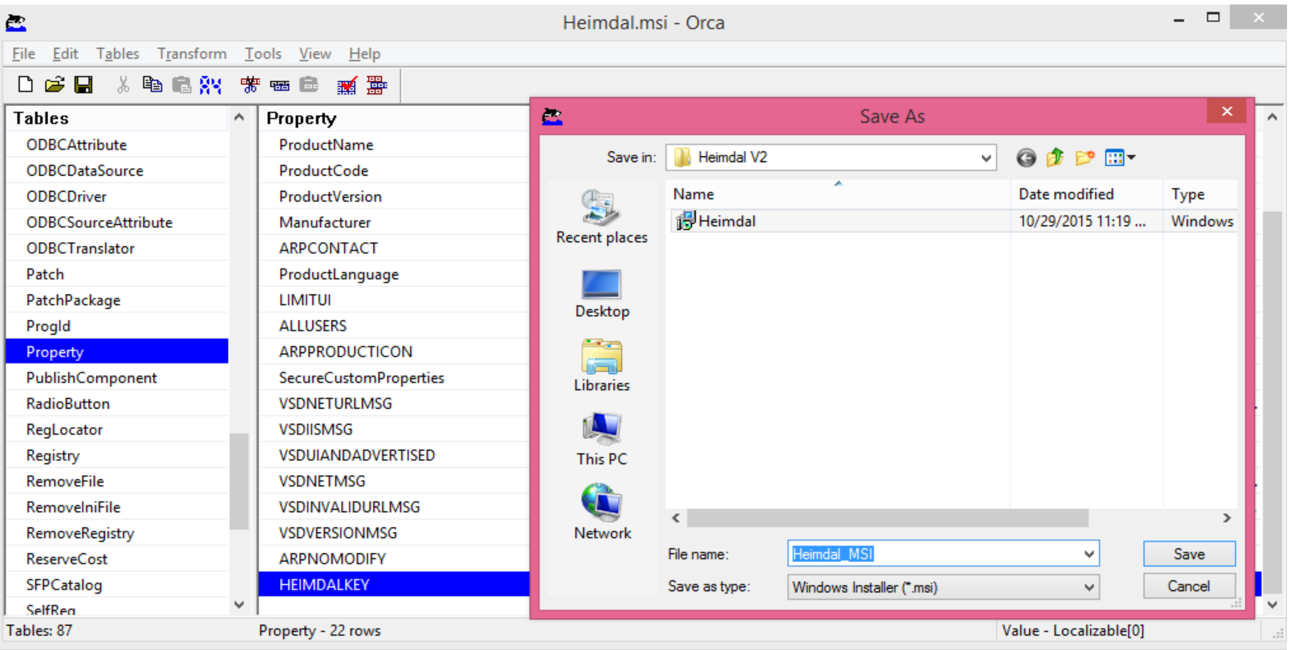
4. To save as a standalone MSI with the activation key built in, click ”File” and ”Save As”.



Tables
Property
PublishComponent
RadioButton
RegLocator
Registry
RemoveFile
RemoveIniFile
RemoveRegistry
ReserveCost
SFPCatalog
SelfReg

rty	Value
ctName	Heimdal Agent
ctCode	{766CACAE-77C4-4095-AA26-170B02EF94DD}
ctVersion	2.0.21
facturer	Heimdal Security
ONTACT	Heimdal Security
ctLanguage	1033
UI	1
SERS	2
ARPPRODUCTICON	_853F67D554F05449430E7E.exe
SecureCustomProperties	PREVIOUSVERSIONSINSTALLED;NEWERPRODUCTFOUND
VSDNETURLMSG	This setup requires the .NET Framework version [1]. Please install the .NET Framework and run this se...
VSDIISMSG	This setup requires Internet Information Server 5.1 or higher and Windows XP or higher. This setup c...
VSDUIANDADVERTISED	This advertised application will not be installed because it might be unsafe. Contact your administrat...
VSDNETMSG	This setup requires the .NET Framework version [1]. Please install the .NET Framework and run this se...
VSDINVALIDURLMSG	The specified path '[2]' is unavailable. The Internet Information Server might not be running or the pa...
VSDVERSIONMSG	Unable to install because a newer version of this product is already installed.
ARPNOMODIFY	1
HEIMDALKEY	abAAA_333_AC/DC_TEST_cafe

Tables: 87 Property - 22 rows Value - Localizable[0]



Save in: Heimdal V2

Name	Date modified	Type
Heimdal	10/29/2015 11:19 ...	Windows

File name: Heimdal_MSI

Save as type: Windows Installer (*.msi)

Remember that MSI files contain your organizations license/serial key and should only be used on the computer, which you have purchased licenses for.

Please note that the activations are constantly monitored by the account management teams.

6.1.3 Deployment of Thor through Active Directory Group Policy Management

Microsoft Active Directory Group Policy Management is an integrated part of Microsoft Active Directory, which helps you do configurations across all the parts or your organizations computers.

To configure an automatic distribution of the Thor agent through Group Policy Management you will need:

- The Thor MSI installation package. You can grab the installer (direct link) here:

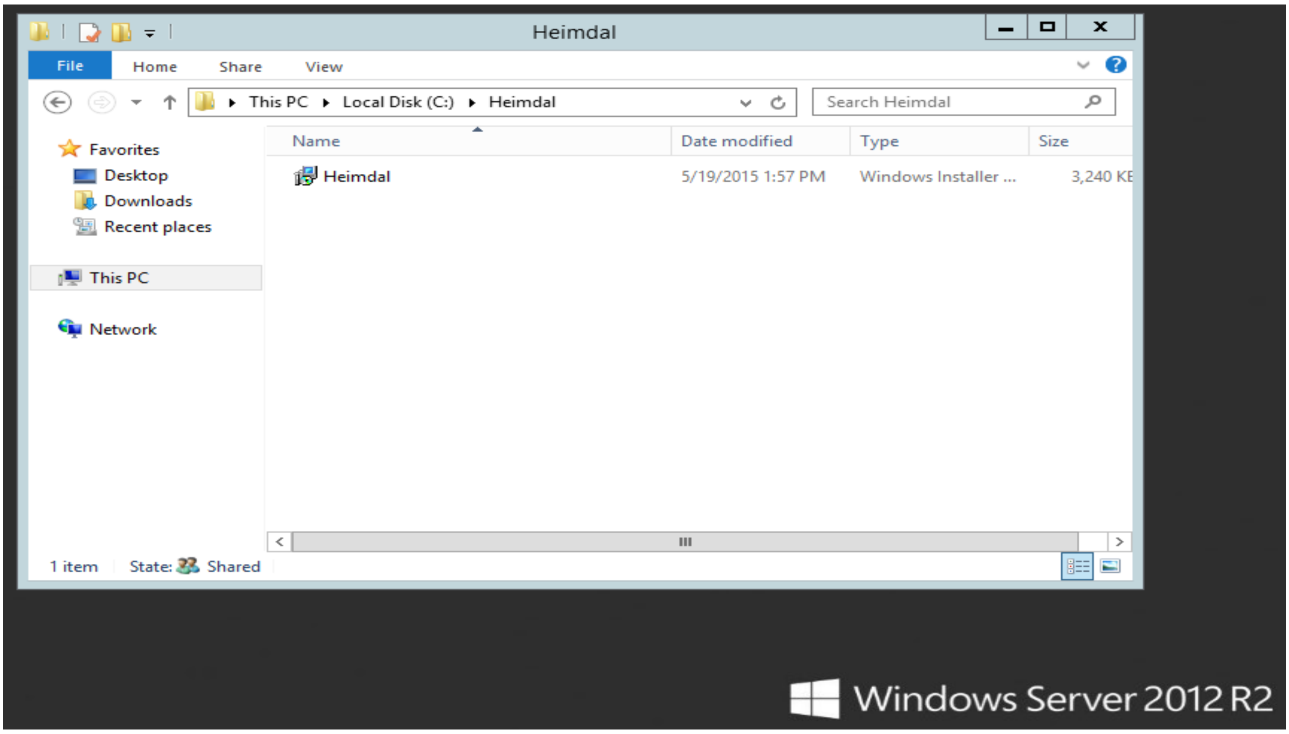
https://heimdalprodstorage.blob.core.windows.net/setup/Heimdal_Thor_Launcher.msi

- A customized MSI file with your organization’s activation key included.
- Access and rights to change the Active Directory group policy for the domain.
- A network path, where the Thor MSI installation file can be placed. All computers, which are going to have the agent installed, must have at least read access to this network path.
- Microsoft .NET Framework 4.6.1 or later - full profile - must be installed on all computers.

The full process works like this:

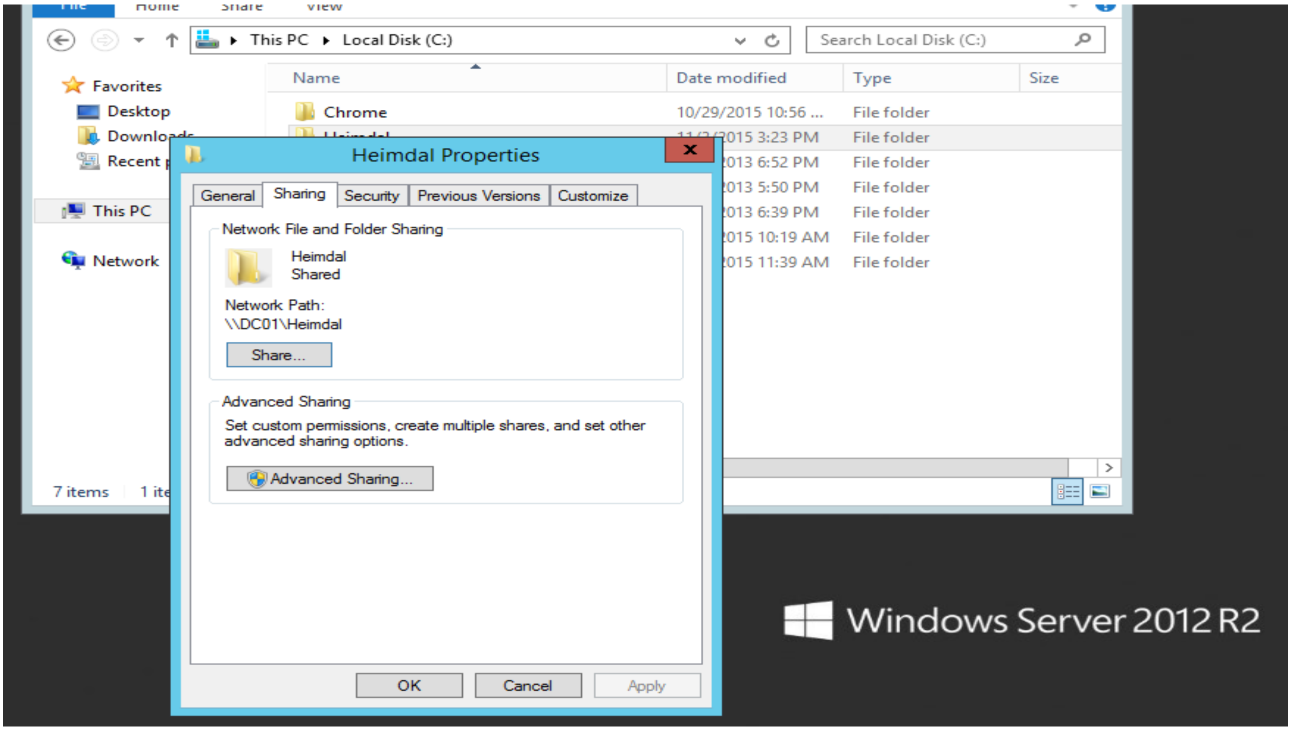
Step 1:

Create the folder where you want to share **Heimdal_Thor_Launcher.msi** from:



Name	Date modified	Type	Size
Heimdal	5/19/2015 1:57 PM	Windows Installer ...	3,240 KE

Make sure the folder is accessible and that the computers have at least read access to the newly created folder



Network File and Folder Sharing

Heimdal
Shared

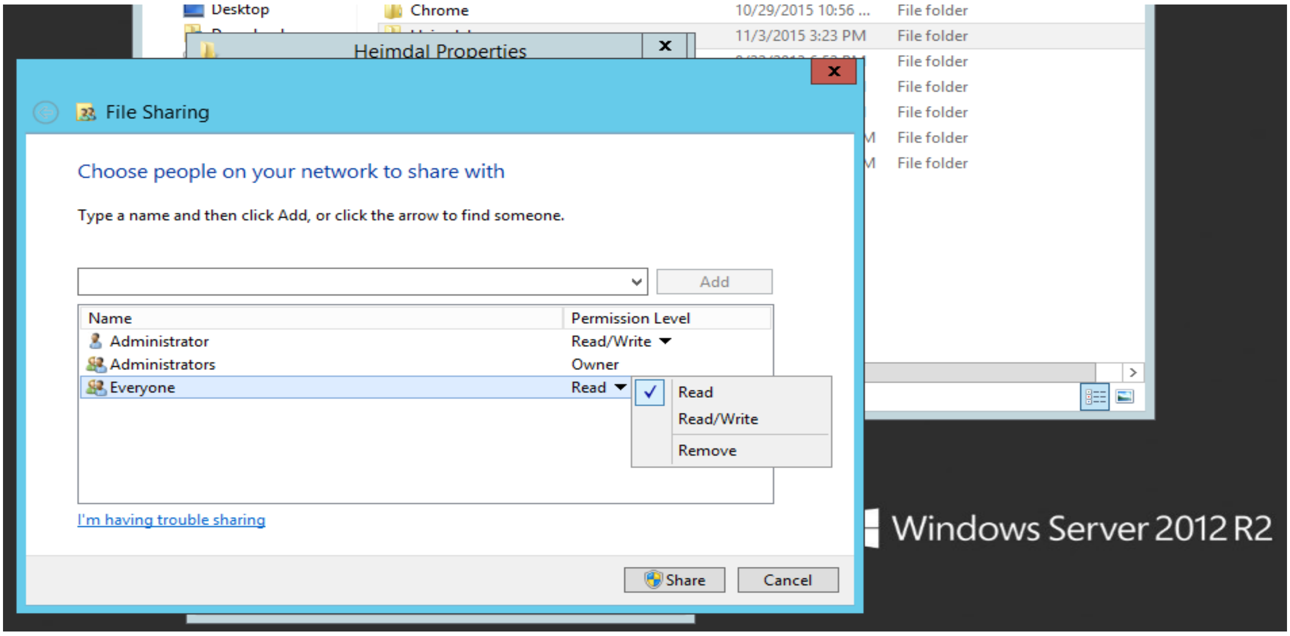
Network Path:
\\DC01\Heimdal

Advanced Sharing

Set custom permissions, create multiple shares, and set other advanced sharing options.

Step 2:

Choose the people in you network you want to share this folder with and establish their permission level.



File Sharing

Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

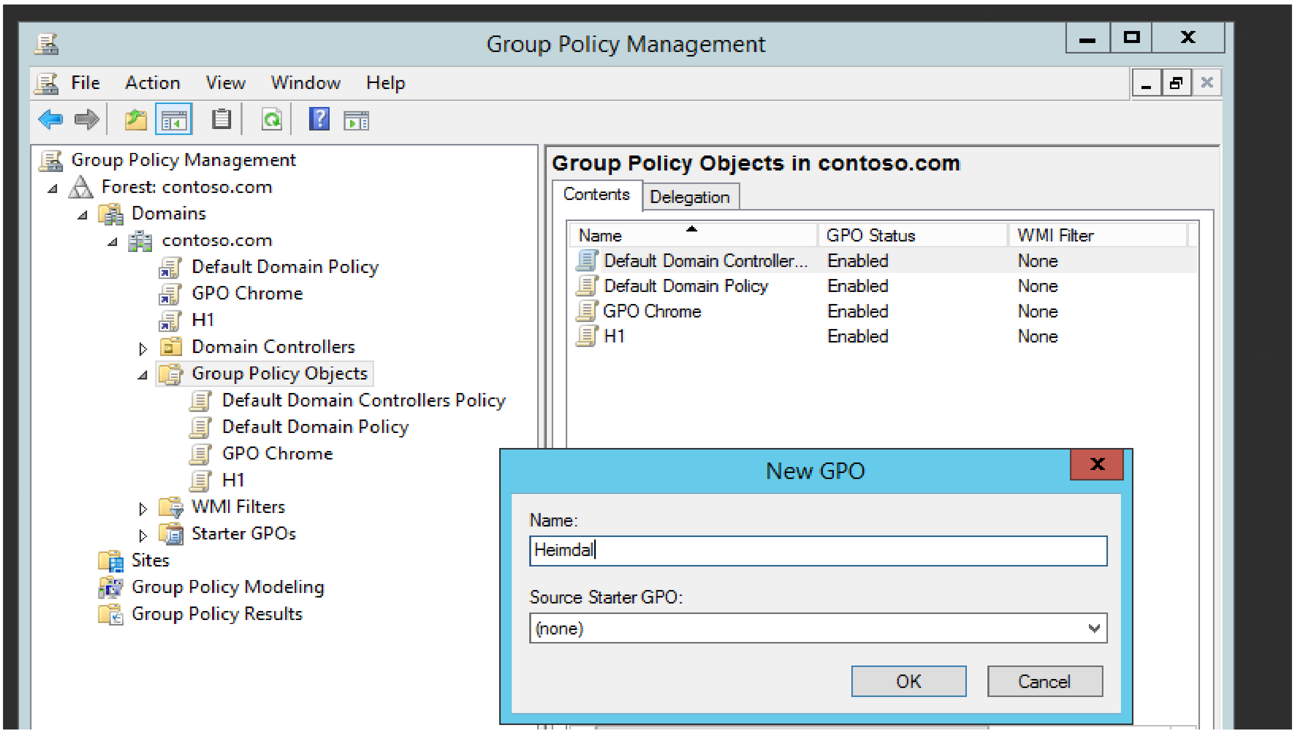
Name	Permission Level
Administrator	Read/Write
Administrators	Owner
Everyone	Read

Step 3:

On the Domain Controller, click on Administrative Tools and then open Group Policy Management.

Under the domain for which you want to create a GPO:

- select Group Policy Objects
- right click
- choose New GPO
- and then select the name (“Thor” in our case).



Name	GPO Status	WMI Filter
Default Domain Controller...	Enabled	None
Default Domain Policy	Enabled	None
GPO Chrome	Enabled	None
H1	Enabled	None

New GPO

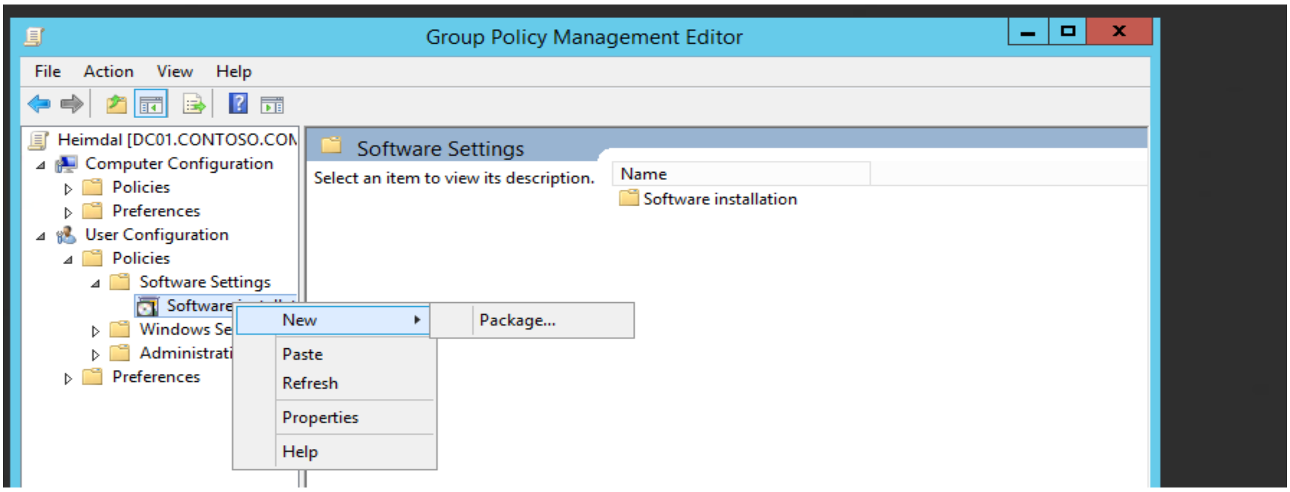
Name: Heimdal

Source Starter GPO: (none)

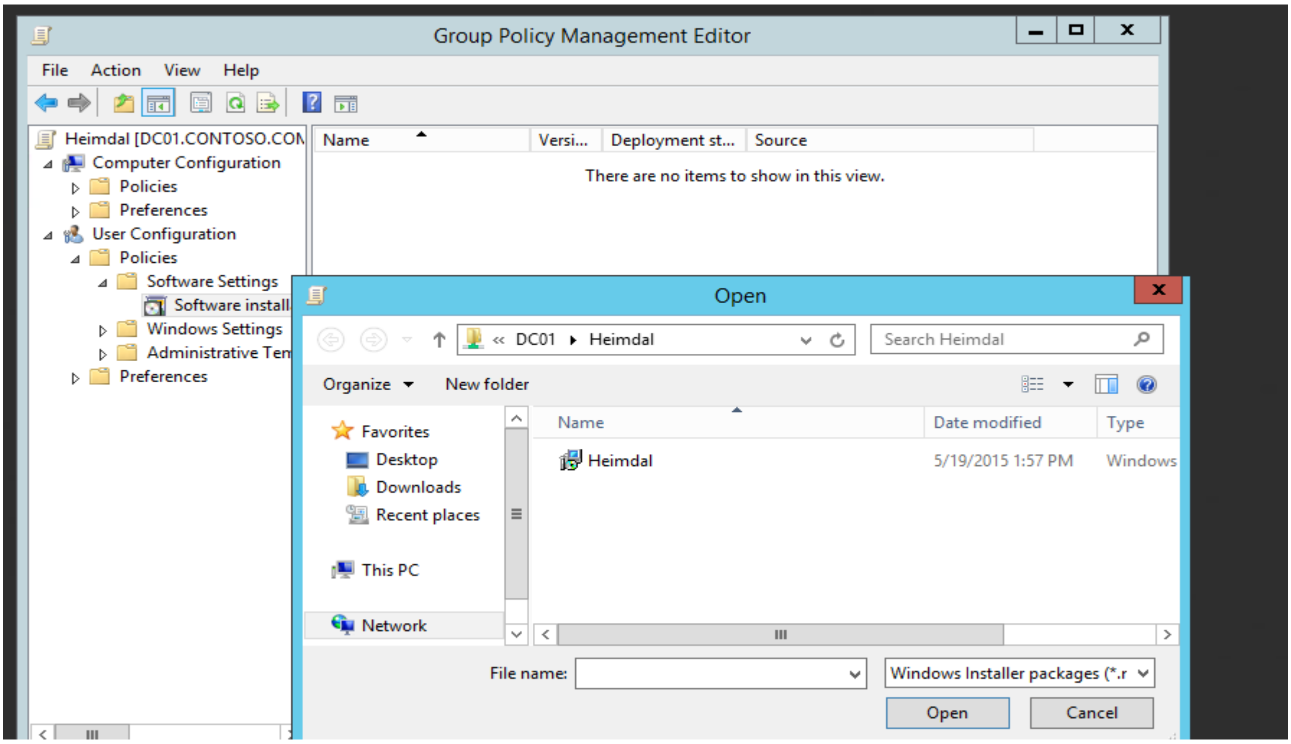
Step 4:

Open the Group Policy Management Editor and select the following:

- User Configuration
- Policies
- Software Settings
- Software Installation
- Package
- right click
- New
- Package.



Make sure to browse to the target msi installer.



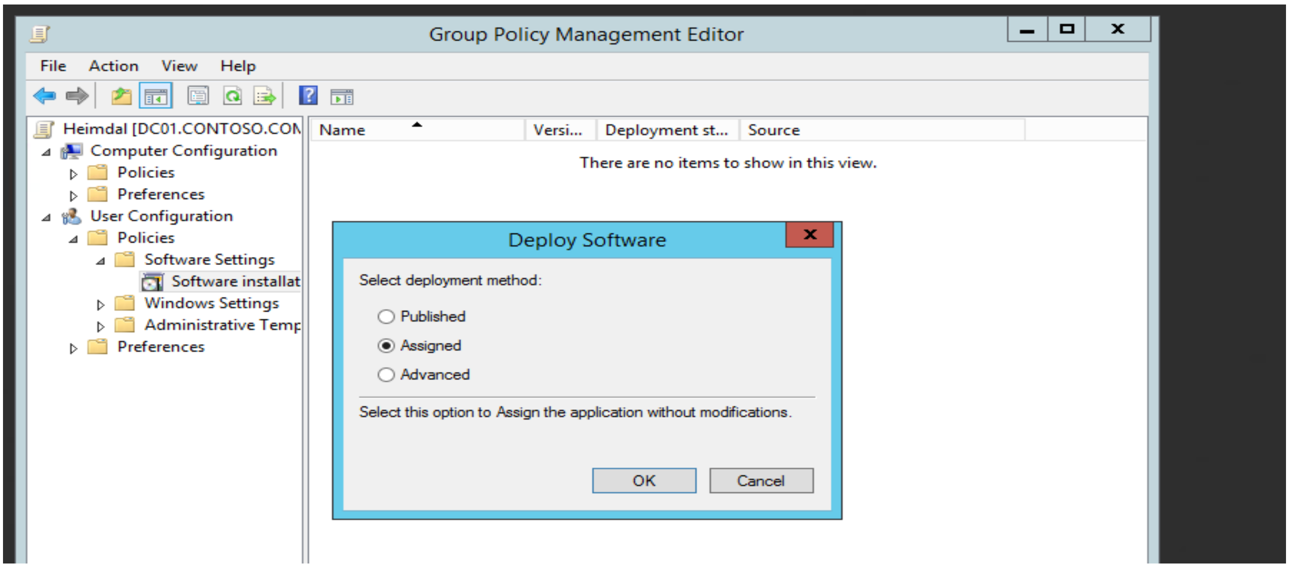
There are no items to show in this view.

Heimdal 5/19/2015 1:57 PM Windows

Windows Installer packages (*.r

Step 5:

For “Deploy Software”, chose the “Assigned” option. This means the installation will run without user interaction:



There are no items to show in this view.

Select deployment method:

○ Published

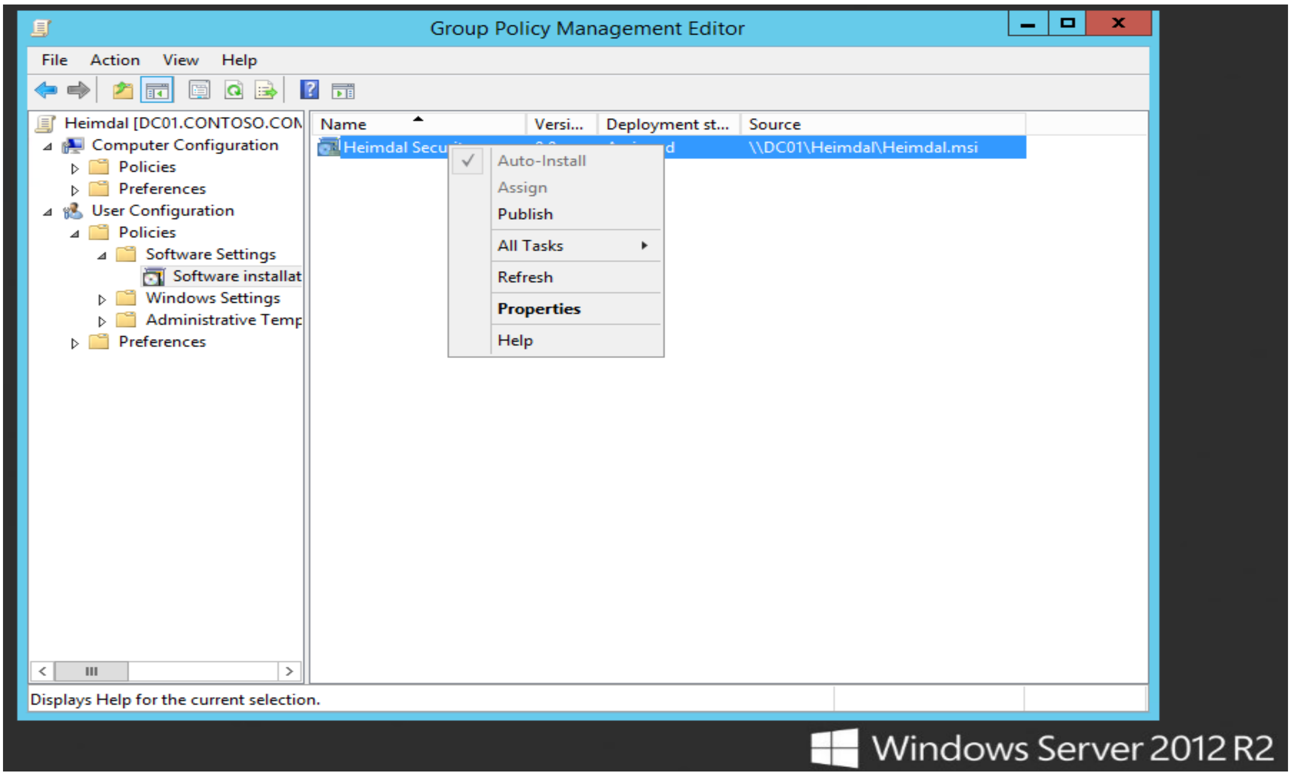
● Assigned

○ Advanced

Select this option to Assign the application without modifications.

