



HEIMDAL™
SECURITY



HEIMDAL™ SECURITY

PRODUCT DOCUMENTATION

Technical specifications and Implementation
guide for corporate environments.

2021



1. Table of content

1. Table of content.....	2
2. Introduction	6
3. Who is Heimdal Security.....	6
4. What are the Heimdal Security products	6
4.1 Heimdal™ Threat Prevention	6
4.2 Heimdal™ Patch and Asset Management	7
4.3 Endpoint Detection	7
4.4 Heimdal™ Forensics.....	7
4.5 Heimdal™ Privileges and App Control	8
4.6 Heimdal™ Email Protection	8
4.6.1. Email Security	9
4.6.2 Email Fraud Prevention	9
5. Minimum System Requirements for Heimdal™ Security products	11
5.1 PC rights.....	11
5.2 Resource usage.....	11
5.3 What system changes do apply when installing Thor Enterprise?.....	12
5.4 Software compliance	12
5.5 Web based administration module	13
6. Function description	13
6.1 Installation of Thor Products	13
6.1.1 Installation Process and usage environments	14
6.1.1.1 Installation via offline MSI file	14
6.1.1.2 Install Thor with no GUI.....	14
6.1.2 Creating adapted MSI installation files	15
6.1.2.1 Orca pre-configuration	16
6.1.2.2 The MSI editing process	17
6.1.3 Deployment of Thor through Active Directory Group Policy Management	19
6.2 AD group binding for Thor.....	27
6.2.1 Thor's Group policies without AD groups	27
6.2.2 Thor's Group policies with AD groups.....	28
6.2.2.1 Applying differentiated Thor policies across distinct AD computer groups.....	28
6.2.2.2 How can I distribute a policy to an AD User group?.....	29
6.2.2.3 Apply a Group Policy based on "ComputerTags" and "UserTags"	29
6.2.2.4 Changing group policy priority	29
6.3 Using Thor while behind an authentication proxy	30
6.4 Internet WebServers for use with Heimdal™ Threat Prevention - Endpoint.....	31



6.5	Static\Dynamic IP DNS Environments Settings for Thor	31
6.6	Virtualization environments	31
6.7	Using Thor in VPN environments – VPN compatibility.....	31
6.7.1	Using Thor with Cisco AnyConnect VPN.....	32
6.7.2	Using Thor with GlobalProtect from Palo Alto	32
6.7.3	Using Thor with VPN clients that modify the DNS settings in the NIC (ex. FortiGate from Fortinet)	33
6.8	Usage on Terminal servers or Citrix servers	33
6.9	Usage on Remote Desktop servers and SQL servers	34
6.10	Internet Protocol Version	34
6.11	Peer to Peer	35
6.12	Uninstall Protection for Thor products	36
7.	Features.....	37
7.1	Features of Heimdal™ Threat Prevention - Endpoint	37
7.1.1	Peer To Peer transfer	37
7.1.2	Traffic check – Malicious websites, zero-day exploits and data ex-filtration	37
7.1.3	Technical Implementation.....	37
7.1.4	Category blocking views in Threat Prevention Endpoint	38
7.2	Features for Heimdal™ Patch & Asset Management	39
7.2.1	Heimdal™ Patch & Asset Management.....	39
7.2.2	The list of supported software	39
7.2.3	Technical implementation.....	39
7.2.4	Software that already has auto update enabled.....	40
7.2.5	Patches deployment method – Bulk or Staged?	40
7.2.6	Uninstall Application Feature for ENTERPRISE clients	41
7.2.7	Patch & Asset Management.....	41
7.2.8	Windows Updates	41
7.3	Features for Heimdal™ Endpoint Detection.....	42
7.3.1	Next Gen Antivirus.....	42
7.3.2	Firewall Management.....	42
7.3.3	Ransomware Encryption Protection.....	42
7.3.4	Mobile Device Management	42
7.4	Features for Heimdal™ Privileges & App Control.....	43
7.4.1	Privileged Acces Mgmt	43
7.4.2	Application Control.....	43
7.5	Forensics	47
7.6	Email Protection	47
7.6.1	Spam Score interval.....	47



7.6.2 Show details button	48
8. Managing the dashboard interface for Thor Products	50
8.1 Account activation and install	51
8.2 Group policies.....	52
8.3 Management interface for Heimdal™ Threat Prevention.....	53
8.3.1 VectorN Detection.....	53
8.3.2 Assets View.....	57
8.3.3 Microsoft Updates.....	59
8.3.4 Threat Prevention Endpoint	62
8.3.5 Forensic view	65
The new view can be found on the left side of the menu:.....	65
8.3.6 Management interface for Heimdal™ Next-Gen Antivirus, Firewall & MDM	66
8.3.6.1 Activation of Heimdal™ Next-Gen Antivirus	66
8.3.6.2 Network and archive scan	68
8.3.6.3 What is the protection cloud?	68
8.3.6.4 Threat types and differentiated threat response.....	68
8.3.6.5 Updating virus definitions locally	68
8.3.6.6 Creating and managing scan profiles	69
8.3.6.7 Creating an exclusion list.....	70
8.3.6.8 Creating a global quarantine list	71
8.3.6.9 Managing the Antivirus detections	71
8.4 Heimdal™ Management.....	73
8.4.1 Active Clients	73
8.4.2 Revoke License Button	74
8.4.3 ROI Report	77
9. Heimdal™ Email Protection	78
9.1 Heimdal™ Email Fraud Prevention	78
9.2 Heimdal™ Email Security	78
10. Miscellaneous.....	78
10.1 How can I activate my dashboard account?	78
10.2 Heimdal™ ApiKey?.....	78
10.3 Dashboard Login FAQ.....	78
10.4 How to use Google Authenticator on Google Chrome browser?	79
10.5 What is Thor RC?	80
10.6 Heimdal™ Next-Gen Antivirus, Firewall & MDM in relationship to other AV products.....	82
11.6.1 Heimdal™ Next-Gen Antivirus, Firewall & MDM versus Windows Defender (WD) and System Centre Endpoint Protection (SCEP)	82
10.7 Where does Heimdal save information in Windows registry?.....	82





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: **Heimdal™ Threat Prevention**, **Heimdal™ Endpoint Detection**, **Heimdal™ Patch and Asset Management**, **Forensics**, **Heimdal™ Privileges & App Control** and **Heimdal™ Email Protection**. 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. Heimdal™ Threat Prevention – Endpoint can be regarded as the product branch which is minimizing threats, closing loopholes in the security of applications and filtering unsafe traffic, while Heimdal™ Next-Gen Antivirus & MDM 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 Heimdal™ Threat Prevention

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.

Heimdal™ Threat Prevention 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: **Threat Prevention Endpoint** and **Vector^N Detection**.



4.2 Heimdal™ Patch and Asset Management

Heimdal™ Patch & Asset Management is designed to have low resource consumption, using as few system resources as possible and works without interrupting the user. Heimdal™ Patch & Asset Management works with our own CDN so pushing new software and updates is fast and reliable. The module identifies and automatically updates 3rd Party Software on any computer and consist two active modules: Patch Management and Infinity Management.

4.3 Endpoint Detection

This product includes the following modules: Heimdal™ Next-gen Antivirus, Firewall and MDM & Ransomware encryption.

Heimdal™ Next-Gen Antivirus & MDM 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 Heimdal™ Threat Prevention 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.

The new **module 'Ransomware encryption Protection'** has the purpose to detect processes that encrypt files on the endpoint with a malicious intent.

Learn more on Ransomware Encryption Protection here: <https://support.heimdalsecurity.com/hc/en-us/articles/360017671857-Ransomware-Encryption-Protection->

4.4 Heimdal™ Forensics

Heimdal™ Forensics helps you keeping the evidences of program execution on Windows systems.

During a forensic analysis of a Windows system, it is often critical to understand when and how a particular process has been started.

In order to identify this activity, we can extract from the target system a set of artifacts useful to collect evidences of program execution.

You can find the module in main Menu of the Dashboard, on the left side.





By accessing it, the user will be redirected to the main view, where it will see the list with all alerts gathered:

Forensics

166 Alerts

Search by Process

Process

Executions (160)

Download CSV

	Process	Process ID	VirusTotal	Hostname	Local IP	Remote IP	Source	Score	Session ID
<input type="checkbox"/>	Teams.exe	8076	-		-	-	DarkLayerGuard	30	1
<input type="checkbox"/>	chrome.exe	16612	-		-	-	DarkLayerGuard	30	1
<input type="checkbox"/>	Teams.exe	13308	-		-	-	DarkLayerGuard	30	1
<input type="checkbox"/>	Teams.exe	13220	-		-	-	DarkLayerGuard	30	1
<input type="checkbox"/>	chrome.exe	10992	-		-	-	DarkLayerGuard	30	1
<input type="checkbox"/>	c:\users\lme\appdata\local\packages\microsoft.windowscommunicationsapps_8wekyb3d8bwe\localstate\files\ad31attac hments\piatona bulk(9971).eml	0	-		-	-	Antivirus	40	0

For more details, please take a closer look on the following article:

4.5 Heimdal™ Privileges and App Control

This product includes the following modules: Privileged Access Mgmt & Application Control.

Privileged Access Mgmt - the feature that allows an end-user to request **admin** access over his machine by sending a request to the System Administrator that can deny or accept his request. The length of the session is limited and all his actions are logged into the Dashboard.

Learn more about Privileged Access Mgmt here: <https://support.heimdalsecurity.com/hc/en-us/articles/360004572638--Heimdal-Privileged-Access-Management-overview>

Application Control - is a module created to control which processes (or applications) can be executed on client machines and how they are executed. You can define a set of rules that describe what processes are allowed or blocked on your machines (in your environment) using details like Software Name, Paths, Publisher, MD5, Signature, or Wildcard Paths. Application Control can handle how a process (it can get automatic elevation from the Heimdal™ Privileged Access Management module, if so configured) or child process (it can allow or block all processes spawned by the process defined by the rule) should run.

Learn more on Application Control here: <https://support.heimdalsecurity.com/hc/en-us/articles/360016091937-Application-Control-overview>

4.6 Heimdal™ Email Protection

This product includes the following modules: Email Security & Email Fraud Prevention.

Heimdal™ Email Protection is the feature that allows you to scan and prevent email fraud.

Heimdal™ Email Protection is an independent module, like Heimdal **Antivirus** or **Threat Prevention Endpoint**. This module will intercept all outlook emails from **Inbox** and **Sent** folder. The module should start when to install Heimdal or refresh group policy if Heimdal™ Email Protection is ON in group policy and outlook is open. If no outlook instance



is open in the current moment, the module will check every 5 minutes if outlook has been opened and try to start Heimdal™ Email Protection module.

For intercepting emails, we created a secondary app named **MailSentryMonitor**. If this app is closed, the module will try to start it, checking its connection every 10 minutes. Also, if Heimdal™ Email Security service is closed, this secondary app should be closed.

Heimdal™ Email Protection will intercept every mail from Inbox and Sent folder and send it for validation. A partial response is received in 10 minutes and a final result will be received in 24 hours. If final/partial status is Infected, mail will be moved to **Heimdal - MailSentry** subfolder from **Inbox**. If the mail was initially infected (moved to **Heimdal - MailSentry** and then in the final result it is considered uninfected, the mail will be moved back to the original folder.

4.6.1. Email Security

Email Security can be found in the Heimdal Dashboard under the EMAIL PROTECTION section.

In the below view, you are able to see all your Inbound and Outbound emails, but also the Domain Status of the domains set up on your account. The Inbound/Outbound View displays a table with all inbound/outbound emails, the recipient, the sender, the timestamp, the email subject, the action, the email status, and the details of each email:

	To	From	Timestamp	Subject	Type	Status	Details
<input type="checkbox"/>			19.04.2021 10:49:55	Test 2	NORMAL	DELIVERED	Show Details
<input type="checkbox"/>			16.04.2021 19:50:58	Test 34	NORMAL	DELIVERED	Show Details
<input type="checkbox"/>			16.04.2021 19:45:59	Test 3	NORMAL	DELIVERED	Show Details
<input type="checkbox"/>			16.04.2021 19:42:18	EXTERNAL Test signature	NORMAL	DELIVERED	Show Details
<input type="checkbox"/>			19.04.2021 19:13:27	Test	NORMAL	UNDELIVERED	Show Details

Learn more on Email Security here: <https://support.heimdalsecurity.com/hc/en-us/articles/360007435238-Heimdal-Email-Protection>

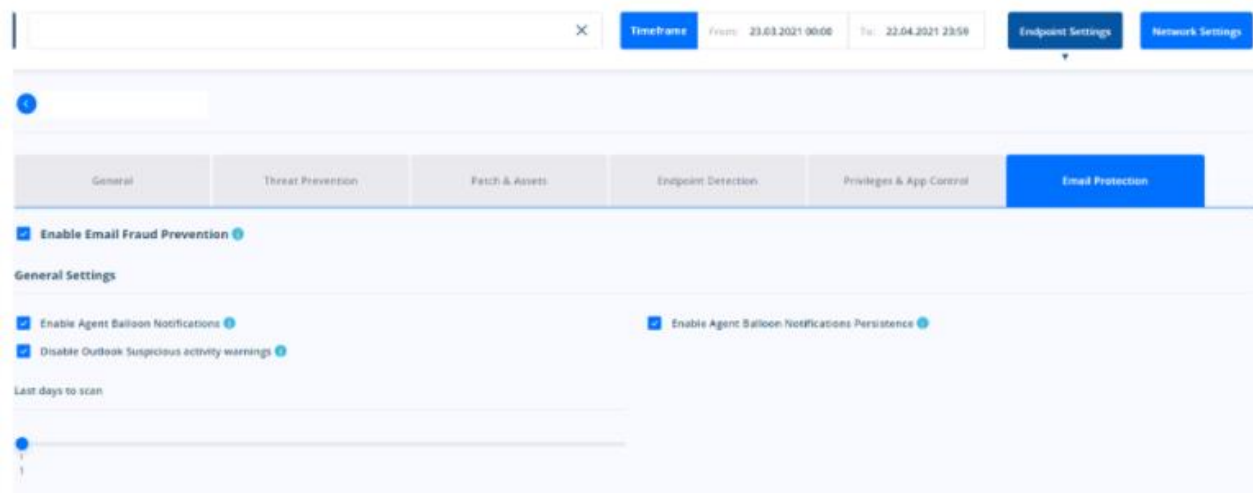
4.6.2 Email Fraud Prevention

Heimdal™ Email Fraud Prevention scans and prevents email fraud by intercepting Inbound and Outbound communications, comparing them with pre-registered signatures, and detecting whether changes have been



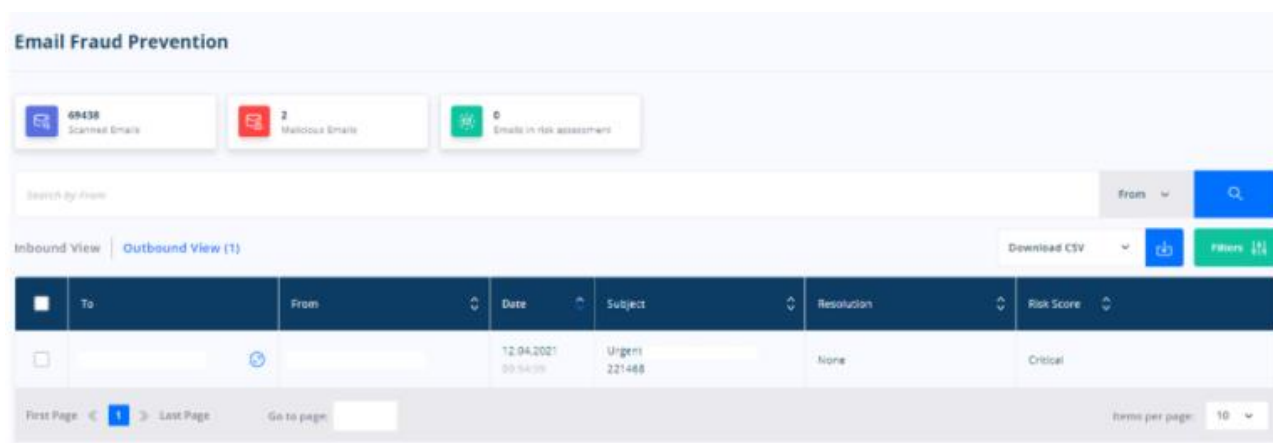
operated or not. This helps flag down the BEC attacks before they have a chance of convincing you to hand over sensitive info.

In order to activate the module, you need to go on your **Endpoint Settings - Email Protection** section:



Heimdal™ Email Fraud Prevention will intercept every email from the **Inbox** and **Sent** folders and send it for validation. A partial response is received in 10 minutes and a final result will be received in 24 hours. If the final/partial status is **Infected**, the email will be moved to **Heimdal - Heimdal™ Email Fraud Prevention** subfolder under the **Inbox** folder. If the email was initially infected (moved to **HeimdalInfectedMails**), and then it is considered uninfected in the final result, the email will be moved back to the initial folder.

Information about Heimdal™ Email Fraud Prevention performances can be seen in the dashboard if you click **Heimdal™ Email Fraud Prevention** from the left menu of the Heimdal Dashboard homepage:



Learn more on Email Fraud Prevention here: <https://support.heimdalsecurity.com/hc/en-us/articles/360004581377-Heimdal-Email-Fraud-Prevention>



5. Minimum System Requirements for Heimdal™ Security products

Please see the following article: [What Are The System Requirements For Heimdal™ Agent?](#)

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:

Installation of Thor Enterprise
Automatic update of Thor Enterprise
Patching 3rd party software*
Threat Prevention Endpoint
Reboot or restart of Thor Enterprise
Manual starting of Thor Enterprise
Changing locked setting for Thor suite in the Enterprise version

Required user rights:

Local/ Domain administrator
Local user
Local user
Local user
Local/ Domain administrator
Local/ Domain administrator
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:

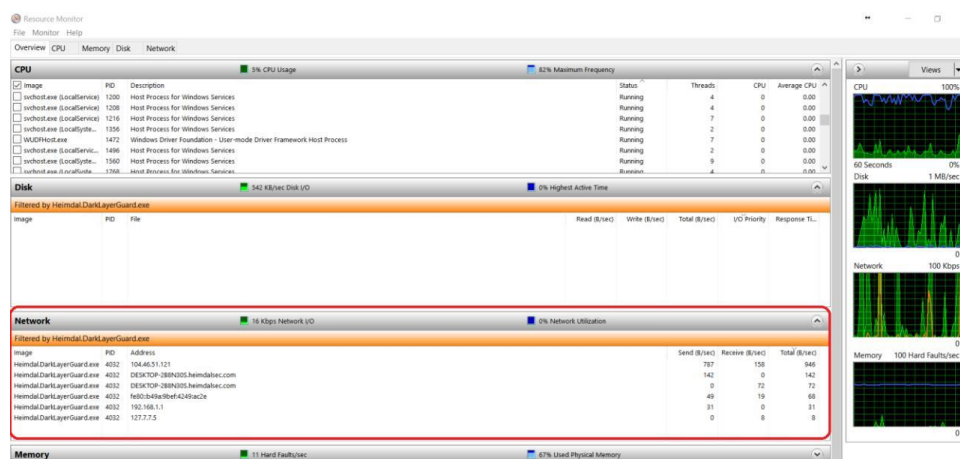
Component:

HeimdalAgent.exe
Heimdal Client Host
Heimdal Threat Prevention Endpoint*
Heimdal Uptime Checker
Heimdal Antivirus
Heimdal Update Service
Heimdal Security Service Monitor
Heimdal™ Privileged Access Management
Heimdal Firewall
Heimdal™ Email Security

Component type:

Application
Service
Service
Service
Service
Service
Task Scheduler
Service
Service
Service

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





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 **Threat Prevention Endpoint** 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? – Heimdal Security](#)

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 Heimdal™ Next-Gen Antivirus, Firewall & MDM is a fully-grown antivirus solution, incompatibilities may arise between this product and the AV that you are currently using. If you use the **Heimdal™ Next-Gen Antivirus, Firewall & MDM** product, you should not have any other AV solution installed on your endpoints.

If you are **only** using the **Heimdal™ Threat Prevention** product, you will not have any incompatibility between it and any pre-existing AV solution.

