



 **CYBONET**



# Cybowall User Guide

Last Modified 6 June 2018



# Contents

<b>Introduction</b> .....	<b>6</b>
The Threat Landscape .....	6
About Cybowall .....	7
Asset Mapping.....	7
Vulnerability Assessment .....	7
Intrusion Detection.....	8
Network Traps .....	8
SIEM Capabilities .....	9
Cybowall Workflow and Components .....	10
Port Mirroring.....	10
The Cybowall Sensor .....	10
Network Asset Mapping .....	10
The Cybowall Scanner .....	11
Event Correlation.....	11
<b>Basic Navigation</b> .....	<b>12</b>
Solution Indicators .....	12
Section Actions.....	13
Applying Changes .....	16
Returning to the Dashboard .....	16
<b>Cybowall Dashboard</b> .....	<b>17</b>
Vulnerability Management.....	17
Status Section .....	18
Vulnerabilities Section .....	22
Risk Assessment Section.....	28
Breach Detection.....	31
Malware Hunter Section .....	31
Lateral Movement Section .....	32
Traffic Analysis Section .....	33
Network Visibility .....	34
Network Map Section.....	34
Network Visibility Section.....	35
Top Scored Hosts.....	36



<b>Network View .....</b>	<b>37</b>
Windows Hosts.....	37
Searching for Hosts .....	38
Windows Host Details .....	39
Other Hosts .....	45
Other Host Details .....	45
Generating a Host Specific Report.....	46
Network Map .....	47
Investigating Hosts .....	47
<b>Network Forensics .....</b>	<b>50</b>
Net Sensor Events .....	50
Searching for Events.....	50
Organizing and Exporting Events.....	51
Intrusion Detection Categories.....	52
Updating or Managing IDS Signature Rules .....	53
Host Events.....	56
<b>Policy .....</b>	<b>58</b>
Network Scanner .....	58
Port Profiles.....	60
Creating Port Profiles .....	60
Assigning Port Profiles .....	61
WMI.....	62
Malware Hunter .....	64
Editing Malware Hunter Profiles .....	64
Creating Malware Hunter Profiles .....	65
IDS .....	66
Selecting IDS Profiles .....	66
Editing IDS Signatures.....	67
Customizing the IDS.....	68
<b>Reports .....</b>	<b>71</b>
Selecting Report Criteria .....	71
Available Reports.....	72
Exporting and Annotating Reports .....	73
<b>System Settings.....</b>	<b>75</b>
Network Devices .....	75
Notifications .....	83



Date and Time ..... 85

Users ..... 86

Network Tools ..... 87

Licensing ..... 88

SSL Certificate..... 89

Backup..... 90

**Revision History ..... 91**

**About CYBONET ..... 92**



# Introduction

This User Guide provides an overview of CYBONET's Cybowall solution; how it works and how to use the solution.

It begins with a section introducing the threat landscape and discussing the capabilities and components of Cybowall. Thereafter it follows the layout of the Cybowall User Interface (UI) – starting with the dashboard and navigating through the various tabs that comprise the Cybowall solution.

This guide is intended for anyone employing Cybowall – including network engineers, system administrators, IT managers, human resource managers and compliance officers.

## The Threat Landscape

Businesses today are exposed to an ever-increasing number of threats:

- Network-based threats — aimed at networks and network infrastructure
- Host-based threats — aimed at individual hosts
- External threats — coming from external attackers
- Internal threats — coming from internal attackers

Although the goal of security solutions is to detect and prevent such threats, no network can be completely protected from them all.

Measures for mitigating risk, identifying vulnerabilities, and detecting threats include the following:

- Identifying patterns of events that indicate a possible threat or vulnerability
- Determining the risk of potentially harmful attacks or compromise
- Enabling targeted responses to identified attacks
- Performing ongoing monitoring and reporting of network and host-based activities



# About Cybowall

Cybowall focuses on mitigating risk, identifying vulnerabilities, detecting threats, and prioritizing responses to the most critical threats and vulnerabilities.

The Cybowall solution helps detect threats and prioritize responses by leveraging the capabilities outlined below.

## Asset Mapping

Performing asset mapping is first essential step to knowing what systems and devices are connected to the network.

Cybowall combines 3 core discovery and inventory technologies to provide visibility into the devices connected to the network.

Features include:

- Active and Passive Network Scanning
- Asset Inventory
- Service Inventory

## Vulnerability Assessment

Integrated vulnerability scanning informs about network vulnerabilities, so that these can be prioritized for patch deployment and remediation. Continuous correlation of the dynamic asset inventory with Cybowall's vulnerability database provides up-to-date information regarding network vulnerabilities in between scheduled scans.

Cybowall identifies assets and devices with unpatched software, insecure configurations, and other network vulnerabilities.

Features include:

- Continuous Vulnerability Monitoring
- Authenticated / Unauthenticated Active Scanning
- Remediation Verification



# Intrusion Detection

Monitoring of network access across both wired and wireless networks using host and network-based detection systems identifies attempts to access those systems, files, and content.

Cybowall coordinates incident response and threat detection across the network with built-in security monitoring technologies.

Features include:

- Network-based Intrusion Detection System (IDS)

# Network Traps

Easily deployed network traps provide detection capabilities that empower Cybowall to proactively identify active intrusions and lateral movement.

Network traps are able to prevent attacks by:

- Slowing down or stopping automated attacks, such as worms or autorooters – attacks that randomly scan an entire network looking for vulnerable systems to put in a ‘holding pattern’
- Deterring human attacks by sidetracking an attacker – causing them to devote attention to activities that cause neither harm nor loss, and enabling the organization to analyze, mitigate and report such breaches



# SIEM Capabilities

Security Information and Event Management (SIEM) capabilities enable relevant data affecting network security to be reviewed and analyzed as a whole, highlighting trends and unusual patterns. Data is monitored for unusual activity, with relevant security event identification helping to pinpoint policy violations and accelerating incident response and analysis.