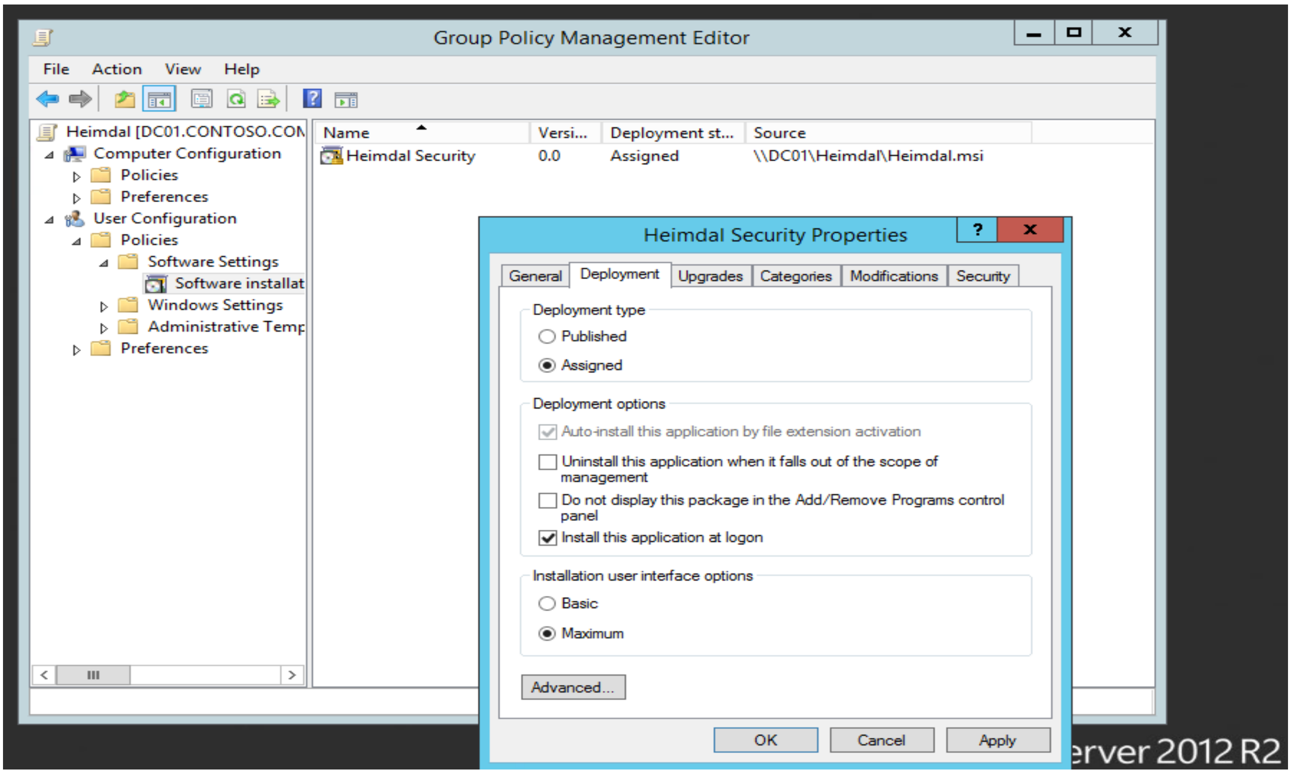
Step 6:

Select package “Heimdal”, right click, select Properties.



Step 7:

Next, go to “Deployment” tab, where you can see deployment types and options. To install Thor Enterprise please choose the “Install this application at logon” option and then hit “Apply”.



Name	Versi...	Deployment st...	Source
Heimdal Security	0.0	Assigned	\\DC01\Heimdal\Heimdal.msi

Heimdal Security Properties

General | Deployment | Upgrades | Categories | Modifications | Security

Deployment type

○ Published

● Assigned

Deployment options

☑ Auto-install this application by file extension activation

□ Uninstall this application when it falls out of the scope of management

□ Do not display this package in the Add/Remove Programs control panel

☑ Install this application at logon

Installation user interface options

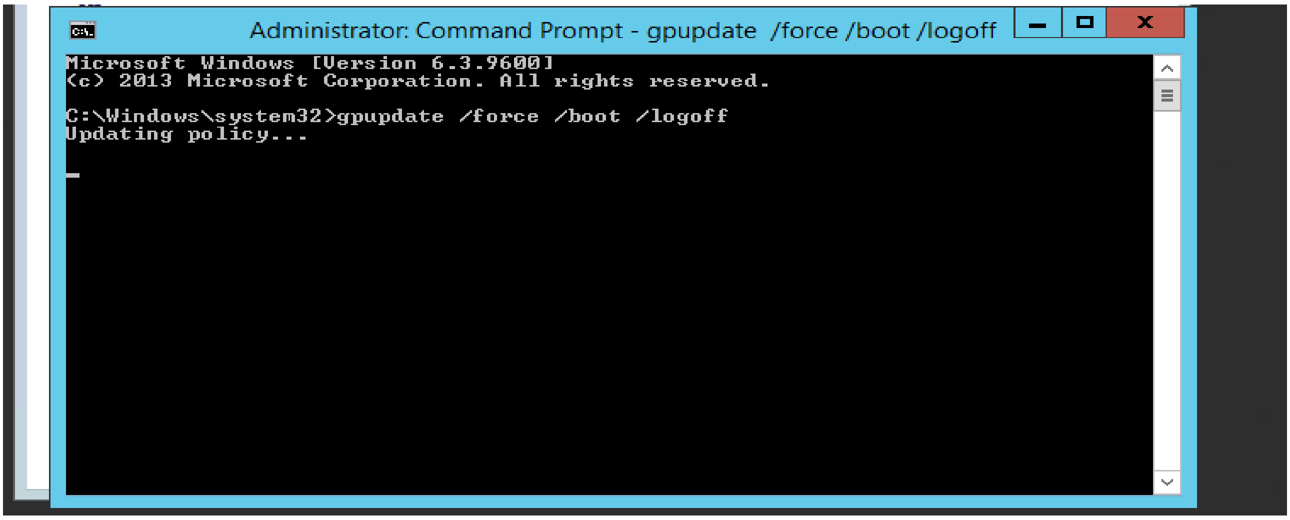
○ Basic

● Maximum

Step 8:

To install Thor Enterprise from the user’s computer, do the following:

- Open Command Prompt as Administrator and type:
- gpupdate /force /boot /logoff

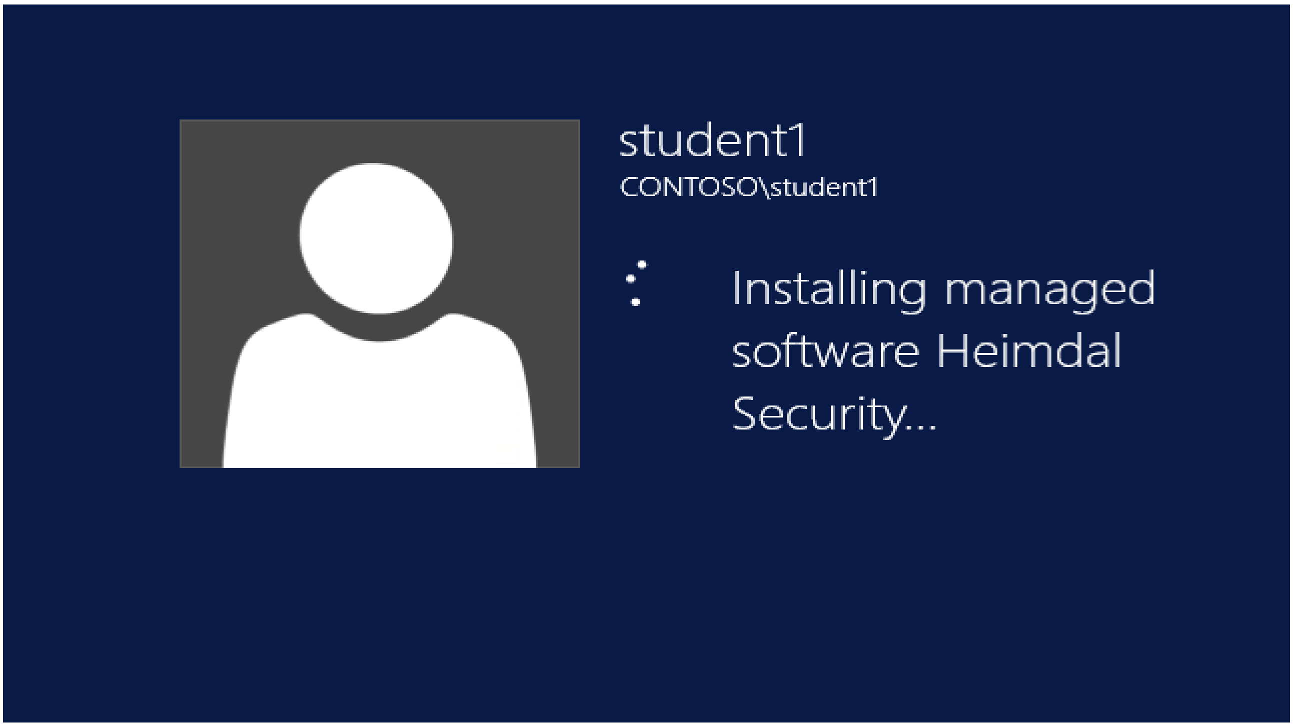

Administrator: Command Prompt - gpupdate /force /boot /logoff

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

_
```

The user’s computer will restart and install the software, as shown below:

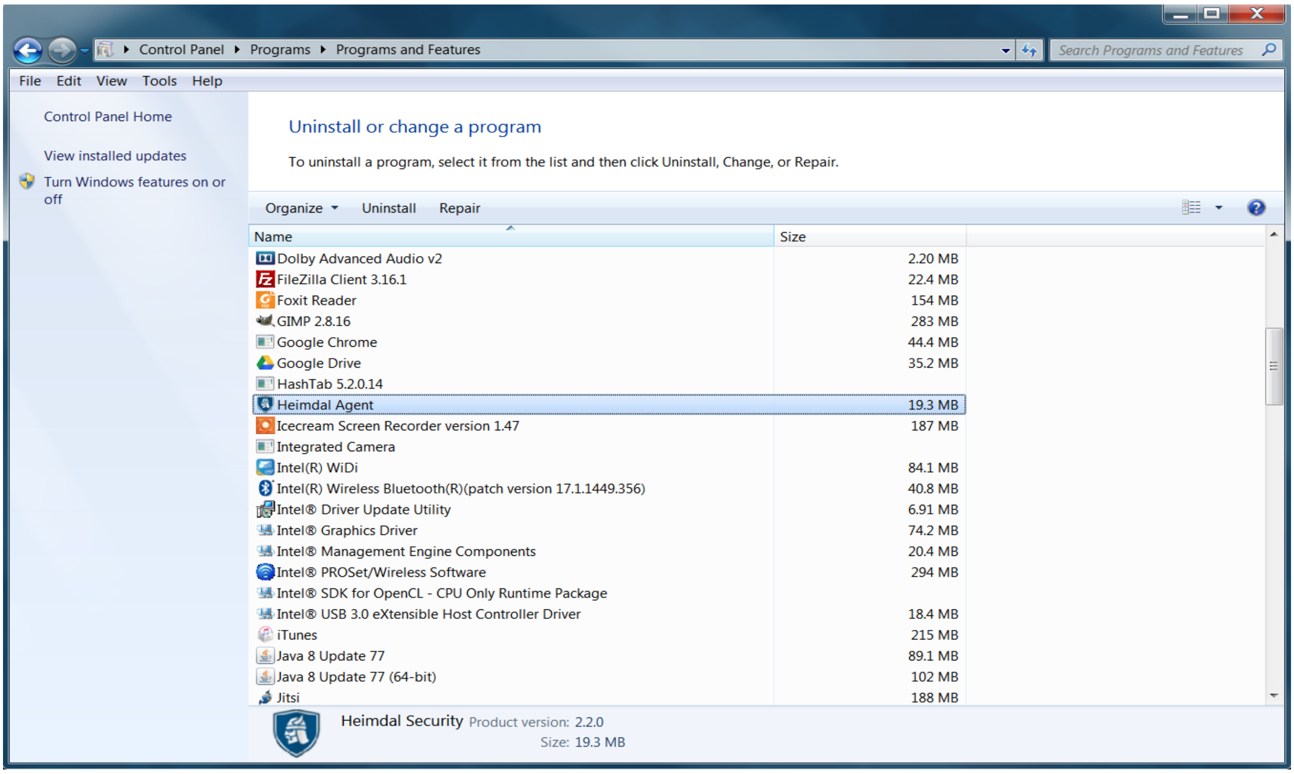


student1

CONTOSO\student1

Installing managed software Heimdal Security...

This is a silent installation. You can check the results in the Control Panel/Programs to verify if Thor was installed successfully.



Control Panel ▸ Programs ▸ Programs and Features
Search Programs and Features
File Edit View Tools Help
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾
Uninstall
Repair

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

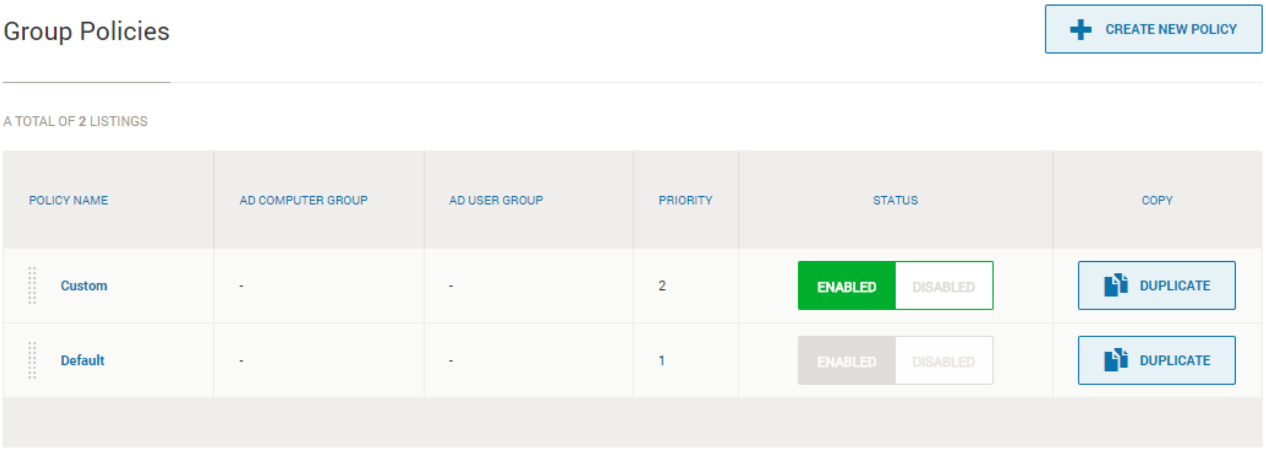
Name	Size
Dolby Advanced Audio v2	2.20 MB
FileZilla Client 3.16.1	22.4 MB
Foxit Reader	154 MB
GIMP 2.8.16	283 MB
Google Chrome	44.4 MB
Google Drive	35.2 MB
HashTab 5.2.0.14	
Heimdal Agent	19.3 MB
Icecream Screen Recorder version 1.47	187 MB
Integrated Camera	
Intel(R) WiDi	84.1 MB
Intel(R) Wireless Bluetooth(R)(patch version 17.1.1449.356)	40.8 MB
Intel® Driver Update Utility	6.91 MB
Intel® Graphics Driver	74.2 MB
Intel® Management Engine Components	20.4 MB
Intel® PROSet/Wireless Software	294 MB
Intel® SDK for OpenCL - CPU Only Runtime Package	
Intel® USB 3.0 eXtensible Host Controller Driver	18.4 MB
iTunes	215 MB
Java 8 Update 77	89.1 MB
Java 8 Update 77 (64-bit)	102 MB
Jitsi	188 MB

Heimdal Security Product version: 2.2.0
Size: 19.3 MB

6.2 AD group binding for Thor

6.2.1 Thor's Group policies without AD groups

By default, all accounts that are created under the dashboard receive a pre-existing policy called "Custom" and a "Default" one. The "Custom" policy ensures that all machines licensed under the corresponding account have basic protection features turned on. The individual features can of course be edited and tweaked later by the admin.



Group Policies

A TOTAL OF 2 LISTINGS

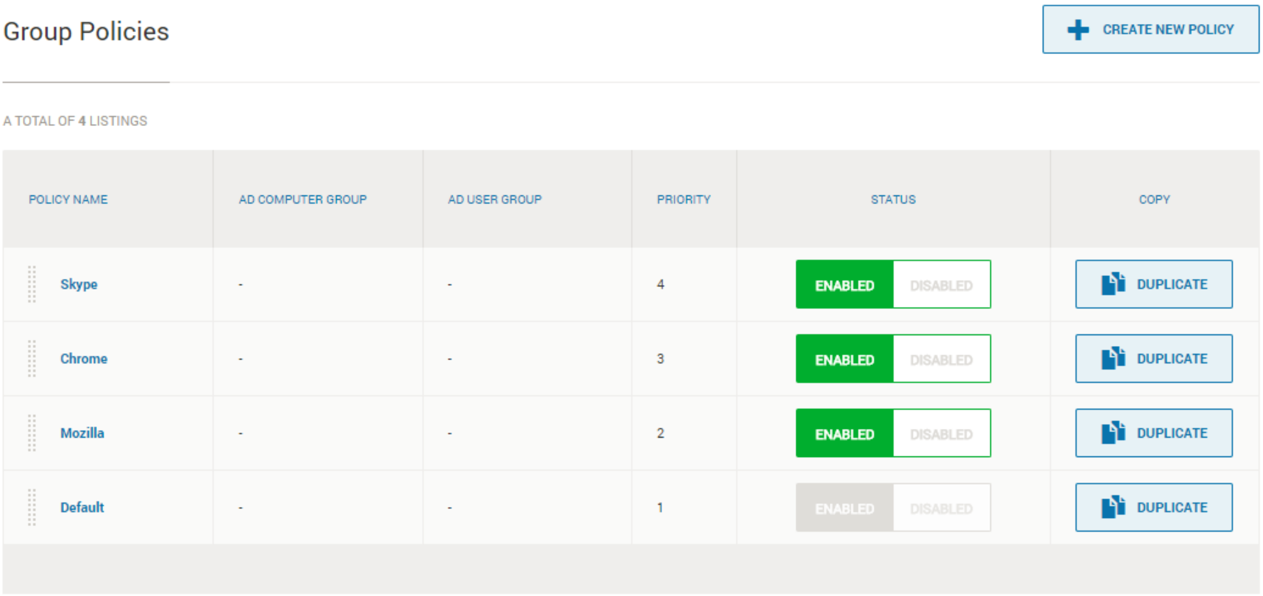
POLICY NAME	AD COMPUTER GROUP	AD USER GROUP	PRIORITY	STATUS	COPY
Custom	-	-	2	ENABLED DISABLED	DUPLICATE
Default	-	-	1	ENABLED DISABLED	DUPLICATE

Please note that the "Default" policy is non-interaction-able and is a policy that is meant to ensure proper communication between the web interface and the local agents.

IMPORTANT

THE DEFAULT POLICY SHOULD ALWAYS HAVE THE LOWEST PRIORITY (PRIORITY 1). PLEASE DO NOT DRAG AND DROP THIS POLICY AROUND THUS MODIFYING ITS INTENDED SYSTEM PRIORITY

Only one policy per Thor agent is allowed and only one shall apply. If there are more which are suitable for application (AD restrictions are not in place for instance), Thor will apply only the one with the highest value of priority (in our case "Skype" policy has the highest value - 4). Therefore, the local Thor agent will only apply the policy called Skype



Group Policies

A TOTAL OF 4 LISTINGS

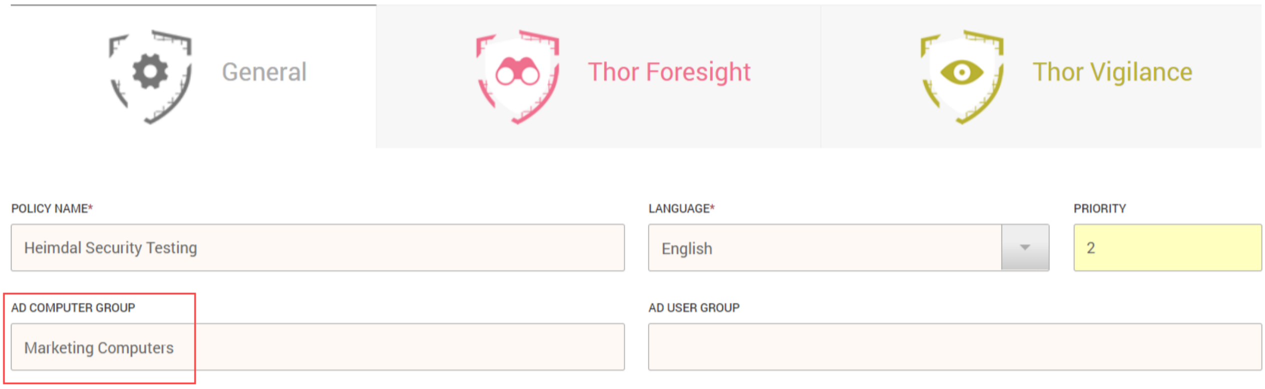
POLICY NAME	AD COMPUTER GROUP	AD USER GROUP	PRIORITY	STATUS	COPY
Skype	-	-	4	ENABLED DISABLED	DUPLICATE
Chrome	-	-	3	ENABLED DISABLED	DUPLICATE
Mozilla	-	-	2	ENABLED DISABLED	DUPLICATE
Default	-	-	1	ENABLED DISABLED	DUPLICATE

6.2.2 Thor's Group policies with AD groups

This feature allows the binding of certain policies only for some users (groups) or for some computers (groups). In turn, this allows for applying different Thor defined policies to different AD groups (either users or computers). It is useful for instance when applying differentiated patches (versioning) across distributed environments.

6.2.2.1 Applying differentiated Thor policies across distinct AD computer groups

If the administrator needs to distribute a policy only to a certain AD computer group, firstly the new policy needs to be created. Afterwards, the "AD Computer Group" field needs to be filled with the name of the corresponding AD computer group. ("Marketing Computers", as shown below).



POLICY NAME*: Heimdal Security Testing

LANGUAGE*: English

PRIORITY: 2

AD COMPUTER GROUP: Marketing Computers

AD USER GROUP:

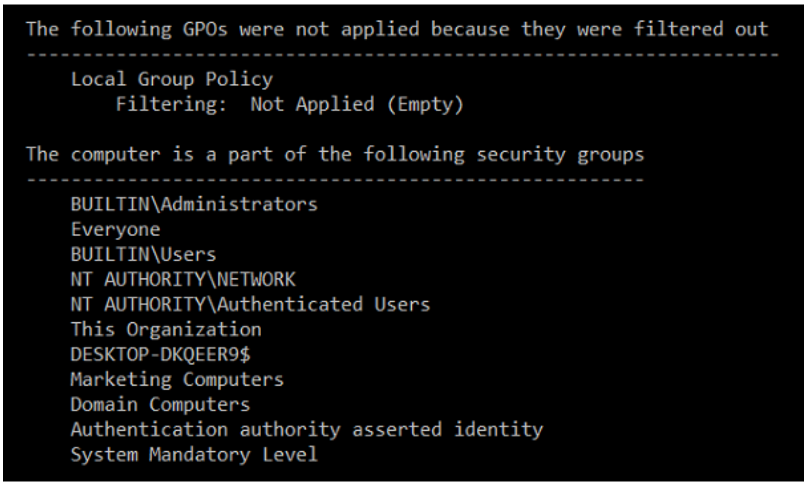
After you create the policy, you only need to enable it to take effect.

IMPORTANT

The local agent does not do LDAP so basically Thor does not interrogate the AD directly. Thor does not communicate with the domain controller or with the AD server for the purpose of data gathering.

The local Thor agent does a gpresult /r locally so basically it interrogates the host about AD computer group membership and AD user group membership.

It then tries to match whatever it detects in the Thor dashboard policy to the results that stem from the gpresult command. If a match is found, then the corresponding Thor policy applies to the matched AD group.