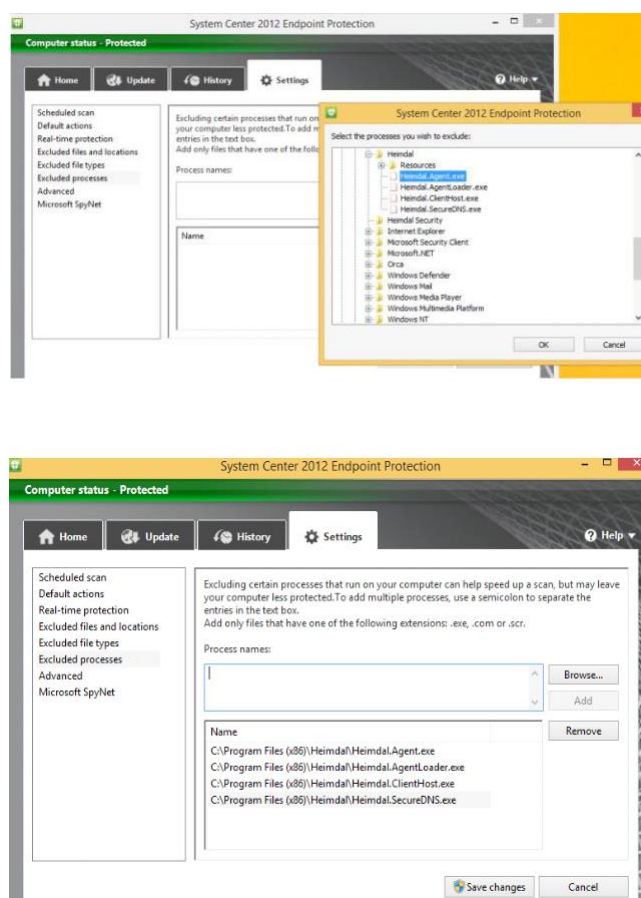
If a **Firewall** or a **Proxy** is installed on the Client, you have to make sure Thor is allowed to communicate with our servers online. To create a rule in your Firewall, Thor needs to be able to access these domains:

- 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:



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 HeimdalTM Next-Gen Antivirus, Firewall & MDM 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: [Heimdal Latest Version](#)

*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:*

[Heimdal Latest Version - RC](#)