Use SIEM to:

- Conduct forensic analysis of events to discover and analyze the source of security attacks and incidents
- Report on security-related incidents and events, such as successful and failed logins, malware activity and other potentially malicious activities
- Obtain alerts of activities that run against pre-determined policy and could indicate a security issue
- Meet compliance mandates by leveraging log data and reporting

Cybowall facilitates the identification, containment, and remediation of threats to the network by prioritizing risk and enabling response procedures.

Features include:

- Log Management
- Event Management
- Event Correlation
- Reporting



# Cybowall Workflow and Components

The Cybowall solution collects raw data from network devices, then parses that data into a stream of events which can be stored, filtered, and correlated to identify threats and vulnerabilities.

Cybowall is easy to deploy in the network. It is available as a physical installation or installed as a virtual host on VMware or Hyper-V. Refer to the Cybowall Quick Installation Guide (QIG) and Cybowall Configuration Guide for step-by-step instructions on installing and configuring Cybowall.

The Cybowall solution incorporates the components detailed below.

## Port Mirroring

Most network core switches have the ability to copy network traffic from one port on the switch to another. This feature, which is called port mirroring or port monitoring, enables Cybowall to capture traffic data for analysis.

## The Cybowall Sensor

Passively collect logs and mirrored traffic, and actively probe assets on the network to obtain information about current network activity.

## Network Asset Mapping

Identify network assets and collect information from target machines as part of the asset mapping feature, leveraging a subset of SMB, NETBIOS, and ICMP protocols. This asset map includes the localhost, IP, computer name, computers list, IP range, whole domain/workgroup and/or organizational unit.



# The Cybowall Scanner

Once assets have been identified, the Cybowall Scanner performs an additional scan that collects information related to the host. Cybowall's scan leverages a variety of techniques to collect this information, ranging from file and folder property checks, registry checks, Windows Management Instrumentation (WMI) commands, SMB commands as well as port scan checks (TCP/UDP) and more. The scanner parses the raw data from different sources and transforms it into a stream of events, each having a common set of data fields.

## Event Correlation

Cybowall correlates events, assesses their risk levels and then stores them for forensic analysis, archiving, and regulatory compliance.

# Basic Navigation

This section provides basic details and tips on navigating and viewing information within the Cybowall UI.

## Solution Indicators

The top menu bar of Cybowall indicates the status of Cybowall:



The **Cbw** and **IDS** indicators show that the system is functioning and a hoverbox provides details of how long it has been active.

The dial provides a snapshot of CPU and Memory usage, with percentage details given in a hoverbox.

Click on **More** to the right of these indicators to view more indicators under the **System settings > System status** tab.



# Section Actions

On the Cybowall dashboard, the **Vulnerabilities** and **Risk assessment** section headers take the following format:



## Section Name

- The green box on the top left shows the name of the section

## Expand View

- To expand a section, click the three dots to the right of the section to see all the information in the expanded view
- To return to the dashboard from an expanded section, click anywhere on the grey area outside the expanded section

## Number of Records in View

To choose the number of records that appear on each page, click the **down arrow** in the orange box to the top right of the expanded view section

Select how many records to view at once (5, 10, 25, 50, 100):



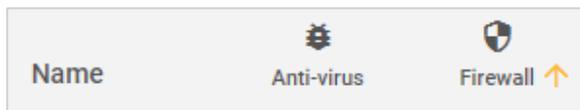
## Page Selection

To view the information appearing on the next/previous page, click the **grey arrow** buttons underneath the list of hosts in the expanded view:



## Order of Hosts

To sort the list of hosts by category, click on the **column heading** for each category. A small orange arrow appears to the right of the category heading:

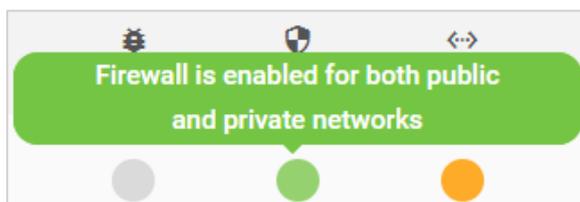


The list of hosts is sorted according to that category. Click again and the order reverses.

To sort alphabetically by host name, click on the **Name** column. The down arrow shows the hosts ordered from A-Z and vice versa.

## Additional Explanations

Hovering over various indicators in Cybwall shows a hoverbox which provides additional explanations of that measure:

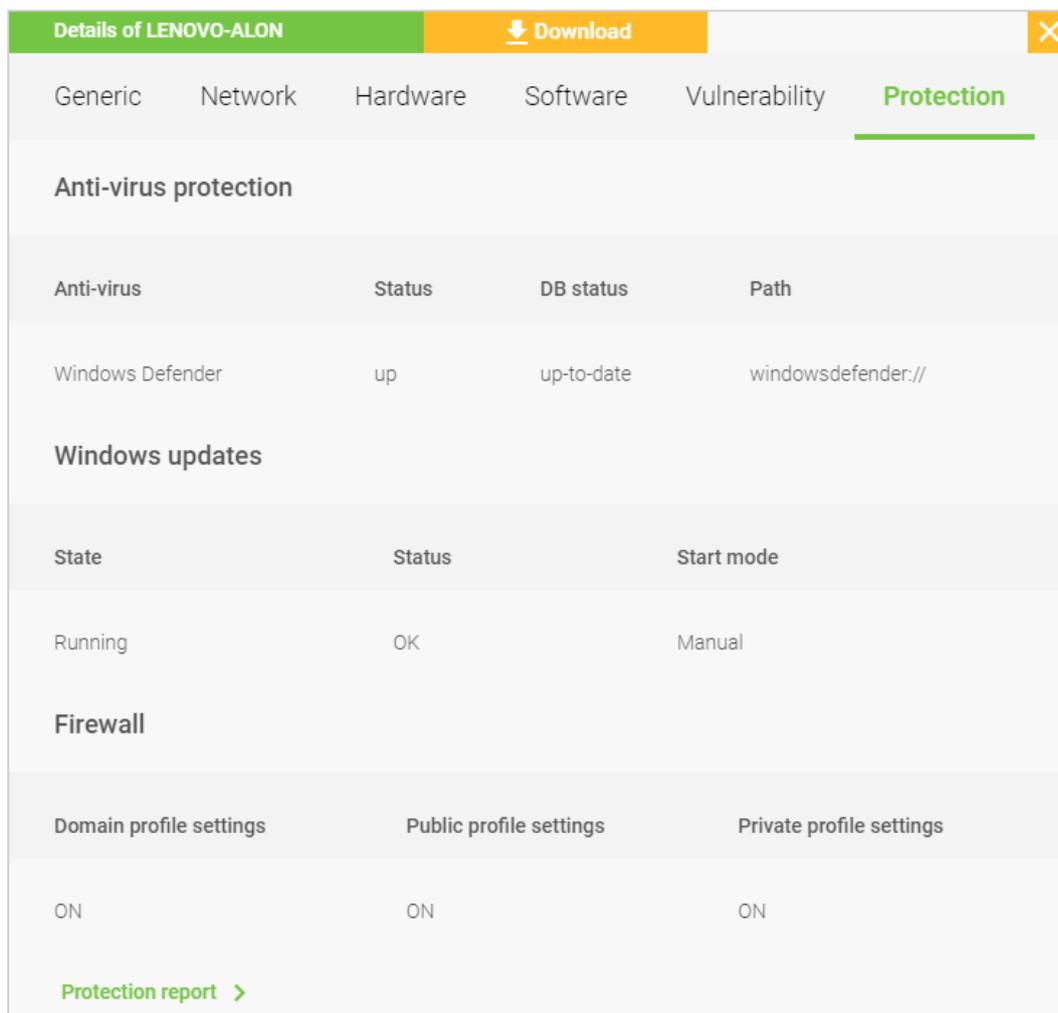


## Investigating Individual Hosts

To drill down further to review the status of a host, click the individual host in the **Name** column:



The **Host details** window appears, with the various tabs providing further information about the individual host:

A screenshot of a web application window titled "Details of LENOVO-ALON". The window has a green header bar with the title and a "Download" button with a download icon. Below the header is a tabbed interface with tabs for "Generic", "Network", "Hardware", "Software", "Vulnerability", and "Protection". The "Protection" tab is active and underlined. The content area shows sections for "Anti-virus protection" and "Windows updates".

Anti-virus	Status	DB status	Path
Windows Defender	up	up-to-date	windowsdefender://

State	Status	Start mode
Running	OK	Manual

Domain profile settings	Public profile settings	Private profile settings
ON	ON	ON

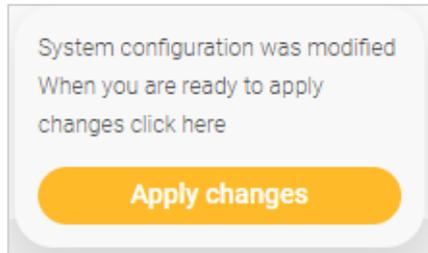
Protection report >

See the Network View – Windows Host Details section of this guide for further information.



# Applying Changes

When configuration changes are made, a pop-up may appear at the bottom right hand side of the view:



Click **Apply changes** to ensure the configuration changes take effect.

# Returning to the Dashboard

To return to the dashboard from any tab within Cybowall, either click on the **Wall** tab heading, or click on **CYBOWALL** or the **CYBONET logo** in the left hand corner of the top menu bar:





# Cybowall Dashboard

The Cybowall dashboard, (the “Wall”), has been designed to enable a single view of the organization’s network security – providing simple, actionable information and alerts.

The dashboard is broken down into separate sections that highlight information on a particular aspect of network security, and is organized as follows:

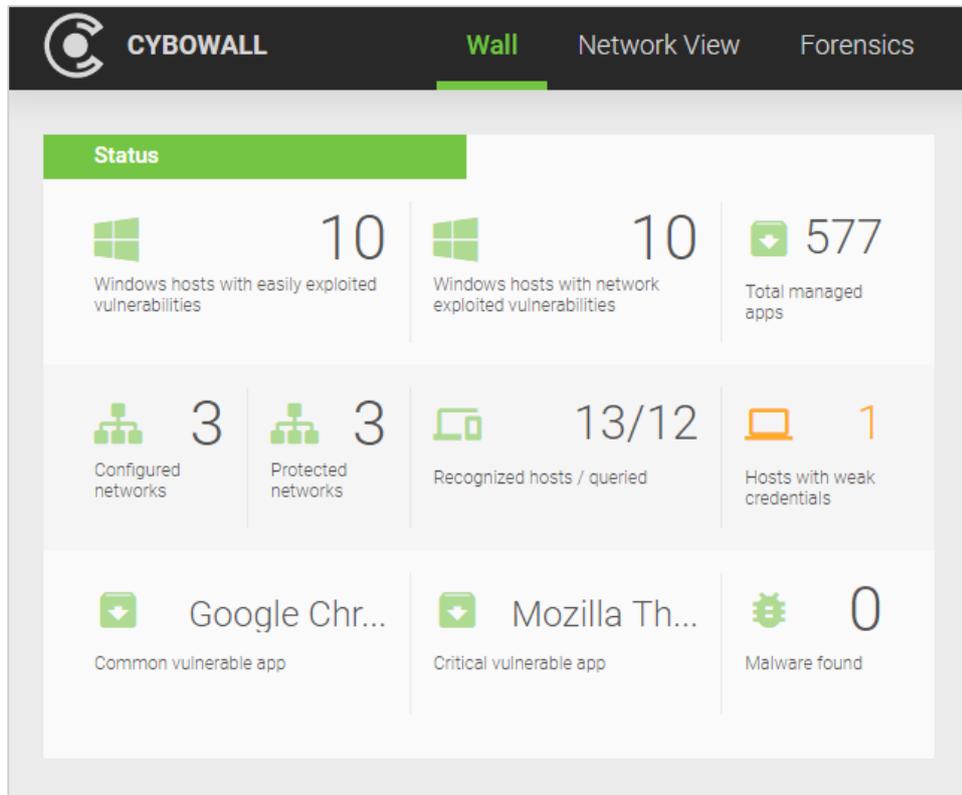
- Top row: **Vulnerability Management**
- Second row: **Breach Detection**
- Third row: **Network Visibility**
- Fourth row: **Top Scored Hosts**