```
The following GPOs were not applied because they were filtered out
---------------------------------------------------------------------
    Local Group Policy
        Filtering:  Not Applied (Empty)

The computer is a part of the following security groups
-------------------------------------------------------
    BUILTIN\Administrators
    Everyone
    BUILTIN\Users
    NT AUTHORITY\NETWORK
    NT AUTHORITY\Authenticated Users
    This Organization
    DESKTOP-DKQEER9$
    Marketing Computers
    Domain Computers
    Authentication authority asserted identity
    System Mandatory Level
```

The adjacent example shows the gpresult /r command in action which finds that the local host on which the Thor agent is installed is part of the "Marketing Computers" AD group.

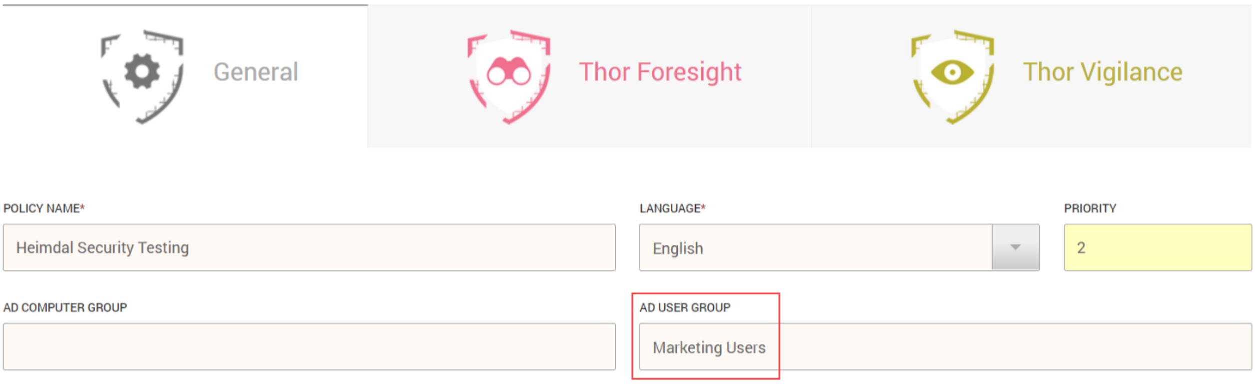
The correct procedure is then to assign inside the Thor Dashboard the same AD group name.

IMPORTANT

- Right now, the only AD group types that are supported are GLOBAL SECURITY GROUPS (COMPUTER OR USER)
- Nested groups as well as AD OU names are not supported for use within the Thor dashboard.
- The group names are case sensitive inside the Thor dashboard so for a successful bind, the names have to be an exact match.
- It is possible to have both fields AD Computer Group and AD User Group filled in for the SAME policy. However, this will make the policy extremely restrictive. It will only apply when both the computer and user membership requirements are met.

6.2.2.2 How can I distribute a policy to an AD User group?

If the administrator needs to distribute a policy only to a certain AD user group, firstly the new policy needs to be created. Afterwards, the "AD User Group" field gets filled with the name of the corresponding AD user group. ("Marketing Users", as shown below):



POLICY NAME*	LANGUAGE*	PRIORITY
Heimdal Security Testing	English	2
AD COMPUTER GROUP	AD USER GROUP	
	Marketing Users	

IMPORTANT

The local agent does not do LDAP so basically Thor does not interrogate the AD directly. Thor does not communicate with the domain controller or with the AD server for the purpose of data gathering.

The local Thor agent does a gpresult /r locally so basically it interrogates the host about AD computer group membership and AD user group membership.

It then tries to match whatever it detects in the Thor dashboard policy to the results that stem from the gpresult command. If a match is found, then the corresponding Thor policy applies to the matched AD group.

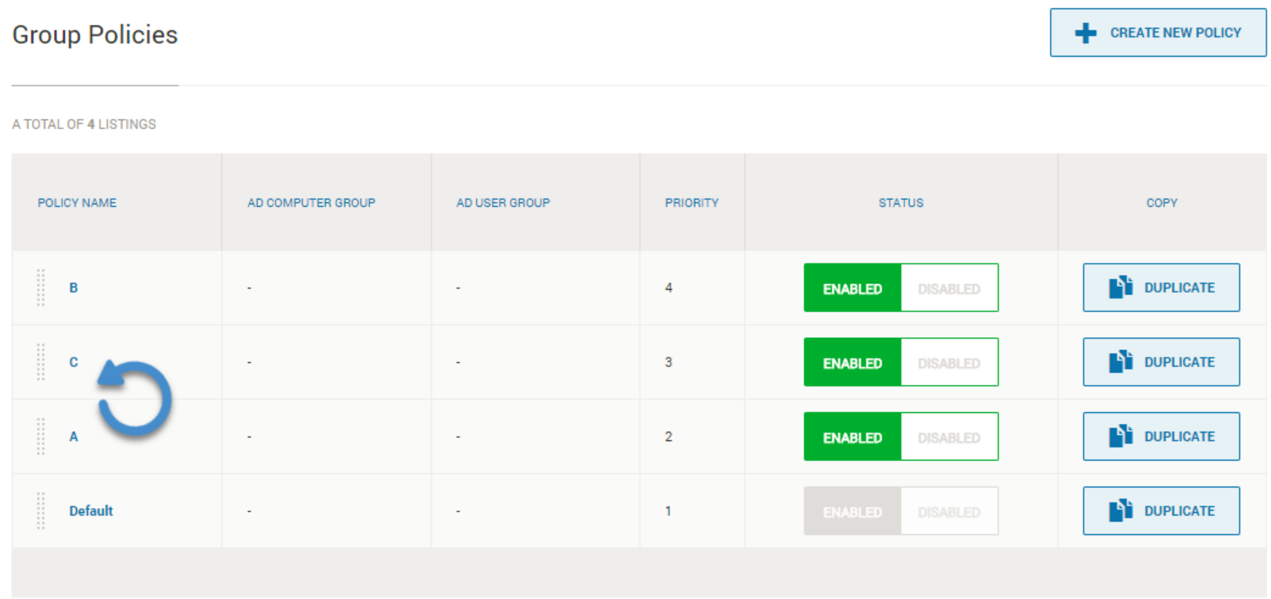
IMPORTANT

- Right now, the only AD group types that are supported are GLOBAL SECURITY GROUPS (COMPUTER OR USER)
- Nested groups as well as AD OU names are not supported for use within the Thor dashboard.
- The group names are case sensitive inside the Thor dashboard so for a successful bind, the names must be an exact match.
- It is possible to have both fields AD Computer Group and AD User Group filled in for the SAME policy. However, this will make the policy extremely restrictive. It will only apply when both the computer and user membership requirements are met.

6.2.2.3 Changing group policy priority

The value/number of priority of a group policy is assigned automatically in an increasing way. The higher the number, the higher the priority.

Changing the policy priority is done via drag and drop from the policy name box. Simply click and do “drag and drop” vertically to change the policy apply order.



Group Policies

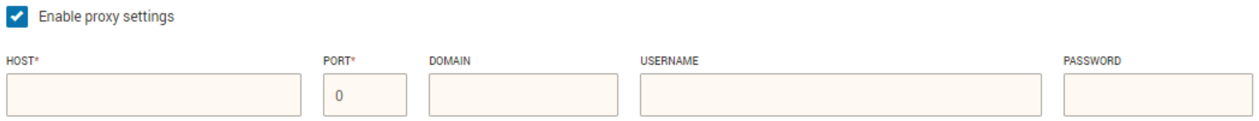
A TOTAL OF 4 LISTINGS

POLICY NAME	AD COMPUTER GROUP	AD USER GROUP	PRIORITY	STATUS	COPY
B	-	-	4	ENABLED DISABLED	DUPLICATE
C	-	-	3	ENABLED DISABLED	DUPLICATE
A	-	-	2	ENABLED DISABLED	DUPLICATE
Default	-	-	1	ENABLED DISABLED	DUPLICATE

6.3 Using Thor while behind an authentication proxy

Thor can be used in combination with IT Security proxies or authentication proxies. The steps below must be followed to use Thor if behind a proxy:

- Login at https://dashboard.heimdalsecurity.com and click Group Policies.
- If you do not already have policies defined, then click ‘Create New Policy’.
- If more than one policy is being used, then the proxy information must be entered into all of them.
- Go to the General Settings Tab and find the option “Enable proxy settings”



☑ Enable proxy settings

HOST*	PORT*	DOMAIN	USERNAME	PASSWORD
	0			

- Once you introduced your Proxy settings in the dashboard, deploy Thor. You may use the command line and specific parameters. Please see the example below:

  ```
  msiexec /qn /i Heimdal.msi heimdalkey="xxxxx-xxxxx-xxxxxx-xxxxxx" proxy="Address=x.x.x.x Port=xy
  Username=XXXX Password=XXXX Domain="
  ```

6.4 Internet WebServers for use with Thor Foresight

Using Thor Foresight with internal webservers is fully supported as long as they use DNS based naming. For example, a request for http://thorforesight.local will be recognized as a valid, supported DNS request and will be able resolvable. On the contrary, a request for http://thorforesight is not supported. IP address-based requests are handled without a problem. Requests like this one are fully supported: http://192.168.0.1

IMPORTANT

This only affects web-based services, not file sharing services or drive share mapping such as \\thorforesight

6.5 Static/ Dynamic IP DNS Environments Settings for Thor

Thor Enterprise is fully compatible with both static and dynamic DNS environments. There should be no issues no matter the initial DNS configuration of your environment.

6.6 Virtualization environments

For virtual machines:

Thor can be successfully installed on machines that stem from the same cloned image.

For Citrix environments: These Citrix environment software versions are minimum requirements for Thor compatibility:

XenServer – Version 6.5
XenApp & XenDesktop – Version 7.6

6.7 Using Thor in VPN environments – VPN compatibility

By default, Thor should be compatible with all VPN clients. Depending on the VPN technology used, there have been observed 3 types of VPN behaviors:

- VPN clients that directly try to modify the NIC settings for DNS

- VPN clients that add an additional virtual network card that they use to route the traffic into the tunnel. They are also known as TAP adapters and they need TAP drivers to work properly.

- VPN clients that add additional network layers on top of IPv4 or IPv6, essentially adding another driver to the existing NIC that they use to route the traffic.

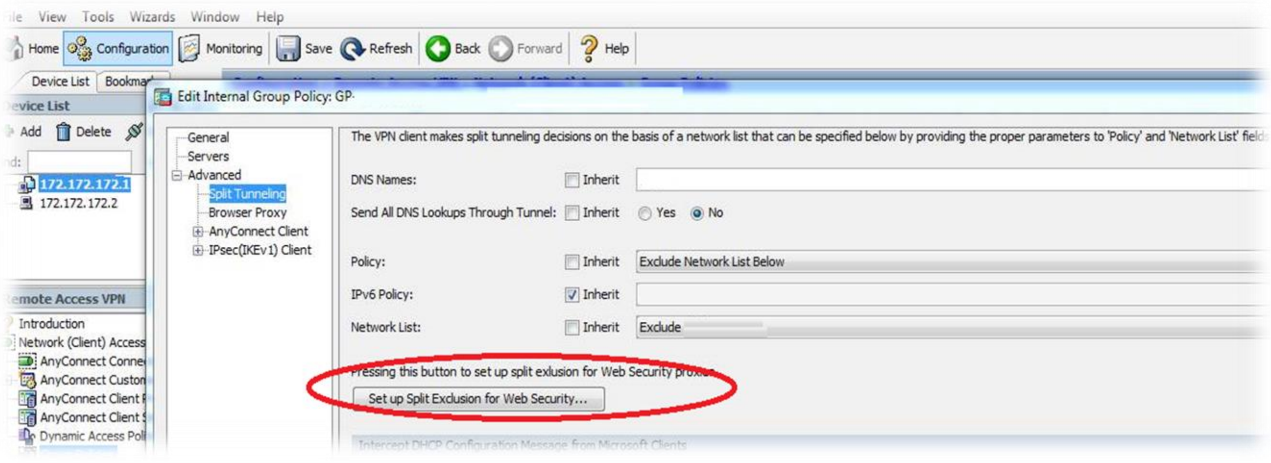
If connectivity issues are observed while having Thor Foresight installed, please have a look at the below case corners:

IMPORTANT: Thor is compatible with all VPN technologies. The connection should be established in a correct and stable way. HOWEVER, if you notice traffic filtering issues like pages not being filtered while connected to the VPN server, please contact the support team at corpsupport@heimdalsecurity.com.

6.7.1 Using Thor with Cisco AnyConnect VPN

Thor Enterprise can be used with Cisco AnyConnect VPN if 2 conditions are met:

1. Set split exclude: 104.46.51.121 (this is the IP address of our cloud services). For the model Cisco ASA 5585-X, you can change as in the next image:



The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network List' field

DNS Names: □ Inherit

Send All DNS Lookups Through Tunnel: □ Inherit ○ Yes ● No

Policy: □ Inherit Exclude Network List Below

IPv6 Policy: ☑ Inherit

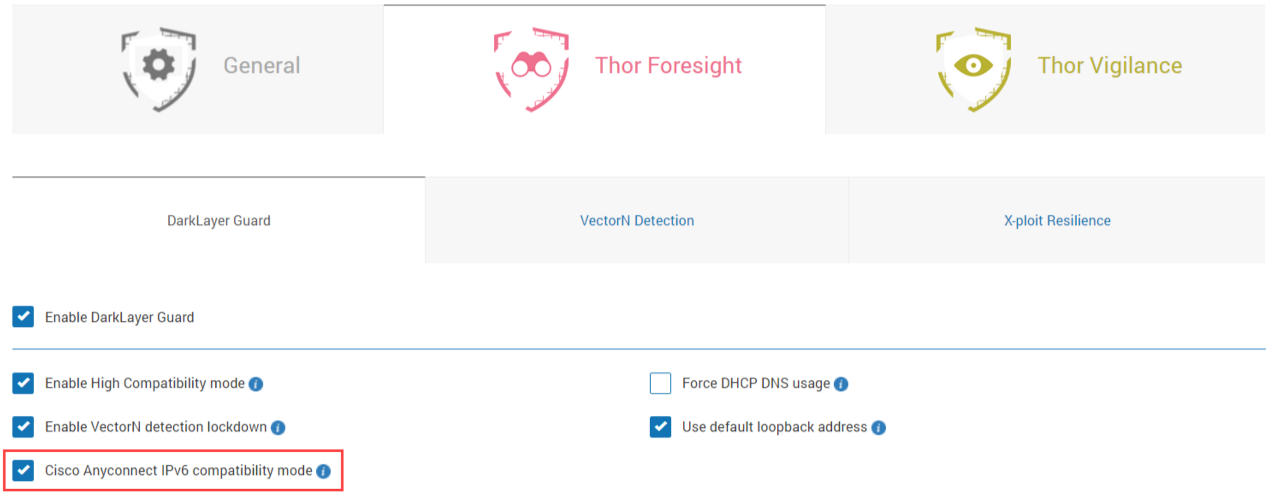
Network List: □ Inherit Exclude

Pressing this button to set up split exlusion for Web Security proxies.

Set up Split Exclusion for Web Security...

Intercept DHCP Configuration Message from Microsoft Clients

2. Go to https://dashboard.heimdalsecurity.com, click Group Policy, open your Group Policy, go to Thor Foresight, navigate to DarkLayer Guard and enable the option called **Cisco AnyConnect IPv6 compatibility mode.**



☑ Enable DarkLayer Guard

☑ Enable High Compatibility mode

☑ Enable VectorN detection lockdown

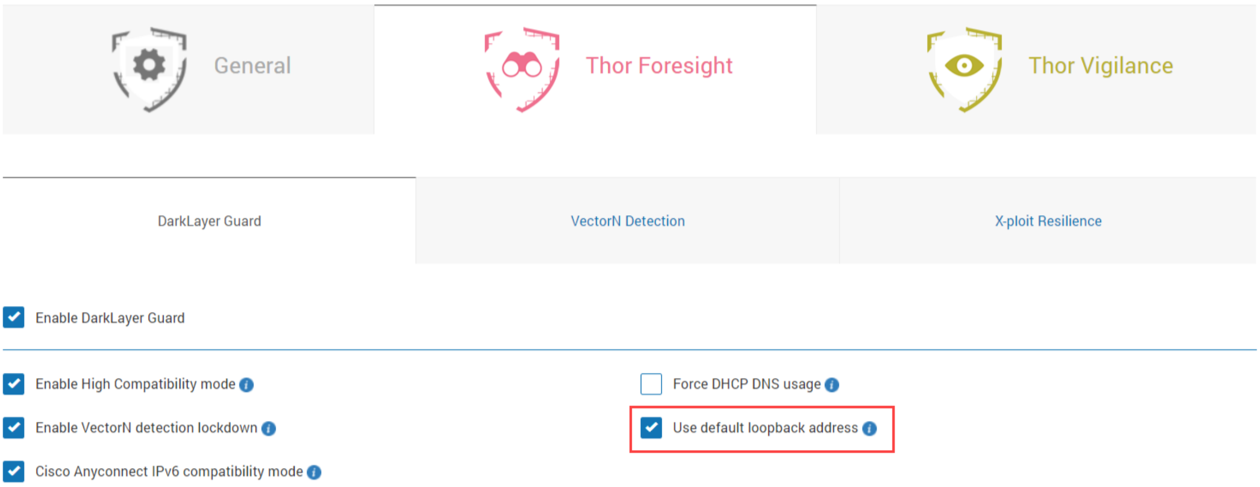
☑ Cisco Anyconnect IPv6 compatibility mode

□ Force DHCP DNS usage

☑ Use default loopback address

6.7.2 Using Thor with GlobalProtect from Palo Alto

From experience we have determined that the VPN client from the Palo Alto manufacturer works best if the admin enforces the DNS IP value 127.0.0.1 – client host IP – on the network card. This option will change the usual 127.7.7.X IP that is placed on the NIC DNS settings as a result.



☑ Enable DarkLayer Guard

☑ Enable High Compatibility mode

☑ Enable VectorN detection lockdown

☑ Cisco Anyconnect IPv6 compatibility mode

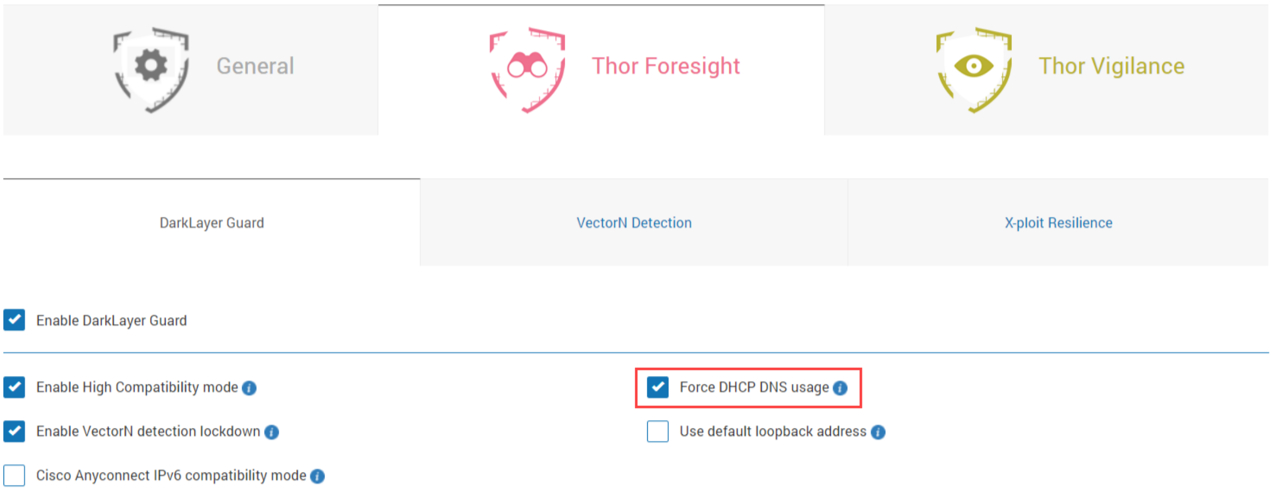
□ Force DHCP DNS usage

☑ Use default loopback address

6.7.3 Using Thor with VPN clients that modify the DNS settings in the NIC (ex. FortiGate from Fortinet)

Thor usage combined with a VPN client that when connected **adds a Static IP on the NIC** and in conjunction with a **DHCP connection,** requires one setting to be made: enable the option called **Force DHCP DNS usage.**

Please enable this option ONLY if the machines from your organization ARE NOT using STATIC IP.



☑ Enable DarkLayer Guard

☑ Enable High Compatibility mode

☑ Enable VectorN detection lockdown

□ Cisco Anyconnect IPv6 compatibility mode

☑ Force DHCP DNS usage

□ Use default loopback address

IMPORTANT!

Do not touch the VPN settings presented in the case corners above if the connection works by default. The settings above should be considered tweaks and not mandatory for the connection via VPN to be functional.

6.8 Usage on Terminal servers or Citrix servers

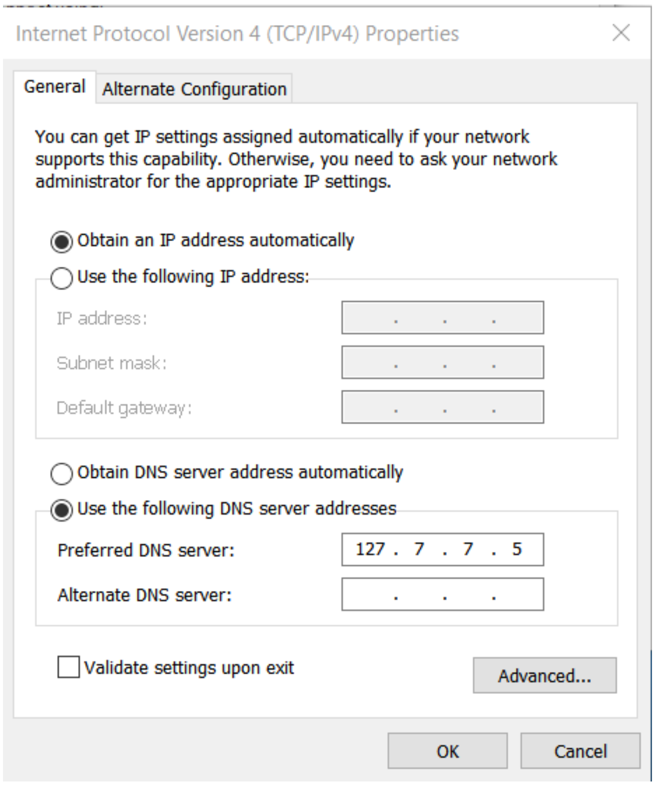
To run Thor Enterprise on Terminal Servers or Citrix servers, we suggest that you use the "Do not show GUI" option inside the general settings of relevant Group Policies.

On details about the showing or hiding the GUI please read chapter 5.1.1.2

6.9 Internet Protocol Version

Thor Foresight can filter network traffic both on IPv4 and IPv6. Please see below the DNS settings made by Thor Foresight when Traffic Filtering is activated.

- On IPv4, the DNS address set by Thor Foresight looks like 127.7.7.X where X is variable. In the example below the assigned DNS value is 127.7.7.5.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

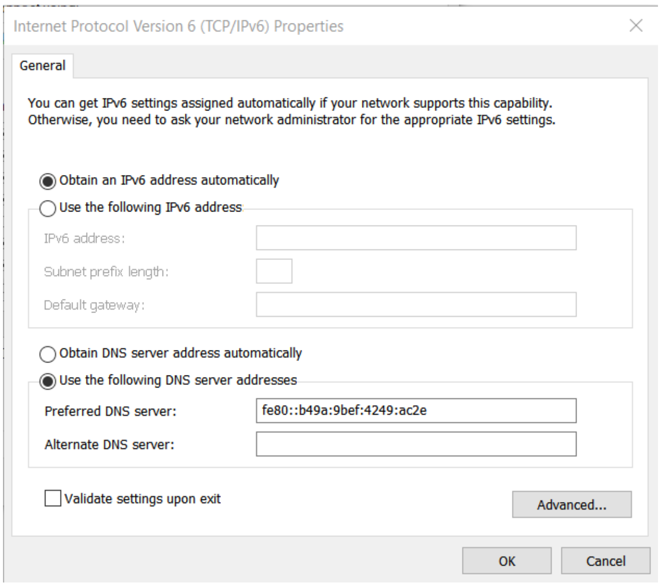
● Use the following DNS server addresses

Preferred DNS server: 127 . 7 . 7 . 5

Alternate DNS server: . . .

□ Validate settings upon exit

- On IPv6, the DNS address set by Thor is **fe80::b49a:9bef:4249:ac2e**



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically

○ Use the following IPv6 address

IPv6 address:

Subnet prefix length:

Default gateway:

○ Obtain DNS server address automatically

● Use the following DNS server addresses

Preferred DNS server: fe80::b49a:9bef:4249:ac2e

Alternate DNS server:

□ Validate settings upon exit

*if **DarkLayer Guard** is disabled from Thor Foresight - the 127.7.7.5 will be removed when the adapter becomes active
* **DarkLayer Guard** can cause issues if the client uses SAP because SSO requires the KDC (Kerberos Domain Controller) to be present as the Primary DNS

6.10 Uninstall Protection for Thor products

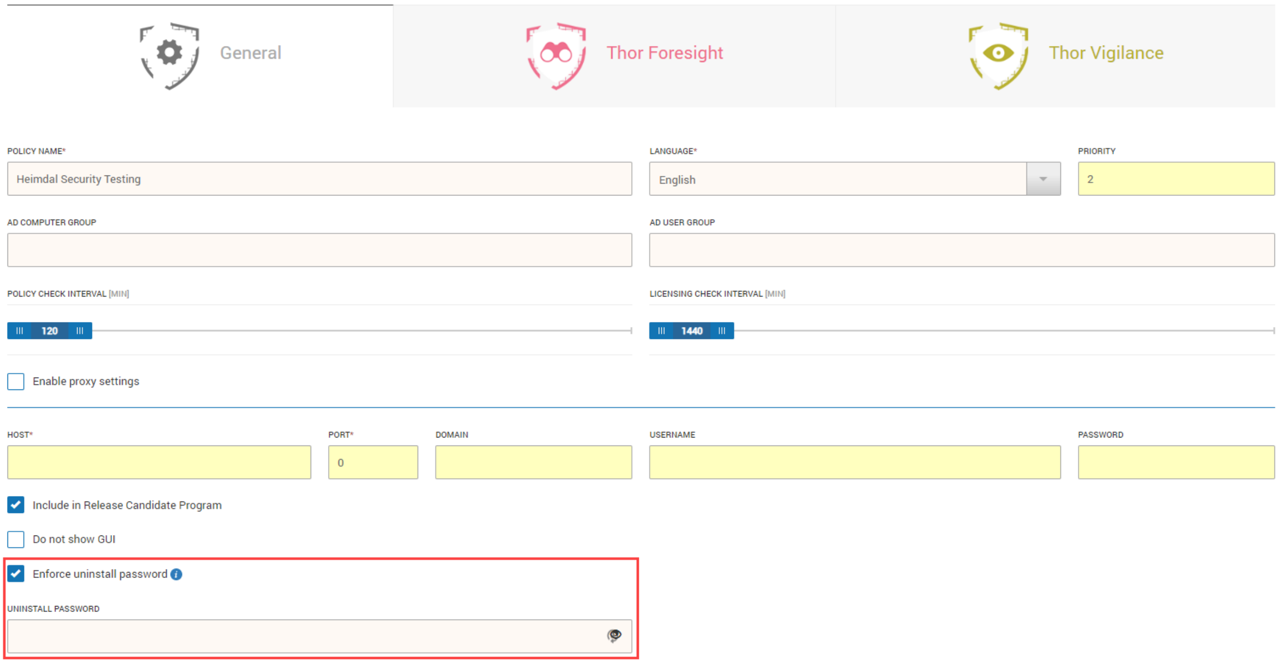
Thor Enterprise offers the administrator the option for setting an uninstall password to avoid 3rd party tools removing Thor and to make sure users will not uninstall Thor by mistake, even with administrative privileges in place.

The **Uninstall Password** feature offers you two options:

1. An **Uninstall Password** per Group Policy
2. A **Master Uninstall Password** that can be applied to all your machines

- **The Uninstall Password** can be found in each Group Policy and if the administrator wants to set an Uninstall Password for a certain Group Policy, these are the steps he needs to follow:

    a. Go to https://dashboard.heimdalsecurity.com
    b. From the Top Menu Select Group Policy
    c. Open the Group Policy that needs modifying
    d. In the General settings section, there will be an option called **Enforce uninstall password**
    e. Enable that option and type a password that will be requested by the agent on uninstall



POLICY NAME*: Heimdal Security Testing

LANGUAGE*: English

PRIORITY: 2

AD COMPUTER GROUP:

AD USER GROUP:

POLICY CHECK INTERVAL [MIN]: 120

LICENSING CHECK INTERVAL [MIN]: 1440

☐ Enable proxy settings

HOST*:

PORT*: 0

DOMAIN:

USERNAME:

PASSWORD:

☑ Include in Release Candidate Program

☐ Do not show GUI

☑ Enforce uninstall password

UNINSTALL PASSWORD:

NOTE: This password will be applied only to those machines that are part of the Group Policy you edited

f. After the password is set, scroll down and press the Update button

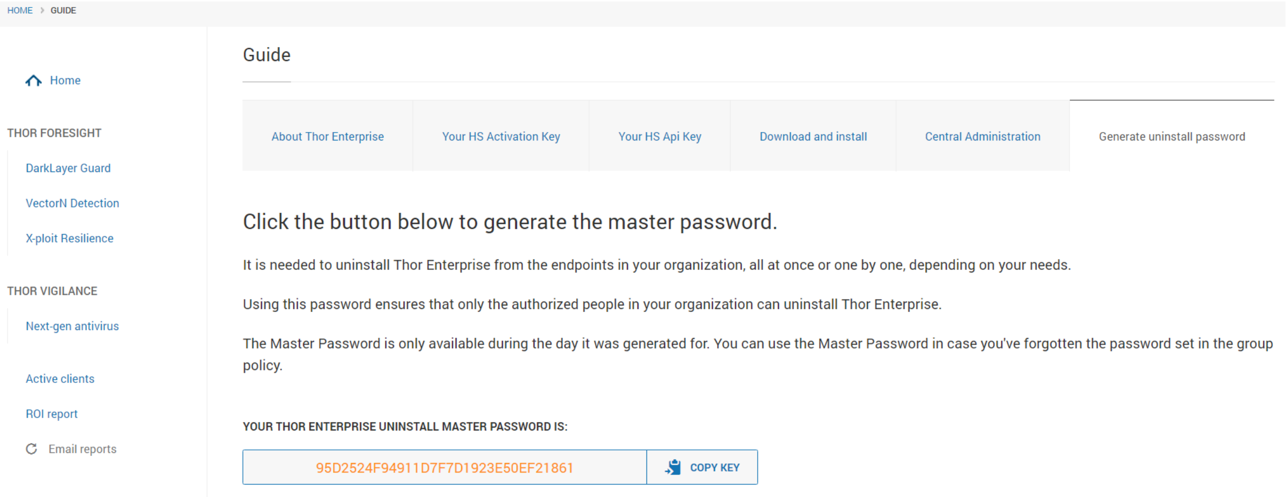
- **The Master Uninstall Password** – the administrator also has the option to generate a Master Password. This option will generate a Master Password automatically for the administrator and can be used on all relevant licensed machines, regardless of the password set per group policy. To generate this master uninstall password, these are the steps that need to be followed:

a. Go to https://dashboard.heimdalsecurity.com

b. From the Top Menu select Guide

c. Navigate to Generate uninstall password

d. Press Generate Password and a master password will be generated



Click the button below to generate the master password.

It is needed to uninstall Thor Enterprise from the endpoints in your organization, all at once or one by one, depending on your needs.

Using this password ensures that only the authorized people in your organization can uninstall Thor Enterprise.

The Master Password is only available during the day it was generated for. You can use the Master Password in case you've forgotten the password set in the group policy.

YOUR THOR ENTERPRISE UNINSTALL MASTER PASSWORD IS: 95D2524F94911D7F7D1923E50EF21861

IMPORTANT

If you want to uninstall Thor silently and you have an uninstall password set, you need to add the following parameter to the uninstall command: **uninstallpassword="passwordgoeshere".**

This applies for both **Uninstall Password** from Group Policy and **The Master Uninstall Password**

The master password takes precedence over the regular uninstall password set per group policy. The master password will be accepted and it will work towards the uninstall regardless of the initial password set in the group policy field.

7. Features

7.1 Features of Thor Foresight

7.1.1 X-Ploit Resilience

Thor Foresight monitors and automatically updates a range of software applications. The patches are downloaded directly from our servers and we only add special code switches to deploy the patches silently and at the correct time. Thor Foresight will never close a running application or automatically reboot the PC after the updates have been installed. Also, Thor Foresight will never request user/ admin permissions or show UAC pop-ups, even if the UAC is enabled.

Applications included and monitored in the Patch Management system are selected on the following criteria:

- One or more versions contain vulnerabilities, which are corrected in updated versions
- Vulnerabilities pose a security risk and are therefore actively used by IT criminals

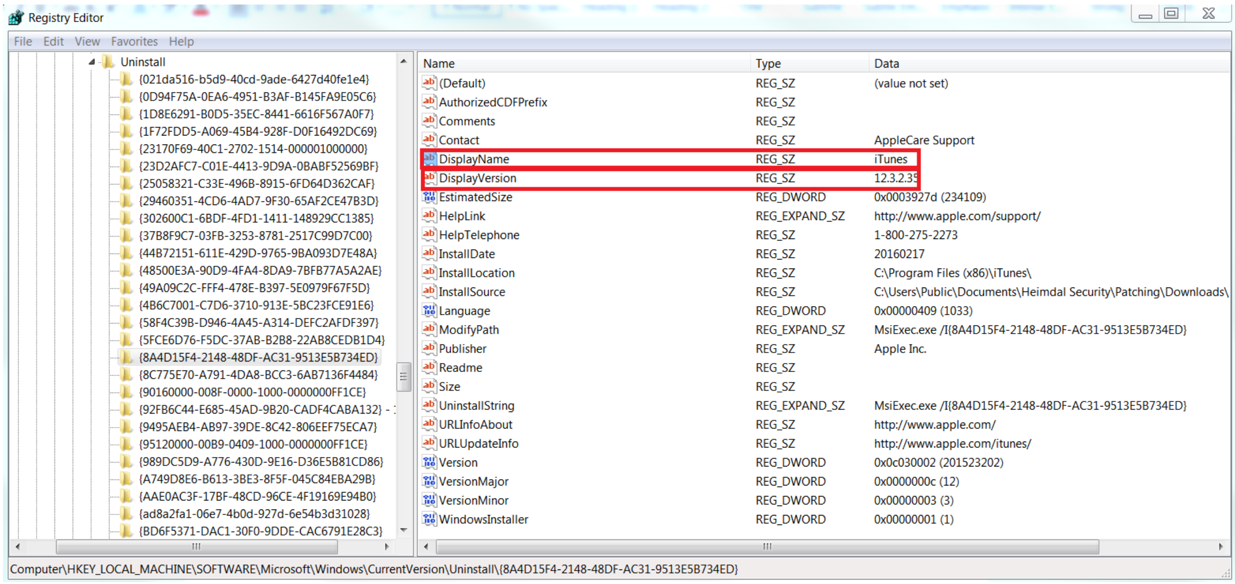
7.1.1.1 The list of supported software

Here you can find the full list of the applications that can be installed or patched by Thor Foresight:

Which Software Does Thor Patch?

7.1.1.2 Technical implementation

Thor receives its information from monitoring the Registry Editor application. Firstly, it looks for the DisplayName property of an app. If this property is not found, the Install button/option is displayed. Secondly, if the DisplayName is found, then it looks to the DisplayVersion properties and it decides if the installed version is older than the latest one. Depending on the comparison result, Thor then applies the patch.