*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"`

```
Administrator: Command Prompt
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 [6.1](#))
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**"

Additional Settings

- ☒ Include in Release Candidate Program
- ☒ Do not show GUI
- *Changes will take effect after restart
- ☒ Skip prompting the client when requesting logs ⓘ
- ☐ Only merge with AD groups specific policies ⓘ
- ☐ Enforce uninstall password ⓘ
- ☒ Synchronize with time server ⓘ
- ☐ Enable Wake on LAN

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

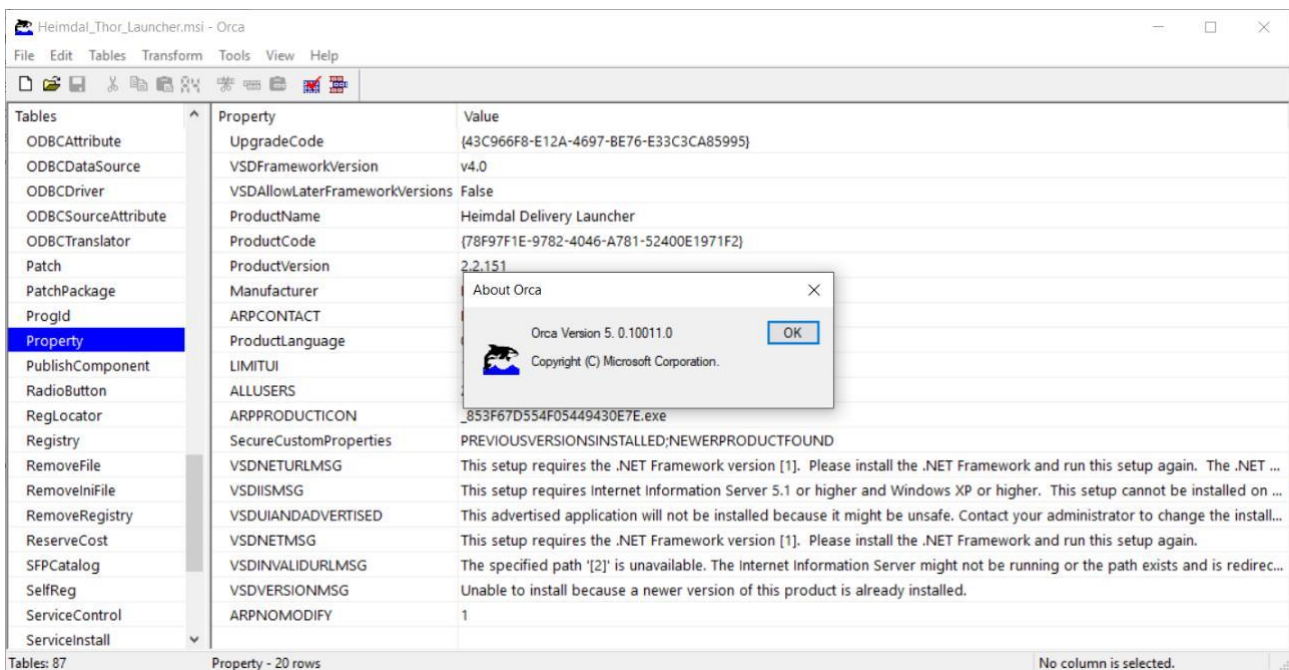
These policy changes will be applied after the machines on which Thor is installed and that respond to the relevant policy will receive a reboot. Please note that the reboot is mandatory for proper GUI-less functionality.

Update GP **Cancel**

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.

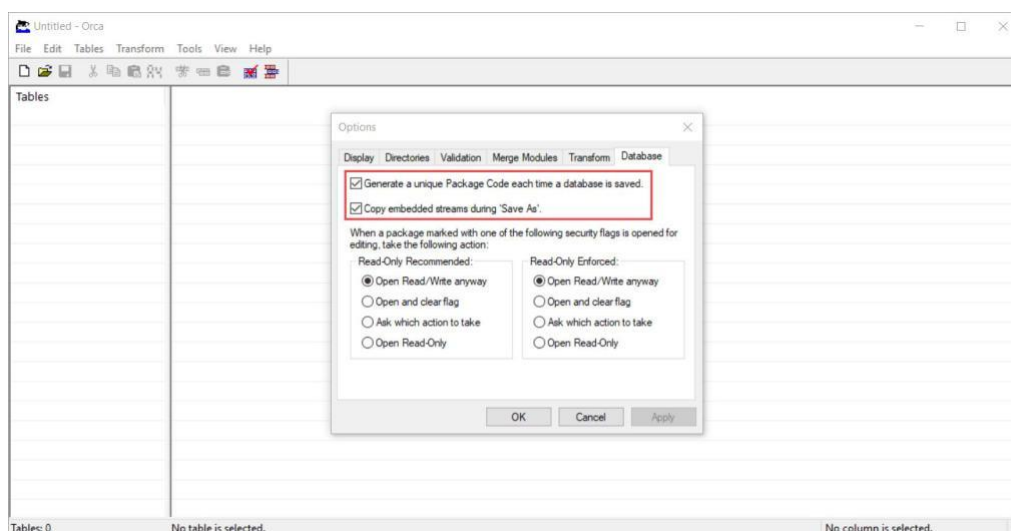
The activation key can be inserted directly into the MSI, as a row with the property "HEIMDALKEY" and Value "[activationkey/serialkey]". The following section shows the approach to be used when inserting the activation key using Orca Version 5.0.10011.0.



6.1.2.1 Orca pre-configuration

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

- Open Orca
- Click on Tools
- Choose Options
- Go to the Database tab
- Check the first two options
- Click Apply

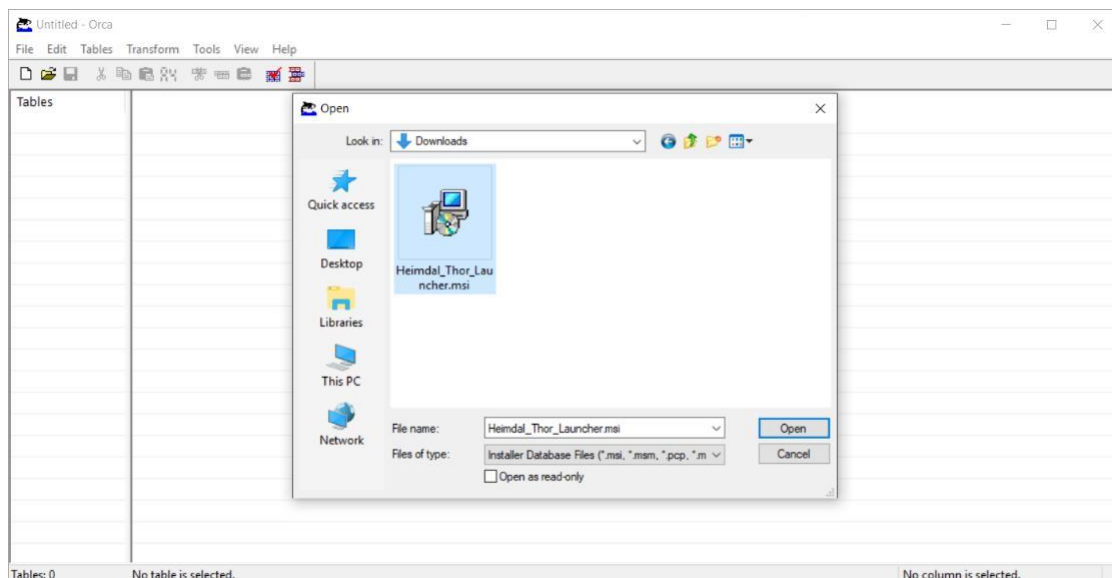




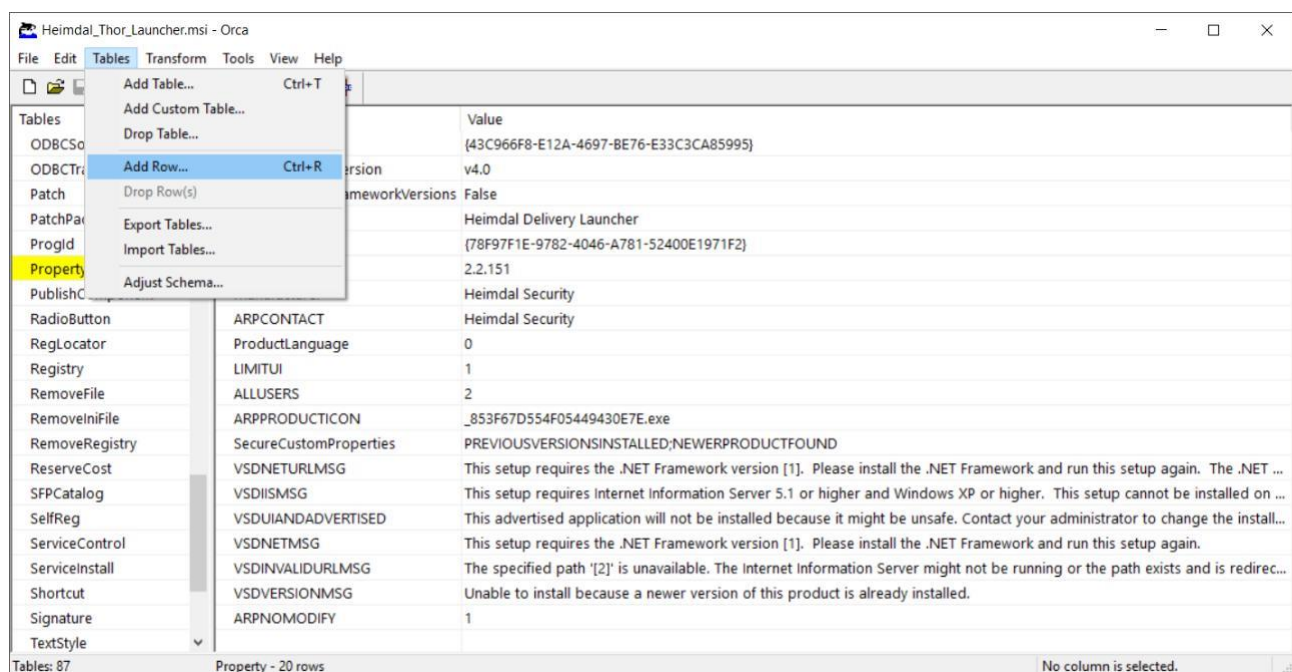
6.1.2.2 The MSI editing process

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

1. Install Orca and open Heimdal.msi:



2. Find and mark the table "Property" and select 'Tables' and click 'Add Row...':





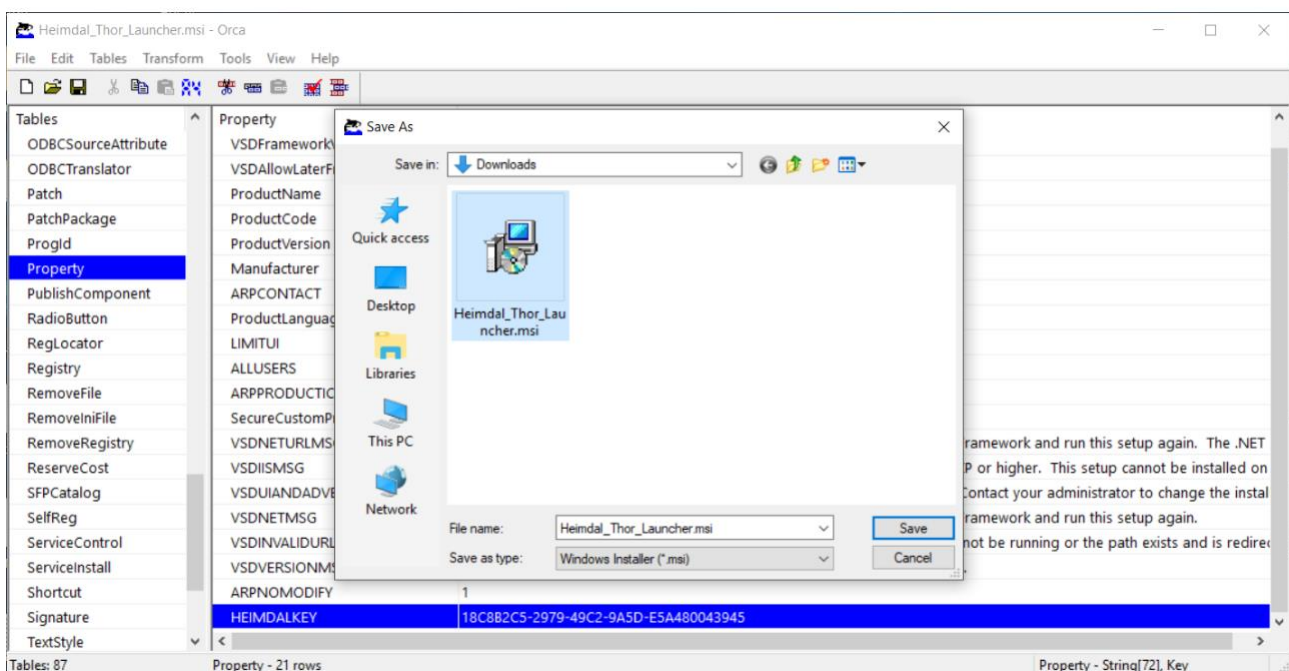
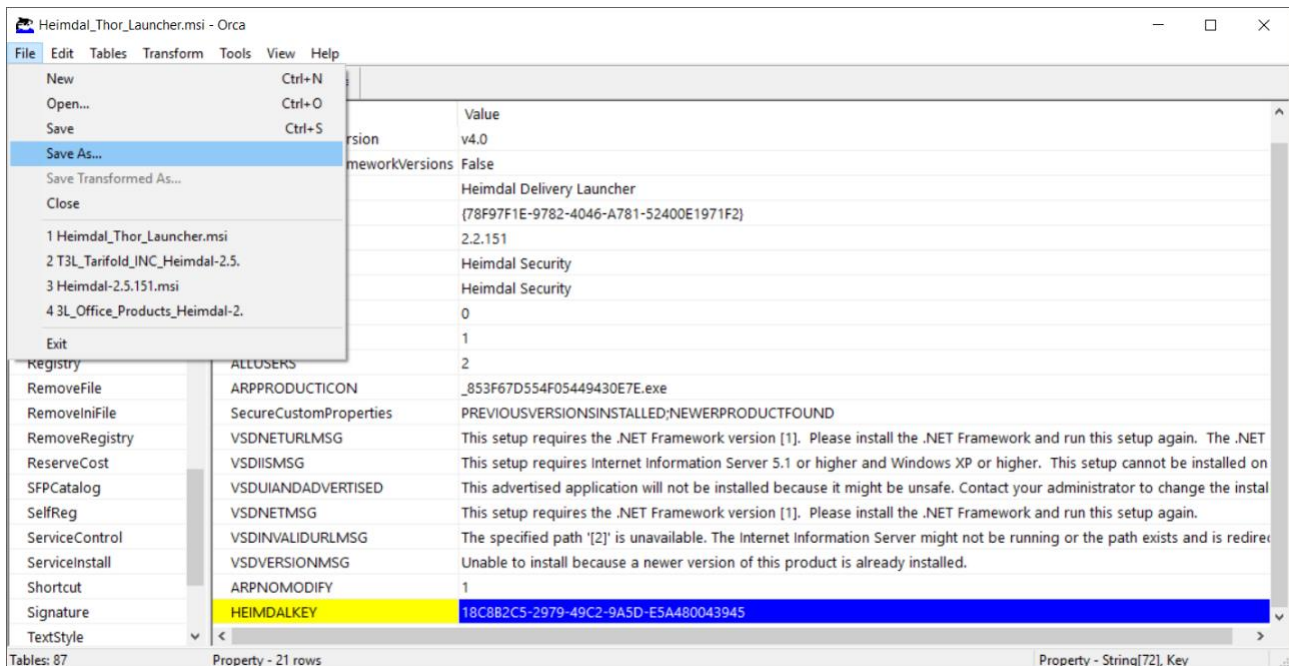
3. In the Property field, write **HEIMDALKEY** and in the Value field paste your activation key

The screenshot shows the Orca MSI editor interface for 'Heimdal_Thor_Launcher.msi'. The 'Property' table is selected in the left pane. The 'Add Row' dialog box is open, showing the 'Name' field with 'HEIMDALKEY' and the 'Value' field with a placeholder activation key. The main table shows various properties like UpgradeCode, VSDFrameworkVersion, ProductName, etc. The bottom status bar indicates 'Property - 21 rows'.

Property	Value
UpgradeCode	{43C966F8-E12A-4697-8E76-E33C3CA85995}
VSDFrameworkVersion	v4.0
VSDAllowLaterFrameworkVersions	False
ProductName	Heimdal Delivery Launcher
ProductCode	{78F97F1E-9782-4046-A781-52400E1971F2}
ProductVersion	2.2.151
Manufacturer	Heimdal Security
ARPCONTACT	Heimdal Security
ProductLanguage	0
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 setup again. The .NET Framework version [1] is unavailable. The Internet Information Server might not be running or the path exists and is redirected to a different location. This setup cannot be installed on this computer.
VSDIISMSG	This setup requires Internet Information Server 5.1 or higher and Windows XP or higher. This setup cannot be installed on this computer.
VSDUIANDADVERTISED	This advertised application will not be installed because it might be unsafe. Contact your administrator to change the installation policy.
VSDNETMSG	This setup requires the .NET Framework version [1]. Please install the .NET Framework and run this setup again.
VSDINVALIDURLMSG	The specified path '[2]' is unavailable. The Internet Information Server might not be running or the path exists and is redirected to a different location.
VSDVERSIONMSG	Unable to install because a newer version of this product is already installed.
ARPNOMODIFY	1
HEIMDALKEY	18C8B2C5-2979-49C2-9A5D-E5A480043945



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



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 of your organizations computers.

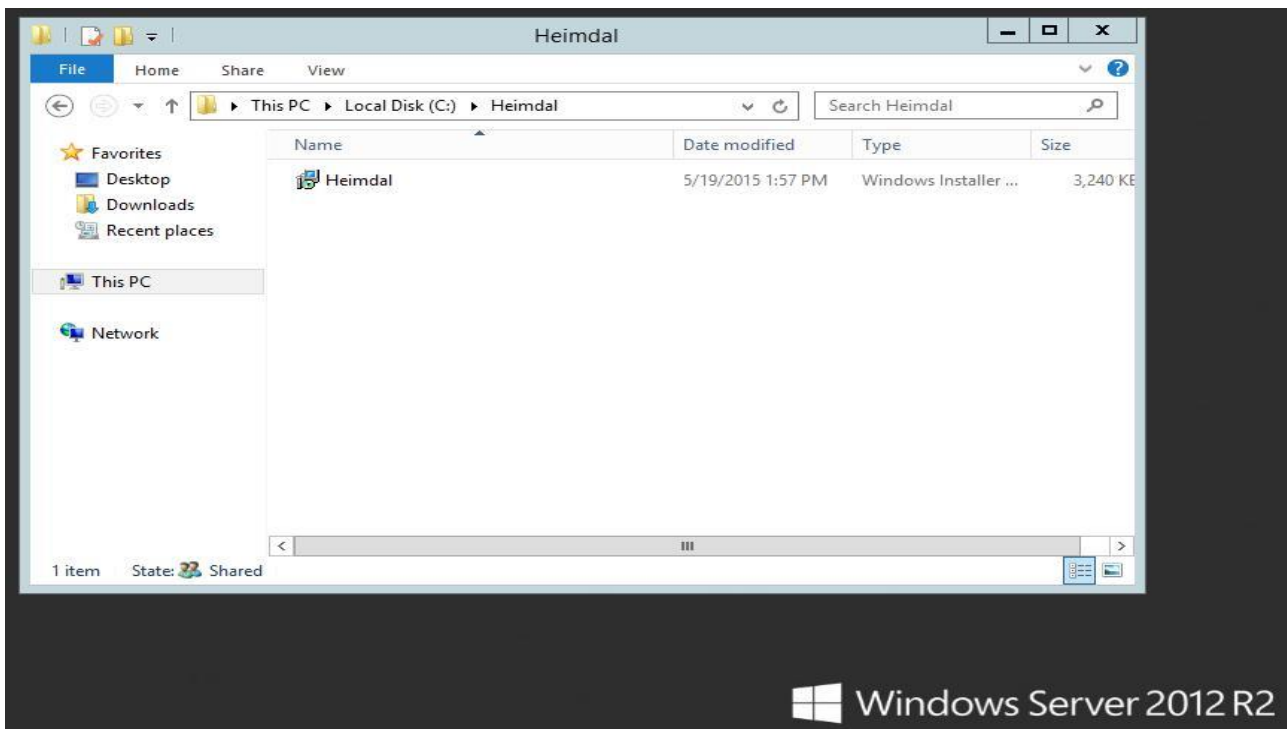
To configure an automatic distribution of the Thor agent through Group Policy Management you will need:



- 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.

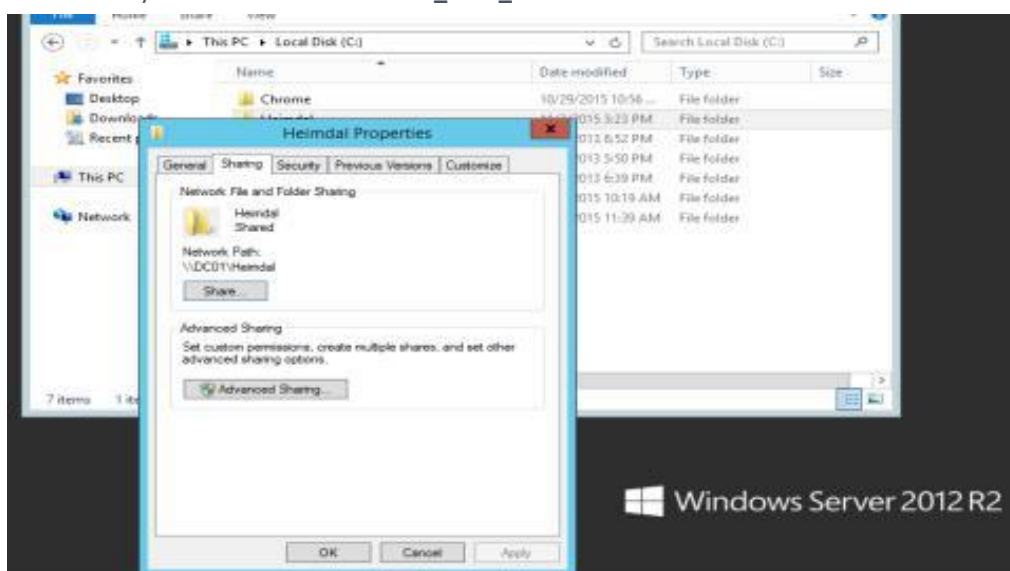


- A network path, where the Thor MSI installation file can be placed. All computers, which are going to have the agent installed, must have at least read access to this network path.
- [Microsoft .NET Framework 4.6.1](#) or later - full profile - must be installed on all computers.

The full process works like this:

Step 1:

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

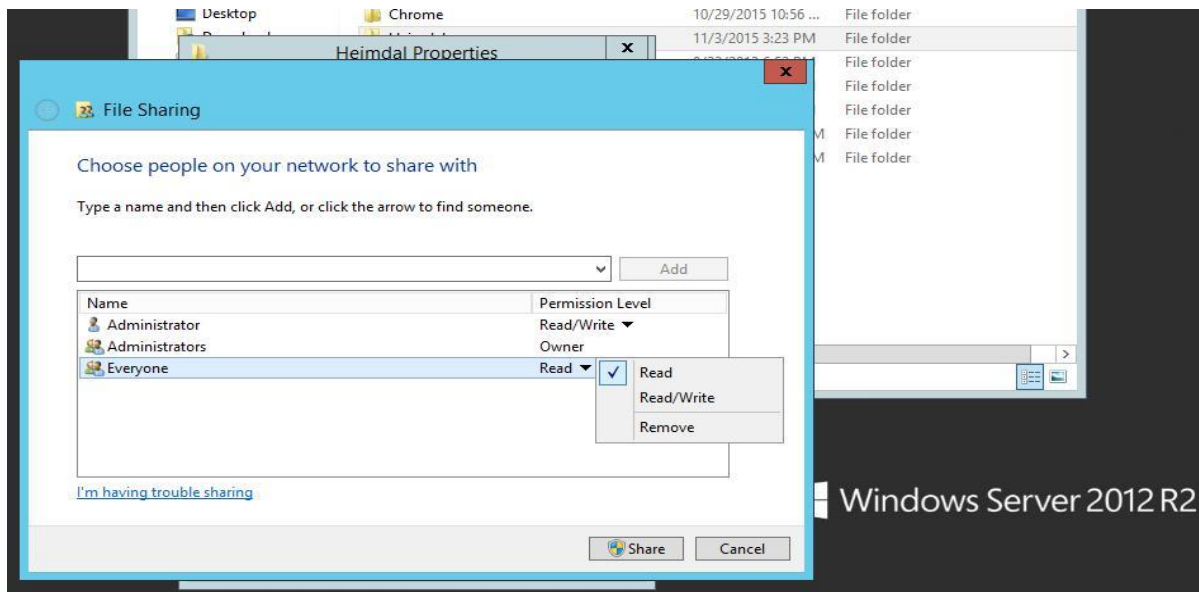




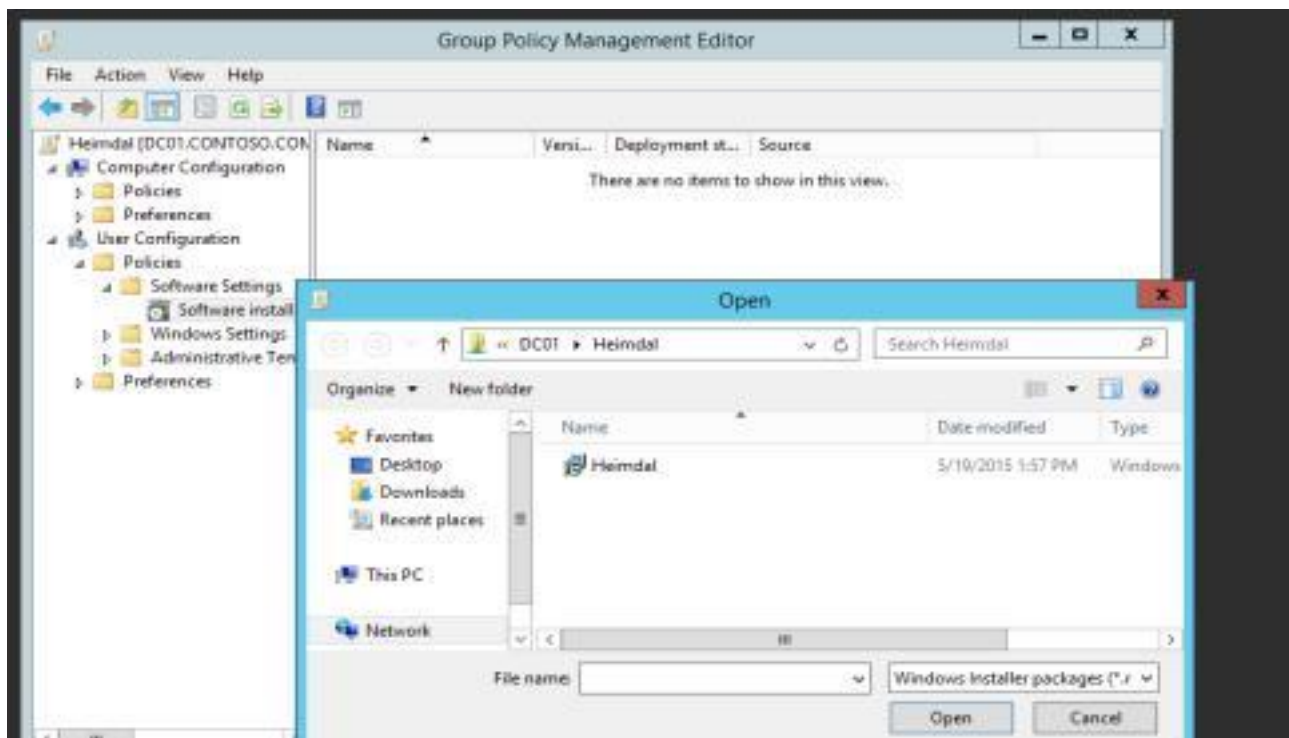
Make sure the folder is accessible and that the computers have at least read access to the newly created folder

Step 2:

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



Make sure to browse to the target msi installer.



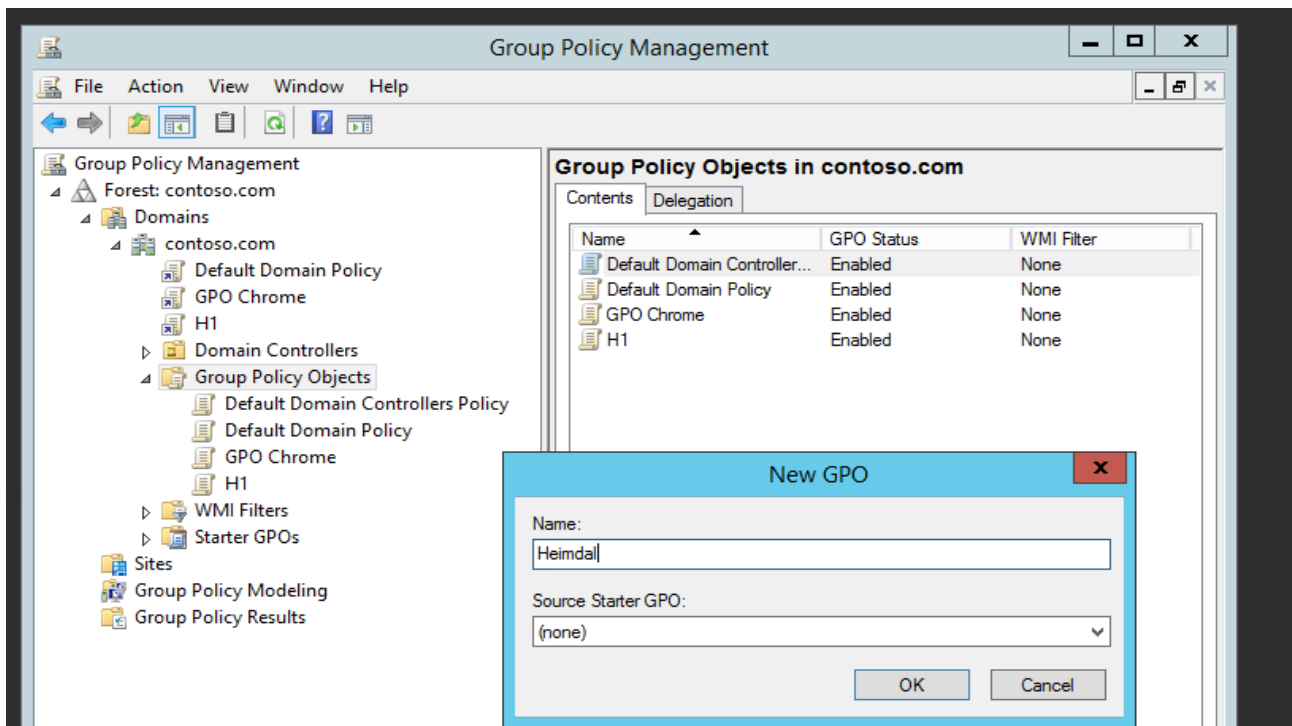


Step 3:

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).



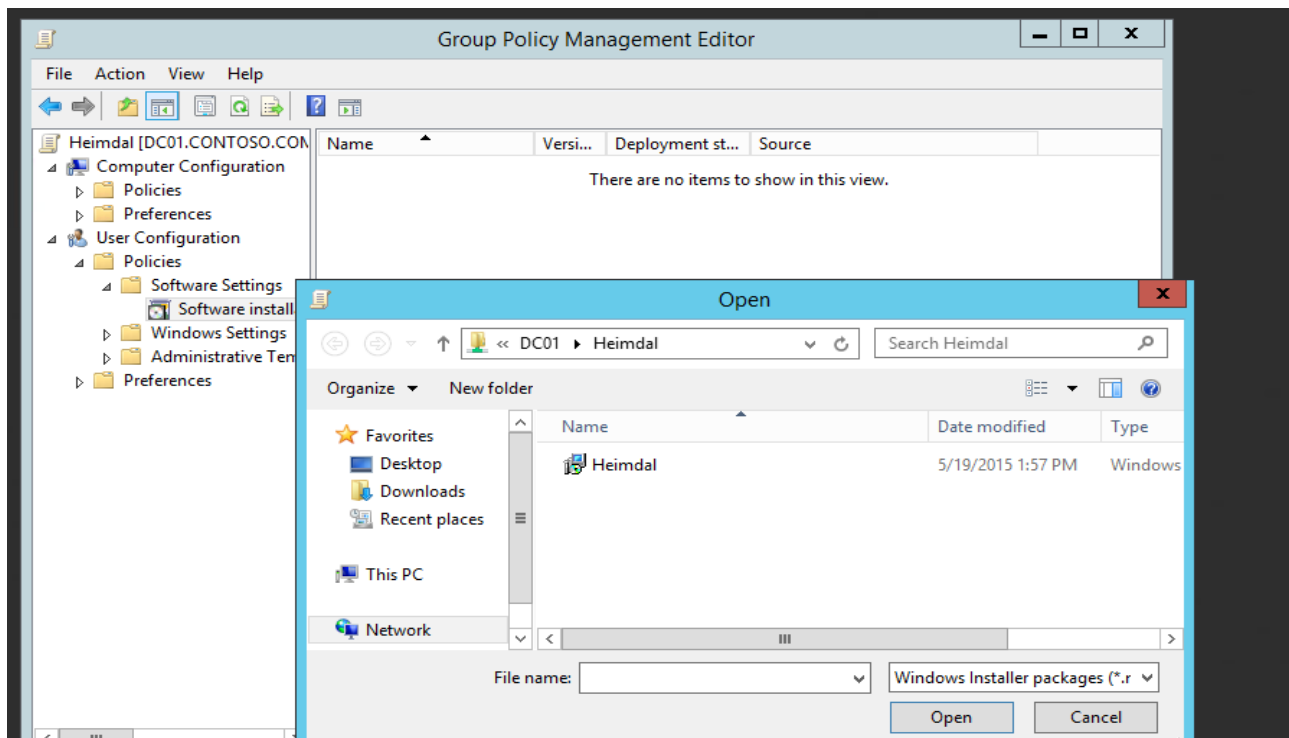
Step 4:

Open the Group Policy Management Editor and select the following:

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

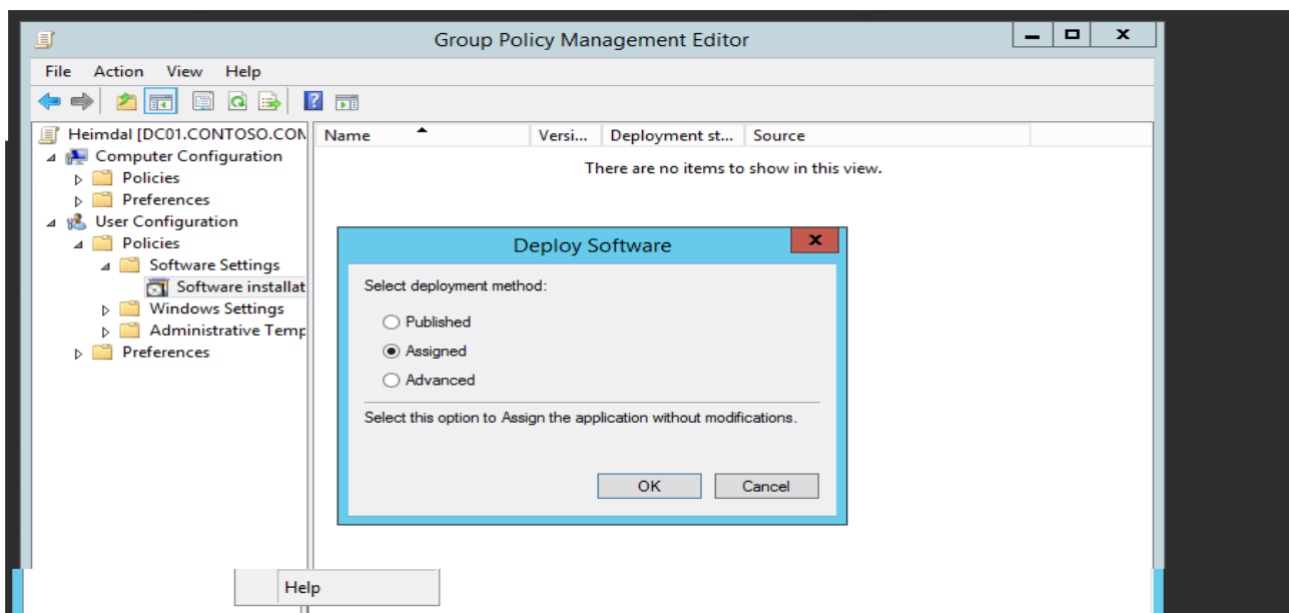


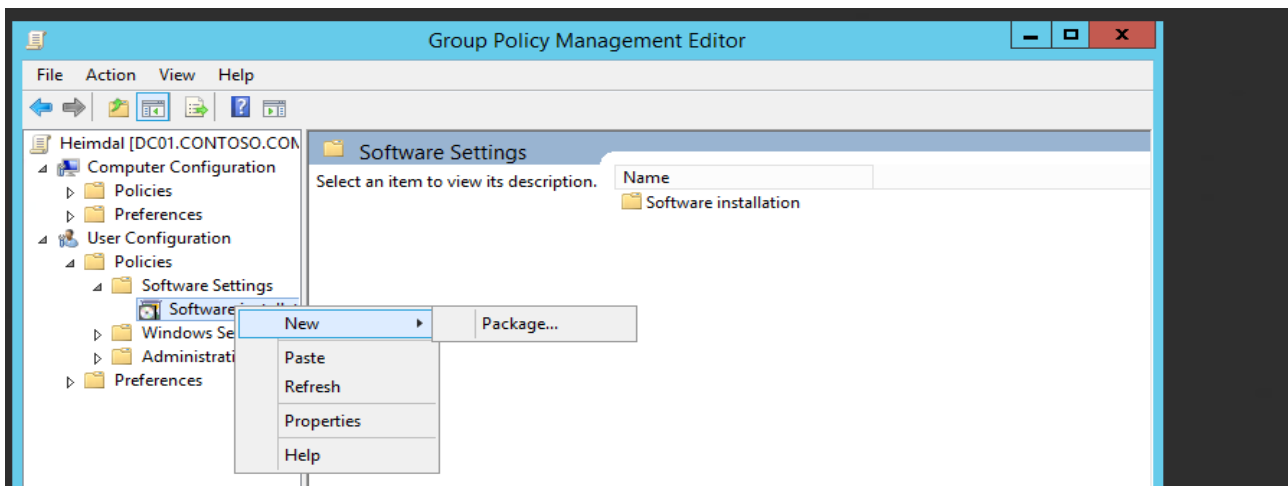
Make sure to browse to the target msi installer.



Step 5:

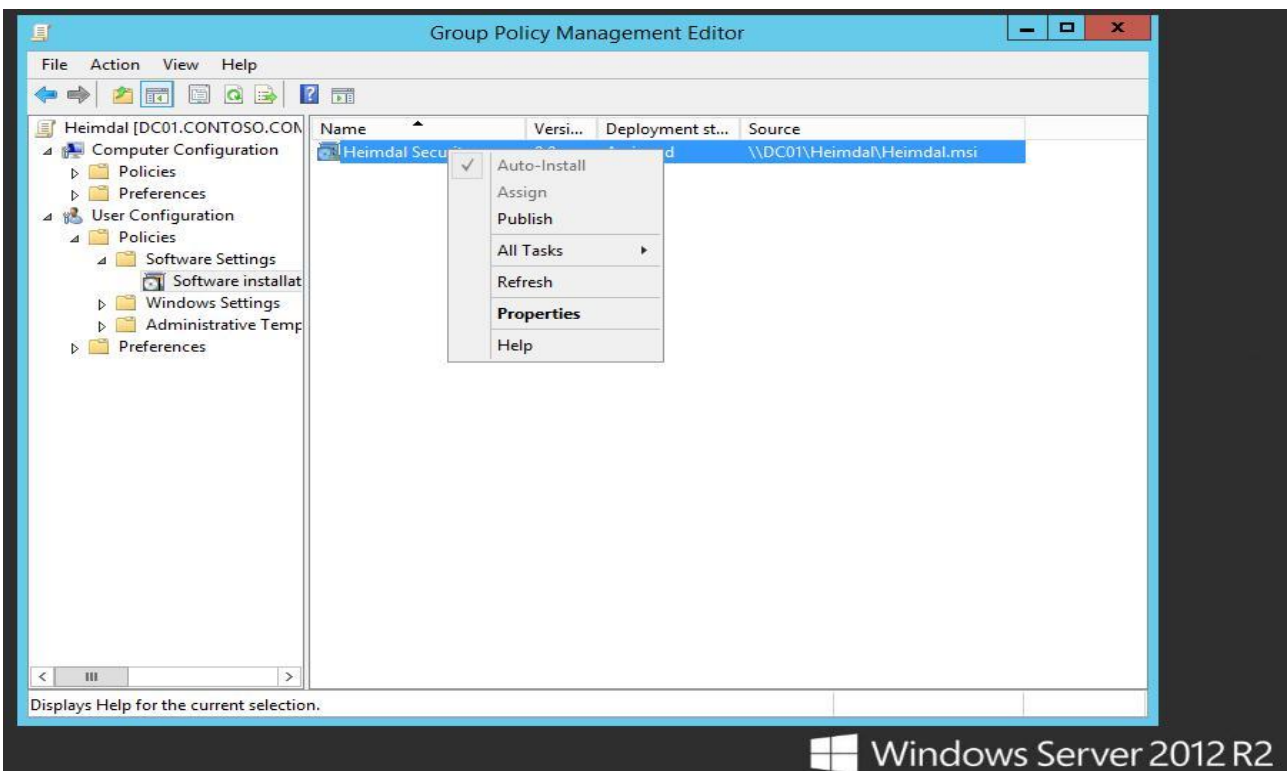
For “Deploy Software”, chose the “Assigned” option. This means the installation will run without user interaction:





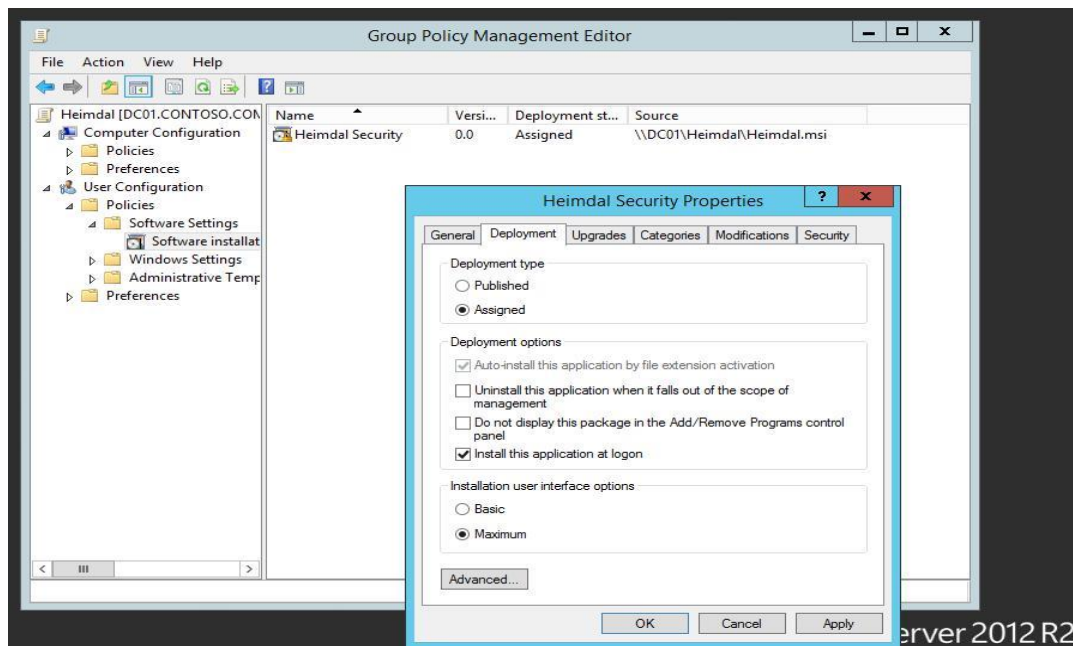
Step 6:

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”.



Step 8:

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

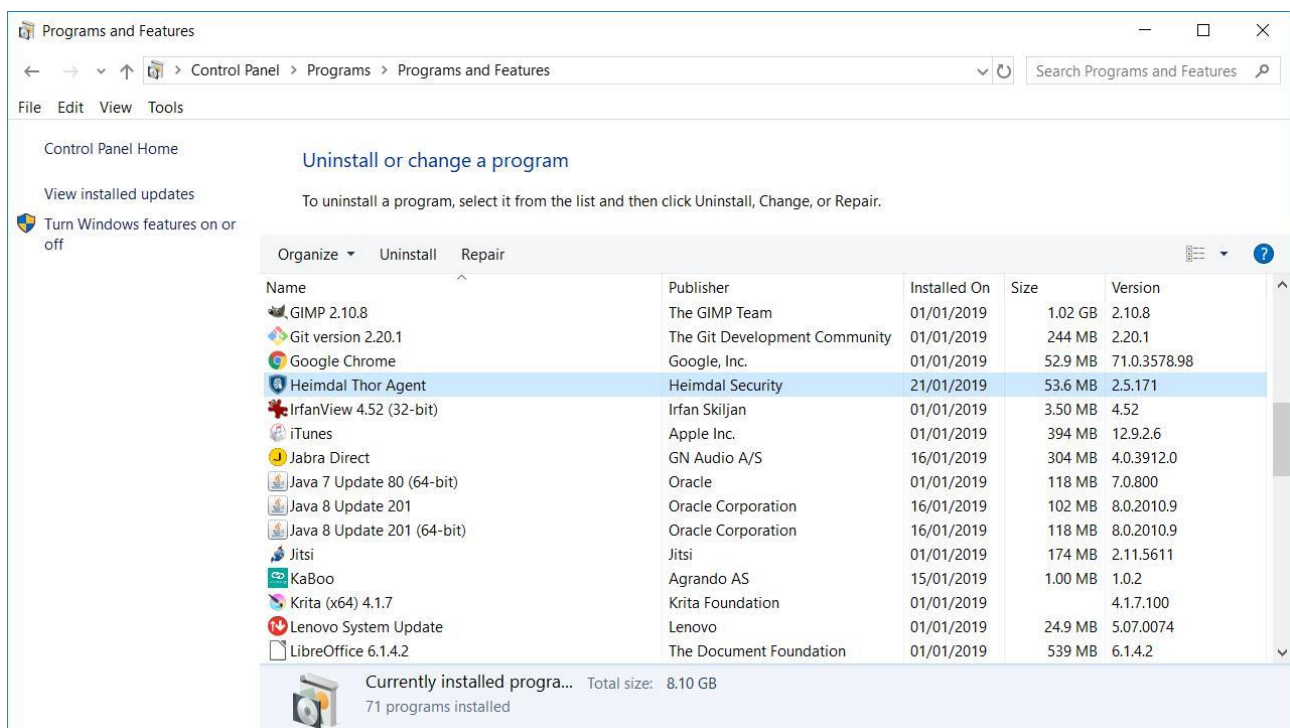
- > Open Command Prompt as Administrator and type:
- > gpupdate /force /boot /logoff



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



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





6.2 AD group binding for Thor

Custom	-	-	2	Enabled	Disabled	Duplicate
Default	-	-	1	Enabled	Disabled	Duplicate

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.

Enable group policies inheritance - this option allows for machines to be included into multiple Group Policies that match but it will only merge the 3rd party software system. Also, the priority of GPs will be kept and endpoints with specific GP will be ignored.

We will merge all the applications based on the priority/group, from the lowest priority to highest.

Windows Endpoints

Windows GP

Mac OS GP

Android GP

Search by Policy Name

Policy Name

A Total of: 7 Listings

☐ Enable group policies inheritance

Create New Policy

Policy Name	AD Computer Group	AD User Group	Priority	Status	Action
Sales Master GP	-	Sales DK	7	<div>Enabled</div> <div>Disabled</div>	<div>Duplicate</div>
Heimdal Support	-	Support Users	6	<div>Enabled</div> <div>Disabled</div>	<div>Duplicate</div>
Heimdal Accounting	-	contabilitate	5	<div>Enabled</div> <div>Disabled</div>	<div>Duplicate</div>
Heimdal Marketing	-	Marketing USERS	4	<div>Enabled</div> <div>Disabled</div>	<div>Duplicate</div>
Morten - NO Mailsentry	-	Sales DK	3	<div>Enabled</div> <div>Disabled</div>	<div>Duplicate</div>
All	-	-	2	<div>Enabled</div> <div>Disabled</div>	<div>Duplicate</div>
Default	-	-	1	<div>Enabled</div> <div>Disabled</div>	<div>Duplicate</div>



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).

General	Threat Prevention	Patch & Assets	Endpoint Detection	Privileges & App Control	Email Protection
<p>Policy name* Heimdal Security Test</p> <p>Language* English</p> <p>Priority 6</p> <p>AD Computer Group Marketing Computers</p> <p>AD User Group </p> <p>External IPs 1</p>					

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