## Vulnerability Management

The top row of the Cybowall dashboard highlights that the solution has been configured correctly, provides a high level snapshot of key indicators for network security, and flags vulnerabilities and risks to allow action to be taken.

## Status Section

The **Status** section of the Cybowall solution appears in the top left corner of the dashboard. It provides an overview of specific threats and system functions that are critical to maintain a secure network:



The individual panes featured in the **Status** section are detailed below.

### Windows Hosts with Vulnerabilities

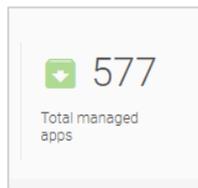


These two panes show Windows hosts with vulnerabilities that represent the greatest threat within the network:

- **Windows hosts with easily exploited vulnerabilities** – vulnerabilities that require less effort for exploitations to be initiated
- **Windows hosts with network exploited vulnerabilities** – vulnerabilities that can be exploited via a remote mechanism

See the Cybowall Dashboard – Vulnerabilities Section of this guide for detailed definitions of the vulnerability categories.

## Number of Total Managed Applications



Click on the **Total managed apps** pane to view a report that lists:

- All installed applications within the network
- Vulnerabilities associated with those applications
- Hosts with those specific applications installed

## Configured Networks versus Protected Networks

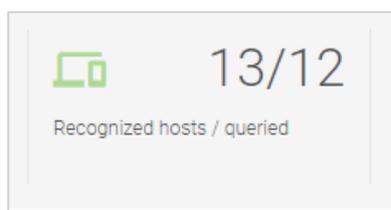


These panes provide a quick visual indicator of whether Cybowall is currently monitoring all networks that have been configured (i.e. all VLANs etc).

Click on the panes to view details of the networks under **Policy > Network scanner** and to identify any potential configuration issues.

For more information, see the Policy – Network Scanner section of this guide.

## Recognized Hosts versus Queried Hosts

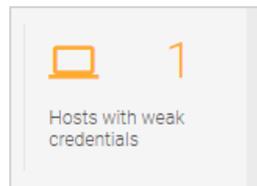


This references the number of hosts eligible to be scanned versus the actual number of hosts being scanned. It highlights if Cybowall is omitting specific hosts from its regular scans.



Click on this pane to view host details under **Network View > Windows hosts**. For more information, see the Network View section of this guide.

## Hosts with Weak Credentials

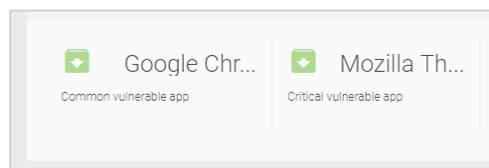


Refers to Cybowall's brute force password protection tool that scans port 22 (ssh), port 80 (http), port 443 (https) and port 21 (ftp).

This section provides alerts about the use of default vendor provided credentials or weak, commonly used passwords for any devices connected to the network – including, but not limited to, switches, IP cameras, printers etc.

See the **Reports > Vulnerability > Default credentials** report for more information on identifying the device with default or weak credentials and its location within the network.

## Vulnerable Applications



The **Common vulnerable app** and **Critical vulnerable app** panes provide a quick update on the more prevalent vulnerable applications within the network.

Hover over these panes to view a hoverbox detailing the full name and version of the application.

Click on this pane to view a report under **Reports > Vulnerability > Software** that defines the vulnerabilities present in each application. See the Cybowall Dashboard – Vulnerabilities Section of this guide for detailed vulnerability definitions.

## Malware Found



This pane provides a summary of the results of the Malware hunter scanning tool deployed by Cybowall. Malware hunter can be configured to scan any specific directories for any defined file extensions on the **Policy > Malware hunter** tab.

If a file hash is found to be a match within the Cybowall database, it creates an alert here, and can be configured to immediately send an email to previously defined users or groups.

Click on this pane to view the **Forensics > Net Sensor events**.

For more detailed information on the configuration and management of the Malware hunter tool, see the Policy – Malware Hunter section of this guide.



## Vulnerabilities Section

A vulnerability is a weakness that can be exploited by an attacker in order to perform unauthorized actions on a host/network.

The **Vulnerabilities** section is located in the center of the top row of the Cybowall dashboard. It summarizes the information that Cybowall collects from the various hosts within the network and displays them according to overall severity and several exploitability metrics:

Vulnerabilities									
Name	Access	Complexity		Privileges		User interaction			
1.  BOYDEM2012	<span>N</span> <span>A</span>	<span>L</span>	<span>M</span>	<span>N</span>	<span>R</span>	<span>N</span>	<span>R</span>		
2.  CYBOSUPPOR...	<span>N</span> <span>A</span>	<span>L</span>	<span>M</span>	<span>N</span>	<span>R</span>	<span>N</span>	<span>R</span>		
3.  LAN30SERVER	<span>N</span> <span>A</span>	<span>L</span>	<span>M</span>	<span>N</span>	<span>R</span>	<span>N</span>	<span>R</span>		
4.  LENOVO-ALON	<span>N</span> <span>A</span>	<span>L</span>	<span>M</span>	<span>N</span>	<span>R</span>	<span>N</span>	<span>R</span>		
5.  LIATAVRAMOV...	<span>N</span> <span>A</span>	<span>L</span>	<span>M</span>	<span>N</span>	<span>R</span>	<span>N</span>	<span>R</span>		

There are many tools which perform Vulnerability Assessments, but a key issue is often prioritizing their remediation (i.e. which weaknesses to fix first).