```
Uninstall
  {021da516-b5d9-40cd-9ade-6427d40fe1e4}
  {0D94F75A-0EA6-4951-B3AF-B145FA9E05C6}
  {1D8E6291-B0D5-35EC-8441-6616F567A0F7}
  {1F72FDD5-A069-45B4-928F-D0F16492DC69}
  {23170F69-40C1-2702-1514-000001000000}
  {23D2AFC7-C01E-4413-9D9A-0BABF52569BF}
  {25058321-C33E-496B-8915-6FD64D362CAF}
  {29460351-4CD6-4AD7-9F30-65AF2CE47B3D}
  {302600C1-6BDF-4FD1-1411-148929CC1385}
  {37B8F9C7-03FB-3253-8781-2517C99D7C00}
  {44B72151-611E-429D-9765-9BA093D7E48A}
  {48500E3A-90D9-4FA4-8DA9-7BFB77A5A2AE}
  {49A09C2C-FFF4-478E-B397-5E0979F67F5D}
  {4B6C7001-C7D6-3710-913E-5BC23FCE91E6}
  {58F4C39B-D946-4A45-A314-DEFC2AFDF397}
  {5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4}
  {8A4D15F4-2148-48DF-AC31-9513E5B734ED}
  {8C775E70-A791-4DA8-BCC3-6AB7136F4484}
  {90160000-008F-0000-1000-0000000FF1CE}
  {92FB6C44-E685-45AD-9B20-CADF4CABA132} - :
  {9495AEB4-AB97-39DE-8C42-806EEF75ECA7}
  {95120000-00B9-0409-1000-0000000FF1CE}
  {989DC5D9-A776-430D-9E16-D36E5B81CD86}
  {A749D8E6-B613-3BE3-8F5F-045C84EBA29B}
  {AAE0AC3F-17BF-48CD-96CE-4F19169E94B0}
  {ad8a2fa1-06e7-4b0d-927d-6e54b3d31028}
  {BD6F5371-DAC1-30F0-9DDE-CAC6791E28C3}
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
AuthorizedCDFPrefix	REG_SZ	
Comments	REG_SZ	
Contact	REG_SZ	AppleCare Support
DisplayName	REG_SZ	iTunes
DisplayVersion	REG_SZ	12.3.2.35
EstimatedSize	REG_DWORD	0x0003927d (234109)
HelpLink	REG_EXPAND_SZ	http://www.apple.com/support/
HelpTelephone	REG_SZ	1-800-275-2273
InstallDate	REG_SZ	20160217
InstallLocation	REG_SZ	C:\Program Files (x86)\iTunes\
InstallSource	REG_SZ	C:\Users\Public\Documents\Heimdal Security\Patching\Downloads\
Language	REG_DWORD	0x00000409 (1033)
ModifyPath	REG_EXPAND_SZ	MsiExec.exe /I{8A4D15F4-2148-48DF-AC31-9513E5B734ED}
Publisher	REG_SZ	Apple Inc.
Readme	REG_SZ	
Size	REG_SZ	
UninstallString	REG_EXPAND_SZ	MsiExec.exe /I{8A4D15F4-2148-48DF-AC31-9513E5B734ED}
URLInfoAbout	REG_SZ	http://www.apple.com/
URLUpdateInfo	REG_SZ	http://www.apple.com/itunes/
Version	REG_DWORD	0x0c030002 (201523202)
VersionMajor	REG_DWORD	0x0000000c (12)
VersionMinor	REG_DWORD	0x00000003 (3)
WindowsInstaller	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{8A4D15F4-2148-48DF-AC31-9513E5B734ED}

Thor Foresight scans the PC every 2 hours by default to find new applications or apply patches to the existing ones. The list of detected software, their version and update status can be seen in the "Patching System" tab from the main user interface as well as in the online management portal.

If an update is available, then the patching process will begin as soon as possible, when the PC is idle and is not using the specific software. If several pieces of software require patching, then these will be managed one at a time. If the agent is unable to patch specific software like a browser plug-in because it may be in use, Thor Foresight will notify the user via a red exclamation mark inside the interface and the relevant information will be added in the dashboard.

7.1.1.3 Software that already has autoupdate enabled

Please note that some of the software apps that Thor Foresight monitors and updates automatically and silently may already have autoupdate enabled in their default settings. This means that updates delivered into the software directly by the software manufacturer (via the autoupdate feature built into the application) may be faster than patches applied by Thor Foresight.

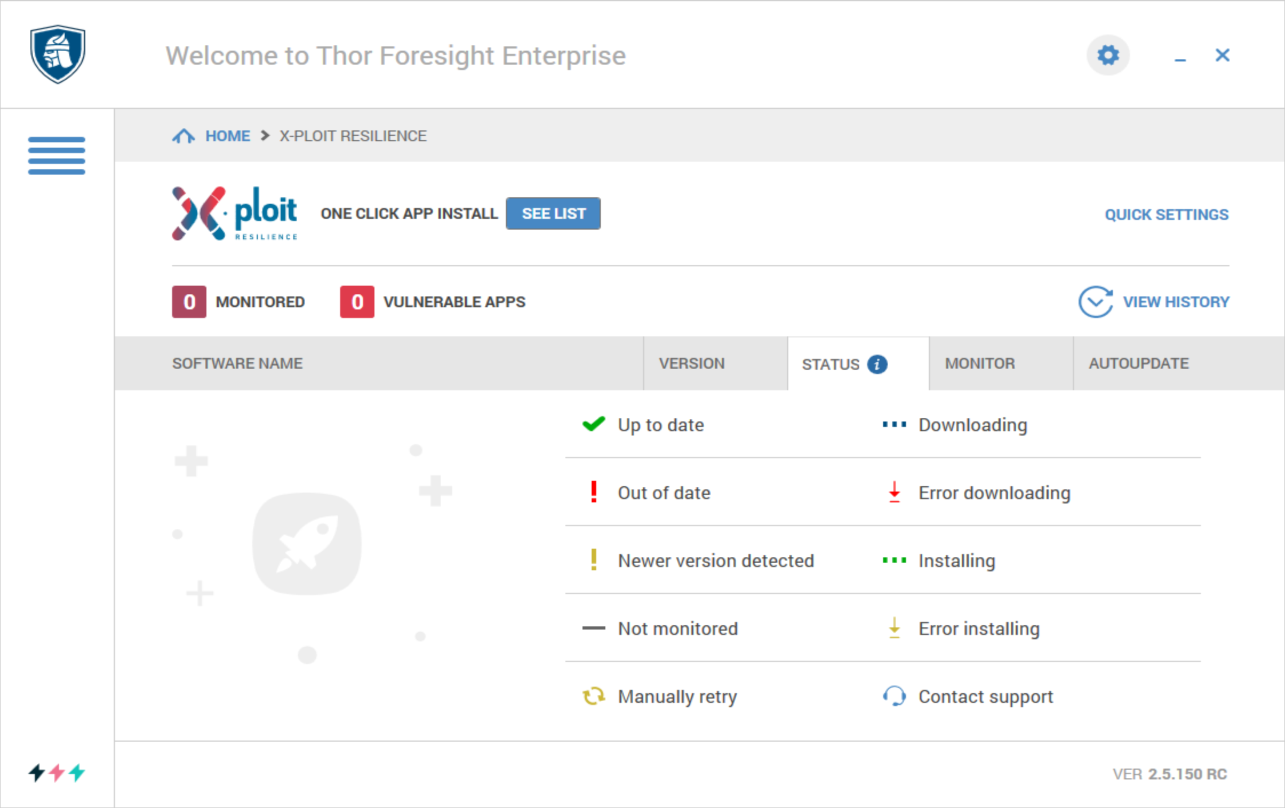
The following applications already have autoupdate enabled by default by the software manufacturer and consequently, may be updated faster than Thor Foresight can deliver the necessary patches: **Google Chrome, Google Drive, Skype, Mozilla Firefox, Mozilla Thunderbird.**

IMPORTANT

If you "select all" for the "install" option in the group policy, when new software is added to the Thor Foresight, the newly added software will be automatically installed in your environment.

7.1.1.4 Patches deployment method – Bulk or Staged?

If you are about to deploy Thor Foresight in your organization and your Group Policy is set to deploy new applications or to patch existing ones, you must know that the patches will be downloaded as the clients check towards the Dashboard, they never check at the same time. This way, we ensure that you'll avoid any traffic load in your organization. If a higher version is already installed on a PC, Thor Foresight will display the warning message **Your computer must be updated** and red exclamation mark next to the application name**.**
Below is a list of possible statuses of an application that X-Ploit Resilience patches:



Welcome to Thor Foresight Enterprise

✓ Up to date	··· Downloading
! Out of date	↓ Error downloading
! Newer version detected	··· Installing
— Not monitored	↓ Error installing
⟳ Manually retry	Contact support

7.1.1.5 Uninstall Application Feature for ENTERPRISE clients

Please read more about this on our article from FAQ:

UNINSTALL APPLICATION Feature Explained

7.1.2 Traffic check – Malicious websites, zero-day exploits and data ex-filtration

Internet traffic checking in Thor Foresight is based on a database and a filtering engine. It blocks websites with malicious content or blocks access to servers which are controlled and operated by IT Criminals. Thor Foresight also incorporates heuristic traffic checking and statistical analysis to discover new and yet unknown threats. By doing so it protects a corporate network or private user from opening backdoors, uploading data into the hands of hackers or from having data ex-filtrated from PCs or Networks.

7.1.2.1 Technical Implementation

The feature runs as a service on the local PC and checks all DNS lookups that are made on the PC. When a lookup is made, Thor Foresight will send the DNS lookup onto the DNS Servers defined in the client DHCP settings and check whether any of them are found in the list of malicious servers or websites.

The list is compiled as a space optimized probabilistic data structure and only takes up 15 MB of disk space. Through this data structure Thor Foresight can decide if the DNS name is either:

a) With 100% certainty not on the list of malicious sites
b) With 98% certainty on the list of malicious sites

If the address is not on the list of malicious servers, Thor Foresight will approve the request from the used DNS servers.

If the address is with a 98% certainty on the list, Thor Foresight will perform an extra check towards our servers to verify whether the address is harmful or not.

a) If it does show up as harmful, the site or traffic is blocked, and a notice will be displayed.
b) If the domain address is not harmful the traffic will be allowed.

The advantage of using a probabilistic data structure is that the speed of the service is much higher, and the size of the database is only roughly 0,5% of the total list.

The traffic check works for all services on the PC and on VPN. It also works on internal as well as private networks.

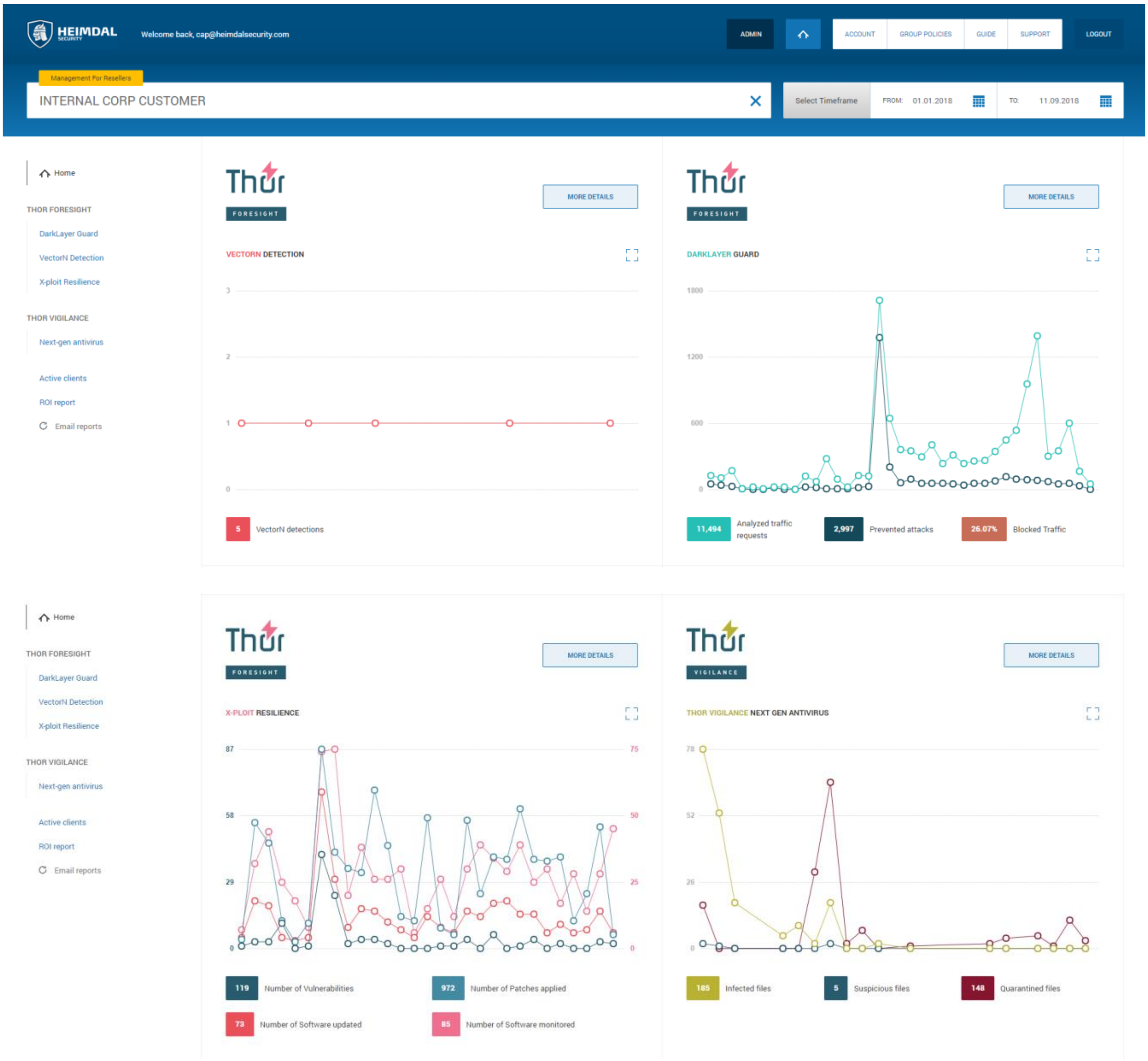
7.2 Features for Thor Vigilance

As a standalone AV product Thor Vigilance features a complex threat scan module that is capable of detecting viruses, trojans, riskware, heuristic threats, adware, backdoor, constructors, dialers, exploits, trash, APCs. Besides the scan module that is available on each Thor installation, the AV as a concept also features:

- reporting and control dashboard (see chapter 7.1.4)
- protection cloud (see chapter 7.1.4)
- local quarantine location
- VDFs (Virus Definition Files)

8. Managing the dashboard interface for Thor Products

Both products that comprise the Thor Enterprise are controlled from a centralized web interface that is commonly known as and referred to as “the dashboard”. The URL that will make it accessible to visitors is https://dashboard.heimdalsecurity.com/home



INTERNAL CORP CUSTOMER

FROM: 01.01.2018 TO: 11.09.2018

5 VectorN detections

11,494 Analyzed traffic requests

2,997 Prevented attacks

26.07% Blocked Traffic

119 Number of Vulnerabilities

972 Number of Patches applied

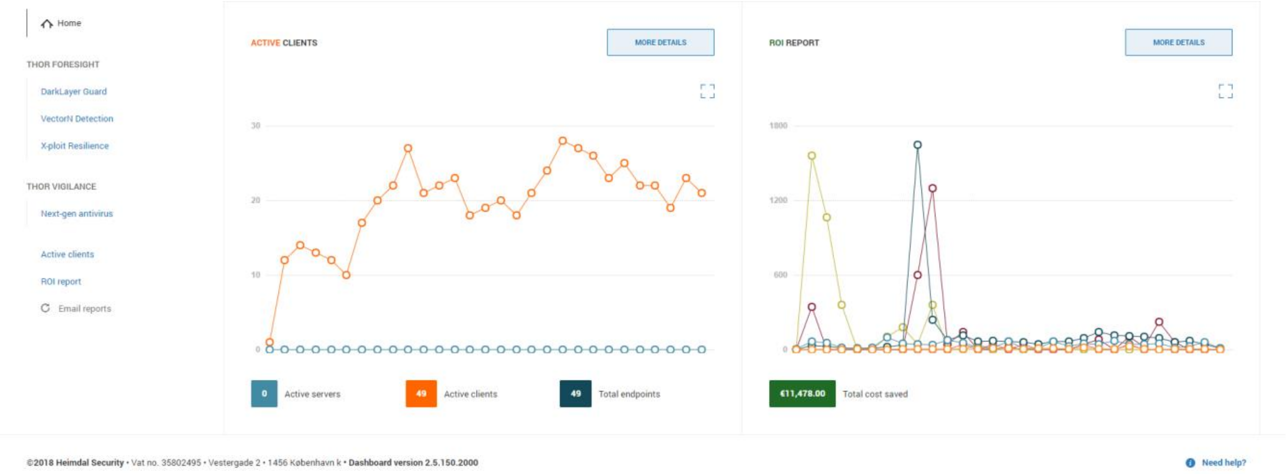
73 Number of Software updated

85 Number of Software monitored

185 Infected files

5 Suspicious files

148 Quarantined files



©2018 Heimdal Security • Vat no. 35802495 • Vestergade 2 • 1456 København k • Dashboard version 2.5.150.2000

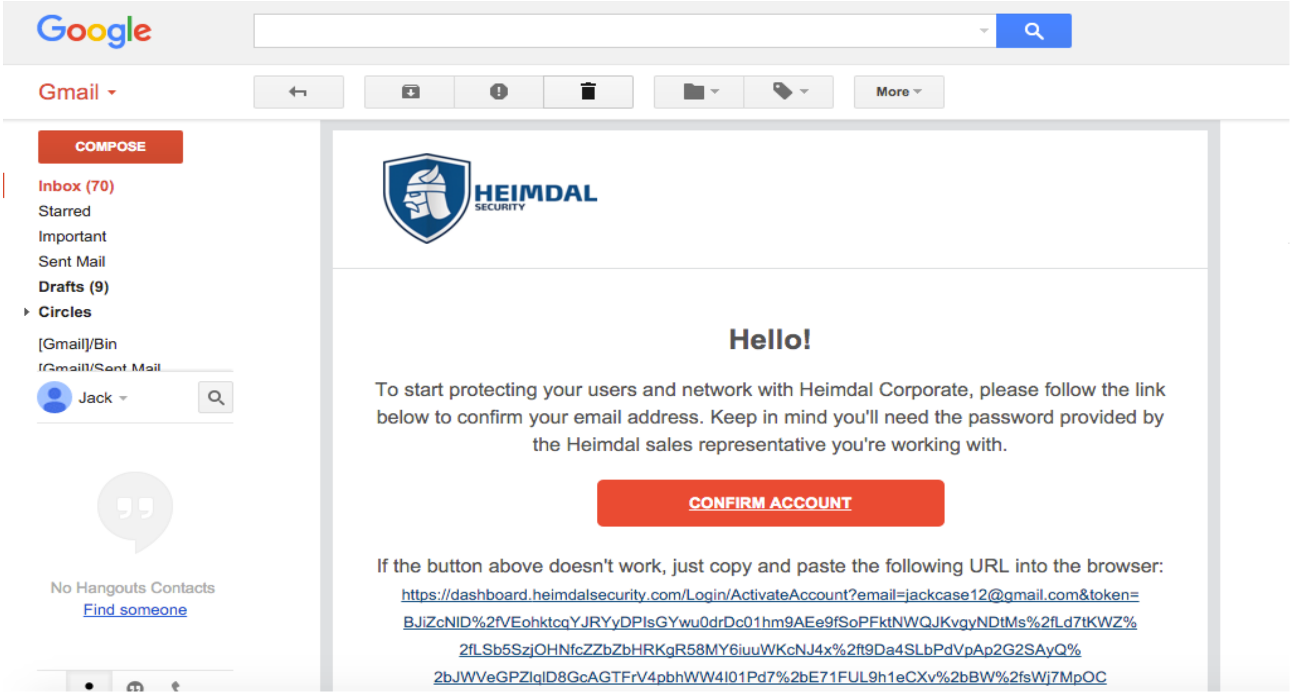
a. The home page contains different graph types that can be visualized and used for reporting purposes – GDPR & audit
b. The left side menu contains product overviews and can be browsed to check data that has been collected from the endpoints on which the 2 Thor products that comprise the Thor Enterprise run.
c. The top options will allow for the definitions of agent behaviors as well as controlling the reporting flows.

8.1.1 Account activation and install

Step 1 - Confirmation

The administrator will receive 2 emails:

- The first email will be from your Account Manager including your Username and Password
- The second email will come from the Thor dashboard which shall have a link – please see below.



Hello!

To start protecting your users and network with Heimdal Corporate, please follow the link below to confirm your email address. Keep in mind you'll need the password provided by the Heimdal sales representative you're working with.

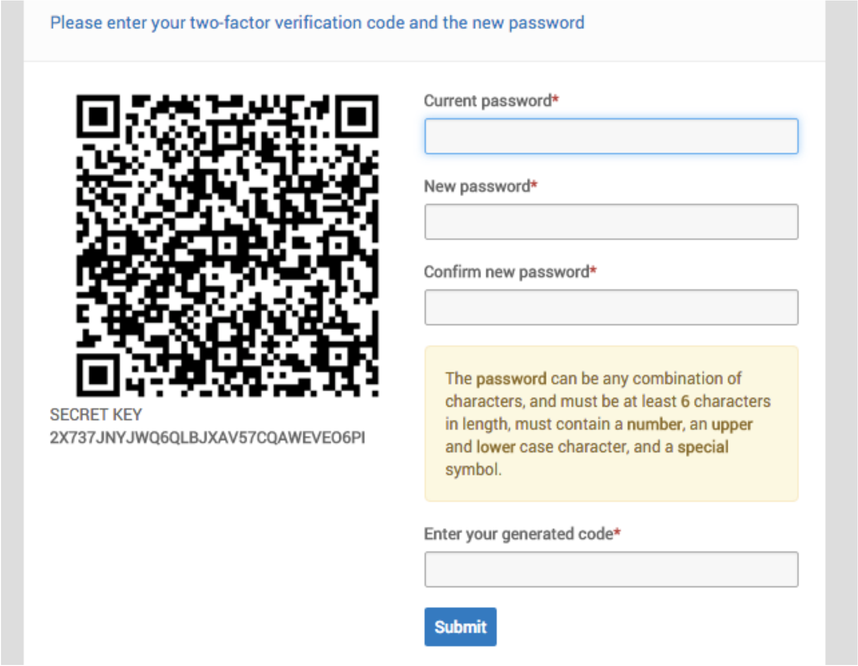
If the button above doesn't work, just copy and paste the following URL into the browser:

https://dashboard.heimdalsecurity.com/Login/ActivateAccount?email=jackcase12@gmail.com&token=
BJiZcNID%2fVEohktcqYJRYyDPIsGYwu0drDc01hm9AEe9fSoPFktNWQJKvgyNDtMs%2fLd7tKWZ%
2fLSb5SzjOHNfcZZbZbHRKgR58MY6iuuWKcNJ4x%2ft9Da4SLbPdVpAp2G2SAyQ%
2bJWVeGPZlqID8GcAGTFrV4pbhWW4I01Pd7%2bE71FUL9h1eCXv%2bBW%2fsWj7MpOC

Step 2 - Logging into the Management Portal

When you have clicked the Confirm Account Link, you will be taken to a page where you will be able to log into the Management Portal – please see below screenshot.

- Please download the Google Authenticator app on your phone (it's free and can be found on Google Play, iTunes and Windows Store)
- Scan the QR code with Google Authenticator, this will then generate a 6-digit code roughly every 30 seconds. You will need to get a code from Google Authenticator every time you log into Thor's Management Portal!
- Enter the password given in the email you received from your Account Manager and then create a new password
- Enter the generated code from Google Authenticator and press the Submit button.



Please enter your two-factor verification code and the new password

SECRET KEY
2X737JNYJWQ6QLBJXAV57CQAWEVEO6PI

Current password*

New password*

Confirm new password*

The password can be any combination of characters, and must be at least 6 characters in length, must contain a number, an upper and lower case character, and a special symbol.