```
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 gresult /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.



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):

General	Threat Prevention	Patch & Assets	Endpoint Detection	Privileges & App Control	Email Protection
Policy name* Heimdal Security Testing					
Language* English		Priority 4			
AD Computer Group 		AD User Group Marketing USERS		External IPs ⓘ 	
Policy check interval [min] 			Licensing check interval [min] 		

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 Group are supported on first level child-OU's (level 1 recursion) for use within the Heimdal Dashboard.
- The group names are case sensitive inside the Thor dashboard so for a successful bind, the names must be an exact match.

Note: In a Group Policy you can find an option called “Only merge with AD groups specific policies”. If this option will be available only if Inheritance mode is ON. If Inheritance mode is OFF, then this option will be grayed out. If this option is enabled, you will be able to apply multiple Group Policies to machines that are part of different AD groups.

6.2.2.3 Apply a Group Policy based on "ComputerTags" and "UserTags"

You can read more about this feature on the following link: <https://support.heimdalsecurity.com/hc/en-us/articles/360001861477-Assigning-a-Group-Policy-to-an-endpoint-or-a-group-of-endpoints>.

6.2.2.4 Changing group policy priority

The value/number of priorities 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.

Windows Endpoints

Windows GP Mac OS GP Android GP

Search by Policy Name Policy Name Q

A Total of: 7 Listings ☐ Enable group policies inheritance Create New Policy

Policy Name	AD Computer Group	AD User Group	Priority	Status	Action
Sales Master GP	-	Sales DK	7	Enabled Disabled	Duplicate
Heimdal Support	-	Support Users	6	Enabled Disabled	Duplicate
Heimdal Accounting	-	contabilitate	5	Enabled Disabled	Duplicate
Heimdal Marketing	-	Marketing USERS	4	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 that must be followed to use Thor if behind a proxy can be found here: [How to install The Heimdal Agent \(For Enterprise\) if I'm behind a Proxy Server?](#)



6.4 Internet WebServers for use with Heimdal™ Threat Prevention - Endpoint

Using Heimdal™ Threat Prevention – Endpoint with internal web servers 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 to resolve. 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 Heimdal™ Threat Prevention installed, please have a look at the below case corners:

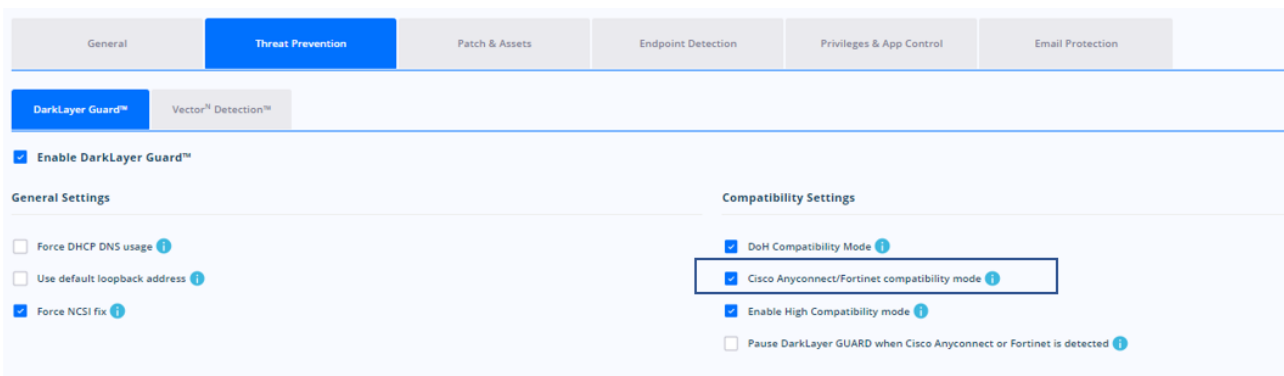
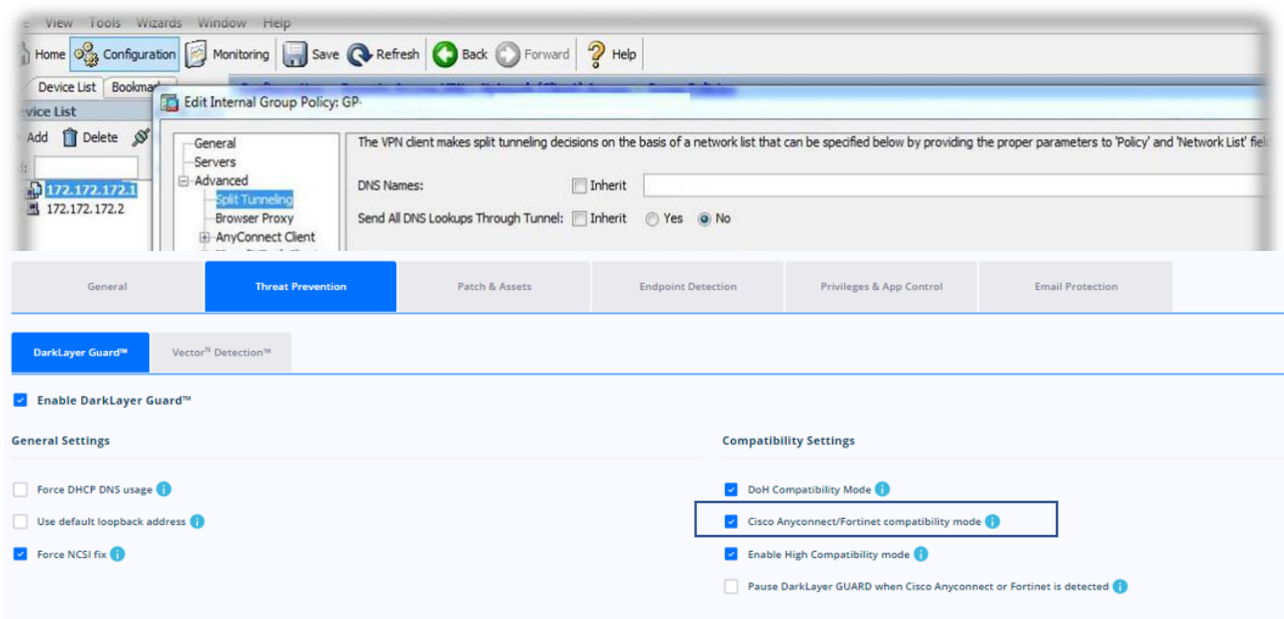


IMPORTANT: Thor is compatible with all VPN technologies. The connection should be established in a correct and stable way. HOWEVER, if you notice traffic filtering issues like pages not being filtered while connected to the VPN server, please contact the support team at corpsupport@heimdalsecurity.com.

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:



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.



General Threat Prevention Patch & Assets Endpoint Detection Privileges & App Control Email Protection

DarkLayer Guard™ Vector™ Detection™

☒ Enable DarkLayer Guard™

General Settings

☐ Force DHCP DNS usage ⓘ

☐ Use default loopback address ⓘ

☒ Force NCSI fix ⓘ

Compatibility Settings

☒ DoH Compatibility Mode ⓘ

☒ Cisco Anyconnect/Fortinet compatibility mode ⓘ

☒ Enable High Compatibility mode ⓘ

☐ Pause DarkLayer GUARD when Cisco Anyconnect or Fortinet is detected ⓘ

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**.

General Threat Prevention Patch & Assets Endpoint Detection Privileges & App Control Email Protection

DarkLayer Guard™ Vector™ Detection™

☒ Enable DarkLayer Guard™

General Settings

☒ Force DHCP DNS usage ⓘ

☐ Use default loopback address ⓘ

☒ Force NCSI fix ⓘ

Compatibility Settings

☒ DoH Compatibility Mode ⓘ

☒ Cisco Anyconnect/Fortinet compatibility mode ⓘ

☒ Enable High Compatibility mode ⓘ

☐ Pause DarkLayer GUARD when Cisco Anyconnect or Fortinet is detected ⓘ

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 Usage on Remote Desktop servers and SQL servers

To run Heimdal Security products on Remote Desktop Servers and SQL servers the following folders have to be whitelisted in Group Policy - Heimdal™ Next-Gen Antivirus & MDM.

Exclusions for Remote Desktop Servers:

- C:\Windows\SoftwareDistribution\Datastore
- C:\Windows\System32\GroupPolicy
- C:\Windows\System32\Wins

Exclusions for the SQL Server installation (depends on the path where the SQL Server is installed):

- C:\ProgramFiles\Microsoft SQL Server\
- C:\ProgramFiles (x86) \Microsoft SQL Server\

In addition to excluding SQL Server and Analysis Services files, it is recommended to exclude the following list of processes from antivirus scans:

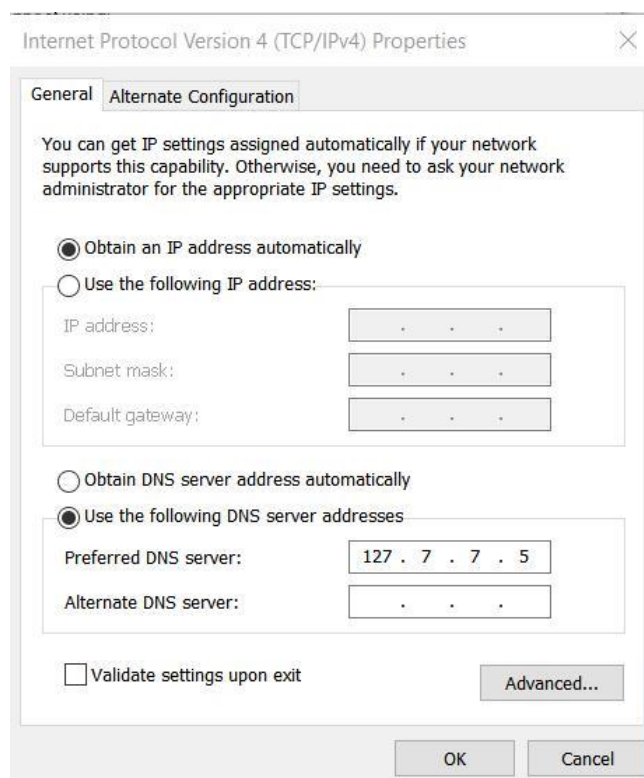
- SQLServr.exe
- ReportingServicesService.exe
- MSMDsrv.exe

For environments where SQL Server is clustered, exclude the C:\Windows\Cluster directory and the Quorum drive.

6.10 Internet Protocol Version

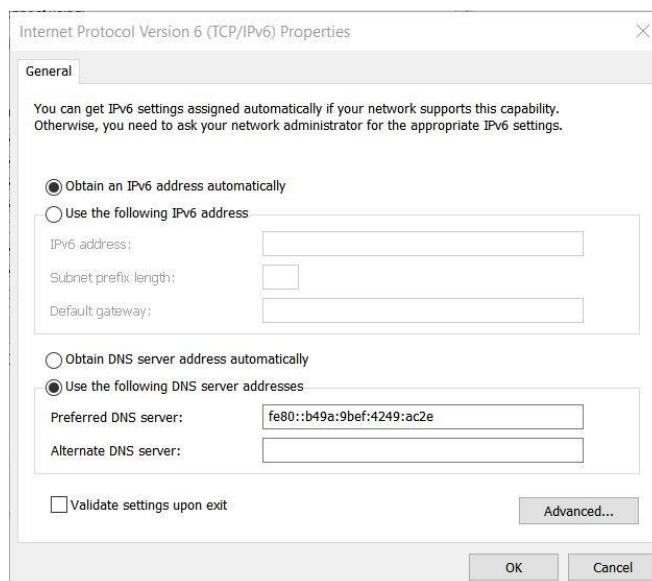
Heimdal™ Threat Prevention – Endpoint can filter network traffic both on IPv4 and IPv6. Please see below the DNS settings made by Heimdal™ Threat Prevention – Endpoint when Traffic Filtering is activated.

- On IPv4, the DNS address set by Heimdal™ Threat Prevention – Endpoint looks like 127.7.7.X where X is variable. In the example below the assigned DNS value is 127.7.7.5.





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



*if Threat Prevention Endpoint is disabled from Heimdal™ Threat Prevention – Endpoint - the 127.7.7.5 will be removed when the adapter becomes active

* Threat Prevention Endpoint can cause issues if the client uses SAP because SSO requires the KDC (Kerberos Domain Controller) to be present as the Primary DNS

6.11 Peer to Peer

To improve device performance, reduce internet bandwidth and lower the costs for clients, Heimdal Security has set-up the Peer-To-Peer feature so that the data downloaded from our servers to a machine will be shared directly to all the other computers in the respective network. The normal distribution rate is of 1 machine to 3 machines having active connections and subsequently 3 machines to 9 machines, 9 to 27, 27 to 81 and so on. You can also set a machine as a designated Priority Update Server (from the Active Clients view) increasing the distribution rate to up to 3000 machines.group

The data transferred via P2P includes:

- Thor agent updates
- 3rd Party Applications updates
- Bloom filter used by Threat Prevention Endpoint
- Applications deployed via Patch & Asset Management

This feature is automatically enabled to all the customers and can be turned off at request, by contacting the Account Manager or the Support Team.

Heimdal also offers you the option to create Priority Update Servers. That means that you can select one or more machine to be Update Servers for the others. The option that deals with this is called Use Priority update servers.

Read more about this option and how to enable it here: <https://support.heimdalsecurity.com/hc/en-us/articles/213634049-Dashboard-Features-Group-Policy-Overview>



6.12 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

The screenshot shows the 'General' settings tab for a Group Policy named 'heimdal Support'. The 'Enforce uninstall password' checkbox is checked, and a password field is visible below it. Other settings include 'Language' (English), 'Priority' (S), 'AD Computer Group', 'AD User Group', 'Support clients', 'Policy check interval (min)' (15), 'Licensing check interval (min)' (1440), 'Cpu Threshold %' (15), 'Memory Threshold %' (1440), 'Proxy Settings' (No proxy), 'Host', 'Port', 'Domain', 'Username', 'Password', 'Additional Settings' (Include in Release Candidate Program, Do not show GUI, Skip prompting the client when requesting logs, Only merge with AD groups specific policies, Use Priority update servers, Keep cached files indefinitely, Additional check interval for normal computers (min) (120)).

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



7. Features

7.1 Features of Heimdal™ Threat Prevention - Endpoint

7.1.1 Peer To Peer transfer

In order to improve the speed of updating a company's software and reduce the downloaded traffic, when communicating with our servers, we have introduced the P2P feature. If this is enabled, Thor Enterprise and all the patches we provide will download and install faster. This works by downloading the executable file on the machines that first ping to our servers then the updates/patches will be distributed to the other computers within the company's network.

Also, another thing that you should know, it is that P2P feature is working through the 57127 port.

To activate P2P, you have to contact your Account Manager or the support team at corpsupport@heimdalsecurity.com and provide a port number that has to be open in your firewall.

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

Internet traffic checking in Heimdal™ Threat Prevention – Endpoint 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. Heimdal™ Threat Prevention – Endpoint 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.

7.1.3 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, Heimdal™ Threat Prevention 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 Heimdal™ Threat Prevention – Endpoint 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, Heimdal™ Threat Prevention – Endpoint will approve the request from the used DNS servers.

If the address is with a 98% certainty on the list, Heimdal™ Threat Prevention – Endpoint 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.



7.1.4 Category blocking views in Threat Prevention Endpoint

You can now find new views in Threat Prevention Endpoint and Active Clients, added for traffic blocked by the category blocking mechanism.

There is a new tab to the Threat Prevention Endpoint view for the domains blocked by the category blocking mechanism. The view displays the total number of blocked domains per endpoint and can be filtered by category/categories using the advanced filter. The advanced filter loads a list of categories that can be selected to filter the view. Clicking the number of blocked categories navigates the user to the Threat Prevention Endpoint Grid in Active Clients. Also added a new statistic showing the total number of blocked categories.