Cybowall addresses this by categorizing the vulnerabilities and enables them to be ranked by individual category. Hosts can be sorted by name (A-Z or the reverse) or ranked by each vulnerability metric by clicking on the appropriate heading.

This clear breakdown of information on the Cybowall dashboard allows remediation actions to be prioritized and taken to reduce vulnerabilities and improve network security.



## Exploitability Metrics

In the dashboard view, Cybowall breaks down vulnerabilities into exploitability metrics – reflecting the ease and technical means by which the vulnerability can be exploited. The exploitability metrics are: **Access, Complexity, Privileges and User interaction.**

The vulnerabilities are color coded according to the riskiness of the metric value of each exploitability metric (see tables below) and the initial of the metric value is shown in the center of the colored circle.

Hovering over the colored circle shows a hoverbox which states the name of the metric value and the number of associated vulnerabilities.

The following tables detail the meaning of each exploitability metric and associated metric values:

### 1. Access:

- How is a vulnerability accessed?
- The more remote an attacker can be to access a vulnerability – for example, it can be accessed over the internet rather than requiring local access – the higher the risk of the vulnerability to the network.

Metric Value	Description
<b>Network (N)</b>	<ul style="list-style-type: none"> <li>• A vulnerability exploitable with network access.</li> <li>• The vulnerable component is bound to the network stack and the attacker's path is through OSI layer 3 (the network layer).</li> <li>• Often termed a 'remotely exploitable' vulnerability – an attack exploitable one or more network hops away (e.g. across layer 3 boundaries from routers).</li> <li>• Example: an attacker causing a denial of service (DoS) by sending a specially crafted TCP packet from across the internet (e.g. CVE 2004 0230).</li> </ul>
<b>Adjacent network (A)</b>	<ul style="list-style-type: none"> <li>• A vulnerability exploitable with adjacent network access.</li> <li>• The vulnerable component is bound to the network stack but the attack is limited to the same shared physical (e.g. Bluetooth, IEEE 802.11), or logical (e.g. local IP subnet) network, and cannot be performed across an OSI layer 3 boundary (e.g. a router).</li> <li>• Example: an ARP (IPv4) or neighbor discovery (IPv6) flood leading to a denial of service on the local LAN segment.</li> </ul>
<b>Local (L)</b> [Shown in the expanded view only]	<ul style="list-style-type: none"> <li>• A vulnerability exploitable with local access.</li> <li>• The vulnerable component is not bound to the network stack, and the attacker's path is via read/write/execute capabilities.</li> <li>• Example: the attacker logs in locally to exploit the vulnerability or relies on user interaction to execute a malicious file.</li> </ul>



## 2. Complexity:

- How complex is it to compromise the network as a result of the vulnerability?
- The more complex – for example, the higher the number of steps needed to exploit the vulnerability – the lower the risk of the vulnerability to the network.

Metric Value	Description
Low (L)	<ul style="list-style-type: none"> <li>• An attacker can expect to repeatedly exploit the vulnerability without having to collect more information about the target or exploit certain system configuration settings etc.</li> </ul>
Medium (M)	<ul style="list-style-type: none"> <li>• An attacker is able to exploit the vulnerability without carrying out significant target specific reconnaissance or investing a high degree of effort, but cannot repeatedly exploit the vulnerability.</li> </ul>
High (H) [Shown in the expanded view only]	<ul style="list-style-type: none"> <li>• A successful attack depends on conditions beyond the attacker's control.</li> <li>• It cannot be accomplished without the attacker investing significant effort in order to prepare for or execute the attack.</li> <li>• For example, the attacker needs to:             <ul style="list-style-type: none"> <li>○ Conduct target-specific reconnaissance on target configuration settings, sequence numbers, shared secrets etc.</li> <li>○ Prepare the target environment to improve exploit reliability, such as overcoming advanced exploit mitigation techniques.</li> </ul> </li> </ul>

## 3. Privileges:

- What level of privileges must be possessed to exploit the vulnerability?
- The lower the level of privileges required, the higher the risk of the vulnerability to the network.

Metric Value	Description
None (N)	<ul style="list-style-type: none"> <li>• An attacker does not require any privileges prior to attack, and does not require any access to settings/files to carry out an attack.</li> </ul>
Low [Combined with High and shown as Required Privileges (R) on the dashboard]	<ul style="list-style-type: none"> <li>• An attacker requires privileges that provide basic user capabilities that could normally affect only settings and files owned by a user.</li> <li>• Alternately, an attacker with low privileges may be able to impact only non-sensitive resources.</li> </ul>
High [Combined with Low and shown as Required Privileges (R) on the dashboard]	<ul style="list-style-type: none"> <li>• An attacker requires privileges that provide significant (e.g. administrative) control over the vulnerable component that could affect component-wide settings and files.</li> </ul>



#### 4. User Interaction:

- Does a user (other than the attacker) need to participate in order to exploit the vulnerability?
- If user interaction is needed – for example, double clicking to execute the vulnerability – this lowers the risk of the vulnerability to the network.