Enter your generated code*

If you are admin and you need access to your account, reset password or add a new IP to your account, please contact your Account Manager.

Step 3 – MSI file and your License Key

With everything set up you can now download Thor onto as many Endpoints and Servers as you like

- Click "Guide" at the top of the Screen
- Here you will find the MSI File to Download and Install Thor
- You will also find Your License Key here
- The Customer you select under "Management for Resellers", it will bring up their license key

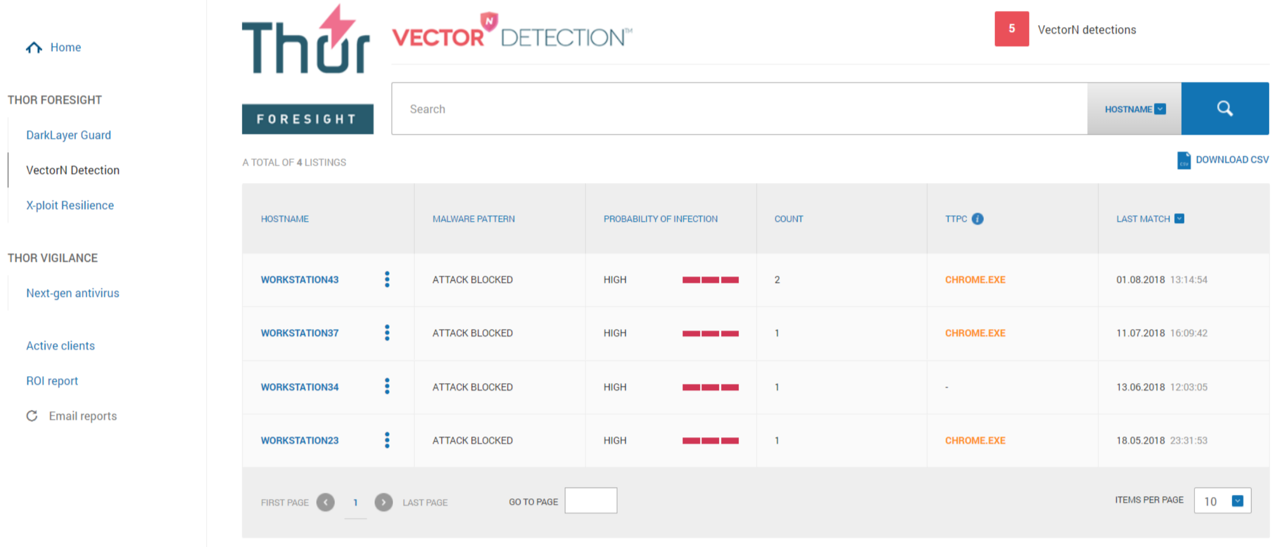
8.1.2 Group policies

To have a better overview of this, please visit our FAQ and read about the Group Policy feature: Dashboard Features: Group Policy Overview

Also, have a look here: How Do I Change The Priority Of A Group Policy?

8.1.3 Management interface for Thor Foresight

8.1.3.1 VectorN Detection



A TOTAL OF 4 LISTINGS

HOSTNAME	MALWARE PATTERN	PROBABILITY OF INFECTION	COUNT	TTPC	LAST MATCH
WORKSTATION43	ATTACK BLOCKED	HIGH	2	CHROME.EXE	01.08.2018 13:14:54
WORKSTATION37	ATTACK BLOCKED	HIGH	1	CHROME.EXE	11.07.2018 16:09:42
WORKSTATION34	ATTACK BLOCKED	HIGH	1	-	13.06.2018 12:03:05
WORKSTATION23	ATTACK BLOCKED	HIGH	1	CHROME.EXE	18.05.2018 23:31:53

VectorN Detection will focus on ensuring **Code Autonomous Protection**™ on both corporate and private endpoints, detecting malware in ways that no other endpoint protection can.

The overview will show the endpoints with the HIGHEST probability of infection across all online detection patterns.

Please note that an entry in this section may hide other detection patterns with lower probability (like moderate for instance) so if you need further info on this, you need to individually click the entries displayed in the VectorN section for details.

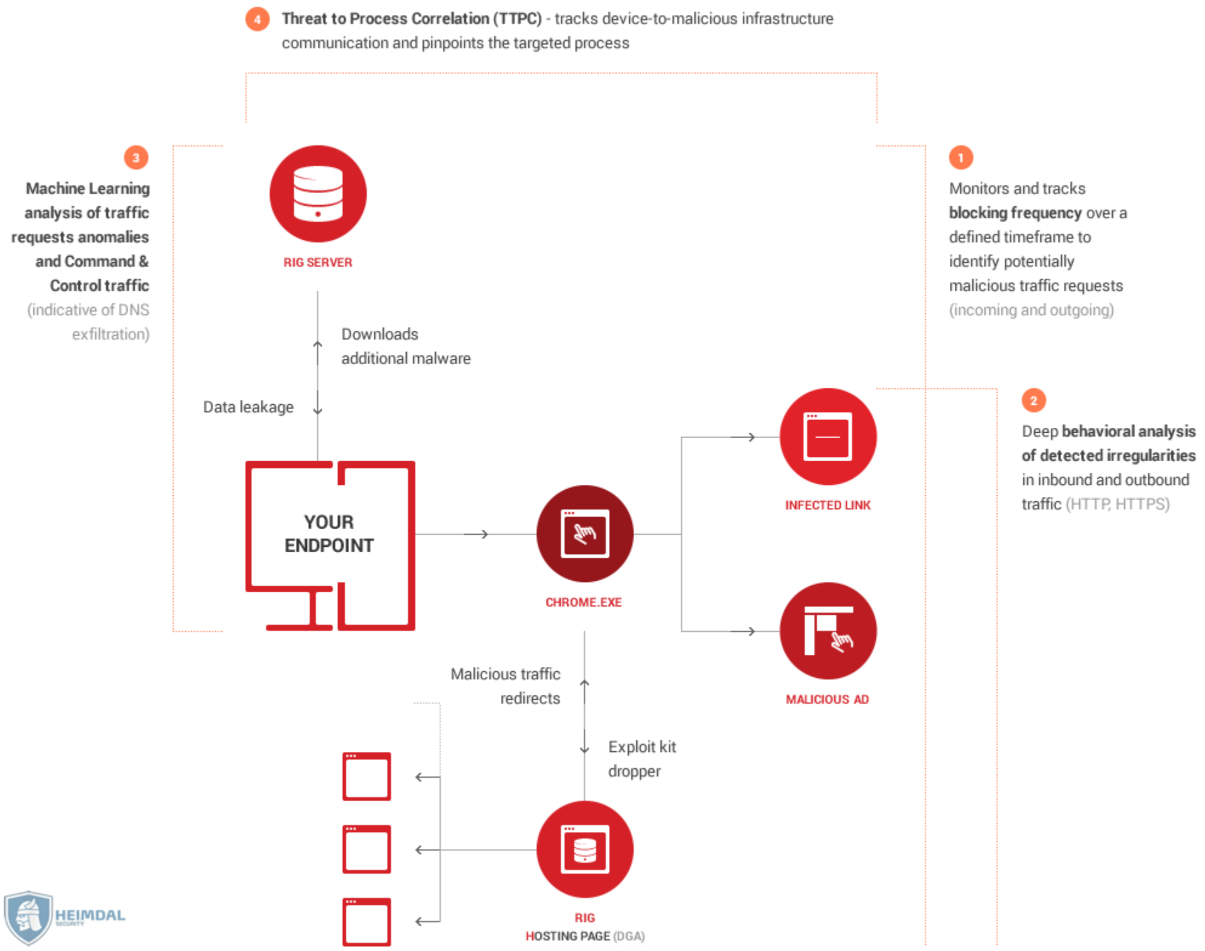
A few key things you should know about VectorN Detection:

- It works across-the-board on any Windows™ device;
- It does not rely on scanning the code or auditing any system processes. Instead, the new technology uses Machine Learning Detection (MLD) to perform an in-depth analysis of all incoming and outgoing HTTP, HTTPS and DNS traffic.
- It matches Machine Learning (MLD) insights with Indicators of compromise/attack (IOC/IOA) and network forensics, turning Thor into a unique proactive cyber security suite.
- It even helps users discover hidden, second generation malware that tries to infect the endpoint or attempts to harvest data from the compromised system.
- By tracking device-to-infrastructure communication, this technology enables users to detect and block advanced malware, regardless of the attack vector.

The graphic below illustrates how **VectorN Detection**^{TM} empowers Thor users to detect and block even hidden malware attacks, preventing malware from infiltrating the system.

USE CASE:

How corroborated Heimdal VECTOR DETECTION™ parameters uncover hidden malware attacks



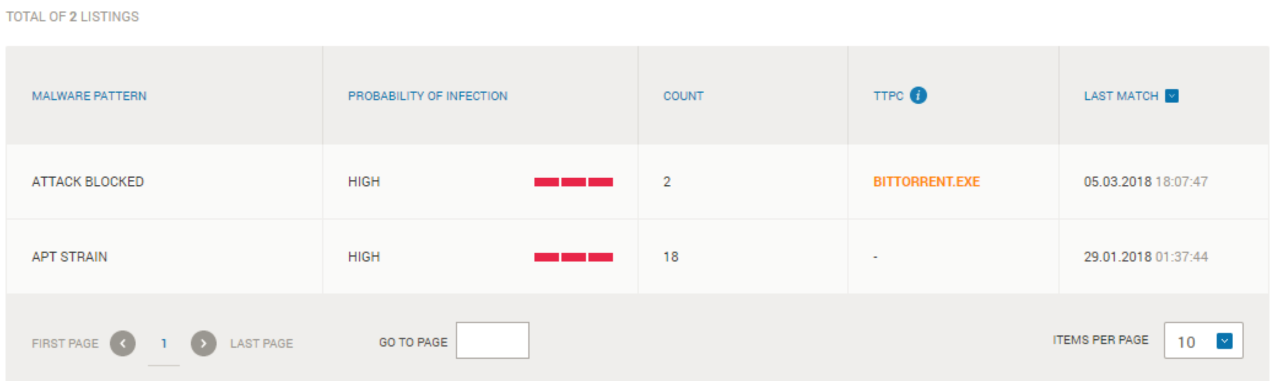
4 **Threat to Process Correlation (TTPC)** - tracks device-to-malicious infrastructure communication and pinpoints the targeted process

3 **Machine Learning analysis of traffic requests anomalies and Command & Control traffic** (indicative of DNS exfiltration)

1 Monitors and tracks **blocking frequency** over a defined timeframe to identify potentially malicious traffic requests (incoming and outgoing)

2 Deep **behavioral analysis of detected irregularities** in inbound and outbound traffic (HTTP, HTTPS)

Clicking on individual VectorN detections will result in showing all malware detections as well as the TTPC (threat to Process correlation)



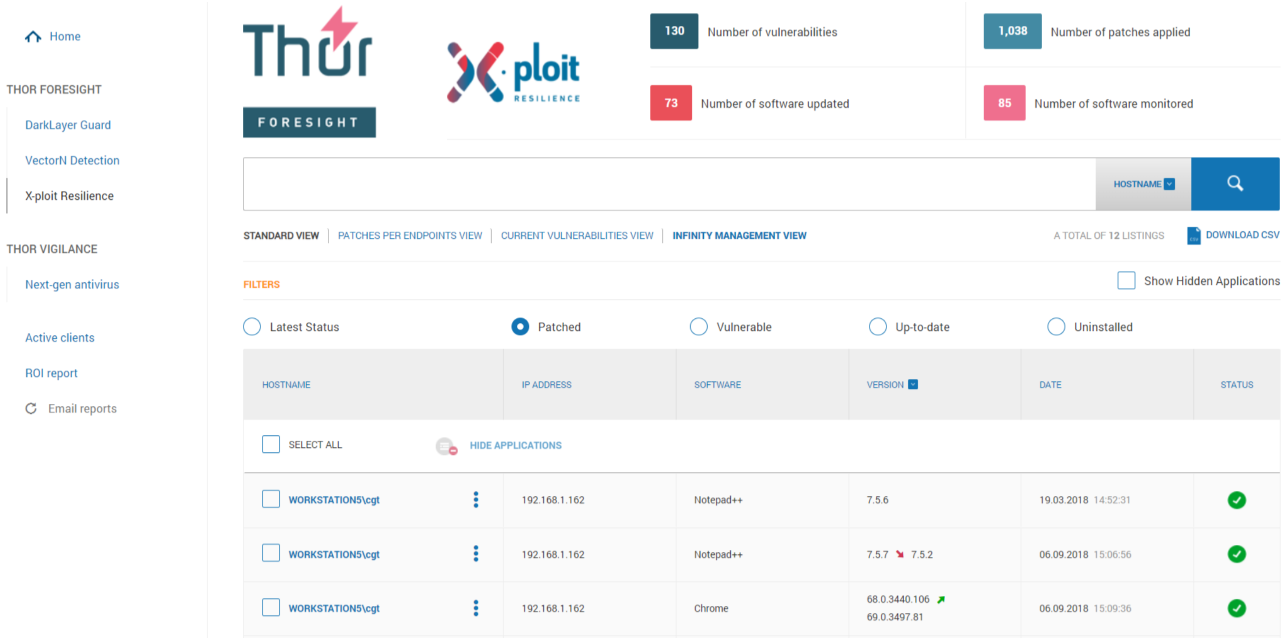
TOTAL OF 2 LISTINGS

MALWARE PATTERN	PROBABILITY OF INFECTION	COUNT	TTPC	LAST MATCH
ATTACK BLOCKED	HIGH ▬▬▬	2	BITTORRENT.EXE	05.03.2018 18:07:47
APT STRAIN	HIGH ▬▬▬	18	-	29.01.2018 01:37:44

8.1.3.2 X-ploit Resilience

The Vulnerability Overview tab provides a centralized view about the vulnerabilities in your environment, enabling you to manage them and prevent security incidents.

In the version column you can see if there was a downgrade marked with a red arrow pointed down, an upgrade marked with green arrow pointed upwards or simply a new installation of a certain application.



130 Number of vulnerabilities
1,038 Number of patches applied
73 Number of software updated
85 Number of software monitored

STANDARD VIEW | PATCHES PER ENDPOINTS VIEW | CURRENT VULNERABILITIES VIEW | INFINITY MANAGEMENT VIEW

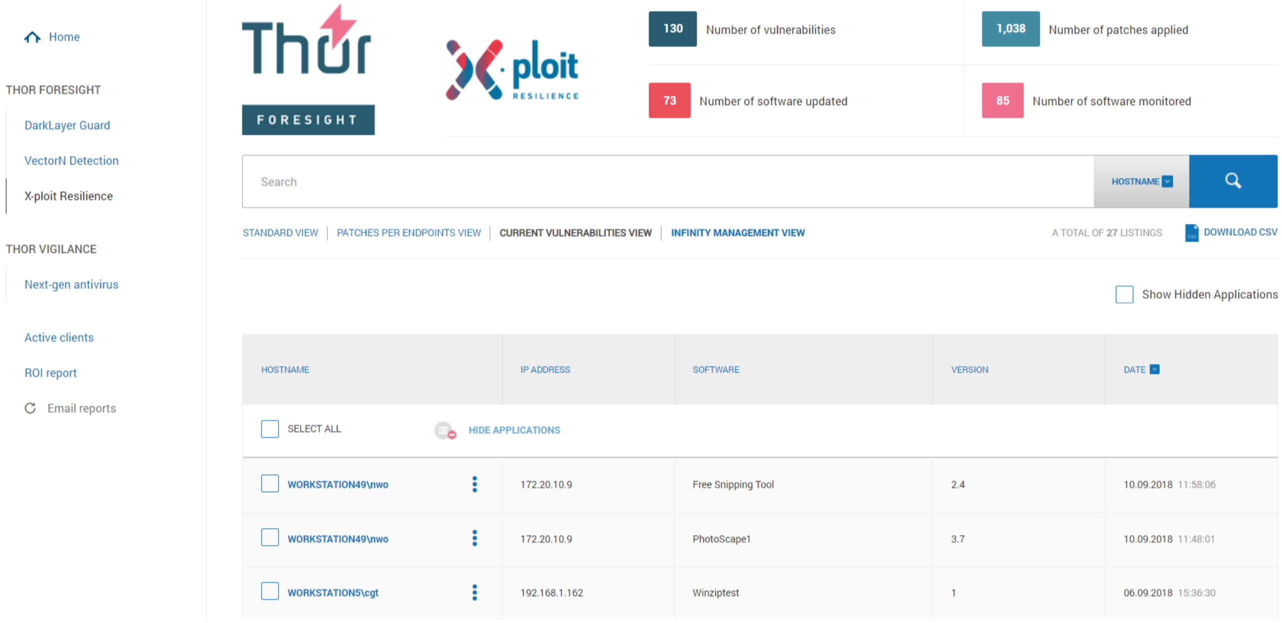
A TOTAL OF 12 LISTINGS DOWNLOAD CSV

FILTERS □ Show Hidden Applications

○ Latest Status ● Patched ○ Vulnerable ○ Up-to-date ○ Uninstalled

HOSTNAME	IP ADDRESS	SOFTWARE	VERSION	DATE	STATUS
□ SELECT ALL HIDE APPLICATIONS					
□ WORKSTATION5\cgt	192.168.1.162	Notepad++	7.5.6	19.03.2018 14:52:31	✓
□ WORKSTATION5\cgt	192.168.1.162	Notepad++	7.5.7 ↘ 7.5.2	06.09.2018 15:06:56	✓
□ WORKSTATION5\cgt	192.168.1.162	Chrome	68.0.3440.106 ↗ 69.0.3497.81	06.09.2018 15:09:36	✓

You can choose what software to install or update using policies from the Group policies tab. More details about group policies in chapter 5.2. The admin has the option to check for current vulnerabilities.



130 Number of vulnerabilities
1,038 Number of patches applied
73 Number of software updated
85 Number of software monitored

STANDARD VIEW | PATCHES PER ENDPOINTS VIEW | CURRENT VULNERABILITIES VIEW | INFINITY MANAGEMENT VIEW

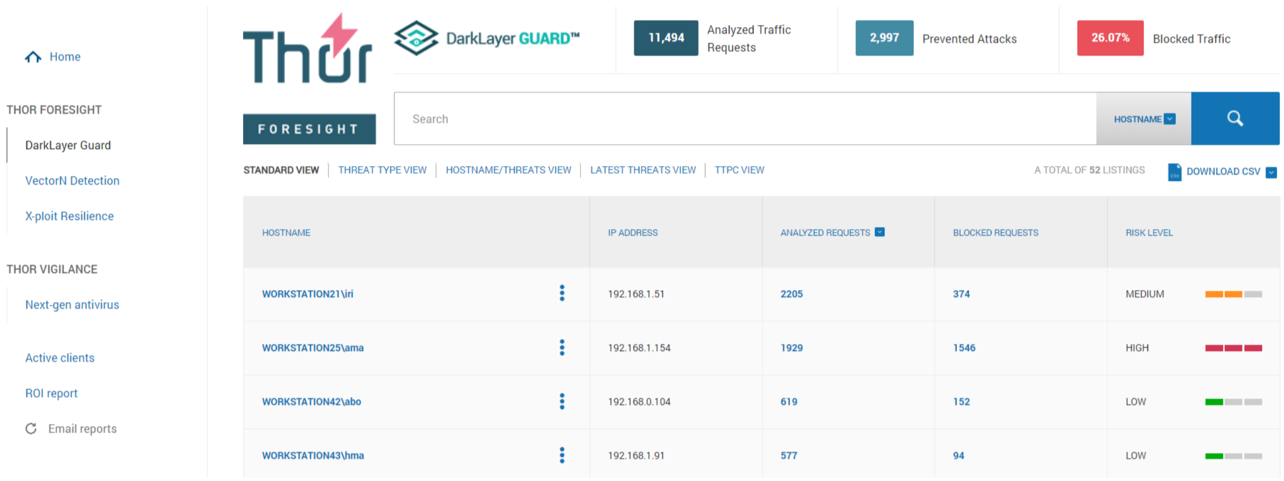
A TOTAL OF 27 LISTINGS DOWNLOAD CSV

□ Show Hidden Applications

HOSTNAME	IP ADDRESS	SOFTWARE	VERSION	DATE
□ SELECT ALL HIDE APPLICATIONS				
□ WORKSTATION49\nwo	172.20.10.9	Free Snipping Tool	2.4	10.09.2018 11:58:06
□ WORKSTATION49\nwo	172.20.10.9	PhotoScape1	3.7	10.09.2018 11:48:01
□ WORKSTATION5\cgt	192.168.1.162	Winziptest	1	06.09.2018 15:36:30

This list contains all outdated pieces of software in the environment that the relevant policy applies to.

8.1.3.3 DarkLayer Guard Overview



11,494 Analyzed Traffic Requests

2,997 Prevented Attacks

26.07% Blocked Traffic

A TOTAL OF 52 LISTINGS

HOSTNAME	IP ADDRESS	ANALYZED REQUESTS	BLOCKED REQUESTS	RISK LEVEL
WORKSTATION21\iri	192.168.1.51	2205	374	MEDIUM
WORKSTATION25\ama	192.168.1.154	1929	1546	HIGH
WORKSTATION42\abo	192.168.0.104	619	152	LOW
WORKSTATION43\hma	192.168.1.91	577	94	LOW

Thor Foresight uses bloom filter technology (the same is used by the Google search engine). This ensures that the module is as fast and as accurate as possible. The bloom filter resides locally on the endpoints which have the agent installed and it will only ask the cloud when there is a partial or full match to the local filter. If there is no match, it passes clean through.

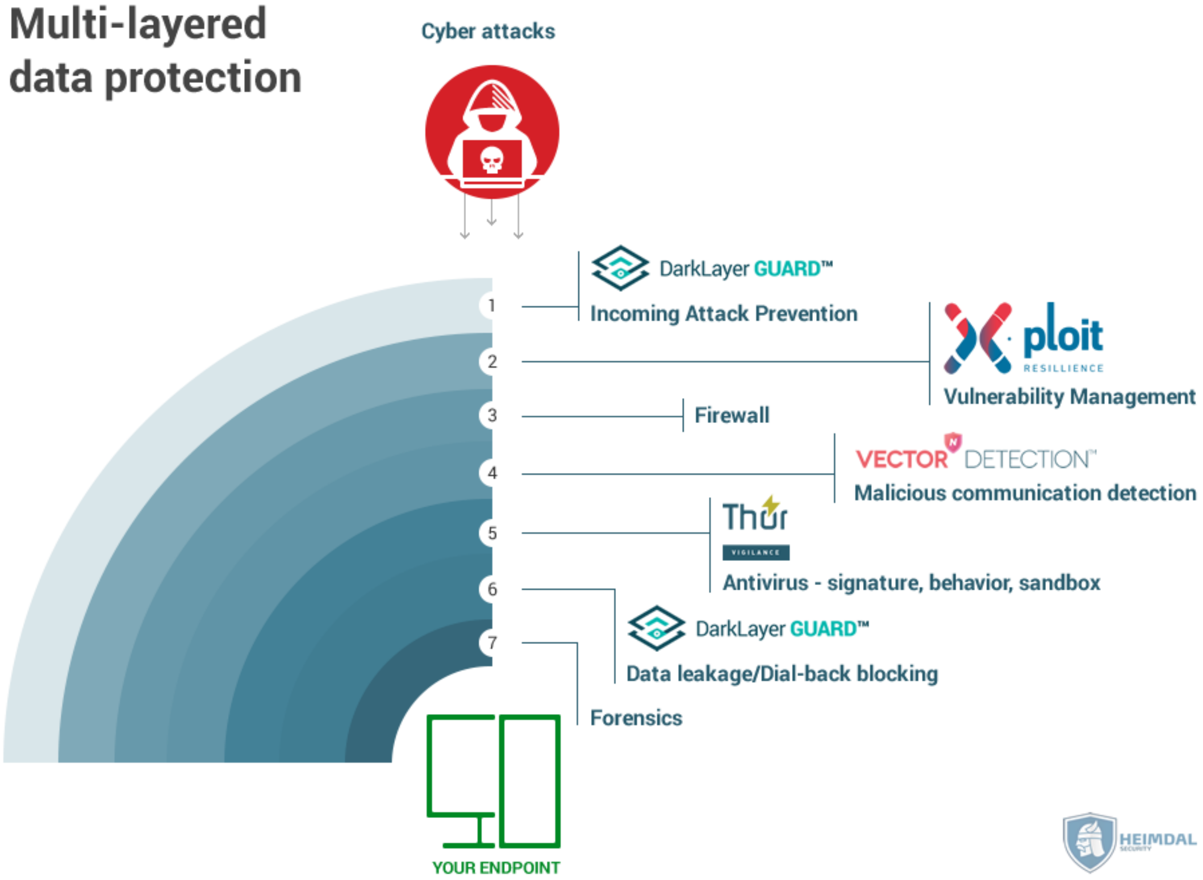
With the size of the filter we use, we get 99.5% accuracy of the local PC. Consequently, we will only have to ask for the remaining 0,5% of information during the DNS interrogation. That's because, out of all the data we check, there will already have been a match in the local database for the most of it.

Out of those 0,5% that we check - about 1-3% are typically malicious, depending on the user profiles.
The benefits of this system are:

- High accuracy
- High performance
- Low false positive blocks

The downside is that about 0,47-0,49% of what we check will be a false positive check (but not a block). This is an optimal solution in order to avoid huge local databases.

The DarkLayer Guard feature communicates using encrypted traffic with the Heimdal Security cloud infrastructure. This ensures that third parties can't intercept network package traffic. Please bear in mind that in certain countries or infrastructures encrypted communication may be refused by the infrastructure owner and hence the DLG feature may not work properly. Using the "Auto Disable" option will resolve this issue. Enabling this feature though may also leave your endpoints unprotected in these scenarios to ensure uptime.



The DarkLayer Guard module protects your users by blocking access to malicious websites. This feature is updated regularly and does not require any administration or maintenance on your part. The graph above will explain the protection level placement for each Thor Foresight module.

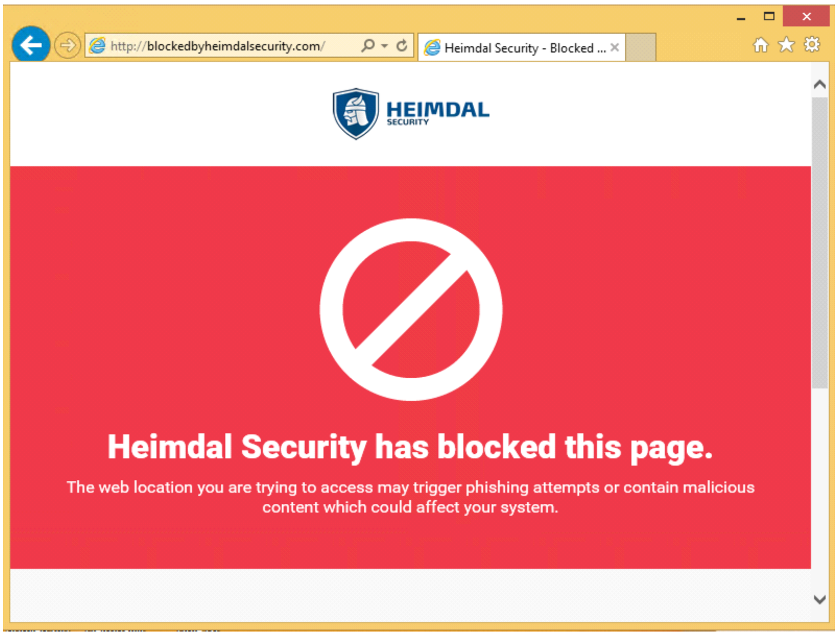
The DLG module filters all network traffic packages and every package is intercepted. This has the following effect: not only the addresses that are manually written by the users in the URL bar are filtered but also all redirects, all additional pages that are opened when unintentionally clicking on a commercial/ link or ad.

Please keep in mind that the DLG does not do SSL dissection, it does not look what's inside the packages and does not try to filter based on content. The DLG works by assessing the package origin and destination and it works by building strong reliable statistics. If an endpoint does too many requests or receives too many requests to or from a domain flagged as infected, the endpoint is flagged as potentially dangerous.

IMPORTANT

If a redirected page is blocked, this page will not open in the browser at all. However, the block will be registered inside the management interface (dashboard).