DarkLayer Guard™ Endpoint [Go to Network Page View](#)

197,521 Analyzed Traffic Requests

10,530 Prevented Attacks

5.33% Prevented Attacks %

902,103 Category Blocks

Search by Category Blocked Domains Category Blocked Domains 🔍

Standard view | Threat Type view | Hostname/Threats View | Latest Threats View | TTTPC View | **Category Blocks view (743)** Download CSV 🔗 Filters

Hostname	Username	IP Address	Category Blocked Domains
	CASH	172.41.192.189	90
	Cash	172.41.192.186	20
	uggcash	172.31.79.13	1967
	tomscash	172.30.231.20	543
	tomscash	172.30.103.13	1730
	tomscash	172.30.103.11	1367

Under the Active Clients view→

- a) Added a new view to the Threat Prevention Endpoint grid under Heimdal™ Threat Prevention, selecting “Category blocked” will display the domain, category and timestamp for the domains blocked using the category blocking mechanism.

⏪ Last Active Username: Last Seen: 20.04.2021 12:01:04 Group Policy: Heimdal Marketing Status: ⚠

General

Threat Prevention

Patch & Asset Management

Endpoint Detection

Forensics

Privileges & App Control

DarkLayer Guard™ Endpoint

Vector^N Detection™

All Statuses | Prevented Attacks | Allowed | Analyzed | **Category Blocks (0)**

Domain	Category	Date
There are no results		

First Page << 1 >> Last Page Go to page: Items per page: 10



7.2 Features for Heimdal™ Patch & Asset Management

7.2.1 Heimdal™ Patch & Asset Management

Heimdal™ Threat Prevention – Endpoint 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. Heimdal™ Threat Prevention – Endpoint will never close a running application or automatically reboot the PC after the updates have been installed. Also, Heimdal™ Threat Prevention – Endpoint 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

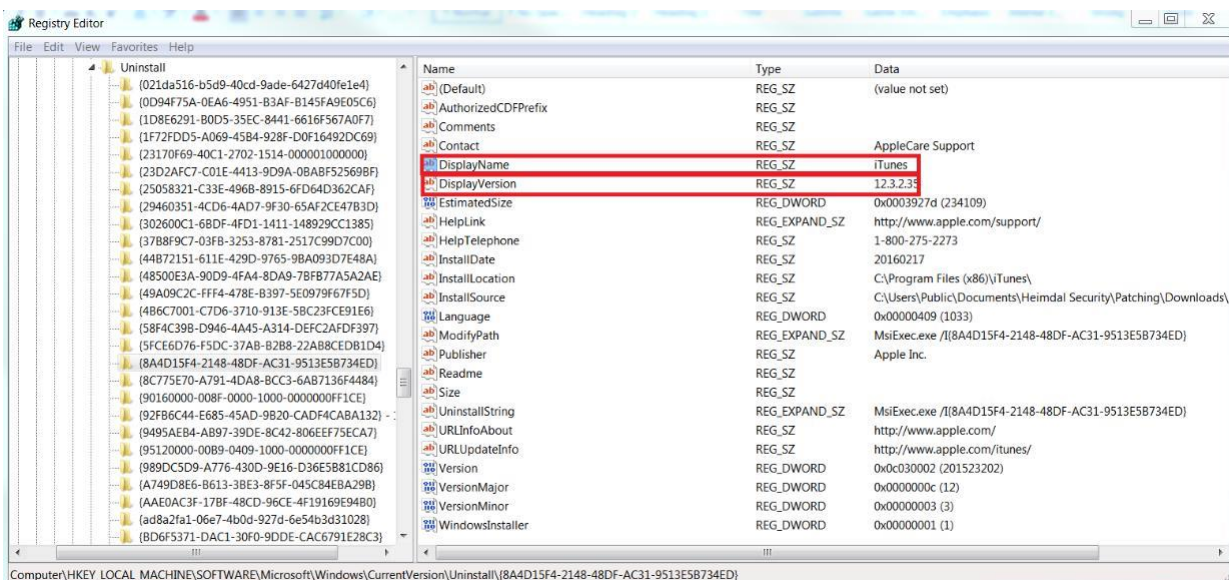
7.2.2 The list of supported software

Here you can find the full list of the applications that can be installed or patched by Heimdal™ Threat Prevention – Endpoint:

[What 3rd Party Applications Does The HEIMDAL™ Agent Patch?](#)

7.2.3 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.



Heimdal™ Threat Prevention – Endpoint 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, Heimdal™ Threat Prevention



– Endpoint will notify the user via a red exclamation mark inside the interface and the relevant information will be added in the dashboard.

7.2.4 Software that already has auto update enabled

Please note that some of the software apps that Heimdal™ Threat Prevention – Endpoint monitors and updates automatically and silently may already have auto update enabled in their default settings. This means that updates delivered into the software directly by the software manufacturer (via the auto update feature built into the application) may be faster than patches applied by Heimdal™ Threat Prevention - Endpoint.

The following applications already have auto update enabled by default by the software manufacturer and consequently, may be updated faster than Heimdal™ Threat Prevention – Endpoint 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 Heimdal™ Threat Prevention - Endpoint, the newly added software will be automatically installed in your environment.

7.2.5 Patches deployment method – Bulk or Staged?

If you are about to deploy Heimdal™ Threat Prevention – Endpoint 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, Heimdal™ Threat Prevention 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 Heimdal™ Patch & Asset Management patches:

Welcome to Thor Foresight Enterprise

HOME > X-PLOIT RESILIENCE

X-ploit RESILIENCE ONE CLICK APP INSTALL SEE LIST QUICK SETTINGS

0 MONITORED 0 VULNERABLE APPS VIEW HISTORY

SOFTWARE NAME	VERSION	STATUS	MONITOR	AUTOUPDATE
		Up to date		Downloading
		Out of date		Error downloading
		Newer version detected		Installing
		Not monitored		Error installing
		Manually retry		Contact support

VER 2.5.150 RC



Please read more about this on our article from FAQ:

7.2.7 Patch & Asset Management

Once this module has been activated for your account, you will find it under the Product section, at Patch & Asset Management tab, from the left menu of the Dashboard.

7.2.8 Windows Updates

b) New feature: Added a new view to the Patch & Asset Management module -> Microsoft Updates -> Available tab, on the right side of the grid action row- a new dropdown filter for the group policy. This filter is used to show the available windows updates only for the machines that have the selected group policy as last retrieved policy.

© Copyright 2019 – Heimdal Security A/S. All rights reserved



7.3 Features for Heimdal™ Endpoint Detection

7.3.1 Next Gen Antivirus

As a standalone AV product Heimdal™ Next-Gen Antivirus & MDM 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:

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

7.3.2 Firewall Management

Read more about the Firewall Management here: [Firewall Management](#)

7.3.3 Ransomware Encryption Protection

Read more about this section here: <https://support.heimdalsecurity.com/hc/en-us/articles/360017671857-Ransomware-Encryption-Protection->

7.3.4 Mobile Device Management

Read more about the MDM services here: [MDM - Android](#)



7.4 Features for Heimdal™ Privileges & App Control

7.4.1 Privileged Access Mgmt

For more details about this section, please access the following article: <https://support.heimdalsecurity.com/hc/en-us/articles/360004572638--Heimdal-Privileged-Access-Management-Overview>

7.4.2 Application Control

Application Control is a module created to control which processes (or applications) can be executed on client machines and how they are executed. You can define a set of rules that describe what processes are allowed or blocked on your machines (in your environment) using details like software name, paths, publisher, MD5, signature, or wildcard. Application Control can handle a process should run (it can get automatic elevation from the Heimdal™ Privileged Access Management module, if so configured) and how child processes (it can allow or block all processes spawned by the process defined by the rule).

The Application Control **view** displays a table with all the intercepted processes. You get information about the Process Name, the number of executions, Publisher, Software Name, Version, Group Policy, MD5, and the Status. The processes can be filtered using the following filters: All intercepted applications, Matching Allow rules, Matching Block rules, Matching Allow by default, Matching Block by default and Matching Allow with auto elevation.

Last Active Username: dka Last Seen: 20.04.2021 12:22:36 Group Policy: Status:							
General Threat Prevention Patch & Asset Management Endpoint Detection Forensics Privileges & App Control							
Privileged Access Mgmt Application Control							
All intercepted applications (1) Matching Allow rules Matching Block rules Matching Allow by default Matching Block by default Matching Allow with auto elevation							
1 2 3 4 5 6 Hide Microsoft Application							
	Process Name	Number of Executions	Publisher	Software Name	Version	MD5	Status
<input type="checkbox"/>	HPSAAppLauncher	1	HP Inc.	HPSACommands	1.0.0.3		Allow by default
First Page < 1 > Last Page Go to page: Items per page: 10							

All intercepted applications - displays all the applications that have been running on the machine(s)

Matching Allow rules - displays the latest interceptions that match the 'Allow' rule

Matching Block rules - displays the latest interceptions that match the 'Block' rule

Matching Allow by default - displays the latest interceptions that match the "Allow by default" status (a process is allowed by default if the Default File Action is set to Allow)



Matching Block by default - displays the latest interceptions that match the "Block by default" status (a process is blocked by default if the Default File Action is set to Block)

Matching Allow with auto elevation - allows the process to automatically get elevated by the Heimdal[™] Privileges & App Control module



Once you select a process, the **Block** and **Allow** buttons will activate:

Privileged Access Mgmt. **Application Control**

All intercepted applications (1) | Matching Allow rules | Matching Block rules | Matching Allow by default | Matching Block by default | Matching Allow with auto elevation

Hide Microsoft Application

	Process Name	Number of Executions	Publisher	Software Name	Version	MD5	Status
Select what action to take	HP Inc.	1	HP Inc.	HPSACommands	1.0.0.3		Allow by default

First Page < 1 > Last Page Go to page: Items per page: 10

Block - adds the selected process to the ruleset with Block as Action Type

Allow - adds the selected process to the ruleset with Allow as Action Type

After hitting the Allow or the Block button, a modal that enables configuration of the rule will appear:

Allow execution ×

☐ Global Update i ☐ Custom Policy Update i

Rule type

Path ▼

Subject

C:\Program Files\WindowsApps\AD2F1837.HPSupportAssistant_9.7.276.0_x64

Priority i

0

☐ Allow auto elevation ☐ Include spawns

Confirm

Cancel



Block execution ✕

☐ Global Update i ☐ Custom Policy Update i

Rule type

Path ▼

Subject

C:\Program Files\WindowsApps\AD2F1837.HPSupportAssistant_9.7.276.0_x64

Priority i

0

Confirm

Cancel

The **Global rule** radio button applies to rule on all the Group Policies, while the Custom policy global block/allow rule - applies to a Group Policy or Group Policies that can be specified in the dropdown field below.

A rule can be configured considering the following Rule Types: Software name, Path, Publisher, MD5, Signature, or Wildcard (once a Rule Type is selected, the Subject field is automatically completed).

Priority - rules are processed based on priority numbers (the higher the number is the higher the priority is). Leaving gaps between each rule is recommended (10, 20, 30, 40, etc.) in order to have an easy and neat rule organization, without having to edit existing rules. Priority ranges between 0 and 1000.

Allow auto elevation - allows the process to automatically get elevated by the HeimdalTM Privileges & App Control module (works together with Privileged Access Management)

Include spawns - allows the spawns of other child-processes from the parent-process

Application Control Group Policy settings:

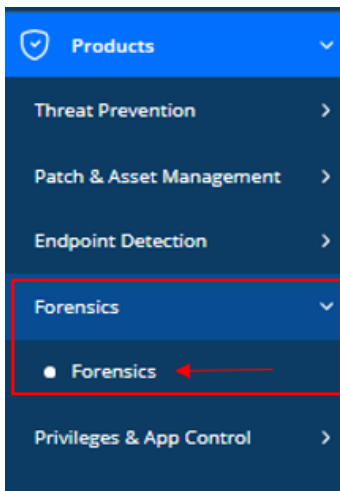
To have a better overview of this, please visit our FAQ and read about the Application Control Overview:

<https://support.heimdalsecurity.com/hc/en-us/articles/360016091937-Application-Control-overview>



7.5 Forensics

Right now, you can find a separate section for the **Forensics** view. This new section can be found in the left-side of the menu, under Products - Forensic view:



During a forensic analysis of a Windows system, it is often critical to understand when and how a particular process has been started.

In order to identify this activity, this module can extract from the target system a set of artefacts useful to collect evidences of program execution.

The module collects, preserves and analyze scientific evidence during the course of an investigation.

For an overview of the module, access the following article: <https://support.heimdalsecurity.com/hc/en-us/articles/360019571817-Forensics-Overview>

For the functionality of the module, click here: <https://support.heimdalsecurity.com/hc/en-us/articles/360019597077-Forensics-Functionality->

7.6 Email Protection

7.6.1 Spam Score interval

This feature is meant to allow you to search emails in the ADVANCED SEARCH area, by using a SPAM score interval. As we already have the minimum score box we also added a maximum spam score box and thus, allowing you to select a SPAM interval based on which emails will be searched and displayed. This option will be in Inbound and Outbound views.



The screenshot shows the 'Email Security' dashboard. At the top, there are four summary boxes: '281 Quarantined Emails', '17 Spam Emails', '2 Virus', and '3 Advanced Threats'. Below these is a search bar and tabs for 'Inbound View (372)', 'Outbound View', and 'Domain Status'. A 'Download CSV' button and an 'Advanced Filter' dropdown are also present. The 'Advanced Filter' section contains several search criteria: 'Domain', 'To', 'From', 'Type', 'Status', 'Spam Classification', 'Minimum Spam Score', and 'Maximum Spam Score'. The 'Minimum Spam Score' and 'Maximum Spam Score' fields are highlighted with a red box, and a red arrow points to them.

7.6.2 Show details button

The Show Details button will display a popup with various email details (Main, Advanced, Header and Body). If the Status of the log is other than Quarantine, the Body tab will be disabled.

The 'Details' popup window has a blue header with a close button. It contains four tabs: 'Main' (selected), 'Advanced', 'Header', and 'Body'. The 'Main' tab displays the following email details:

- ID: 1e2d7247-a298-11eb-85d1-000d3aadf580-node6.esf-we (1db19d2d-a298-11eb-85d1-000d3aadf580)
- Status: DELIVERED
- Subject: [EXT]Target Active Customers using Cisco IronPort
- From: anna.kelly@freemanadvisory.com
- To: test3@centiumtest.com
- Received: 21.04.2021 14:52:59
- Delivered: 21.04.2021 14:53:04
- Size: 12927 Bytes

Below the details is a text box containing 'centiumtest.com' with a red 'X' icon. Underneath are six buttons: 'Blacklist Sender', 'Whitelist Sender', 'Blacklist Domain', 'Whitelist Domain', 'Blacklist Email based on subject', and 'Whitelist Email based on subject'. At the bottom are four buttons: 'Release', 'Resend', 'Report', and 'CANCEL'.

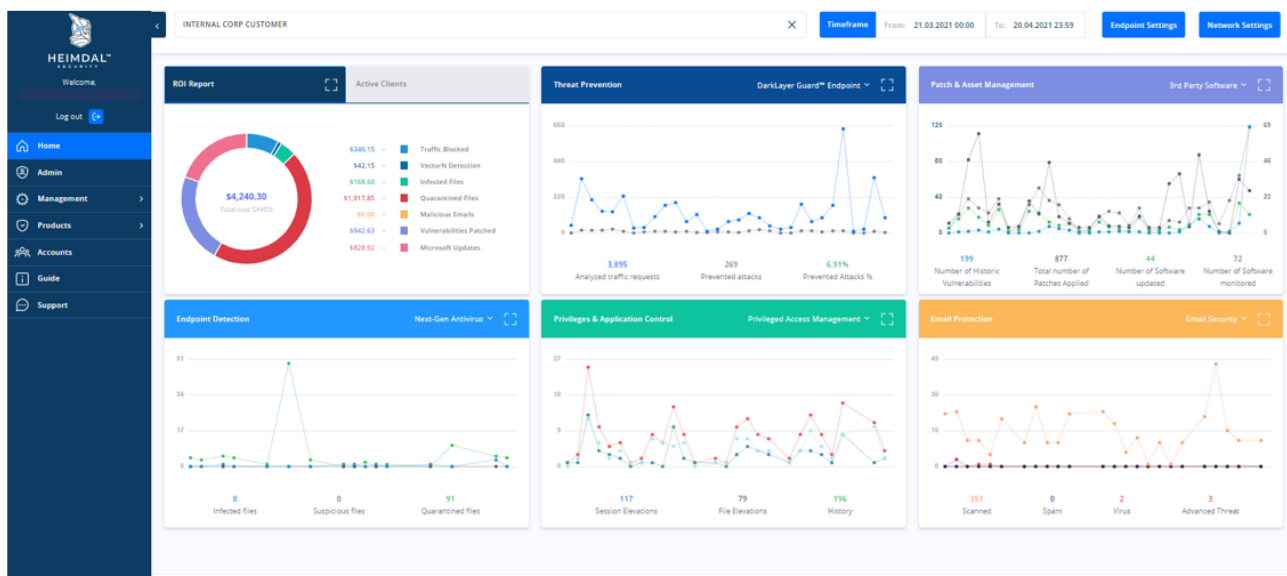
For more details access the following article: <https://support.heimdalsecurity.com/hc/en-us/articles/360007435238-Heimdal-Email-Protection>





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>



- The home page contains different graph types that can be visualized and used for reporting purposes – GDPR & audit.
- 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.
- The top options will allow for the definitions of agent behaviors as well as controlling the reporting flows.

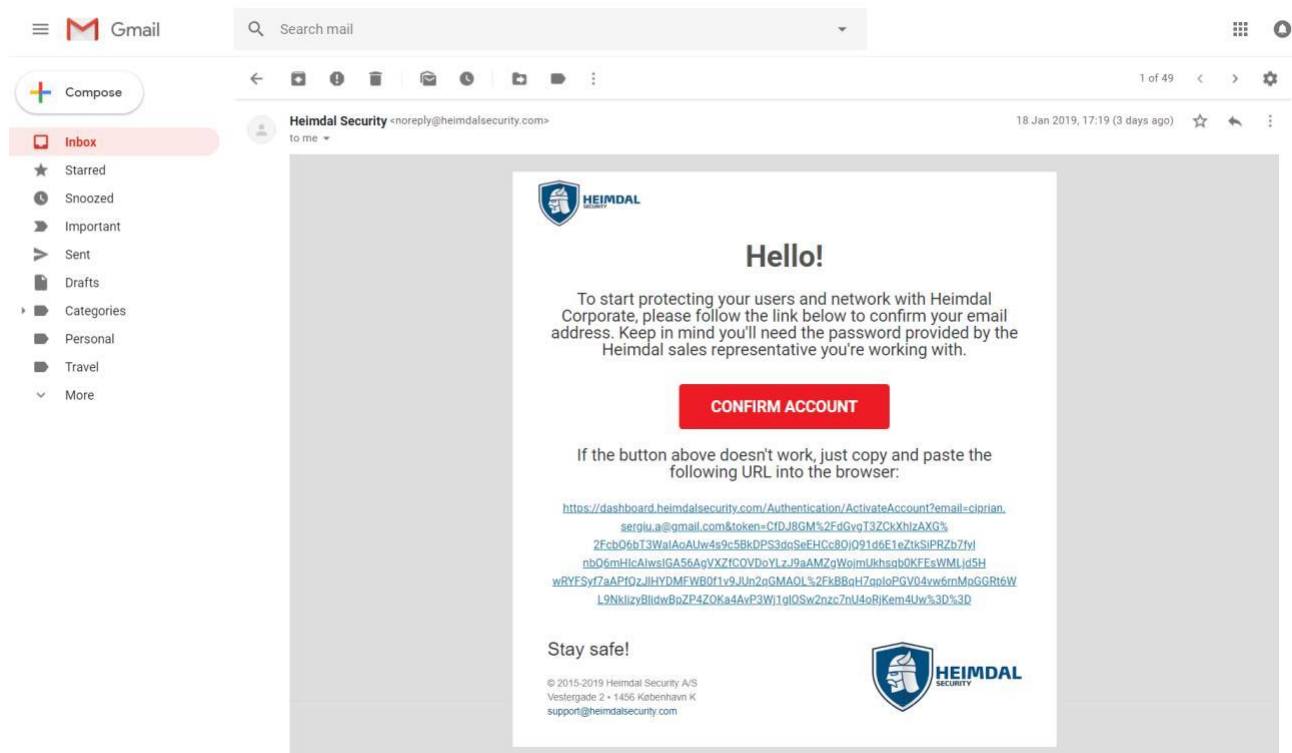


8.1 Account activation and install

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




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
2X737JNYJWQ6QLBJXAV57CQAWVEVE06PI

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

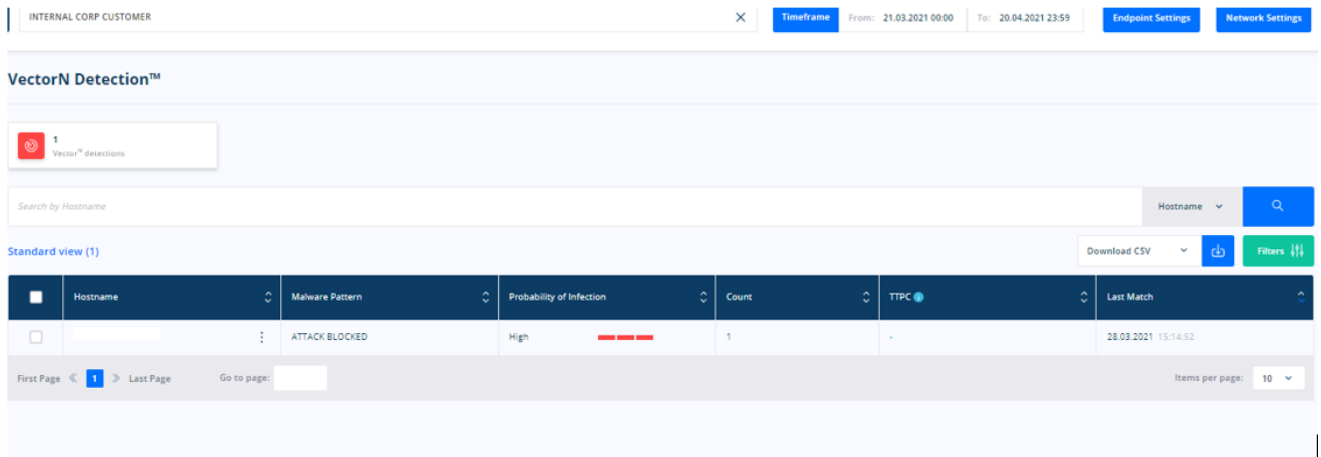
8.2 Group policies

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: <https://support.heimdalsecurity.com/hc/en-us/articles/115001856589-AD-Computer-Group-and-AD-User-Group-priority-in-Group-Policy->

8.3 Management interface for Heimdal™ Threat Prevention

8.3.1 VectorN Detection



INTERNAL CORP CUSTOMER

Timeframe: From: 21.03.2021 00:00 To: 20.04.2021 23:59

Endpoint Settings Network Settings

VectorN Detection™

1 VectorN detections

Search by Hostname

Standard view (1)

Download CSV

	Hostname	Malware Pattern	Probability of Infection	Count	TTPC	Last Match
<input type="checkbox"/>		ATTACK BLOCKED	High	1		28.03.2021 15:14:52

First Page 1 Last Page Go to page: Items per page: 10

Vector^N 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 Vector^N section for details.