Metric Value	Description
None (N)	<ul style="list-style-type: none"><li>• The vulnerability can be exploited without any user interaction.</li></ul>
Required (R)	<ul style="list-style-type: none"><li>• A user must take some action before the vulnerability can be exploited.</li><li>• Example: a successful exploit is only possible during the installation of an application by a system administrator.</li></ul>



## Vulnerabilities Expanded View

Click on the 3 dots to the right of the **Vulnerabilities** heading to expand this section:

Vulnerabilities																	10
Name	Severity					Access			Complexity			Privileges			User interaction		
	Critical	High	Medium	Low	Total	Network	Adjacent network	Local	Low	Medium	High	None	Low	High	None	Required	
1. BOYDEM2012	374	91	265	40	770	645	5	120	341	403	26	124	26	1	408	355	
2. CONROOM...	180	180	171	4	535	532	-	3	322	208	5	106	5	-	341	193	
3. CYBOSUPPO...	393	39	120	5	557	548	-	9	235	311	11	151	5	-	256	300	
4. LAN30SERV...	51	62	60	31	204	89	4	111	111	86	7	13	17	1	131	67	
5. LENOVO-AL...	99	26	72	4	201	197	-	4	71	126	4	152	7	-	76	124	
6. PINEDC	51	82	137	31	301	185	4	112	149	145	7	109	18	1	207	70	
7. PINEX13	51	65	66	31	213	98	4	111	116	89	8	15	19	1	138	69	
8. SION-LP	98	28	79	6	211	205	-	6	78	128	5	153	7	-	85	125	
9. SUPPORT30...	319	189	194	4	706	700	-	6	396	305	5	133	6	-	418	287	
10. SUPPORT40...	562	202	354	12	1130	1118	5	7	587	523	20	107	5	-	652	477	

This view shows the exploitability metrics in full, with the number of associated vulnerabilities detailed to the right of the colored circle.

It also includes an overall **Severity** measure for the vulnerabilities found on each host – shown to the left of the **Access** metrics.

### Severity:

- How severe is the vulnerability overall?
- This takes into account the exploitability metrics as well as the impact/consequences of a successful exploit, the presence of, for example, a simple to use exploit kit or official patch, and factors relevant to a particular business environment.
- It is based on the framework of the Common Vulnerability Scoring System (CVSS) which ensures repeatable accurate measurement of vulnerabilities, and provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.

Metric Value	Description
Critical	• Vulnerabilities with a CVSS score of 9.0 - 10.0.
High	• Vulnerabilities with a CVSS score of 7.0 - 8.9.
Medium	• Vulnerabilities with a CVSS score of 4.0 - 6.9.
Low	• Vulnerabilities with a CVSS score of 0.1 - 3.9.
Total	• The sum of the above vulnerabilities.

For further detail on the CVSS, please see here: <https://www.first.org/cvss/specification-document>



## Investigating Individual Hosts

To drill down further to review the details of a host's vulnerabilities, click the individual host in the **Name** column. The **Host details** window opens on the **Vulnerability** tab:

Operating system vulnerability		
Operating System	Details	Top score
Microsoft Windows 10 1703 ✓	CVE-2017-8589 ✓	10

Software vulnerability		
Application	Details	Top score
Cisco Packet Tracer 5.2 ✓	CVE-2010-3135 ✓	9.3
Cisco Webex Meetings Server ✓	CVE-2018-0104 ✓	9.3
Google Chrome 0.1.38.1 ✓	CVE-2012-1846 ✓	10

Further details of the vulnerabilities identified by Cybowall can be viewed by clicking the green text to expand these sections. See the Network View – Windows Hosts section of this guide for more information.



# Risk Assessment Section

The **Risk assessment** section of the Cybowall dashboard (top right) assesses key security measures for each computer connected to the network, facilitating review and action to improve host security:

Risk assessment		Anti-virus	Firewall	Ports not in profile	Windows updates
1.	BOYDEM2012	Grey	Green	Orange	Orange
2.	ZOOM	Grey	Green	Yellow	Orange
3.	PINEX13	Grey	Green	Orange	Orange
4.	LAN30SERVER	Grey	Green	Green	Orange
5.	LENOVO-ALON	Green	Green	Orange	Yellow

It provides a high level snapshot of a computer’s security, and enables issues that prevent the host from complying with security best practices to be easily viewed and addressed.

## Risk Assessment Expanded View

The expanded **Risk assessment** view breaks down the security posture of each computer into the following categories relating to the individual host: **Anti-virus, Firewall, Ports not in profile, Windows updates, Vulnerabilities** and **Wireless access**:

Risk assessment		Anti-virus	Firewall	Ports not in profile	Windows updates	Vulnerabilities	Wireless access
1.	BOYDEM2012	Grey	Green	Orange	Orange	Red	Green
2.	ZOOM	Grey	Green	Yellow	Orange	Red	Green
3.	PINEX13	Grey	Green	Orange	Orange	Red	Green
4.	LAN30SERVER	Grey	Green	Green	Orange	Red	Green
5.	LENOVO-ALON	Green	Green	Orange	Yellow	Red	Green
6.	SUPPORTST1-PC	Green	Green	Green	Yellow	Red	Green
7.	SUPPORT300-PC	Green	Green	Green	Orange	Red	Green
8.	NATALIAF-PC	Green	Green	Green	Orange	Green	Green
9.	SUPPORT_139-PC	Green	Red	Green	Green	Red	Green
10.	CONROOM-PC	Green	Green	Green	Orange	Green	Green

In both this view and the dashboard view, the hosts can be sorted by name (A-Z or the reverse) or by the status of each risk category by clicking on the appropriate heading.



## Risk Assessment Status

Color coding indicates the status of each host in relation to a specific security category, and hovering over the colored circle shows a hoverbox which provides additional explanation – as shown in the table below.

A grey circle indicates that there is not enough information to provide an assessment.