If a DNS request is blocked on a client (browser level), following a manual URL being written inside the URL bar or a suspicious link being clicked, the user will see the following within the browser:

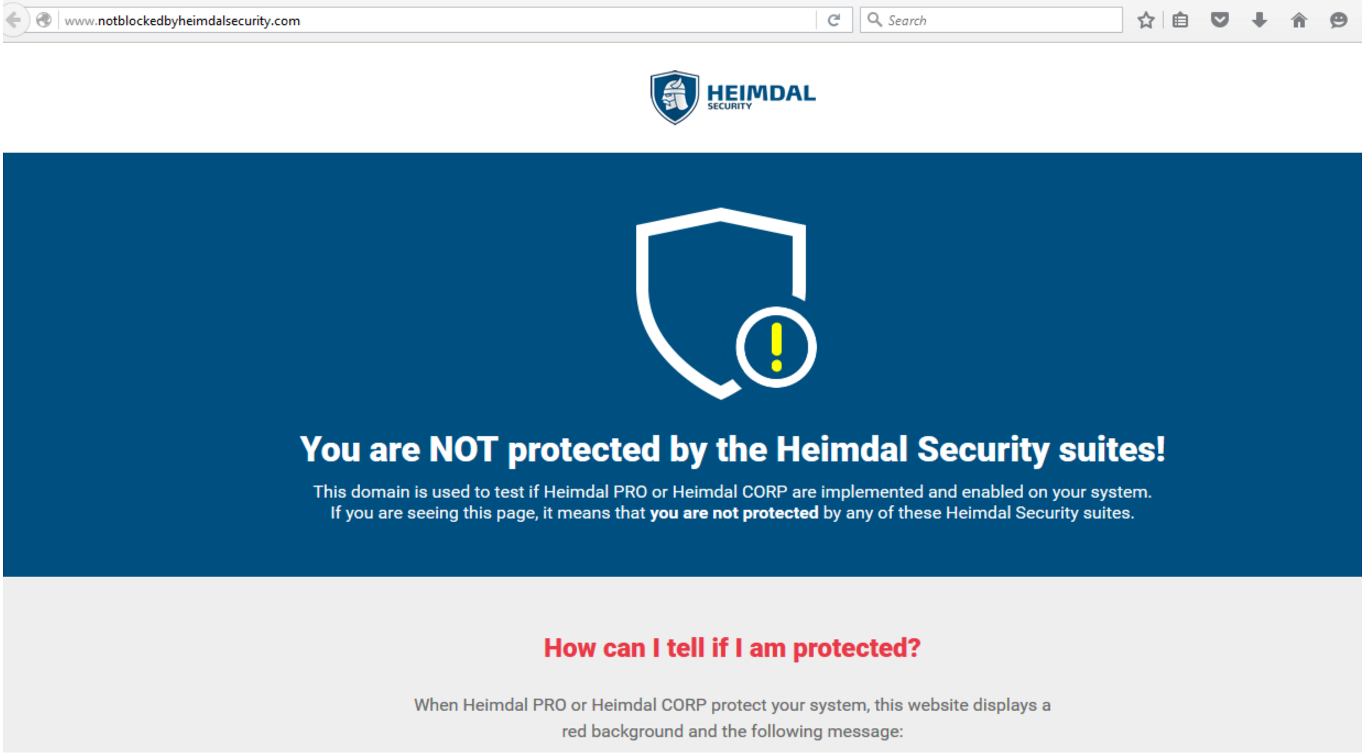


http://blockedbyheimdalsecurity.com/
Heimdal Security - Blocked ...
HEIMDAL SECURITY

Heimdal Security has blocked this page.

The web location you are trying to access may trigger phishing attempts or contain malicious content which could affect your system.

To test at client level whether the DLG is enabled or not, visit the following website (owned and operated by Heimdal Security): http://notblockedbyheimdalsecurity.com. If the DLG is not working or you don't have the DLG option enabled, the users will get the following page shown:



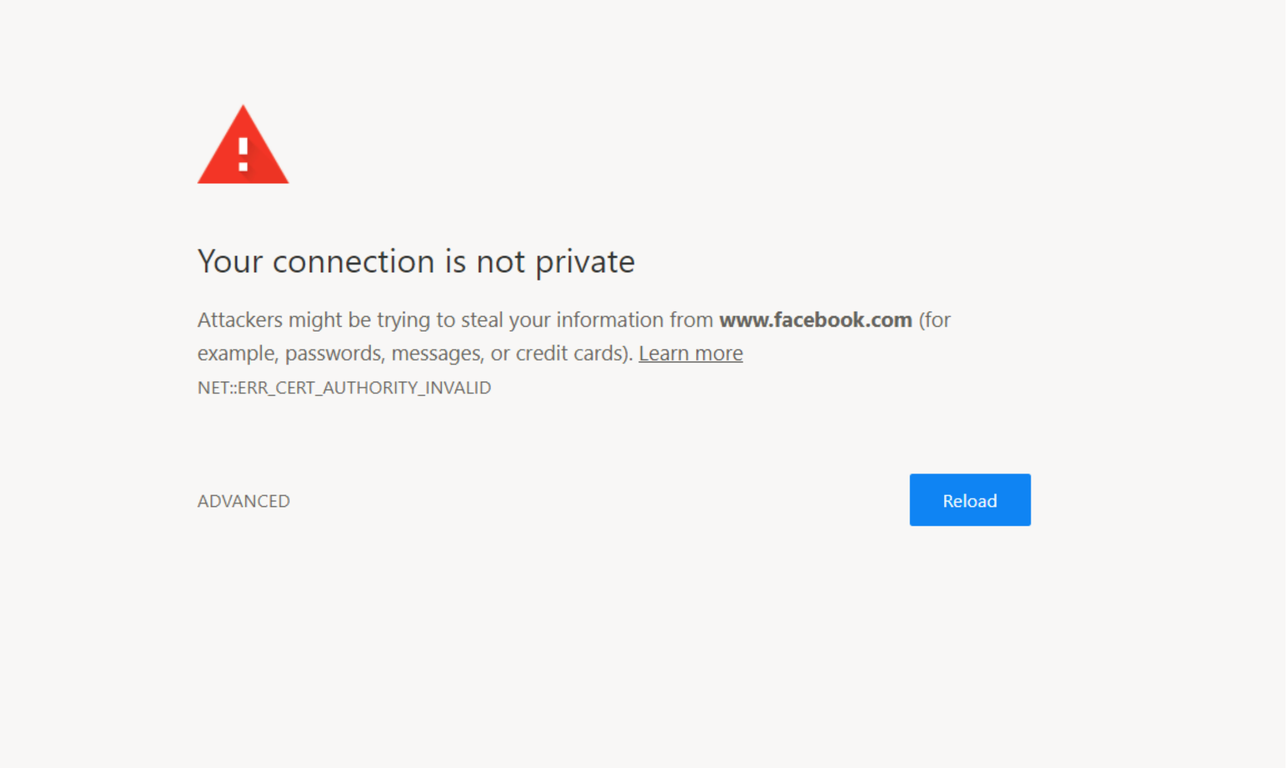
You are NOT protected by the Heimdal Security suites!

This domain is used to test if Heimdal PRO or Heimdal CORP are implemented and enabled on your system. If you are seeing this page, it means that **you are not protected** by any of these Heimdal Security suites.

How can I tell if I am protected?

When Heimdal PRO or Heimdal CORP protect your system, this website displays a red background and the following message:

What happens when we prevent an HTTPS page from loading?



Your connection is not private

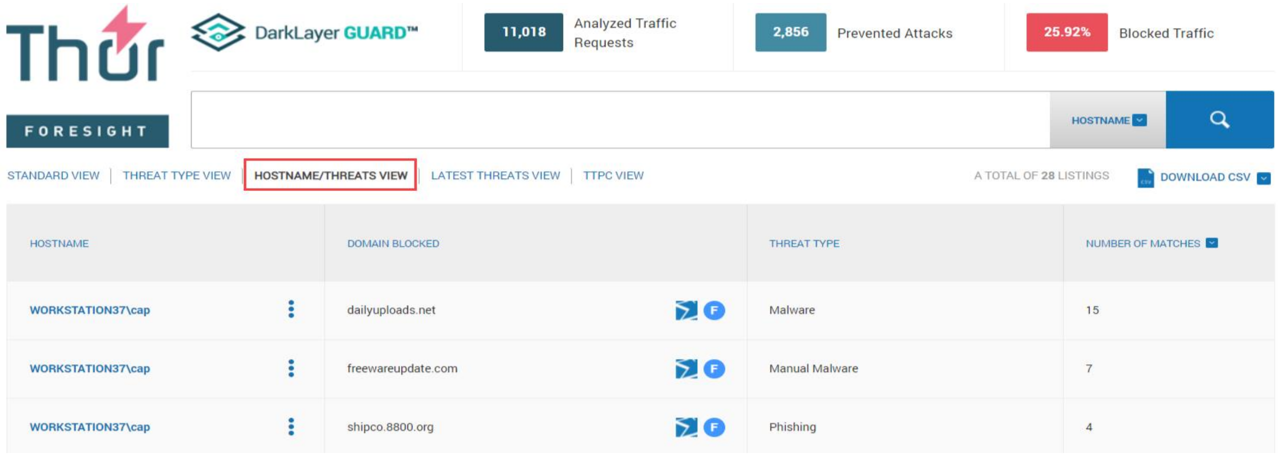
Attackers might be trying to steal your information from **www.facebook.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

The DLG cannot display the Thor block page when a HTTPS address is blocked because HTTPS needs a certificate validation.

For example, if you decide to block Facebook for your users, each time one of your users tries to go on facebook.com the local endpoint browser will receive the above error, because facebook.com uses the https protocol. That means that when the user tries to access facebook.com, the browser expects a certificate validation from Facebook. The validation will not be received and instead the browser session will receive the Heimdal Security certificate, therefore the request will fail.

If the administrator is interested in finding out the threat types vs. the hostnames, there is a special view inside the dashboard management interface. This view, also known as the "threat tab" will show the most blocked threat type from the target environment.



11,018 Analyzed Traffic Requests

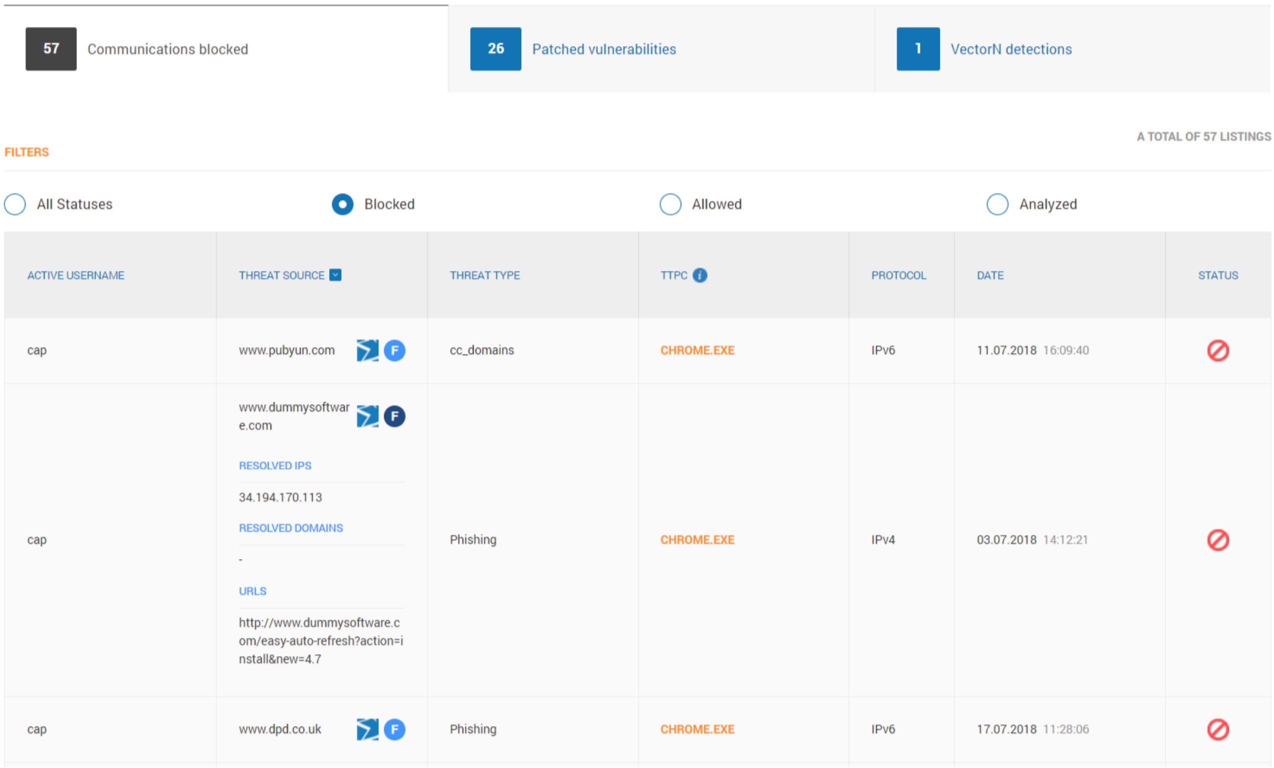
2,856 Prevented Attacks

25.92% Blocked Traffic

A TOTAL OF 28 LISTINGS

HOSTNAME	DOMAIN BLOCKED	THREAT TYPE	NUMBER OF MATCHES
WORKSTATION37\cap	dailyuploads.net	Malware	15
WORKSTATION37\cap	freewareupdate.com	Manual Malware	7
WORKSTATION37\cap	shipco.8800.org	Phishing	4

8.1.3.4 Forensic view



57 Communications blocked | 26 Patched vulnerabilities | 1 VectorN detections

FILTERS

A TOTAL OF 57 LISTINGS

○ All Statuses ● Blocked ○ Allowed ○ Analyzed

ACTIVE USERNAME	THREAT SOURCE	THREAT TYPE	TTPC	PROTOCOL	DATE	STATUS
cap	www.pubyun.com F	cc_domains	CHROME.EXE	IPv6	11.07.2018 16:09:40	⊘
cap	www.dummysoftware.com F RESOLVED IPS 34.194.170.113 RESOLVED DOMAINS - URLS http://www.dummysoftware.com/easy-auto-refresh?action=install&new=4.7	Phishing	CHROME.EXE	IPv4	03.07.2018 14:12:21	⊘
cap	www.dpd.co.uk F	Phishing	CHROME.EXE	IPv6	17.07.2018 11:28:06	⊘

Clicking on any entry inside the DLG will show the extended threat view for that particulat hostname/user. If the administrator clicks on the blue “F”, the forensics view will be uncovered.

Forensic view is an option that will provide more information about the domains that the DLG inside the Thor Foresight blocked. This feature will provide you the following information:

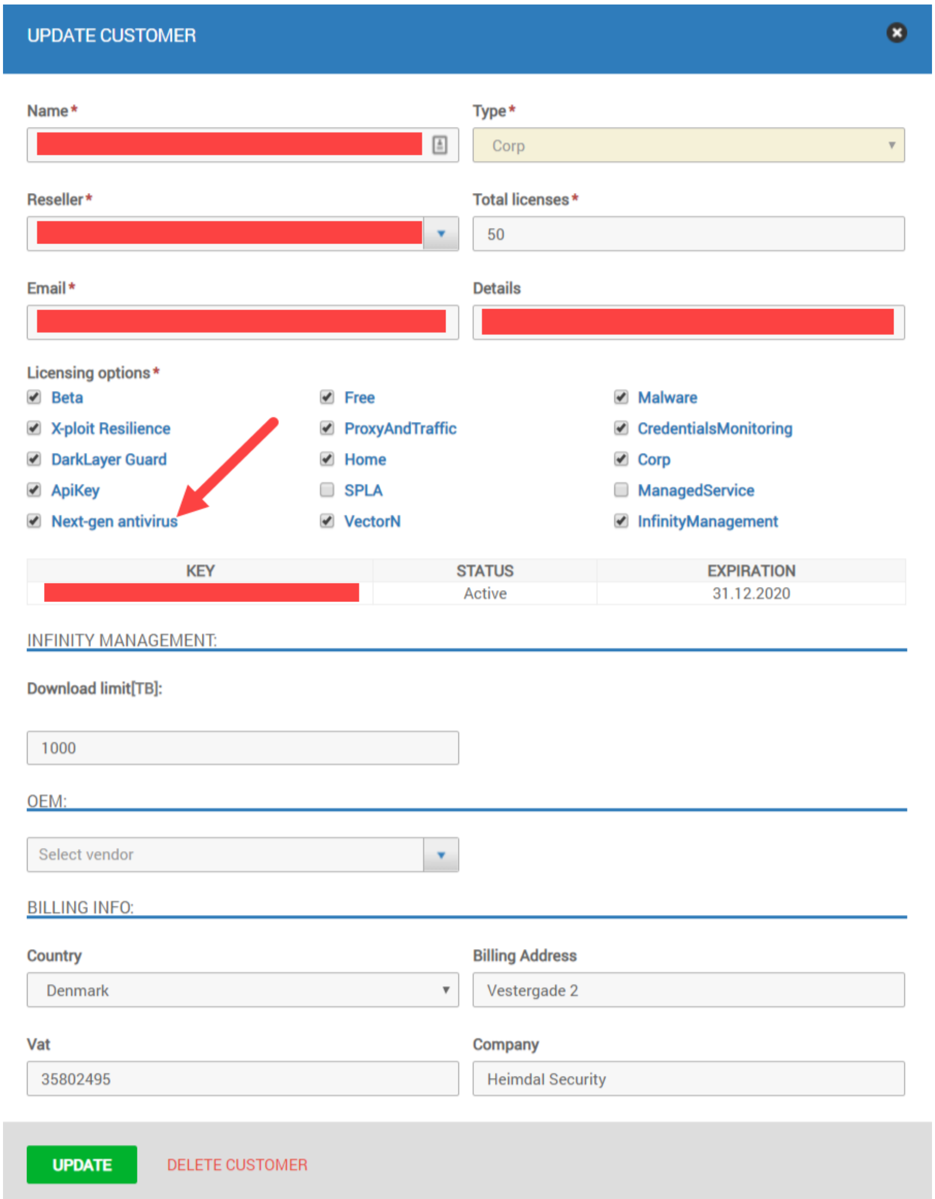
- Resolved IPs – these are the IPs of the domain we blocked
- Resolved Domains – is the domain we have blacklisted in our database
- URLs – is the domain the machine received or made a request from/to it.

In case no information is showed, it means the domain is not available anymore and it was taken down, or it could mean that the requests were not outbound, but inbound.

Next to the blue “F” button there is the icon for the VirusTotal website that redirects to the page where an analysis of the blocked domain can be viewed. This way you can know more about the threats a page is posing on your computers.

8.1.4 Management interface for Thor Vigilance

First of all, to be able to activate the Thor Vigilance product, the dashboard customer needs to have this enabled in the admin console as follows:



UPDATE CUSTOMER

Name* [redacted]

Type* Corp

Reseller* [redacted]

Total licenses* 50

Email* [redacted]

Details [redacted]

Licensing options*

☑ Beta
☑ X-ploit Resilience
☑ DarkLayer Guard
☑ ApiKey
☑ Next-gen antivirus
☑ Free
☑ ProxyAndTraffic
☑ Home
□ SPLA
☑ VectorN
☑ Malware
☑ CredentialsMonitoring
☑ Corp
□ ManagedService
☑ InfinityManagement

KEY	STATUS	EXPIRATION
[redacted]	Active	31.12.2020

INFINITY MANAGEMENT:

Download limit[TB]: 1000

OEM:

Select vendor

BILLING INFO:

Country Denmark

Billing Address Vestergade 2

Vat 35802495

Company Heimdal Security

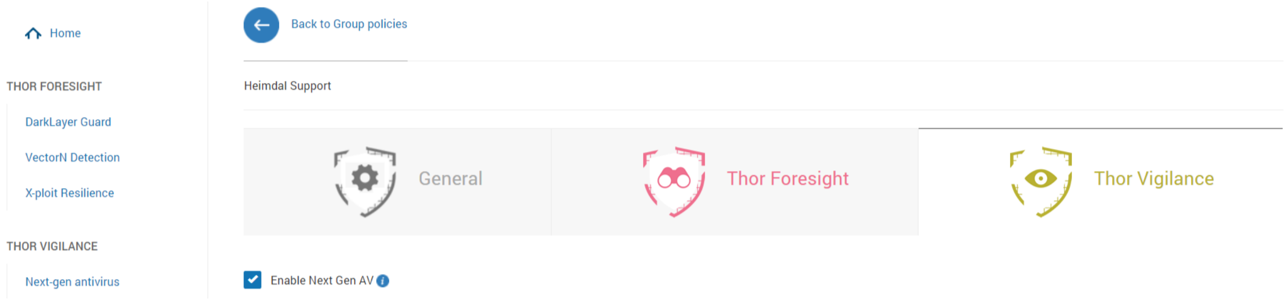
This is doable by:

- the sales team (account managers)
- the dashboard administrators
- the support team
- resellers
- distributors

If you do not have the possibility to activate this yourself inside the admin console, please contact the account manager or the support team.

8.1.4.1 Activation of Thor Vigilance

In order to turn on the Thor Vigilance product, it needs to be activated from the Group Policies tab, which is possible if you have purchased the module. Please see the screen below:



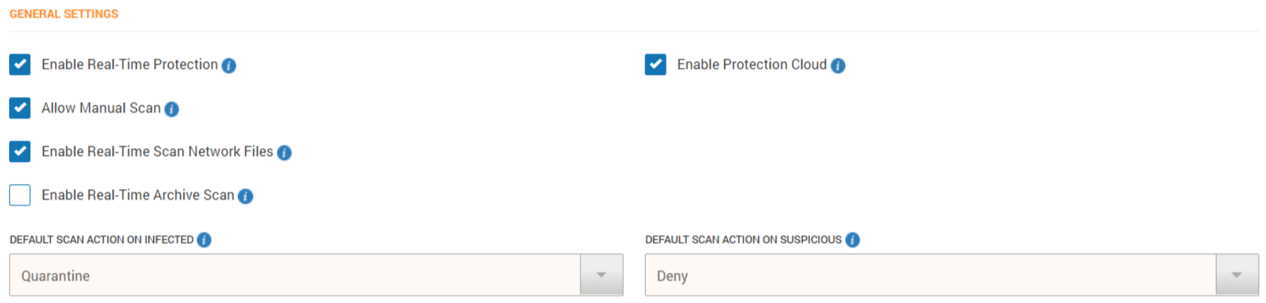
☑ Enable Next Gen AV

In other words, the controls for the Foresight and the Vigilance product are modular, independent from each other and can be activated individually. This means that depending on your environment and what you want to achieve in it, you may opt for policies that:

- only work as a preventive protection layer (only Thor Foresight active)
- act as a strong reactive countermeasure against viruses (only Thor Vigilance active)
- benefit from both products for maximum protection against both online and offline threats.

Once the product has been enabled, it can be configured at will, according to the intent and need of the administrator.

The first section of the policy that you can configure is the general scan settings according to the printscreen below:



GENERAL SETTINGS

☑ Enable Real-Time Protection

☑ Allow Manual Scan

☑ Enable Real-Time Scan Network Files

□ Enable Real-Time Archive Scan

☑ Enable Protection Cloud

DEFAULT SCAN ACTION ON INFECTED: Quarantine

DEFAULT SCAN ACTION ON SUSPICIOUS: Deny

Real time protection is available for use with any policy. This means that the local agent is closely watching in real time what the opened and accessed local files are. Before opening and executing files the agent is actively scanning the file.

If want to allow the employees to be able to scan on demand the computers they are using you can enable Manual Scans.

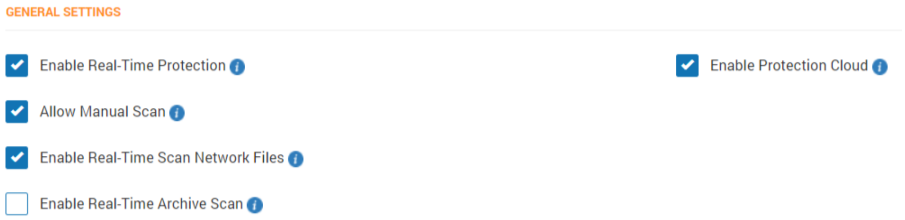
You may define a set of actions here that will be executed by default upon opening or executing an infected or suspicious file. There are 3 options available and they are the same for both infected/suspicious files:

a) **Deny** – means that the file will not be able to be opened or executed by the user. This is valid also for users with local admin privileges. This is done from windows settings and not the AV client. The default message that the users will receive upon trying to open such a file is that the system does not have enough resources to execute the command.

b) **Quarantine** – means that the file will be automatically moved to the Quarantine and will become unavailable until removed from Quarantine.

c) **Allow** – the real time protection is bypassed, and the files become accessible even if found to be infected or suspicious.

8.1.4.2 Network and archive scan



GENERAL SETTINGS

☑ Enable Real-Time Protection ⓘ

☑ Allow Manual Scan ⓘ

☑ Enable Real-Time Scan Network Files ⓘ

□ Enable Real-Time Archive Scan ⓘ

☑ Enable Protection Cloud ⓘ

It is possible to configure additional options like real time protection for network files and real time protection for archives. This is especially useful if you’re seeing performance drops in environments like file servers which contain multiple network hosted files and/ or archives. Disabling these options will increase your overall performance, but will expose you to more threats. In the end, it is up to each system administrator to configure their environment as best fit for their organization.

8.1.4.3 What is the protection cloud?

Protection cloud is a service which Heimdal Security offers by default to all their customers. If a file looks suspicious to the local AV agent, a copy of the file is uploaded in our cloud, in a sandboxed environment and its hash is checked against our own real time database. Further standard tests are performed on the file to determine if it’s really infected or not. You may want to set the default action to deny the access to the file if deemed suspicious and then if you have the protection cloud enabled, we will analyse it and find out more about the file.

This provides an additional layer of security and extra info when trying to determine the infection status of a file.

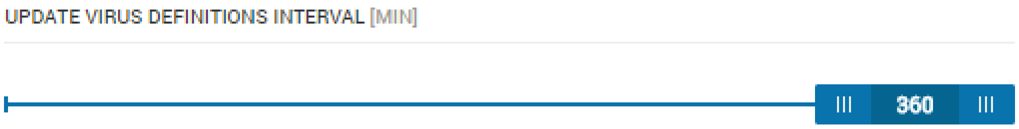
8.1.4.4 Threat types and differentiated threat response

Thor Vigilance differentiates between infected files and suspicious files. Suspicious files are the files that exhibit the behaviour of infected files (accessing the same memory areas, accessing other system files, etc…). You may define real time protection default response for both infected and suspicious files.

Please note that some files we are 100% sure to be malicious viruses get deleted automatically by the AV and are not even sent to quarantine.

8.1.4.5 Updating virus definitions locally

The slider that is shown in the general settings tab controls how often does the agent check to see whether there are new virus definitions files (VDF’s) within the Thor cloud. If a new VDF is available, this gets automatically downloaded to the local agent database.



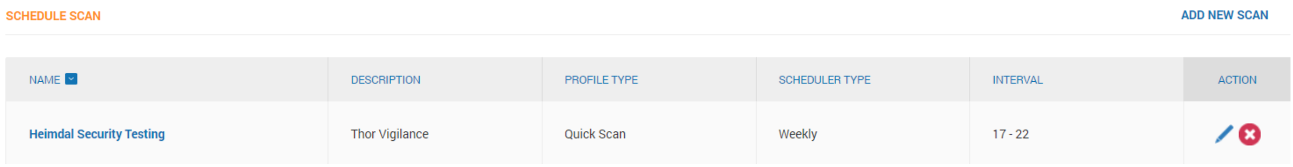
UPDATE VIRUS DEFINITIONS INTERVAL [MIN]

360

As designed, the minimum is set to 120 minutes, but it can also be increased up to 360 minutes if you need to keep your network traffic to a minimum. We wholeheartedly recommend that this setting is kept as low as possible (120 mins) so that checks are made often, and the latest virus definition files are immediately downloaded locally to identify and recognize threats as soon as they potentially reach the computer environment. Any delay in recognizing that a local file or files may potentially be dangerous could result in a viral infection that ultimately could have been avoided.

8.1.4.6 Creating and managing scan profiles

Defining scan profiles is crucial for the way the local Thor agent works. Basically the scan profile defines the way the local agent performs all the local scans. This includes the scan frequency, the target file location and the timeframe for performing the scheduled scans.