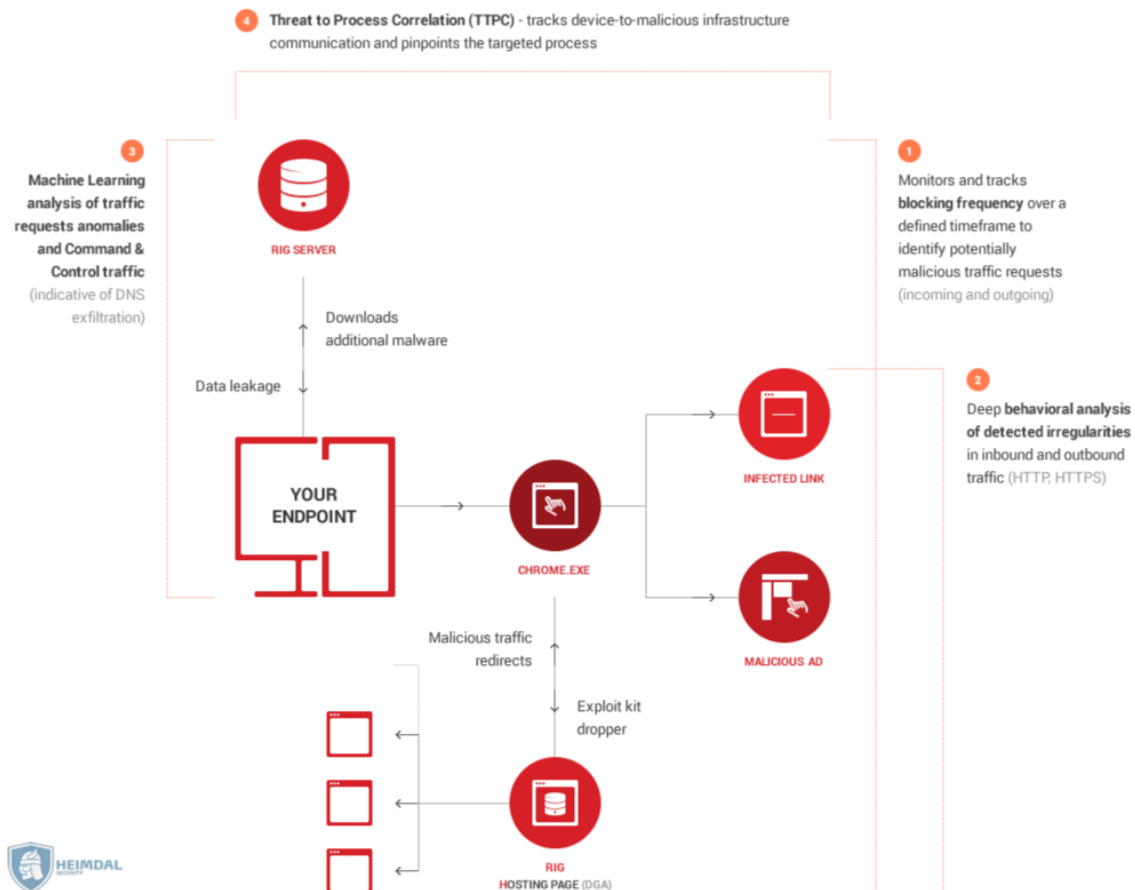
A few key things you should know about **Vector^N Detection**:

- 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 **Vector^N DetectionTM** empowers Thor users to detect and block even hidden malware attacks, preventing malware from infiltrating the system.

USE CASE:

USE CASE: **How corroborated Heimdal VECTOR^N DETECTIONTM parameters uncover hidden malware attacks**



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

If your environment is also protected by Heimdal™ Next-Gen Antivirus, Firewall & MDM, any malicious TTPC can be send to quarantine directly from the VectorN view by pressing the **Add to quarantine** button.

The **Add to storage** button will add the file or the process to your private storage from where you can download it. This button can also be found in the Quarantine view of the dashboard. The button is enabled only for non-visitor users.



VectorN Detection™

494
VectorN™ detections

Search by Hostname

Hostname

Download CSV

Filters

Standard view (21)

	Hostname	Malware Pattern	Probability of Infection	Count	TPC	Last Match
<div>Select what action to take</div> <div>Quarantine</div> <div>Add to storage</div>		BOTNET STRAIN	Moderate	53	-	19.04.2021 15:38:13
		ATTACK BLOCKED	High	1	SYSTEM IDLE PROCESS	18.04.2021 00:55:50
		ATTACK BLOCKED	High	1	CHROME.EXE	16.04.2021 19:38:30
		APT STRAIN	High	158	CHROME.EXE	15.04.2021 01:48:11

If file is quarantine, the zip from storage will contain “.hsq” file from Quarantine Heimdal folder.

After the button has been pressed you will find the file under the hostname in the active client view by clicking on that specific hostname.

Description of VectorN types:

- APT Strain is characterized by something lying on the machine that rings out at fixed intervals or times
- Attack blocked is characterized by an attempted drive-by on the machine or cross-site redirects
- Erratic communication - Reporting **erratic** activity can confirm the existence of a vulnerability or infection, helping to end an active watering hole **attack**.
- BOTNET Strain is characterized by a collection of internet-connected devices infected by malware that allow hackers to control them.

Patch & Asset Management

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

This new tab consists in two modules: 3rd Party Software and Microsoft Updates.

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.

181
Number of current vulnerabilities

877
Total numbers of patches applied

44
Number of software updated

72
Number of software monitored

Search by Hostname

Hostname

Download CSV

Latest Patch

Select view

Show Hidden Apps

Standard View (425) | Patches per Endpoint View | Assets View

	Hostname	Username	Software	Version	CVE	CVSS	Date	Status
		ageox	Google Chrome x64	90.0.4430.72	CVE-2020-16010	8.8	20.04.2021 13:16:19	✓
		ageox	AOVPN	1.0	N/A	-	20.04.2021 13:11:44	✓
		ageox	Heimdal Hostfix	1.0.1	N/A	-	20.04.2021 13:11:39	✓
		apo	Heimdal Encryption Tool	2.5.150	N/A	-	20.04.2021 12:10:58	✓
		vun	WinRAR x64	6.00.0 → 6.01.0	N/A	-	20.04.2021 12:09:16	✓



Microsoft Updates

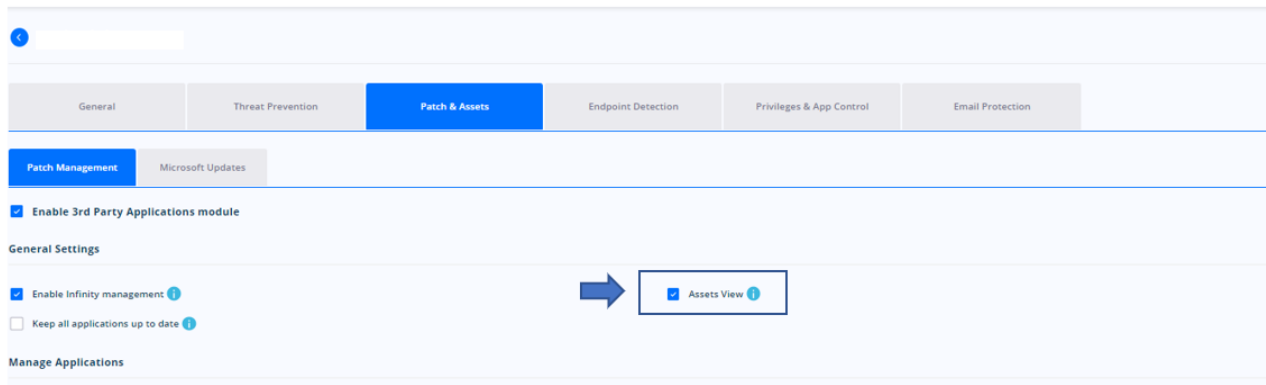
You can choose what software to install or update using policies from the Group policies tab. More details about group policies in chapter 5.2. The admin has the option to check for current vulnerabilities and by hovering the cursor over an application name, the reason for it not being updated will be displayed.

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



8.3.2 Assets View

This section displays all the applications, that are installed on the machines that run Heimdal Security suite in your organization, even if they are not patched by us. The view can be activated from the Group Policy – Patch & Assets – Patch Management.



If you select Stacked, you have an outlook of the applications names, their version and on how many computers and servers they are available.

3rd Party Updates

181
Number of current vulnerabilities

878
Total numbers of patches applied

44
Number of software updated

72
Number of software monitored

Search by Application Name

Application Name

Standard View | Patches per Endpoint View | **Assets View (589)**

Hide Microsoft Products

Download CSV

Stacked

Select view

Filters

	Application Name	Version	GUID	Installed Endpoints	Installed Servers	Uninstallable	Supported
<input type="checkbox"/>	7-Zip 18.01 (x64)	18.01	-	1	0		
<input type="checkbox"/>	7-Zip 19.00	19.00.00.0	23170F69-40C1-2701-1900-000001000000	4	0		
<input type="checkbox"/>	7-Zip 19.00 (x64 edition)	19.00.00.0	23170F69-40C1-2702-1900-000001000000	107	0		
<input type="checkbox"/>	Accordance	13.1.5	-	3	0		
<input type="checkbox"/>	Accordance	13.1.7	-	5	0		
<input type="checkbox"/>	Adobe Acrobat 2017	17.011.30194	AC768A86-1033-FFFF-7760-0E1108756300	19	0		
<input type="checkbox"/>	Adobe Acrobat DC	19.012.20035	AC768A86-1033-FFFF-7760-0C0F074E4100	1	0		

By clicking on the numbers next to the name of an application, a new page will be opened where you can check on which machines that program has been installed.

3rd Party Updates

181
Number of current vulnerabilities

878
Total numbers of patches applied

44
Number of software updated

72
Number of software monitored

Search by Application Name

Application Name

Standard View | Patches per Endpoint View | **Assets View (589)**

Hide Microsoft Products

Download CSV

Stacked

Select view

Filters

	Application Name	Version	GUID	Installed Endpoints	Installed Servers	Uninstallable	Supported
<input type="checkbox"/>	7-Zip 18.01 (x64)	18.01	-	1	0		
<input type="checkbox"/>	7-Zip 19.00	19.00.00.0	23170F69-40C1-2701-1900-000001000000	4	0		
<input type="checkbox"/>	7-Zip 19.00 (x64 edition)	19.00.00.0	23170F69-40C1-2702-1900-000001000000	107	0		
<input type="checkbox"/>	Accordance	13.1.5	-	3	0		
<input type="checkbox"/>	Accordance	13.1.7	-	5	0		



In this page, by clicking on Details, you can also see more information about the application: name, version, publisher and if it can be uninstalled from the activate or if it is patched by Heimdal Security.

[Back to Assets View](#)

Software Name: 7-Zip 18.01 (x64)
Version: 18.01 GUID: - Publisher: Ig Uninstallable: Supported:

Search by Hostname Hostname

Assets (1)

Hostname	Username	Server	Uninstallable	Supported
	nvo	No		

The Non-stacked option allows to view each version of a software and on which hostname it is installed.

3rd Party Updates

181 Number of current vulnerabilities 878 Total numbers of patches applied 44 Number of software updated 72 Number of software monitored

Search by Application Name Application Name

Standard View | Patches per Endpoint View | **Assets View (3392)** Hide Microsoft Products Download CSV Non-stacked Select view Filters

	Application Name	Version	GUID	Hostname	Username	Machine Type	Uninstallable	Supported	Date
<input type="checkbox"/>	7-Zip 18.01 (x64)	18.01	-						20.04.2021 15:23:32
<input type="checkbox"/>	7-Zip 19.00	19.00.00.0	23170F69-40C1-2701-1900-000001000000						17.04.2021 15:33:15
<input type="checkbox"/>	7-Zip 19.00	19.00.00.0	23170F69-40C1-2701-1900-000001000000						20.04.2021 09:33:34
<input type="checkbox"/>	7-Zip 19.00	19.00.00.0	23170F69-40C1-2701-1900-000001000000						20.04.2021 12:00:08

When you select an application that has the green tick under the *uninstall* column you have the option to add it to a Group Policy's uninstall list. Applications can be removed by Heimdal only in the cases where they can be uninstalled silently.

If an application has a green tick under the *supported* column, then you can add it to a GP in which it is not selected for installation for easier management so that it will be installed or kept up to date.

3rd Party Updates

181 Number of current vulnerabilities 878 Total numbers of patches applied 44 Number of software updated 72 Number of software monitored

Search by Application Name Application Name

Standard View | Patches per Endpoint View | **Assets View (3392)** Hide Microsoft Products Download CSV Non-stacked Select view Filters

	Application Name	Version	GUID	Hostname	Username	Machine Type	Uninstallable	Supported	Date
<input type="checkbox"/>	7-Zip 19.00	19.0.17.135	-						20.04.2021 09:50:49
<input type="checkbox"/>	Mozilla Maintenance Service	88.0	-						20.04.2021 09:50:49
<input type="checkbox"/>	Intel(R) Network Connections Drivers	20.2	-						20.04.2021 09:50:49

Add to Group Policy Apply

- ☐ Add to Group Policy
- ☐ Uninstall

Hide Microsoft products button, if selected, will hide from Assets view all the Microsoft product.



8.3.3 Microsoft Updates

The Microsoft Updates tab displays and allows filtering by the title, KB, the number of devices and on which OS that was installed on and the category.

Microsoft Updates

5784 Installed

255 Available/Pending

Search by Title

Title

Installed (1016)

Pending

Available

Updates Per Endpoint

Compliance View

Show Hidden Updates

Download CSV

Select Group Policy

Select GP

	Title	KB	Severity	Endpoints	Servers	CVE	CVSS	Products	Categories
<input type="checkbox"/>	Windows Malicious Software Removal Tool x64 - v5.87 (KB890830)	890830	None	71	0	N/A	-	Windows 10, Windows 10 LTSB, Windows 10, version 1903 and later	Update Rollups
<input type="checkbox"/>	Windows Malicious Software Removal Tool x64 - February 2020 (KB890830)	890830	None	22	0	N/A	-	Windows 10, Windows 10 LTSB	Update Rollups
<input type="checkbox"/>	Windows Malicious Software Removal Tool x64 - November 2019 (KB890830)	890830	None	16	0	N/A	-	Windows 10, Windows 10 LTSB	Update Rollups
<input type="checkbox"/>	Windows Malicious Software Removal Tool x64 - v5.88 (KB890830)	890830	None	99	0	N/A	-	Windows 10, Windows 10 LTSB, Windows 10, version 1903 and later	Update Rollups

In case you want to find out more details about a certain KB, clicking on its number will redirect you to the Microsoft Support page.

For each update we provide information such as name, number, release date and a short description.

Back to Microsoft Updates

Update name: Windows Malicious Software Removal Tool x64 - v5.87 (KB890830)
KB ID: (KB890830)

Install

Remove

Hide Update

Show Update

Installed

Pending

Available

Details

Update Details

Update Name:	Windows Malicious Software Removal Tool x64 - v5.87 (KB890830)
KB ID:	(KB890830)
Security Bulletin:	-
CVE:	N/A
CVSS:	0
Release Date:	09.03.2021 02:00:00
Products:	Windows 10, Windows 10 LTSB, Windows 10, version 1903 and later
Categories:	Update Rollups
Description:	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Blaster, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.

Also, the lists of machines where it was installed, where is pending installation or on which computers the update is available to be deployed.



Microsoft Updates

5784
Installed

255
Available/Pending

Search by Title

Title

Installed (1016) | Pending | Available | Updates Per Endpoint | Compliance View

Show Hidden Updates

Download CSV



Select Group Policy

Select GP

	Title	KB	Severity	Endpoints	Servers	CVE	CVSS	Products	Categories
<input type="checkbox"/>	Windows Malicious Software Removal Tool x64 - v5.87 (KB890830)	890830	None	71	0	N/A	-	Windows 10, Windows 10 LTSC, Windows 10, version 1903 and later	Update Rollups
<input type="checkbox"/>	Windows Malicious Software Removal Tool x64 - February 2020 (KB890830)	890830	None	22	0	N/A	-	Windows 10, Windows 10 LTSC	Update Rollups
<input type="checkbox"/>	Windows Malicious Software Removal Tool x64 - November 2019 (KB890830)	890830	None	16	0	N/A	-	Windows 10, Windows 10 LTSC	Update Rollups
<input type="checkbox"/>	Windows Malicious Software Removal Tool x64 - v5.88 (KB890830)	890830	None	99	0	N/A	-	Windows 10, Windows 10 LTSC, Windows 10, version 1903 and later	Update Rollups

Installed | Pending (34) | Available | Updates Per Endpoint | Compliance View

Show Hidden Updates

Download CSV



Select Group Policy

Select GP

	Title	KB	Severity	Endpoints	Servers	Reboot	CVE	CVSS	Products	Categories
<input type="checkbox"/>	Windows Malicious Software Removal Tool x64 - v5.87 (KB890830)	890830	None	1	0	Maybe	N/A	-	Windows 10, Windows 10 LTSC, Windows 10, version 1903 and later	Update Rollups
<input type="checkbox"/>	Windows Malicious Software Removal Tool x64 - v5.88 (KB890830)	890830	None	6	0	Maybe	N/A	-	Windows 10, Windows 10 LTSC, Windows 10, version 1903 and later	Update Rollups
<input type="checkbox"/>	Feature update to Windows 10, version 20H2	5001330	None	2	0	Maybe	CVE-2021-27092	9.8	-	Upgrades
<input type="checkbox"/>	2021-04 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5001330)	5001330	None	38	0	Maybe	CVE-2021-27092	9.8	-	Security Updates
<input type="checkbox"/>	2021-03 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5000802)	5000802	None	2	0	Maybe	CVE-2021-26893	9.8	-	Security Updates
<input type="checkbox"/>	2021-02 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Windows 10 Version 20H2 for x64 (KB4601554)	4601554	None	2	0	Maybe	N/A	-	Windows 10, version 1903 and later	Updates

Microsoft Updates

5784
Installed

255
Available/Pending

Search by Title

Title

Installed | Pending | Available (28) | Updates Per Endpoint | Compliance View

Show Hidden Updates

Download CSV



Select Group Policy

Select GP

	Title	KB	Severity	Endpoints	Servers	Reboot	CVE	CVSS	Products	Categories
<input type="checkbox"/>	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.335.1249.0)	2267602	None	3	0	No	N/A	-	Microsoft Defender Antivirus	Definition Updates
<input type="checkbox"/>	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.335.1234.0)	2267602	None	1	0	No	N/A	-	Microsoft Defender Antivirus	Definition Updates
<input type="checkbox"/>	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.335.1193.0)	2267602	None	1	0	No	N/A	-	Microsoft Defender Antivirus	Definition Updates
<input type="checkbox"/>	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.335.1254.0)	2267602	None	1	0	No	N/A	-	Microsoft Defender Antivirus	Definition Updates
<input type="checkbox"/>	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.335.966.0)	2267602	None	1	0	No	N/A	-	Microsoft Defender Antivirus	Definition Updates



How to roll out Microsoft Updates from Heimdal™ Patch & Asset Management:

1. Go to Available section
2. Select desired updates
3. Click on Install button at the top of the form

Microsoft Updates

5784 Installed | 255 Available/Pending

Search by Title

Installed | Pending | Available (28) | Updates Per Endpoint | Compliance View

Show Hidden Updates | Download CSV | Select Group Policy | Select GP

Title	KB	Severity	Endpoints	Servers	Reboot	CVE	CVSS	Products	Categories
<div>Select what action to take</div> <div><input checked="" type="checkbox"/> Install <input type="checkbox"/> Hide Updates</div>									
for Microsoft Defender on 1.335.1249.0	2267602	None	3	0	No	N/A	-	Microsoft Defender Antivirus	Definition Updates
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.335.1234.0)	2267602	None	1	0	No	N/A	-	Microsoft Defender Antivirus	Definition Updates
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.335.1193.0)	2267602	None	1	0	No	N/A	-	Microsoft Defender Antivirus	Definition Updates
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.335.1254.0)	2267602	None	1	0	No	N/A	-	Microsoft Defender Antivirus	Definition Updates

4. A dialog box will be displayed
5. Select Suppress Reboot if you want to offset the restart of the PCs after updating
6. Select Global Install to apply the updates to all Group Policies or Custom Policy then choose only the relevant GPs to be patched

INSTALL MICROSOFT UPDATES ×

INSTALL SELECTED MICROSOFT UPDATES TO:

☒ Suppress Reboot i

☐ Global install i ☐ Custom policy global install i

Yes **Cancel**

7. Then go to Group Policy, select the desired GP and make sure *Enable Microsoft Updates* is ticked under Heimdal™ Threat Prevention - Endpoint tab – Heimdal™ Patch & Asset Management- Microsoft updates.



Together with the Installed and Not Installed views, in the Dashboard you can check the Updates per Endpoint and see all the computers along with the number of patches from Microsoft for each of them.