This table shows the status represented by the color coding:

Category	Description
<b>Anti-virus</b>	<ul style="list-style-type: none"> <li>Green – Anti-virus is installed and up to date</li> <li>Yellow – Anti-virus is installed but not up to date</li> <li>Red – Anti-virus is not installed</li> </ul>
<b>Firewall</b>	<ul style="list-style-type: none"> <li>Green – Firewall is enabled for all network profiles (domain, public, private)</li> <li>Yellow – Firewall is enabled for the majority of network profiles</li> <li>Orange – Firewall is enabled for one network profile</li> <li>Red – Firewall is not enabled</li> </ul>
<b>Ports not in profile</b>	<ul style="list-style-type: none"> <li>Green – All ports are configured in the profile</li> <li>Yellow – One port detected is not configured in the profile</li> <li>Orange – More than one port detected is not configured in the profile</li> </ul>
<b>Windows updates</b>	<ul style="list-style-type: none"> <li>Green – Windows update service is running and downloading updates automatically</li> <li>Yellow – Windows update service is running and downloading updates manually</li> <li>Orange – Windows update service has stopped</li> <li>Red – Windows update service has stopped and disabled</li> </ul>
<b>Vulnerabilities</b>	<ul style="list-style-type: none"> <li>Green – No network vulnerabilities</li> <li>Yellow – Minor network vulnerabilities found (CVSS &lt; 4.0)</li> <li>Orange – Major network vulnerabilities found (CVSS &gt;= 4.0)</li> <li>Red – Critical network vulnerabilities found (CVSS &gt;= 7.0)</li> </ul>
<b>Wireless access</b>	<ul style="list-style-type: none"> <li>Green – No wireless access</li> <li>Yellow – Wireless access</li> </ul>



## Investigating Individual Hosts

To drill down further to review the status of a host, click the individual host in the **Name** column. The **Host details** window opens:

The screenshot shows a window titled "Details of LENOVO-ALON" with a "Download" button and a close button. The window has several tabs: Generic, Network, Hardware, Software, Vulnerability, and Protection. The Protection tab is selected and underlined. The content of the Protection tab is as follows:

Anti-virus protection			
Anti-virus	Status	DB status	Path
Windows Defender	up	up-to-date	windowsdefender://

Windows updates		
State	Status	Start mode
Running	OK	Manual

Firewall		
Domain profile settings	Public profile settings	Private profile settings
ON	ON	ON

At the bottom of the Protection tab, there is a link: [Protection report >](#)

The status of the individual host can be investigated by clicking on the relevant tab: **Generic**, **Network**, **Hardware**, **Software**, **Vulnerability** and **Protection**. See the Network View – Windows Hosts section of this guide for further information.

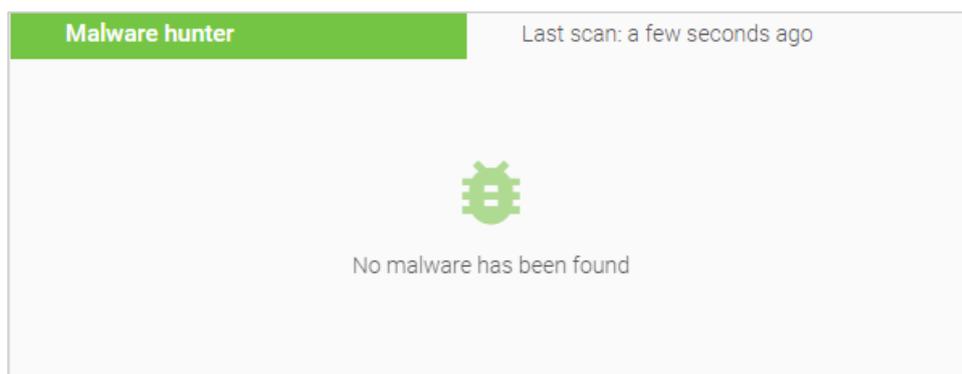
# Breach Detection

The second row of the Cybowall dashboard assists with the identification and management of suspicious and potentially malicious network behavior by utilizing three specific tools:

- Malware Hunter
- Lateral Movement – Distributed Network Traps
- Traffic Analysis – Intrusion Detection

## Malware Hunter Section

This section expands on the **Malware found** pane in the **Status** section of the dashboard, providing an alert that updates if malware is discovered on a host:



**Malware hunter** can be configured to scan any specific directories for any defined file extensions.

If a file hash is found to be a match within the Cybowall database, this section alerts to the specific host and the IP address associated with that host where malware was detected.

If no malware is detected, this section reports when the last system scan took place.

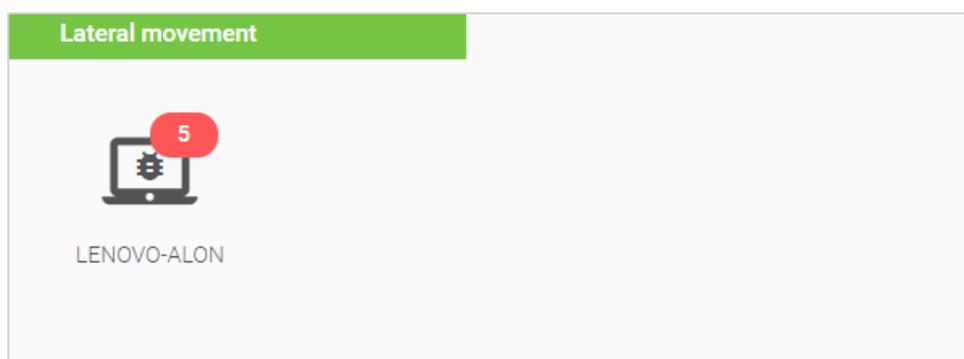
## Lateral Movement Section

Lateral movement commonly refers to any techniques used once a cyber attack has breached the network to move within the perimeter and search for key data and assets.