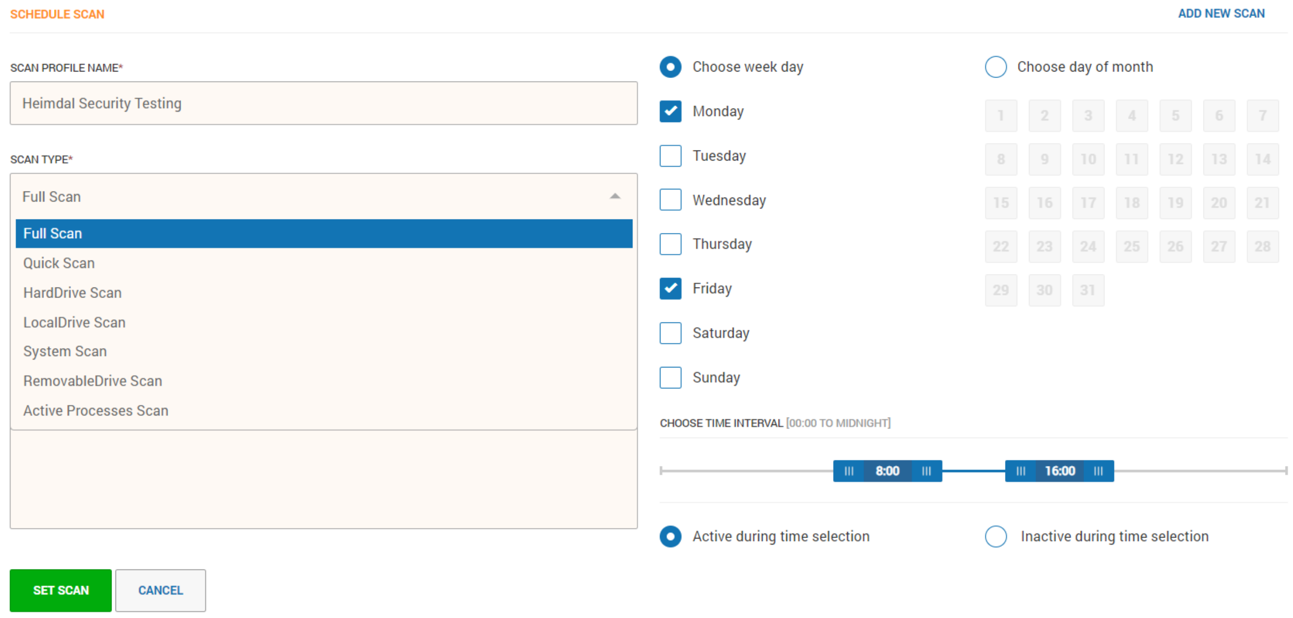
SCHEDULE SCAN

ADD NEW SCAN

NAME	DESCRIPTION	PROFILE TYPE	SCHEDULER TYPE	INTERVAL	ACTION
Heimdal Security Testing	Thor Vigilance	Quick Scan	Weekly	17 - 22	✎ ✖

As the printscreen below illustrates, there are a few scan types that can be used to create a new scan profile. These are consistent with common AV activity scenarios in a business environment. The administrator can choose between:

- **Full scan** – profile will scan all the local files on the endpoints that have the policy applied
- **Quick scan** – profile will scan critical OS locations and the most usual target folders which are known for virus activity
- **HardDrive scan** – profile will scan all files on the hard drive while ignoring the files on all external media types
- **LocalDrive scan** – profile will scan all files that are hosted on the partition hosting the OS
- **System scan** – profile will scan system files only
- **RemovableDrive scan** – profile will only scan for files that become accessible from external sources like flash drives
- **Active Processes Scan** – profile will only scan for processes currently running on the target machine



SCHEDULE SCAN

ADD NEW SCAN

SCAN PROFILE NAME*

Heimdal Security Testing

SCAN TYPE*

Full Scan

- Full Scan
- Quick Scan
- HardDrive Scan
- LocalDrive Scan
- System Scan
- RemovableDrive Scan
- Active Processes Scan

● Choose week day ○ Choose day of month

☑ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☑ Friday
☐ Saturday
☐ Sunday

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

CHOOSE TIME INTERVAL [00:00 TO MIDNIGHT]

8:00 – 16:00

● Active during time selection ○ Inactive during time selection

SET SCAN CANCEL

The scan profile also lets the administrator choose the timeframe for the scan to be performed.

Two schedule types are available: **weekly** and **monthly** and they allow the control of the timeframe in which the scans are performed. Monthly scans can be used in corporate environments where there are strict maintenance policies in regard to the timeframe when IT interventions can be performed. The scan timing can be controlled pretty strictly and it can be narrowed down to even the time interval when the scans can be performed.

When all options are configured to satisfy the scan profile behaviour, the set scan button can be used to create the scan profile.

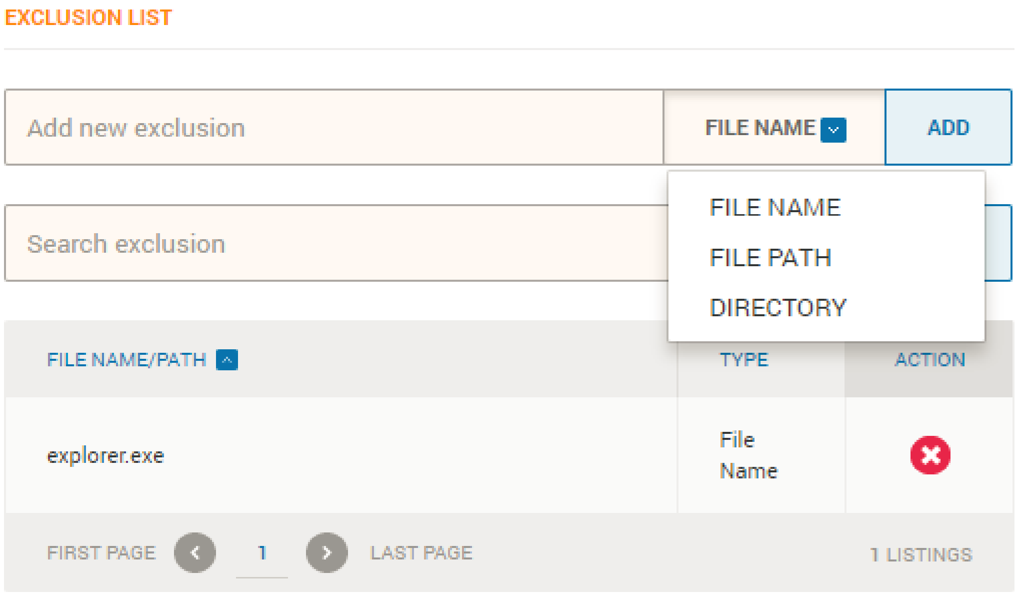
IMPORTANT!

- The scan profile does not apply automatically in the policy after clicking the "set scan" button. The administrator needs to confirm this by clicking the "update policy" button. If the update is not clicked, the defined scan profile will be lost if the current page is left before updating the policy.
- Multiple scan profiles can be created inside a single Thor Vigilance policy. However, the scan type is exclusive. This means that it is not possible to create multiple profiles with the same scan type. Example: no 2 scan profiles can be defined to perform full scans in the same policy.

8.1.4.7 Creating an exclusion list

An exclusion list in the policy works pretty much like a whitelist. The Thor Vigilance agent will ignore whatever the administrator decides to add in the exclusion list.

Multiple elements can be added in the exclusion list like file names, file paths and whole directories. The AV agent will not scan for threats inside the elements defined here. This can be used to whitelist processes for 3rd party software that are not supposed to be picked up as threats. The added exclusions can be searched and can be removed from the list if needed.

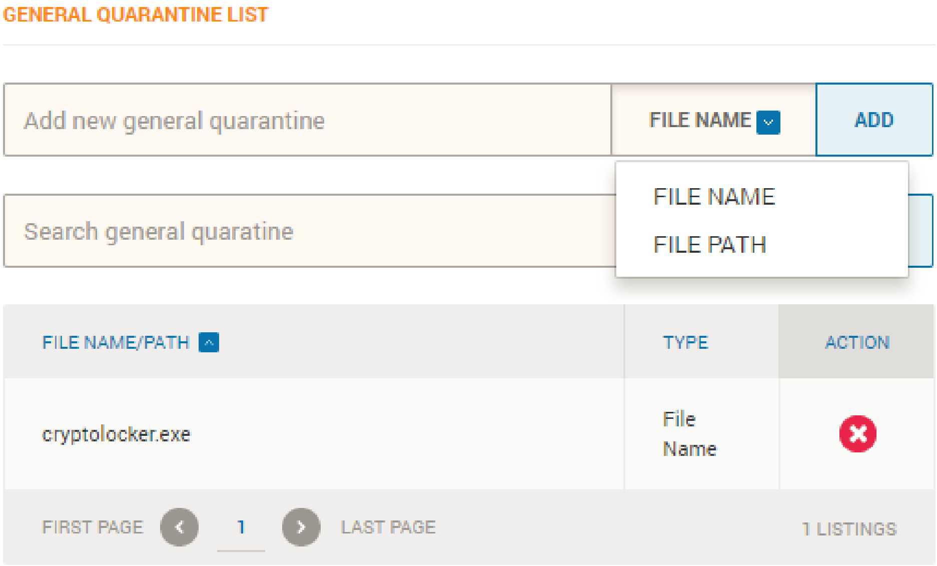


FILE NAME/PATH	TYPE	ACTION
explorer.exe	File Name	✖

8.1.4.8 Creating a general quarantine list

A general quarantine list works pretty much like a conventional blacklist. It is used to define a certain AV behavior when a certain file with a distinct file name is created on the hard drive. Also, it can be tweaked to only apply to files in a certain physical location.

Basically, the administrator is telling the agent that whenever a certain file name is found on the hard drive, the file gets automatically quarantined. As already stated, this is also valid for file paths: whenever a file is detected on a certain path, that file gets quarantined immediately.



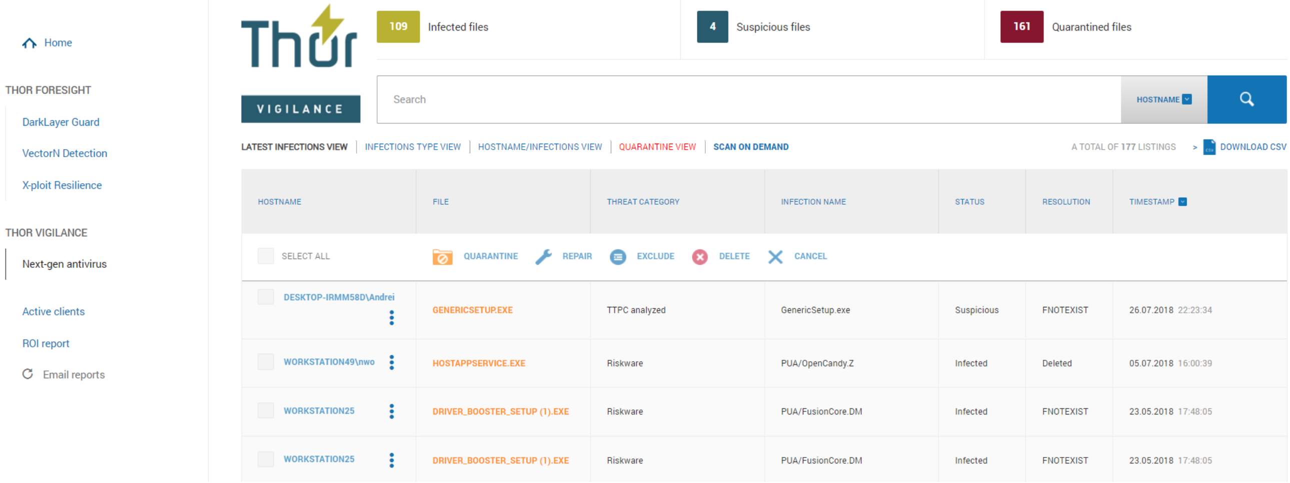
GENERAL QUARANTINE LIST

FILE NAME/PATH	TYPE	ACTION
cryptolocker.exe	File Name	✕

As with the exclusion list, the quarantine list can be searched and can be edited by the administrator.

8.1.4.9 Managing the AV detections

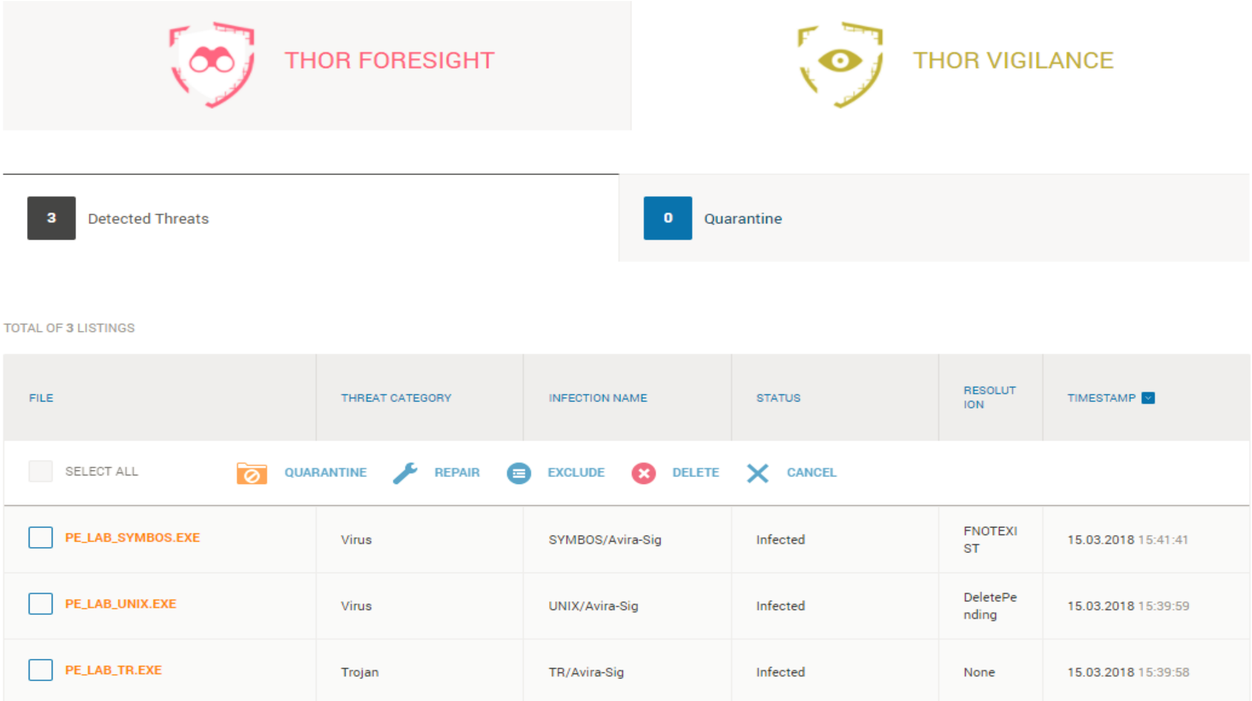
Once the policy was applied successfully and the AV has found infected or suspicious files, these are listed under the next-gen antivirus section of the Thor Vigilance module like in the below screenshot:



HOSTNAME	FILE	THREAT CATEGORY	INFECTION NAME	STATUS	RESOLUTION	TIMESTAMP
DESKTOP-IRMM58D\Andrei	GENERICSETUP.EXE	TTPC analyzed	GenericSetup.exe	Suspicious	FNOTEXIST	26.07.2018 22:23:34
WORKSTATION49\nwo	HOSTAPPSERVICE.EXE	Riskware	PUA/OpenCandy.Z	Infected	Deleted	05.07.2018 16:00:39
WORKSTATION25	DRIVER_BOOSTER_SETUP (1).EXE	Riskware	PUA/FusionCore.DM	Infected	FNOTEXIST	23.05.2018 17:48:05
WORKSTATION25	DRIVER_BOOSTER_SETUP (1).EXE	Riskware	PUA/FusionCore.DM	Infected	FNOTEXIST	23.05.2018 17:48:05

The view is compact, contains information about detected infections and shows the available actions that can be undertaken for each detected infection. You get details about the name of the infected file, the threat type and status. Depending on the status there are certain sets of actions that can be undertaken.

Once you click on an entry from the AV overview you can see all threats that have been registered under the host.

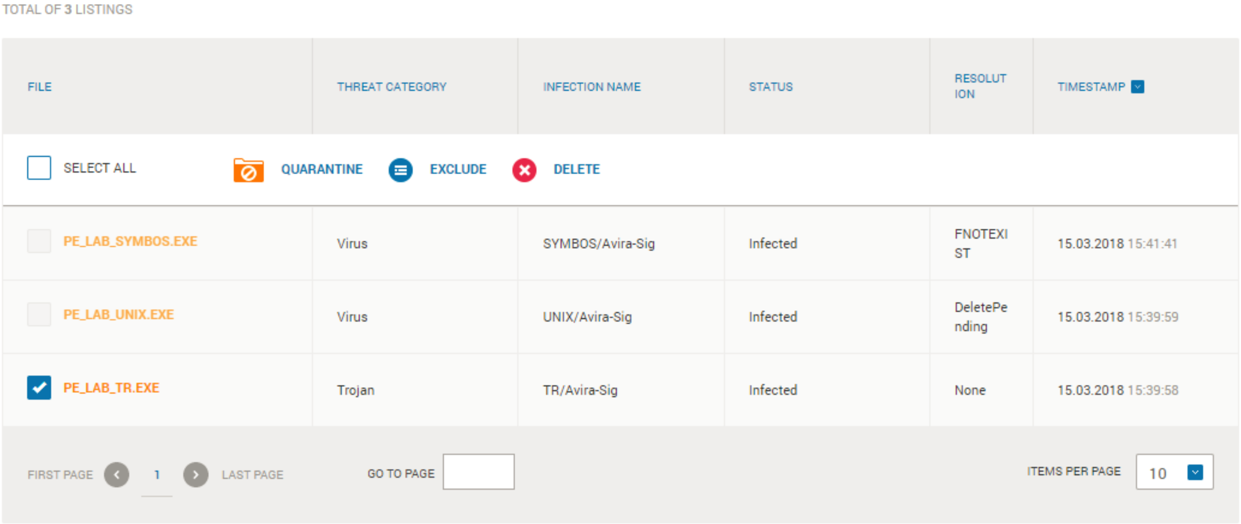


TOTAL OF 3 LISTINGS

FILE	THREAT CATEGORY	INFECTION NAME	STATUS	RESOLUTION	TIMESTAMP
□ PE_LAB_SYMBOS.EXE	Virus	SYMBOS/Avira-Sig	Infected	FNOTEXIST	15.03.2018 15:41:41
□ PE_LAB_UNIX.EXE	Virus	UNIX/Avira-Sig	Infected	DeletePending	15.03.2018 15:39:59
□ PE_LAB_TR.EXE	Trojan	TR/Avira-Sig	Infected	None	15.03.2018 15:39:58

Depending on the real time protection resolution, when selecting a threat there are multiple actions available:

- Quarantine
- Exclude
- Delete

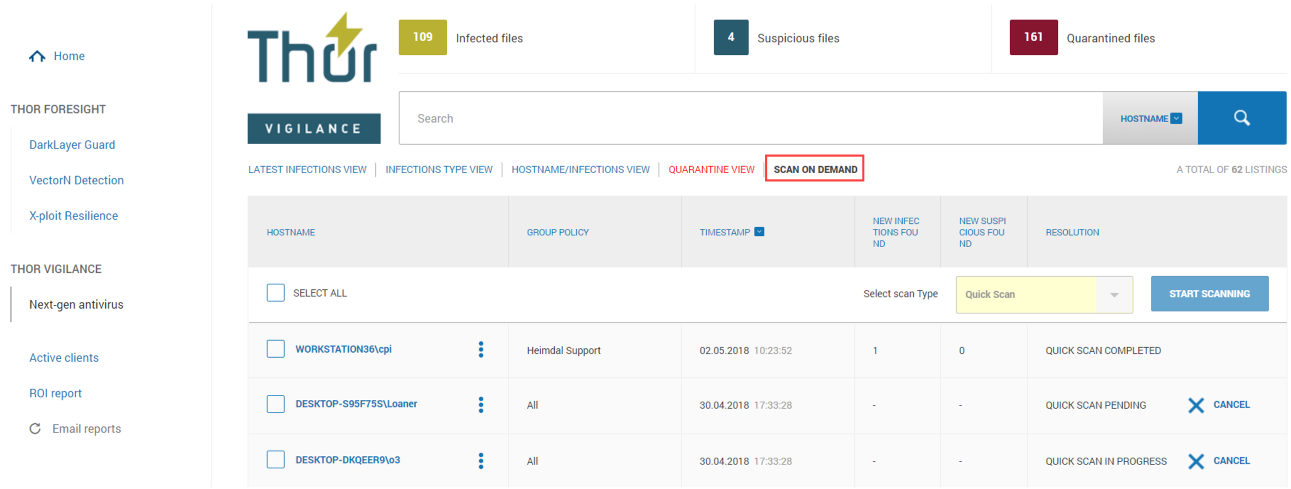


TOTAL OF 3 LISTINGS

FILE	THREAT CATEGORY	INFECTION NAME	STATUS	RESOLUTION	TIMESTAMP
□ PE_LAB_SYMBOS.EXE	Virus	SYMBOS/Avira-Sig	Infected	FNOTEXIST	15.03.2018 15:41:41
□ PE_LAB_UNIX.EXE	Virus	UNIX/Avira-Sig	Infected	DeletePending	15.03.2018 15:39:59
☑ PE_LAB_TR.EXE	Trojan	TR/Avira-Sig	Infected	None	15.03.2018 15:39:58

- First infected file has the FNOExist resolution which means that the file has already been removed from the host. The deletion was performed either by the user directly or by the Thor agent following a command from the dashboard. For this file there are no actions available
- The second infected file has been marked for deletion. The only available action is cancelation of the deletion
- The third infected file has the resolution “none” which means all actions are available for it: move to quarantine, exclude from detection or deletion.

From the Scan On Demand tab you can view a history of the actions that ran on the computers. Also, if there are any active or pending scans you can cancel them or you can just initiate any scan type on selected machines.



HOSTNAME	GROUP POLICY	TIMESTAMP	NEW INFECTIONS FOUND	NEW SUSPICIOUS FOUND	RESOLUTION
□ WORKSTATION36\cpi	Heimdal Support	02.05.2018 10:23:52	1	0	QUICK SCAN COMPLETED
□ DESKTOP-S95F75S\Loaner	All	30.04.2018 17:33:28	-	-	QUICK SCAN PENDING ✕ CANCEL
□ DESKTOP-DKQEER9\o3	All	30.04.2018 17:33:28	-	-	QUICK SCAN IN PROGRESS ✕ CANCEL

8.2 Active clients

For a PC to appear in the dashboard and to count as an active client it needs to use the following 3 identifiers. Thus it can generate a machine info to the dashboard.

- Hostname
- Motherboard serial
- HDD serial

Based on these 3 identifiers an endpoint gets identified and counts towards the total number of licenses available.

IMPORTANT

If one of the 3 components changes, it will be marked as a new endpoint in the dashboard because the machine info generated changes.

The Active Clients tab shows a list of the active workstations protected by Thor Enterprise using the same activation key. This module lets the administrator check which are the active clients. The administrator can list them and search after the following criteria: Hostname, IP Address, Agent Version, Operating System, Current Group Policy, Selected Group Policy, Last Seen and Status.

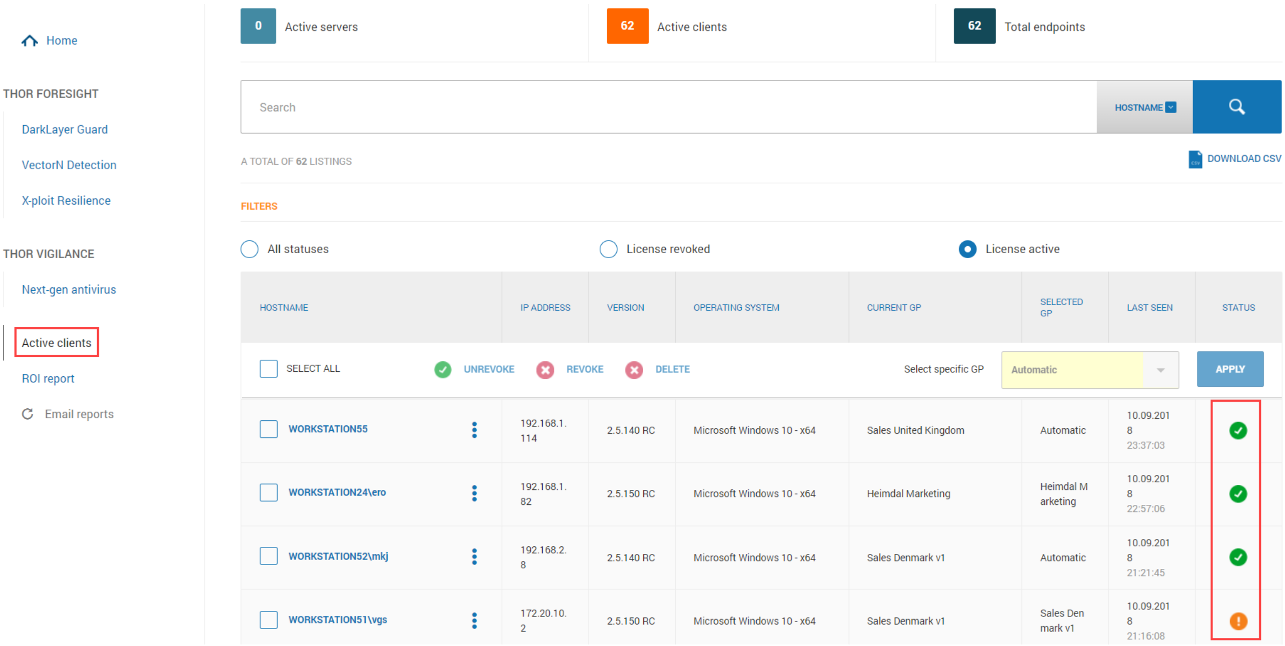
Total Endpoints – is the number of endpoints on which you have Thor installed to.

Active Clients – is the number of machines that are active and reporting in the Dashboard

Active Servers – is the number of servers that are active and reporting in the Dashboard

Last Seen – refers to when was the last time Thor was active on that endpoint.

Delete Button – is Active only for Admins (Heimdal Security Employees)



Home

THOR FORESIGHT

- DarkLayer Guard
- VectorN Detection
- X-ploit Resilience

THOR VIGILANCE

- Next-gen antivirus
- Active clients
- ROI report
- Email reports

0 Active servers | 62 Active clients | 62 Total endpoints

Search | HOSTNAME

A TOTAL OF 62 LISTINGS | DOWNLOAD CSV

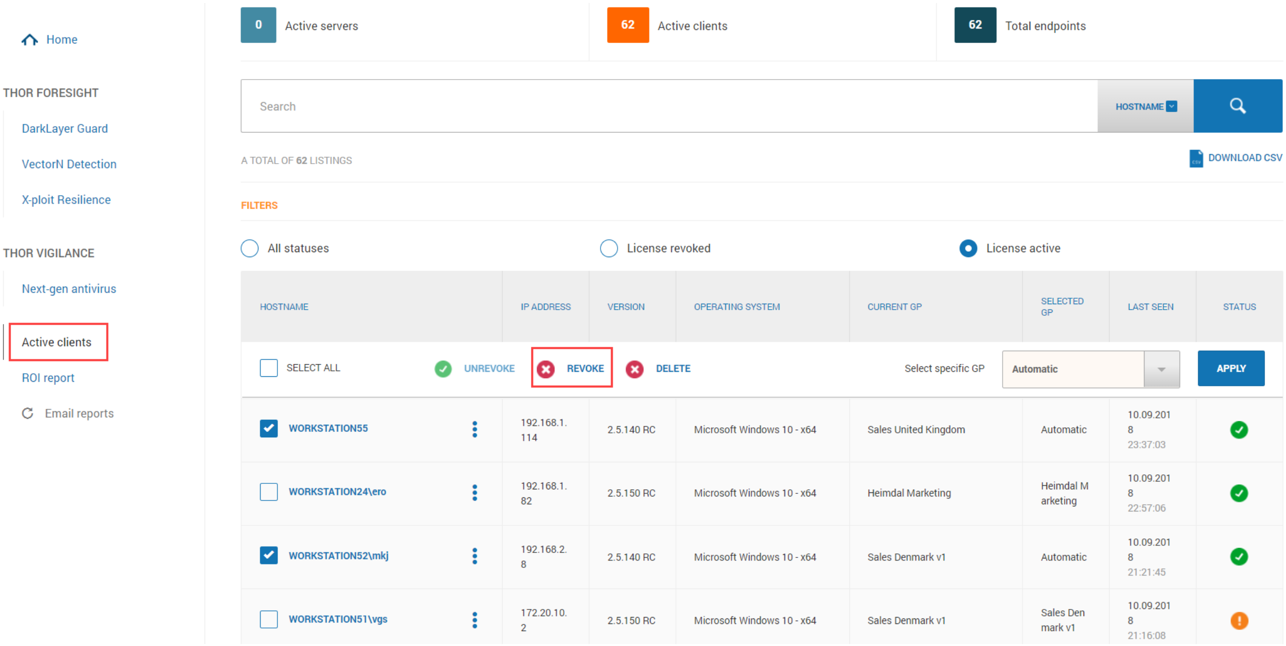
FILTERS

○ All statuses ○ License revoked ● License active

HOSTNAME	IP ADDRESS	VERSION	OPERATING SYSTEM	CURRENT GP	SELECTED GP	LAST SEEN	STATUS
□ SELECT ALL ✓ UNREVOKE ☒ REVOKE ☒ DELETE				Select specific GP	Automatic		APPLY
□ WORKSTATION55	192.168.1.114	2.5.140 RC	Microsoft Windows 10 - x64	Sales United Kingdom	Automatic	10.09.2018 23:37:03	✓
□ WORKSTATION24\ero	192.168.1.82	2.5.150 RC	Microsoft Windows 10 - x64	Heimdal Marketing	Heimdal Marketing	10.09.2018 22:57:06	✓
□ WORKSTATION52\mkj	192.168.2.8	2.5.140 RC	Microsoft Windows 10 - x64	Sales Denmark v1	Automatic	10.09.2018 21:21:45	✓
□ WORKSTATION51\vgs	172.20.10.2	2.5.150 RC	Microsoft Windows 10 - x64	Sales Denmark v1	Sales Denmark v1	10.09.2018 21:16:08	!