Microsoft Updates

5784 Installed

255 Available/Pending

Search by Hostname

Hostname

Download CSV

Installed

Select View

Hostname	Username	Updates Per Endpoint
		134
		128
		123
		112
		108
		108
		107

8.3.4 Threat Prevention Endpoint

DarkLayer Guard™ Endpoint

3,913 Analyzed Traffic Requests

270 Prevented Attacks

6.90% Prevented Attacks %

0 Category Blocks

Search by Hostname

Hostname

Download CSV

Filters

Standard view (125) | Threat Type view | Hostname/Threats View | Latest Threats View | TTPC View | Category Blocks view

Hostname	Username	IP Address	Analyzed Requests	Prevented Attacks	Risk Level
		192.168.0.52	96	19	Low
		192.168.0.234	127	17	Low
		192.168.100.16	238	15	Low
		192.168.43.34	24	14	Low
		192.168.0.104	21	14	Low
		192.168.0.80	85	12	Low
		192.168.0.8	88	11	Low

Heimdal™ Threat Prevention 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 Threat Prevention Endpoint 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 Threat Prevention Endpoint 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 D Threat Prevention Endpoint 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 Heimdal™ Threat Prevention – Endpoint module.

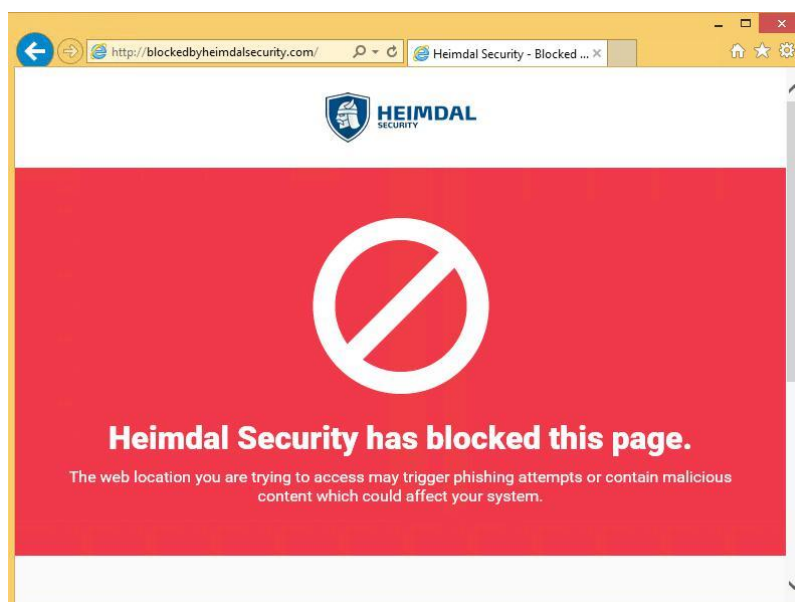
The Threat Prevention Endpoint module filters all network traffic packages and every package is intercepted. This has the following effect: not only the addresses that are manually written by the users in the URL bar are filtered but also all redirects, all additional pages that are opened when unintentionally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

Please keep in mind that the Threat Prevention Endpoint does not do SSL dissection, it does not look what's inside the packages and does not try to filter based on content. The Threat Prevention Endpoint 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

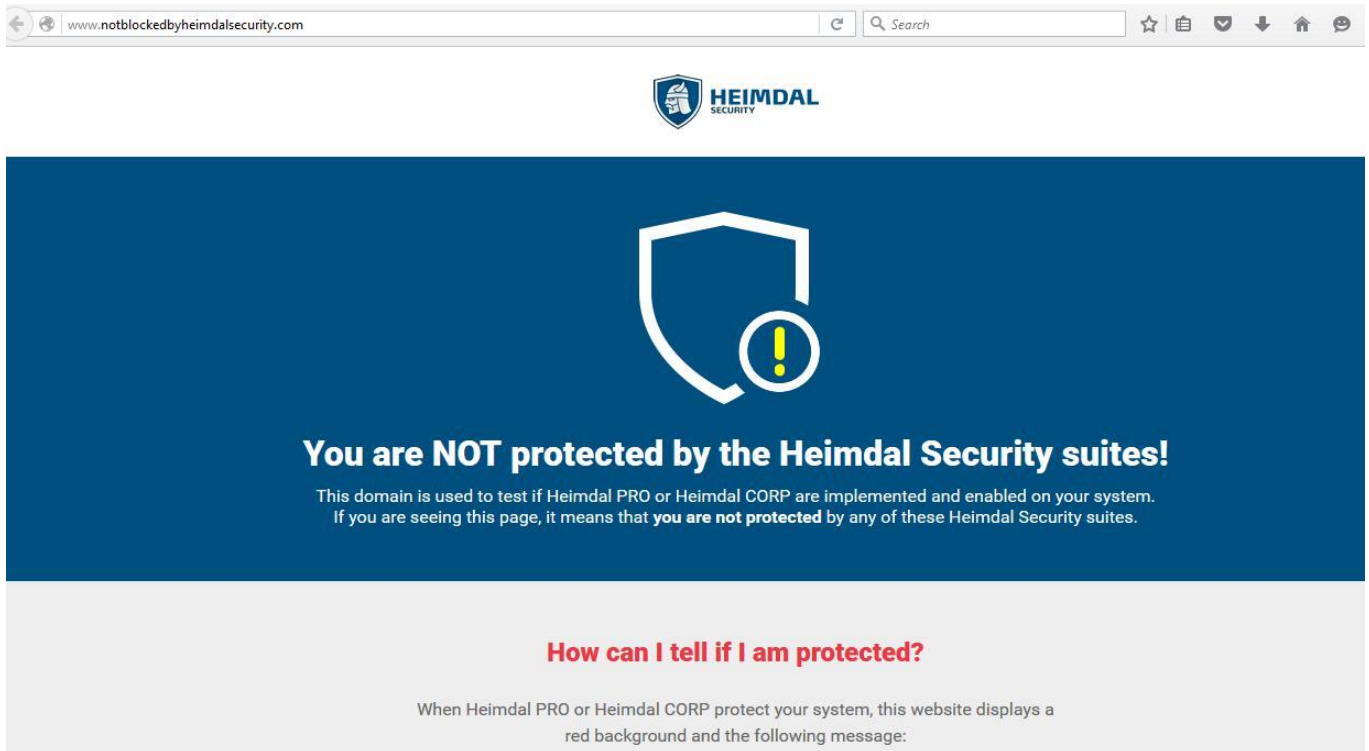
If a redirected page is blocked, this page will not open in the browser at all. However, the block will be registered inside the management interface (dashboard).

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:

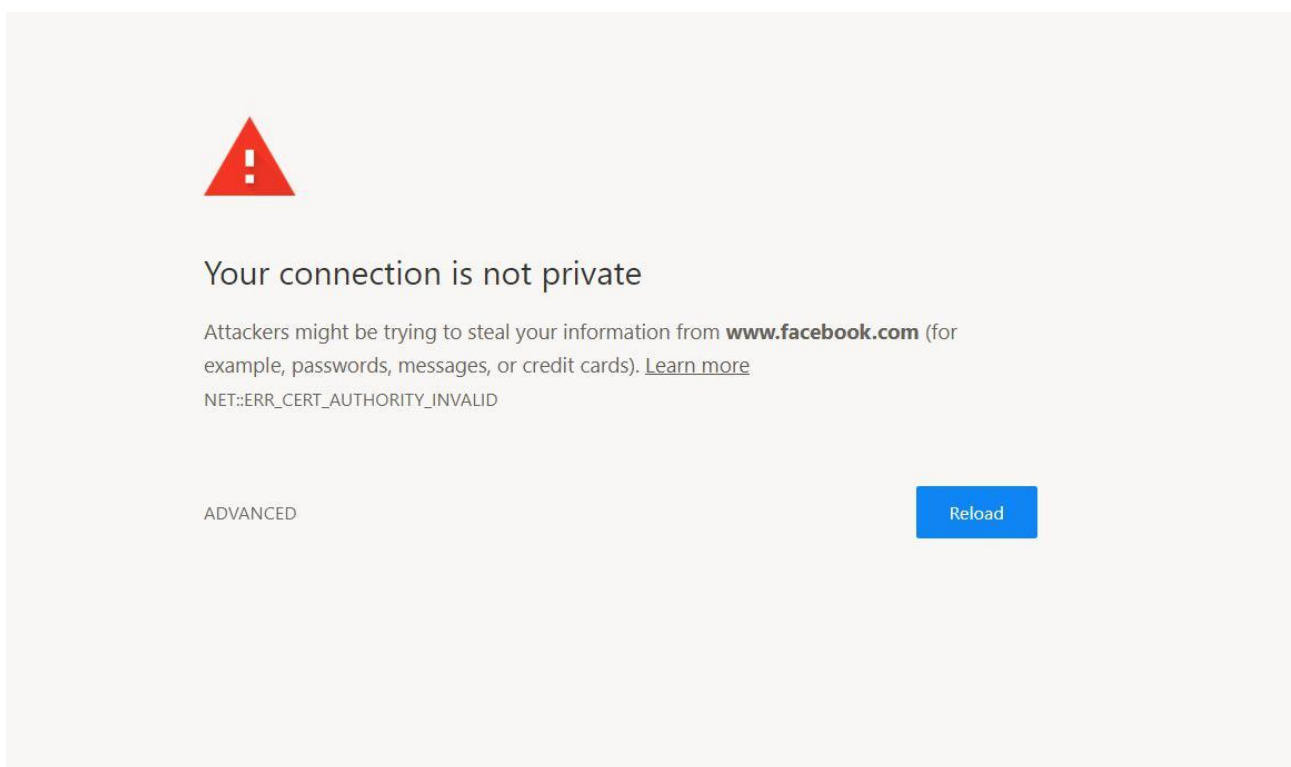




To test at client level whether the Threat Prevention Endpoint is enabled or not, visit the following website (owned and operated by Heimdal Security): <http://notblockedbyheimdalsecurity.com>. If the Threat Prevention Endpoint is not working or you don't have the Threat Prevention Endpoint option enabled,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



What happens when we prevent an HTTPS page from loading?





The **Threat Prevention Endpoint** 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.

DarkLayer Guard™ Endpoint Go to Network Page View

3,913 Analyzed Traffic Requests 270 Prevented Attacks 6.90% Prevented Attacks % 0 Category Blocks

Search by Hostname Hostname 🔍

Standard view | Threat Type view | **Hostname/Threats View (176)** | Latest Threats View | TTPC View | Category Blocks view Download CSV 📄 Filters

	Hostname	Username	Domain Blocked	Threat Type	Number of matches
<input type="checkbox"/>		adc	www.obsidian.ro	Malware	1
<input type="checkbox"/>		adi	qd.admetricspro.com	Malware	7
<input type="checkbox"/>		adi	infopicked.com	drive_by_exploits	3
<input type="checkbox"/>		adi	apprefaculty.pro	Malware	1
<input type="checkbox"/>		adi	hvacdirect.com	cc_domains	1
<input type="checkbox"/>		adi	insolencewhoeverinsult.com	Malware	1

8.3.5 Forensic view

The new view can be found on the left side of the menu:

Forensics

4 Alerts

Search by Process Process 🔍

Executions (4) Download CSV 📄

	Process	Process ID	VirusTotal	Hostname	Local IP	Remote IP	Source	Score	Session ID
<input type="checkbox"/>	Heimdal.SetupBuilder	13628	-		-	-	EncryptionDetection	0	0
<input type="checkbox"/>	php	18948	-		-	-	EncryptionDetection	0	0
<input type="checkbox"/>	maverickransomware	13496	-		-	-	EncryptionDetection	0	0
<input type="checkbox"/>	openshot-qt	14688	-		-	-	EncryptionDetection	0	0

First Page 1 Last Page Go to page: Items per page: 10



Forensic view is an option that will provide more information about the domains that the **Threat Prevention Endpoint** inside the Heimdal™ Threat Prevention – Endpoint 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.

8.3.6 Management interface for Heimdal™ Next-Gen Antivirus, Firewall & MDM

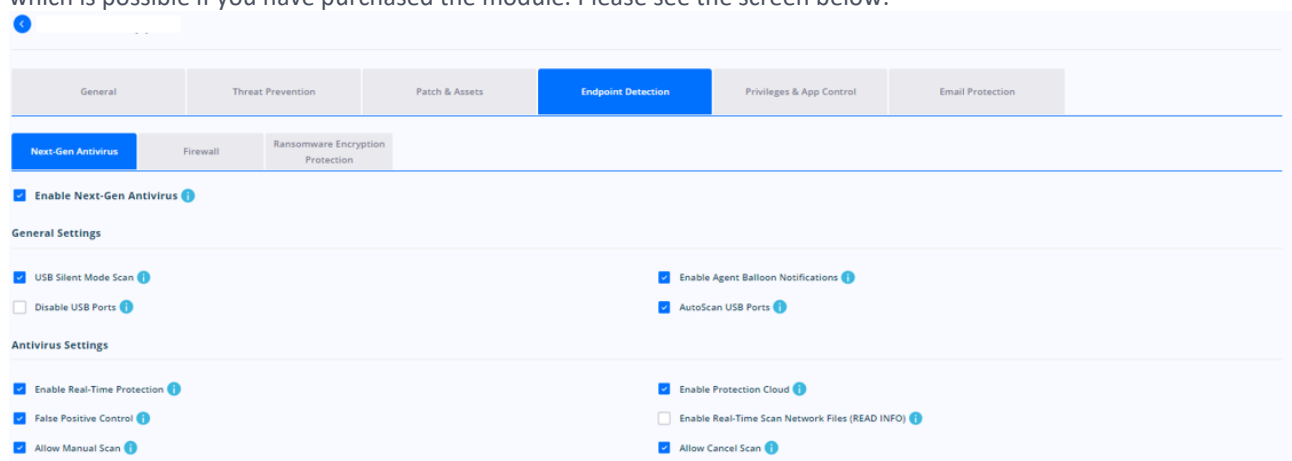
First of all, to be able to activate the Heimdal™ Next-Gen Antivirus, Firewall & MDM product, the dashboard customer needs to have this enabled in the admin console by:

- 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.

8.3.6.1 Activation of Heimdal™ Next-Gen Antivirus

In order to turn on the Heimdal™ Next-Gen Antivirus 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:





In other words, the controls for the Heimdal™ Threat Prevention and the Next-Gen Antivirus & MDM products 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 Heimdal™ Threat Prevention – Endpoint active)
- act as a strong reactive countermeasure against viruses (only Heimdal™ Next-Gen Antivirus & MDM 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.

To learn more about how to configure your Heimdal™ Next-Gen Antivirus & MDM and all its settings, please read more here:

<https://support.heimdalsecurity.com/hc/en-us/articles/213634049-Dashboard-Features-Group-Policy-Overview>

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:

- 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 access. 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.
- Quarantine** – means that the file will be automatically moved to the Quarantine and will become unavailable until removed from Quarantine.
- Allow** – the real time protection is bypassed, and the files become accessible even if found to be infected or suspicious.



8.3.6.2 Network and archive scan

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.

8.3.6.3 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.

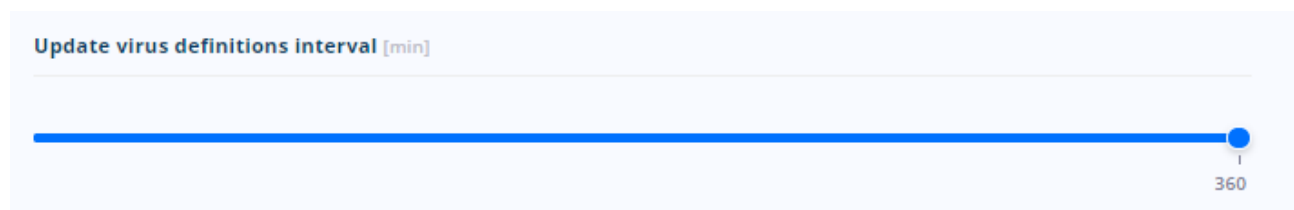
8.3.6.4 Threat types and differentiated threat response

Heimdal™ Next-Gen Antivirus, Firewall & MDM differentiates between infected files and suspicious files. Suspicious files are the files that exhibit the behavior 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 Antivirus and are not even sent to quarantine.

8.3.6.5 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.



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.



8.3.6.6 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	
Full Scan	-	Full Scan	Weekly	6 - 21	Edit Delete	
Quick Scan	-	Quick Scan	Weekly	6 - 21	Edit Delete	

As the print screen below illustrates, there are a few scan types that can be used to create a new scan profile. These are consistent with common Antivirus 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*	<input type="radio"/> Choose week day	<input type="radio"/> Choose day of month	
<input type="text"/>	<input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday	<input type="text"/>	
Scan Type*	<input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday	<input type="text"/>	
Full Scan	<input type="checkbox"/> Sunday	<input type="text"/>	
Full Scan		<input type="text"/>	
Quick Scan		<input type="text"/>	
HardDrive Scan		<input type="text"/>	
LocalDrive Scan		<input type="text"/>	
System Scan		<input type="text"/>	



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 behavior, 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 Heimdal™ Next-Gen Antivirus & MDM 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.

8.3.6.7 Creating an exclusion list

An exclusion list in the policy works pretty much like a whitelist. The Heimdal™ Next-Gen Antivirus, Firewall & MDM 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 and also patterns. You can add multiple sets of exclusions for some specific windows products (Ex: SQL Server, Windows Server 2012). In dashboard you can see a dropdown added to Normal and Realtime exclusions where those specific windows products will appear with a checkbox along them. By selecting one of these checkboxes, a list of exclusions will be added to customer currently exclusion list. A checkbox will be marked only if all exclusions from its set are in the customer’s list.



8.3.6.8 Creating a global quarantine list

A global 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.

Global Quarantine List ⓘ			
Exclusions *.CSV file	Import	Add new global quarantine	File Name ▾ Add
Search global quarantine			
File Name			
File Path			
File Name/Path	Type	Action	
chrome.exe	File Name		
cryptolocker.exe	File Name		
eclipse-inst.exe	File Name		
Zoom.exe	File Name		
ZoomInstaller.exe	File Name		

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

8.3.6.9 Managing the Antivirus detections

Once the policy was applied successfully and the Antivirus has found infected or suspicious files, these are listed under the next-gen antivirus section of the Heimdal™ Next-Gen Antivirus, Firewall & MDM module like in the below screenshot:

Next-Gen Antivirus									
Go to Firewall View									
757 Infected Files	57 Suspicious Files	301 Quarantined Files							
Search by Hostname									Hostname ▾ 🔍
Latest Infections View Infections Type view Hostname/Infections view Quarantine View (310) Exclude View Scan History									
Download CSV ▾ 📄 Filters 🏠									
	Hostname	Username	File	MD5	Threat Category	Infection name	Status	Resolution	Timestamp
<input type="checkbox"/>		:	googleupdate.a3x	84a5746202dece74d907a37015a01d4	Worm	Worm/verecno.gen2	Infected	Quarantined	21.04.2021 08:12:07
<input type="checkbox"/>		:	14b3eac7-4030-4b5b-8b95-33c4777b91fe.hsq.hsp	2c0d78dce96e06ce6fb7a210e12cee09	Ap/spr	Spr/ool.monitor.8baeed	Infected	Quarantined	21.04.2021 01:55:56
<input type="checkbox"/>		:	bulvidsetup.exe	83dd3b4746bc89e75ee6561f29c15f97	Riskware	Pua/seasuite.gen	Infected	Delete/Quarantine Pending	20.04.2021 10:53:16
<input type="checkbox"/>		:	protectn.exe	39d8249d45d112970ebf8ca0134c678d	Heuristic	Heur/jagen.1108440	Infected	Delete/Quarantine Pending	20.04.2021 04:51:51

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 Endpoint – Next gen Antivirus overview you can see all threats that have been registered under the host.



General

Threat Prevention

Patch & Asset Management

Endpoint Detection

Forensics

Privileges & App Control

Detected Threats

Quarantine

Scan History

Firewall rules

Firewall Alerts

REP

A Total of: 2 Listings

<div><div></div><div>▼</div></div>	File		MDS	Threat Category	Infection Name	Status	Resolution	Timestamp
<input type="checkbox"/>	aa_v3.exe	Σ	2c0d78dce96e06ce6fb7a210e12cee09	Apc/spr	Sprtool.monitor.8baeed	Infected	ErrorQuarantine	21.04.2021 06:20:20
<input type="checkbox"/>	aa_v3.exe	Σ	2c0d78dce96e06ce6fb7a210e12cee09	Apc/spr	Sprtool.monitor.8baeed	Infected	ErrorQuarantine	17.04.2021 06:17:59

First Page

<

1

>

Last Page

Go to page:

Items per page:

10

▼

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

- Quarantine
- Exclude
- Delete

<input type="checkbox"/>			santivirusclient.exe	d61b911487899a0150514a3d00f06859	Riskware	Pua/segurazo.gen	Infected	ErrorQuarantine	20.04.2021 23:03:55
<input type="checkbox"/>			aa_v3.exe	2c0d78dce96e06ce6fb7a210e12cee09	Apc/spr	Sprtool.monitor.8baeed	Infected	FNOTEXIST	20.04.2021 22:54:23
<input type="checkbox"/>			protecon.exe	39d8249e45d112970eb78ca0134e678d	Heuristic	Heur/agen.1108440	Infected	Deleted	20.04.2021 22:48:54

- The first infected file has the 'ErrorQuarantine' status. When Thor detects a file that is in use it will wait until a reboot is performed to run the task and if it cannot then one of the above error messages will be displayed.
- The second infected file has the FNOTEXIST 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 third infected file has been marked for deletion. The only available action is cancelation of the deletion

From Scan History you can view a list of past scans that ran on the computers or the pending ones that will be performed at the next policy update on the machines.

Also, if there are any active or pending scans you can cancel them or you can just initiate any scan type on selected devices.