8.2.1 Revoke License Button

This option can be found on the Active Clients list.



Home

THOR FORESIGHT

- DarkLayer Guard
- VectorN Detection
- X-ploit Resilience

THOR VIGILANCE

- Next-gen antivirus
- Active clients
- ROI report
- Email reports

0 Active servers | 62 Active clients | 62 Total endpoints

Search | HOSTNAME

A TOTAL OF 62 LISTINGS | DOWNLOAD CSV

FILTERS

○ All statuses ○ License revoked ● License active

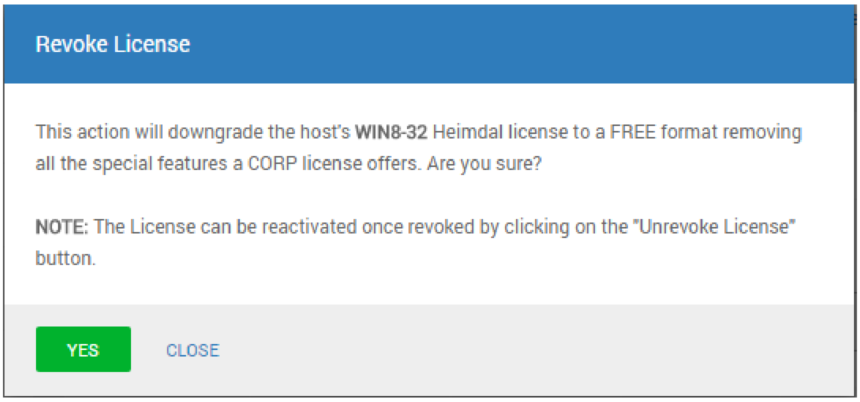
HOSTNAME	IP ADDRESS	VERSION	OPERATING SYSTEM	CURRENT GP	SELECTED GP	LAST SEEN	STATUS
□ SELECT ALL ✓ UNREVOKE ☒ REVOKE ☒ DELETE				Select specific GP	Automatic		APPLY
☑ WORKSTATION55	192.168.1.114	2.5.140 RC	Microsoft Windows 10 - x64	Sales United Kingdom	Automatic	10.09.2018 23:37:03	✓
□ WORKSTATION24\ero	192.168.1.82	2.5.150 RC	Microsoft Windows 10 - x64	Heimdal Marketing	Heimdal Marketing	10.09.2018 22:57:06	✓
☑ WORKSTATION52\mkj	192.168.2.8	2.5.140 RC	Microsoft Windows 10 - x64	Sales Denmark v1	Automatic	10.09.2018 21:21:45	✓
□ WORKSTATION51\vgs	172.20.10.2	2.5.150 RC	Microsoft Windows 10 - x64	Sales Denmark v1	Sales Denmark v1	10.09.2018 21:16:08	!

This option allows the Account Administrator to revoke the Thor usage rights on a certain Host/Machine. This means that, once the REVOKE LICENSE button will be clicked, **Thor** will **never** receive the information from the Policies set in the Dashboard *(you will be able to install Thor on that machine, but it will always revert to the FREE version since a policy cannot be applied)*

You access the feature by clicking the green checkmark in the STATUS column!

We recommend you use this option **ONLY** when a machine/computer **leaves** your organization (lost/ stolen, etc)

If you decide to revoke the license for specific clients, then click the green checkbox and you will be prompted to confirm this:

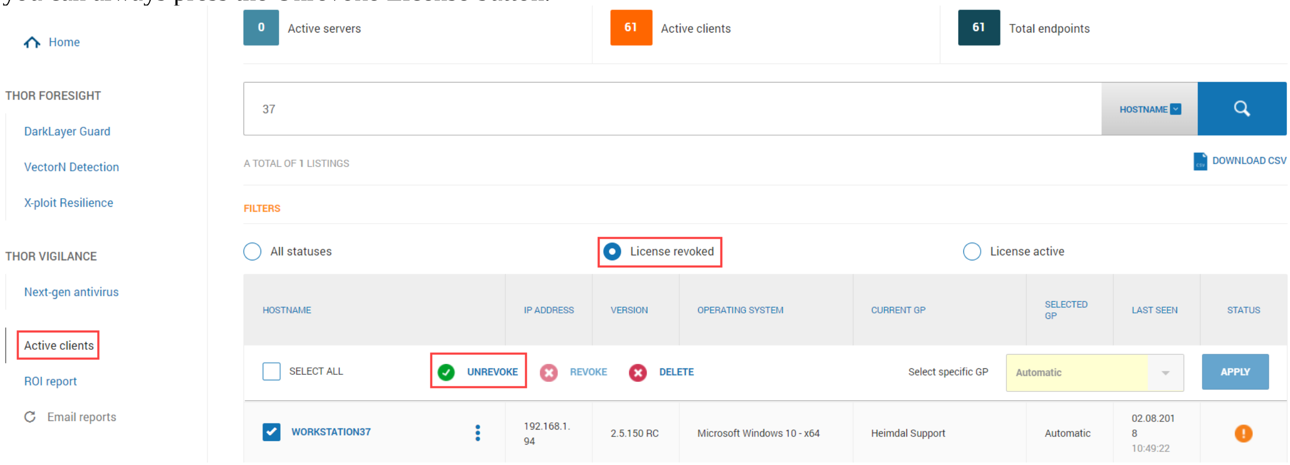


Revoke License

This action will downgrade the host's **WIN8-32** Heimdal license to a FREE format removing all the special features a CORP license offers. Are you sure?

NOTE: The License can be reactivated once revoked by clicking on the "Unrevoke License" button.

Once you pressed "Yes", the machine for which you revoked the license will stop receiving information from the Group Policy and it will not be updated correctly. If you pressed the Revoke button by mistake or you want to revert the action, you can always press the Unrevoke License button.



37

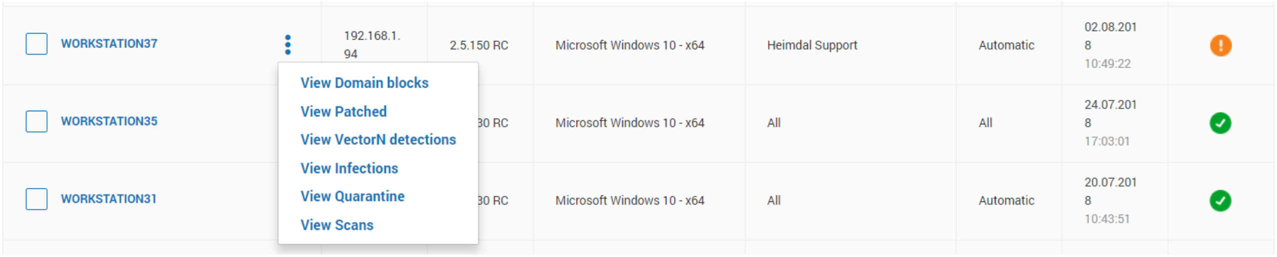
A TOTAL OF 1 LISTINGS

○ All statuses ● License revoked ○ License active

HOSTNAME		IP ADDRESS	VERSION	OPERATING SYSTEM	CURRENT GP	SELECTED GP	LAST SEEN	STATUS
□ SELECT ALL	UNREVOKE REVOKE DELETE				Select specific GP	Automatic	APPLY	
☑ WORKSTATION37	⋮	192.168.1.94	2.5.150 RC	Microsoft Windows 10 - x64	Heimdal Support	Automatic	02.08.2018 10:49:22	!

By pressing this button, the administrator will give all the rights back to the machine that was removed from the organization and after a reboot, the machine should receive again the Group policy the administrator has set in the Dashboard.

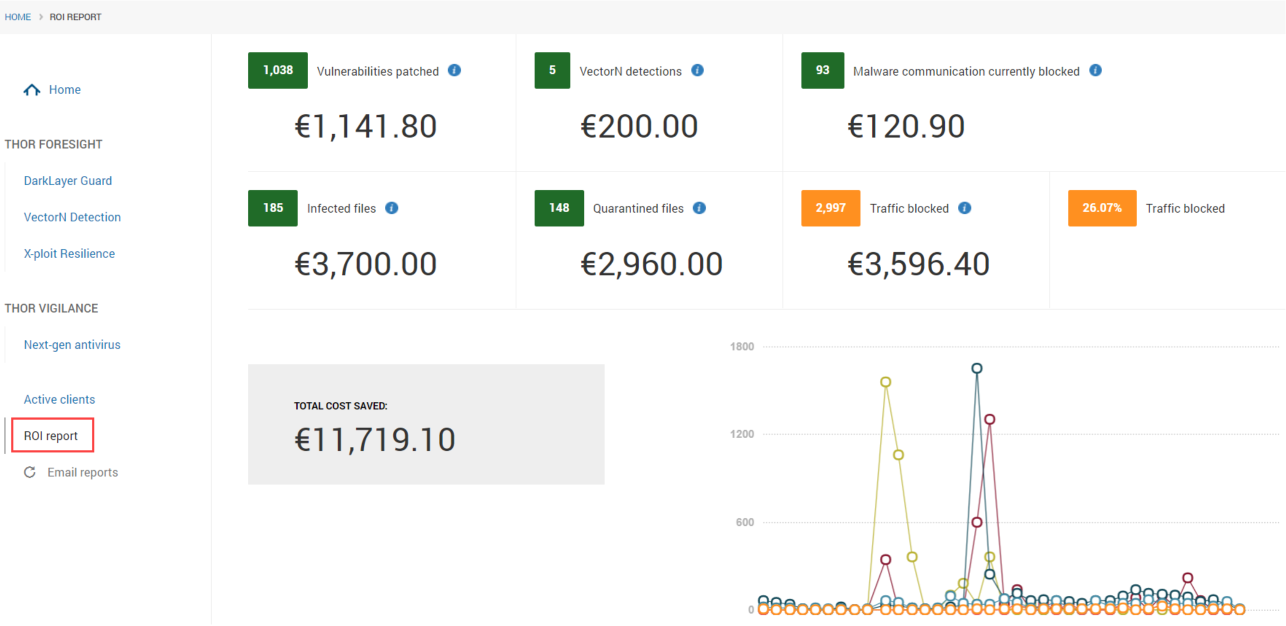
In any view where you can see list of computers, by clicking on the 3 dots next to the hostname a menu will be available that allows you to go to directly to various pages with details about the machine: Blocked Domains, Patches, VectorN detections, Infections, Quarantined files or to Scans.



□ WORKSTATION37	⋮	192.168.1.94	2.5.150 RC	Microsoft Windows 10 - x64	Heimdal Support	Automatic	02.08.2018 10:49:22	!
□ WORKSTATION35			30 RC	Microsoft Windows 10 - x64	All	All	24.07.2018 17:03:01	✓
□ WORKSTATION31			30 RC	Microsoft Windows 10 - x64	All	Automatic	20.07.2018 10:43:51	✓

8.3 ROI Report

The ROI Report tab depicts an estimated return on investment provided by Thor Enterprise in terms of financial resources saved by protecting the users and data in the environment monitored by Thor products.



HOME > ROI REPORT

Home

THOR FORESIGHT

DarkLayer Guard

VectorN Detection

X-ploit Resilience

THOR VIGILANCE

Next-gen antivirus

Active clients

ROI report

Email reports

1,038 Vulnerabilities patched €1,141.80	5 VectorN detections €200.00	93 Malware communication currently blocked €120.90
185 Infected files €3,700.00	148 Quarantined files €2,960.00	2,997 Traffic blocked €3,596.40	26.07% Traffic blocked

TOTAL COST SAVED:
€11,719.10

The ROI considers factors like cost per hour for employees when recovering data, overtime, and cost of bitcoin. If needed, we can provide on demand the algorithm used to calculate the ROI.

9. Miscellaneous

9.1 How can I activate my dashboard account?

You can ask your account manager about it. All we need is your email address and your IP. Please notice that you can access your account **only** from the IP provided. In case you need to access your account from a different location, just ask your account manager to add this new IP in your Dashboard account.

9.2 Heimdal ApiKey?

Please find details about the Heimdal API here: https://support.heimdalsecurity.com/hc/en-us/articles/115003784445-Heimdal-Security-ApiKey

9.3 Dashboard Login FAQ

On Android phones, when trying to download the app, you get the following error: "Google Play authentication is required".

Have a look at this guide: https://www.androidpit.com/how-to-fix-google-play-authentication-is-required-error

“Codes generated by the Authenticator do not work.”

This is most likely because it is not synced correctly. You can try the following:

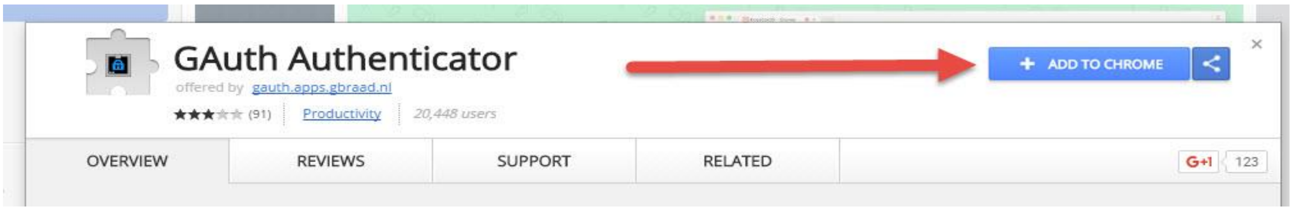
Go to the main menu on the Google Authenticator app:
Click Settings
Click Time correction for codes
Click Sync now

How can I synchronize the time on iPhone?
You can synchronize the time following these steps: Settings -> General -> Date & Time -> Set Automatically

9.4 How to use Google Authenticator on Google Chrome browser

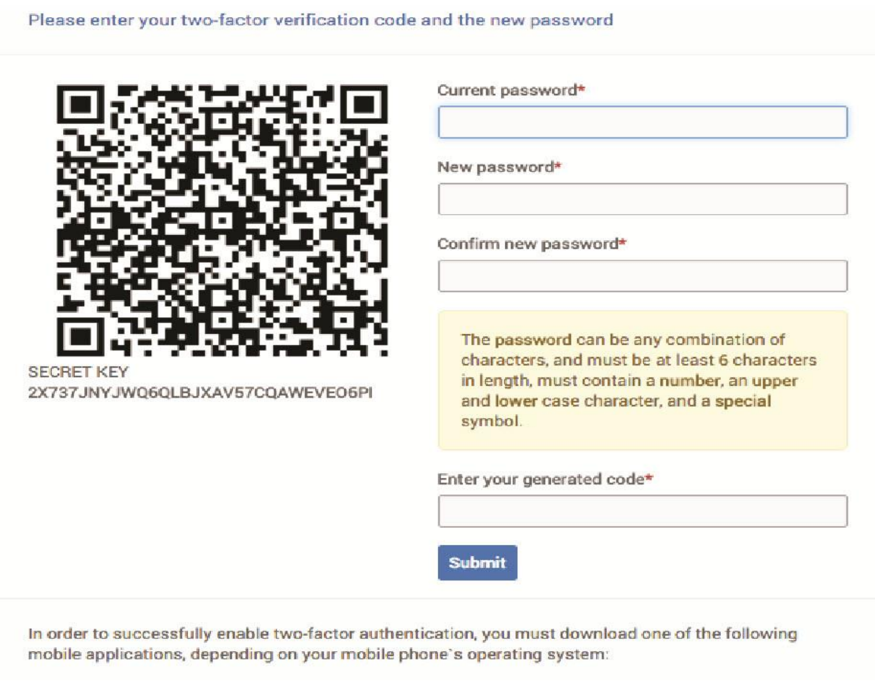
This guide will show you the steps you need to follow so you can add Google Authenticator to Chrome browser.

Step 1.
Click on: Download and add the GAuth Authenticator extension to the browser if asked to do so or click on the *Add to Chrome button > Add extension*



Step 2.

1. Now that the extension is added to the browser, open it and start configuring it: Click on the Thor Dashboard link: https://dashboard.heimdalsecurity.com/
2. Log in using the credentials sent by the account manager
3. After logging in, you’ll need to change your password.



Please enter your two-factor verification code and the new password

SECRET KEY
2X737JNYJWQ6QLBJXAV57CQAWEVEO6PI

Current password*

New password*

Confirm new password*

The password can be any combination of characters, and must be at least 6 characters in length, must contain a number, an upper and lower case character, and a special symbol.

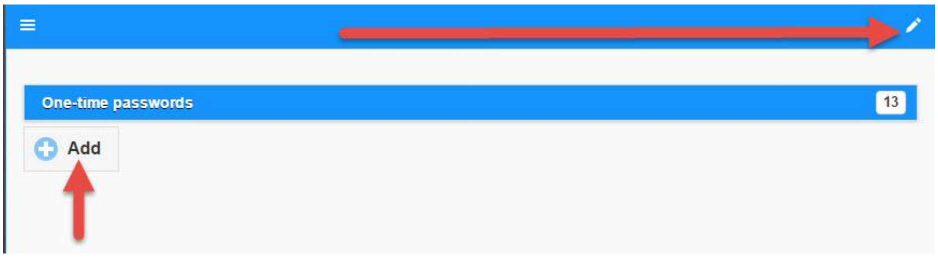
Enter your generated code*

Submit

In order to successfully enable two-factor authentication, you must download one of the following mobile applications, depending on your mobile phone`s operating system:

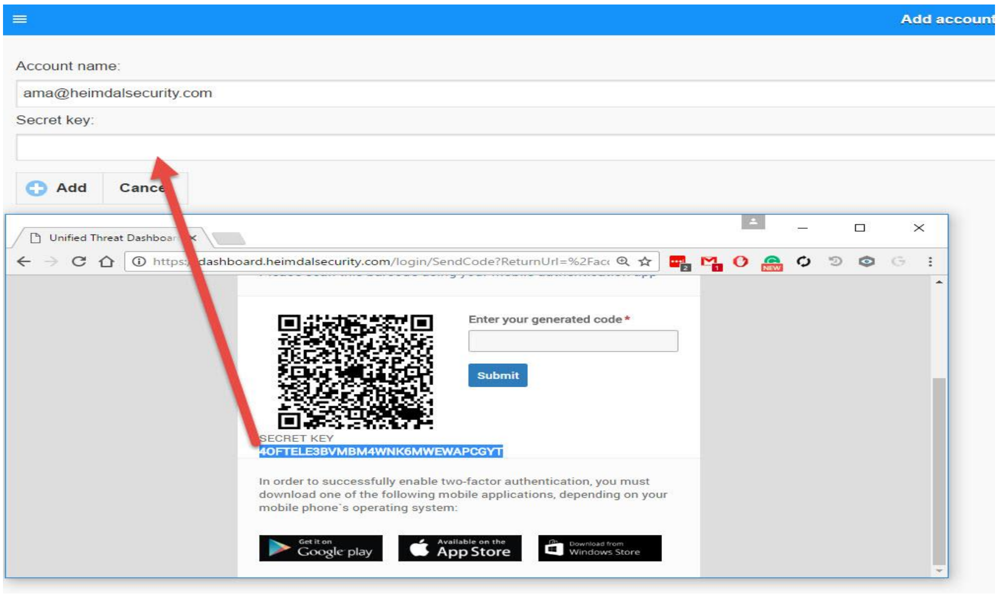
Step 3. While on this page, click on the GAuth Authenticator extension and click on the Pencil icon to begin adding the account.

Step 4. Next, click on the + *Add* and Insert the email address and the *Secret Code* is the one from the dashboard login page.



Step 5. After the *Secret Code* is inserted please press *Add*

- At this point, the Authenticator is set up on the browser.
- The Dashboard login page must not be closed or logged into yet.


Add account
Add
Cance
Unified Threat Dashboar
https://dashboard.heimdalsecurity.com/login/SendCode?ReturnUrl=%2Facc
Submit
Get it on Google play
Available on the App Store
Download from Windows Store

Account name: ama@heimdalsecurity.com

Secret key:

Enter your generated code *

SECRET KEY
4OFTELE3BVMBM4WNK6MWEWAPCGYT

In order to successfully enable two-factor authentication, you must download one of the following mobile applications, depending on your mobile phone`s operating system:

Step 6. Start generating the codes directly from the extension and use them to login the dashboard.

9.5 What is Thor RC?

Thor RC is the release candidate (beta version) that is in pre-production.

We recommend you install this version only if someone from the Heimdal Security team recommends you doing it. Otherwise, this version might cause issues in your organization because of its relative instability.

How can I upgrade to Thor RC? – Enterprise users

1. Open dashboard.heimdalsecurity.com.
2. Login to your account.
3. Select Group Policies.
4. Open the policy in which you want to activate and install Thor RC
5. Go to “General”
6. Enable “Include in the Release Candidate Program”.

Does Thor upgrade automatically when a new version appears?
And what happens if I already have Thor RC installed?

Yes, Thor updates itself automatically in one of the following scenarios:

A. If you have Thor 2.2.8 installed and version 2.2.9 is released, Thor will automatically update to version 2.2.9.
B. If you have Thor 2.2.8 RC and version 2.2.9 is released, Thor will automatically update to version 2.2.9.

Thor will NOT update itself automatically in the following circumstances:

If you have Thor 2.2.9 RC and version 2.2.9 is released, Thor will **not** automatically update to version 2.2.9.

Thor’s upgrade is based on the version number.

If Thor detects a **lower** version on the system, it upgrades automatically.
But if it detects a version that is **equal or higher** than the latest version released (2.2.9 in this example), Thor will not upgrade itself automatically the latest version.

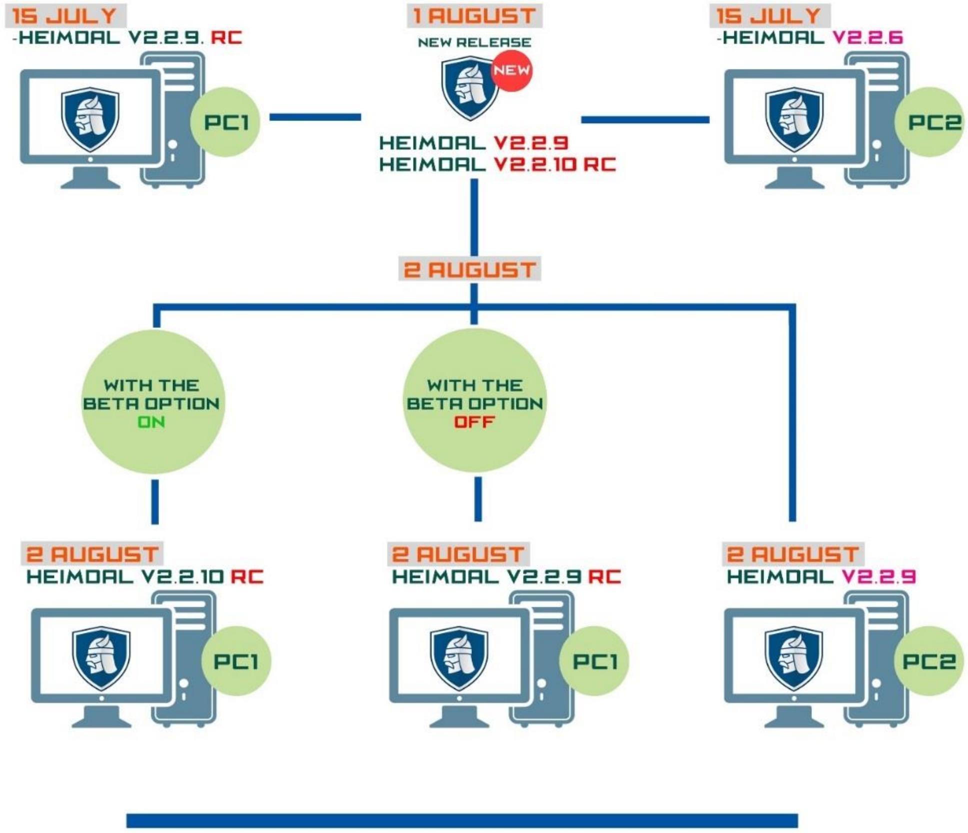
!!! The official update will always have a lower version number than the RC version (release candidate).

Example: If we launch Thor 2.2.9 official release, we will launch at the same time, Thor 2.2.10 RC. Consequently, the next official release version will be 2.2.10.

So, if you decide to use Thor 2.2.10 RC, when version 2.2.10 will official be released, Thor 2.2.10 RC will **not** be automatically updated.

If the current version installed on the endpoint is **equal** to the RC version, the automatic update will **not** happen: 2.2.10 RC will NOT update to 2.2.10 official release.

If the current version installed on the endpoint is **lower** to the RC version, the automatic update **will** happen: 2.2.9 RC will update to 2.2.10 official release.



*Having a set of endpoints that constantly run the RC (Release Candidate) version of Thor can greatly help you anticipate potential issues that Thor might cause organization-wide, before releasing a new version to all your endpoints.

As a result, we recommend that the administrator enrolls 1-2% of the active endpoints into a separate Active Directory group. A specific group policy can be set to that set of endpoints, for them to always run the RC version of Thor.
Our support team will always be within reach, so we can work out the potential issues and ensure that your organization is making the most of what Heimdal Security products have to offer!

9.6 Thor Vigilance in relationship to other AV products

As a rule of thumb, please always consider that generally speaking two AV products are not compatible if ran on the same host. Always consider uninstalling the currently residing AV product from the machines before deploying Thor Vigilance in your environment.

Each time you deploy Vigilance into an environment that has previously been protected by an AV product, a restart is required to finish the uninstallation of the former residing AV product. The restart will also trigger the download of VDFs (Virus Definition Files) from our cloud.

If you deploy into an environment that has not been previously protected by an AV product, the restart is NOT mandatory and the installation should proceed without any issues.

9.6.1 Thor Vigilance versus Windows Defender (WD) and System Center Endpoint Protection (SCEP)

By default, installing Thor Vigilance on a system that is protected ONLY by WD, this will result in WD being disabled automatically. (No matter the OS: Windows 7, 8 or 10)

On Windows 10 Operating Systems, installing Thor Vigilance on a machine that is protected by Windows Defender and System Center Endpoint Protection, this will result in the Microsoft solutions (both WD and SCEP) automatically being turned off. This is largely due to the fact that after the Windows 10 1803 Release, both WD and SCEP became integrated.

On Windows 7 and 8 Operating Systems, installing Thor Vigilance on a machine that is protected by Windows Defender and System Center Endpoint Protection, this will result in WD being turned off, but SCEP will still be turned on. Thor Vigilance and SCEP will be running side by side BUT Vigilance will have the priority at detecting and removing viruses and SCEP will have nothing to detect.

It is therefore our recommendation that if you are using SCEP on Windows 7 or 8, you disable it centrally or uninstall it completely prior to installing Vigilance.