Latest Infections View	Infections Type view	Hostname/Infections view	Quarantine View	Exclude View	Scan History (1)	Download CSV	Filters
<input type="checkbox"/>	Hostname	Username	Group Policy	Timestamp	New Infections Found	New Suspicious Found	Resolution
Select what action to take <input type="button" value="Apply"/>							
<input checked="" type="checkbox"/>		mdl	Heimdal Support	19.04.2021 09:33:38	0	0	FULL SCAN COMPLETED
First Page < 1 > Last Page						Go to page: <input type="text"/>	Items per page: 10



8.4 HeimdalTM Management

8.4.1 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 change, 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)

	Hostname	Username	IP address	Version	Operating System	Current GP	Selected GP	Last Seen	Enabled Modules	Status
<input type="checkbox"/>			10.10.10.129	2.5.341 RC	Microsoft Windows 10 - x64	Sales Master GP	Automatic	21.04.2021 10:19:54	10 Modules >	
<input type="checkbox"/>			192.168.100.15	2.5.350 RC	Microsoft Windows 10 - x64	Heimdal Marketing	Automatic	21.04.2021 10:19:13	10 Modules >	
<input type="checkbox"/>			192.168.0.128	2.5.350 RC	Microsoft Windows 10 - x64	Heimdal Support	Automatic	21.04.2021 10:18:07	9 Modules >	
<input type="checkbox"/>			192.168.1.70	2.5.341 RC	Microsoft Windows 10 - x64	Sales Master GP	Automatic	21.04.2021 10:17:35	10 Modules >	

A Hardware view of the machine is available as well by switching from the standard view to the hardware view:



Active Clients

0 Active servers

140 Active endpoints

140 Total devices

Search by Hostname

Hostname

Download CSV

Active

Select view

Filters

Hostname	CPU	CPU %	Memory	Memory %	Disk	Disk %	Last Seen	Status
	Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz	7	8 GB	74	238 GB	2	21.04.2021 10:27:00	✓
	Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz	29	8 GB	88	238 GB	2	21.04.2021 10:26:11	⚠
	Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz	11	8 GB	81	238 GB	3	21.04.2021 10:25:37	⚠
	11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz	10	16 GB	56	476 GB	4	21.04.2021 10:25:14	✓
	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz	9	16 GB	52	476 GB	4	21.04.2021 10:24:53	⚠
	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz	42	16 GB	31	476 GB	41	21.04.2021 10:22:41	✓

8.4.2 Revoke License Button

This option can be found on the Active Clients list.

Active Clients

0 Active servers

140 Active endpoints

140 Total devices

Search by Hostname

Hostname

Download CSV

Active

Select view

Filters

	Hostname	Username	IP address	Version	Operating System	Current GP	Selected GP	Last Seen	Enabled Modules	Status
<div>Select what action to take</div> <div><div>Revoke</div><div>Delete</div><div>Isolate</div></div>			10.10.10.129	2.5.341 RC	Microsoft Windows 10 - x64	Sales Master GP	Automatic	21.04.2021 10:19:54	10 Modules >	⚠
			192.168.100.15	2.5.350 RC	Microsoft Windows 10 - x64	Heimdal Marketing	Automatic	21.04.2021 10:19:13	10 Modules >	⚠
<input type="checkbox"/>			192.168.0.128	2.5.350 RC	Microsoft Windows 10 - x64	Heimdal Support	Automatic	21.04.2021 10:18:37	9 Modules >	✓
<input checked="" type="checkbox"/>			192.168.1.70	2.5.341 RC	Microsoft Windows 10 - x64	Sales Master GP	Automatic	21.04.2021 10:17:35	10 Modules >	⚠

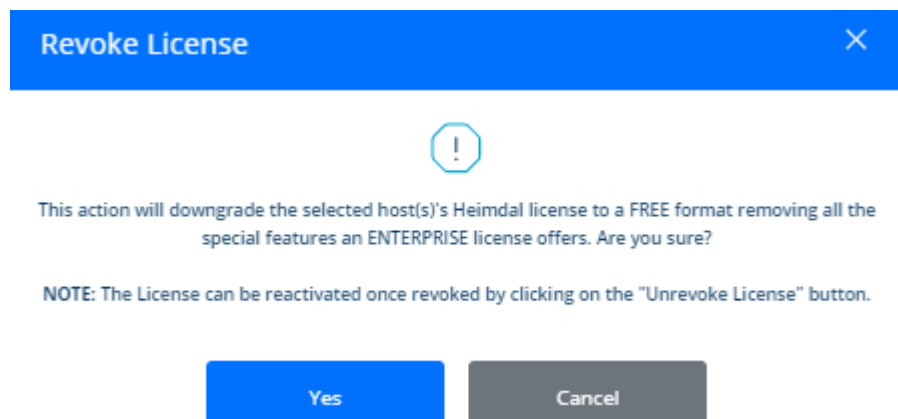
This option allows the Account Administrator to revoke the Thor usage rights on a certain Host/Machine. This means that, once the REVOKE LICENSE button will be clicked, **Thor** will **never** receive the information from the Policies set in the Dashboard (*you will be able to install Thor on that machine, 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!

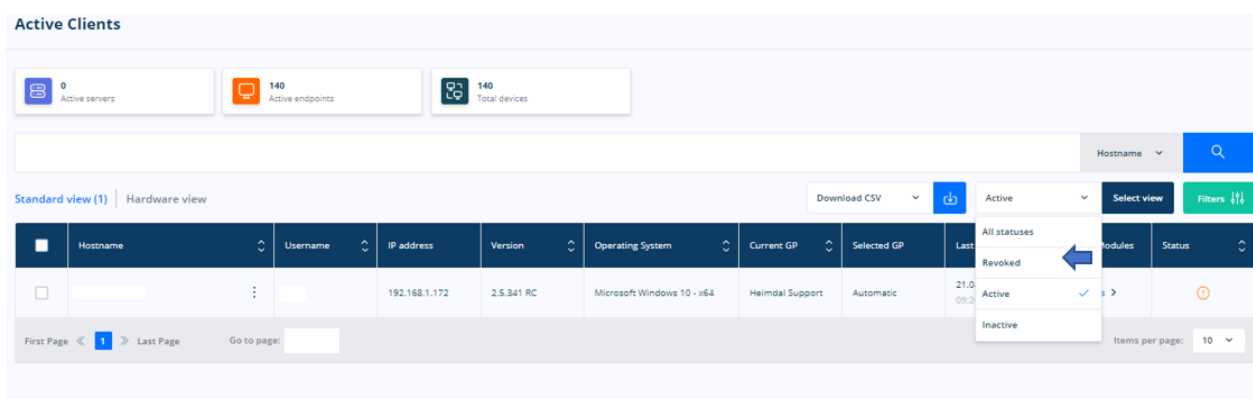
We recommend you use this option **ONLY** when a machine/computer **leaves** your organization (lost/ stolen, etc)



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

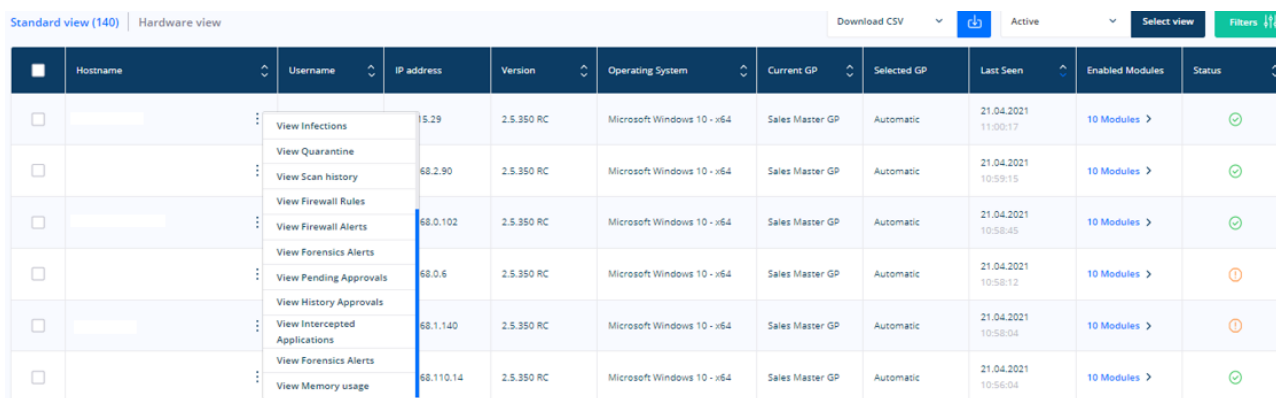


Once you pressed “Yes”, the machine for which you revoked the license will stop receiving information from the Group Policy and it will not be updated correctly. If you pressed the Revoke button by mistake or you want to revert the action, you can always press the Unrevoked License button.



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 a 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 such as: Machine info, Domain blocks, Vector^N detections, 3rd party software and Microsoft updates, Infections, Quarantine or to Scan history.





When you select the View Machine info you will be redirected to a new page that displays under the General tab details of the computer. The information is divided into 4 sections: Service Info, Operating system info and Hardware info, DNS info (tell you what DNS addresses is Heimdal using behind the scene), Enabled Modules, VDF Version and VDF timestamp.

General

Threat Prevention

Patch & Asset Management

Endpoint Detection

Forensics

Privileges & App Control

Machine info

Logs

Device Info

Hostname
Username
Last seen
Agent version
IP

nsf
21.04.2021 11:00:17
2.5.350.2000
10.0.15.29

Hardware Info

Bios version
Bios manufacturer
Motherboard serial
Motherboard serial 2
Motherboard manufacturer
Model
CPU
No. of cores
Memory
Disk serial
Disk usage

LENOVO - 1D0 | R16ET29W (1.15) | Lenovo - 1D0
LENOVO
20RD001FUK
Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz (Usage: 12 %)
4
8 GB (Usage: 71 %)
ACE4_2E00_9591_858E.
238 GB (Usage: 3 %)

Operating System Info

Description
Version
Build version
Service pack
Last reboot

Microsoft Windows 10 - x64
10.0.19042.0
19042
-
20.04.2021 19:03:51

Antivirus Info

VDF Version
VDF Timestamp

20.04.2021 18:16:12

DNS Info

Adapter Name
WiFi (DHCP DNS)

DNS Addresses
MAC Address

Enabled Modules

DarkLayer Guard

Infinity Management

Email Fraud Prevention

Ransomware Encryption Protection

VectorN

Microsoft Updates

Firewall

ThirdParty Applications

Next-gen Antivirus

Privileged Access Management

The **Logs** tab will allow you to:

- Status History of the machine
- retrieve the HeimdalLogs from the hostname
- retrieve the Windows EventViewer Logs
- download the TTPC files or the malicious files detected by HeimdalTM Next-Gen Antivirus & MDM

General

Threat Prevention

Patch & Asset Management

Endpoint Detection

Forensics

Privileges & App Control

Machine info

Logs

Status History (10) | Heimdal Endpoint Logs | Windows Event Viewer Logs | Files

Details	Started Timestamp	Resolved Timestamp	Status
An update has started!	21.04.2021 10:59:12	21.04.2021 11:00:16	
DarkLayerGuard was disabled by the uptime checker.	19.04.2021 20:09:27	20.04.2021 10:18:34	
The machine is rebooting to complete a Microsoft Update.	16.04.2021 18:42:52	19.04.2021 10:08:59	

How to apply a specific group policy to your machines

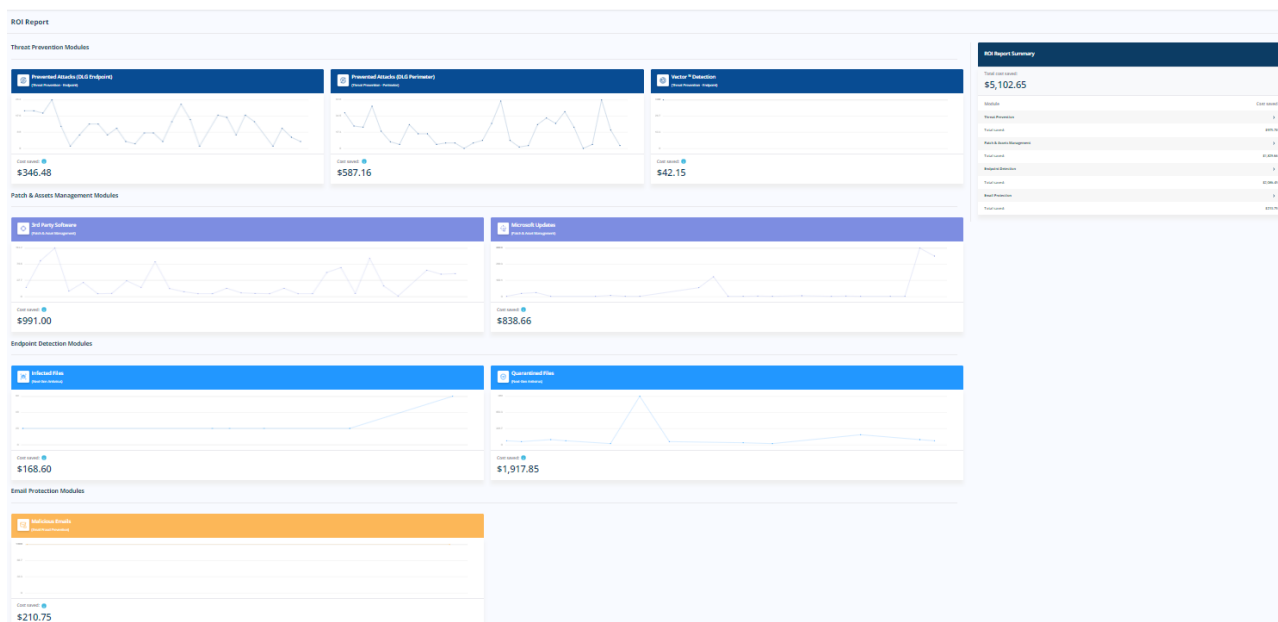
See more details here: [Apply a specific Group Policy for your machines](#)



8.4.3 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.

The new view divided this estimated return on investment by modules:



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. Heimdal™ Email Protection

9.1 Heimdal™ Email Fraud Prevention

Read here more about Email Fraud Prevention module: [Heimdal™ Email Fraud Prevention - E-Mail Fraud Prevention](#)

Read how to configure Heimdal™ Email Protection in the Group Policy here : <https://support.heimdalsecurity.com/hc/en-us/articles/213634049-Heimdal-Dashboard-features-Group-Policy-Overview>

9.2 Heimdal™ Email Security

Read here more about Email Security module: [Heimdal™ Email Security](#)

Read how to configure Heimdal™ Email Security in the Group Policy here : [Heimdal™ Email Security \(Configuration\)](#)

10. Miscellaneous

10.1 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.

10.2 Heimdal™ ApiKey?

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

10.3 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?

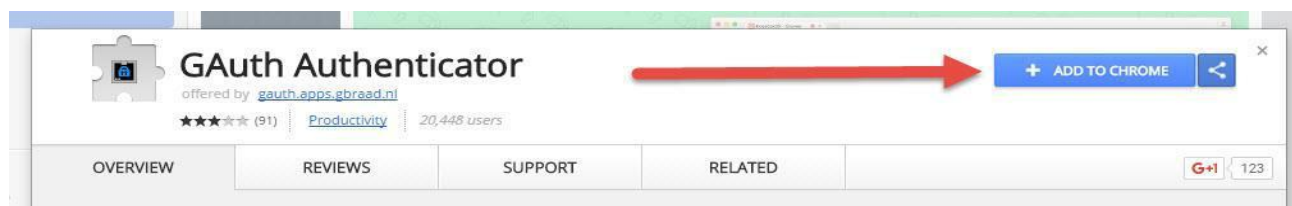
You can synchronize the time following these steps: Settings -> General -> Date & Time -> Set Automatically

10.4 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
2X737JNYJWQ6QLBJXAV57CQAWVE06PI

Current password*

New password*

Confirm new password*

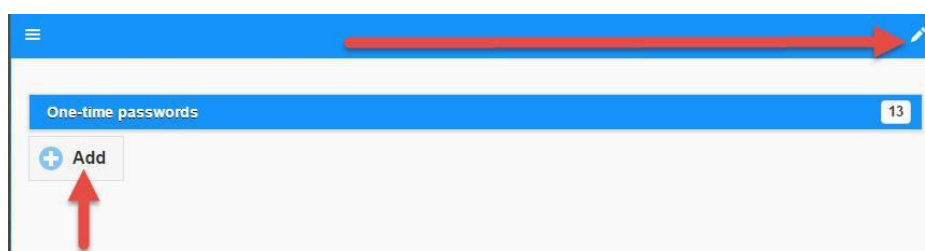
The password can be any combination of characters, and must be at least 6 characters in length, must contain a number, an upper and lower case character, and a special symbol.

Extension ready

Submit

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

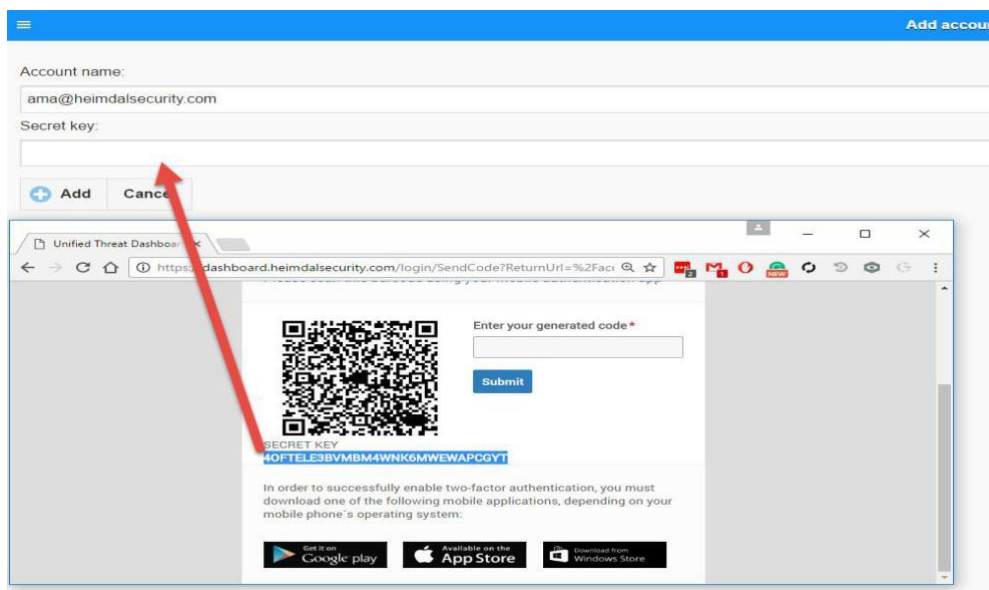
Step 4. Next, click on the + Add and Insert the email address and the Secret Code is the one from the dashboard login page.



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.



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

10.5 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 <https://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 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.

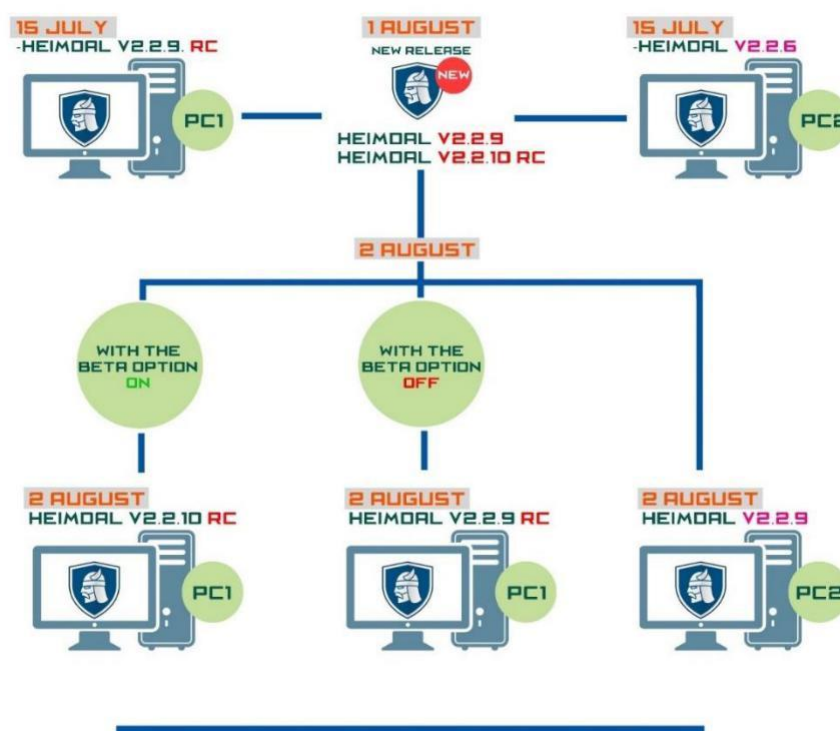
!!! The official update will always have a lower version number than the RC version (release candidate).

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!



10.6 Heimdal™ Next-Gen Antivirus, Firewall & MDM 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 Heimdal™ Next-Gen Antivirus, Firewall & MDM in your environment.

Each time you deploy Heimdal™ Next-Gen Antivirus 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.

11.6.1 Heimdal™ Next-Gen Antivirus, Firewall & MDM versus Windows Defender (WD) and System Centre Endpoint Protection (SCEP)

By default, installing Heimdal™ Next-Gen Antivirus, Firewall & MDM 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 Heimdal™ Next-Gen Antivirus, Firewall & MDM on a machine that is protected by Windows Defender and System Centre 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 Heimdal™ Next-Gen Antivirus, Firewall & MDM on a machine that is protected by Windows Defender and System Centre Endpoint Protection, this will result in WD being turned off, but SCEP will still be turned on. Heimdal™ Next-Gen Antivirus & MDM and SCEP will be running side by side BUT Heimdal™ Next-Gen Antivirus, Firewall & MDM 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 Heimdal™ Next-Gen Antivirus & MDM.](#)

10.7 Where does Heimdal save information in Widows registry?

[Agent] Log agent info in fixed registry key

In registry will be stored new values about Agent Version, GP Id and All modules enabled status (GP Name will not be stored because it is not retrieved on agent).

The above info will be stored every time clienthost retrieves or update the GP.

Flow

- Agent

- Regedit/Registry editor -> HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\HeimdalSecurity\Info or HKEY_LOCAL_MACHINE\SOFTWARE\HeimdalSecurity\Info (based on windows version 64 or 32)



The info is stored additional after install and updates of agent version because the GP retrieve/update is called when clienthost starts and will assure that the correct values are stored.