When Cybowall is installed within a network, it immediately deploys a series of configurable and scalable network traps (sometimes referred to as honeypots).

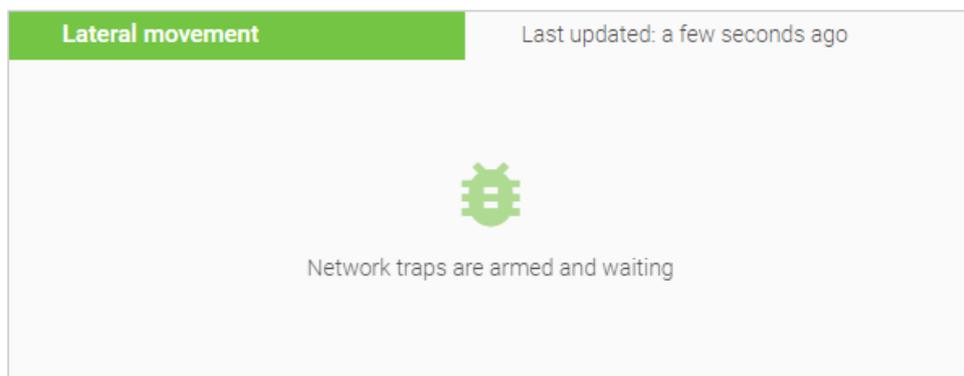
When these network traps are interacted with, Cybowall collects information regarding the type and origin of that interaction.

This section identifies the host that is the source of the tampering and the number of network events flagged by the network traps:



Click on the host to navigate to **Forensics > Net Sensor events** to view the details of these events.

If no active lateral movement is detected by the network traps, this section confirms that the traps are operational and working as intended.





## Traffic Analysis Section

This section provides a 24-hour summary of events being tracked by Cybowall's Intrusion Detection engines and organizes it according to predefined rule categories:



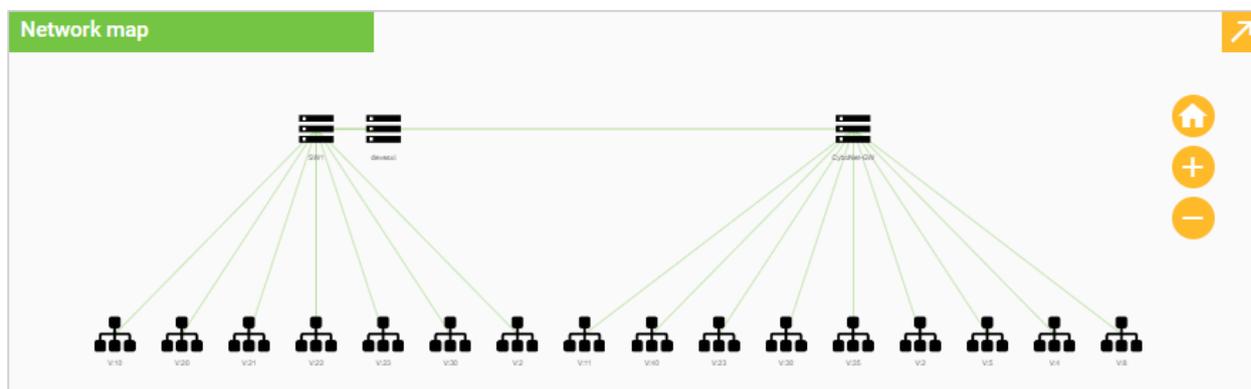
Each rule category in this section can be clicked and opens a list of specific category level events within the **Network Forensics** tab of Cybowall.

# Network Visibility

The third row of the Cybowall dashboard provides a visual snapshot of the network and enables a deeper dive to be taken on specific topics.

## Network Map Section

The network topology map provides a visual representation of the network's hosts and their relation to each other, allowing changes to be more easily viewed:



Use the orange **plus** and **minus signs** to zoom in and out on the map, or click on a particular host to view further details.

Click on the orange **arrow icon** in the top right hand corner of this section to navigate to the **Network View > Network map** tab of Cybowall – see the corresponding section of this guide for further information.

# Network Visibility Section

A number of key network parameters are represented as dials in this section to allow for easy access drill down and further investigation:



## Network View

An interactive dial showing the type and ratio of Operating Systems (OS) deployed within the network. To examine the list of all hosts connected to network on the **Network View** tab, click the green **Network View** link.

## Threat Source

An interactive dial showing the origin and ratio of network threats by geographic region. It links directly to the **Threat source** report on the **Reports > Traffic analysis** tab. This provides a summary map of network threat origins by country as well as an inventory of host events by country.

## Open Ports

An interactive dial that displays current open ports on the network. It links directly to a summary report of all open ports on the network and hosts with specific port access under **Reports > Vulnerability > Open ports**.

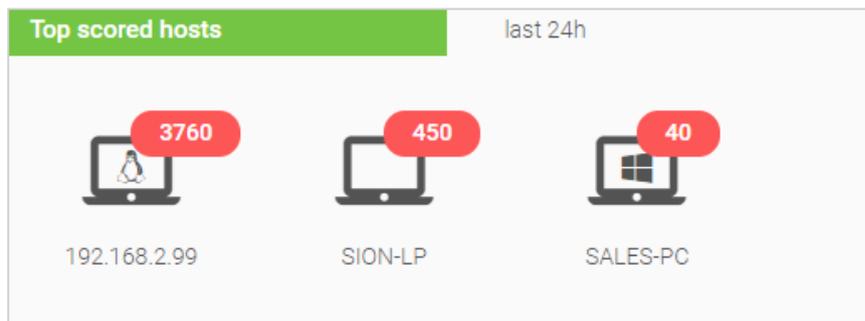
## Forensics

An interactive dial on the source of events reporting collected in Cybowall. It links directly to the **Forensics** tab of Cybowall, which provides detailed information on network events.

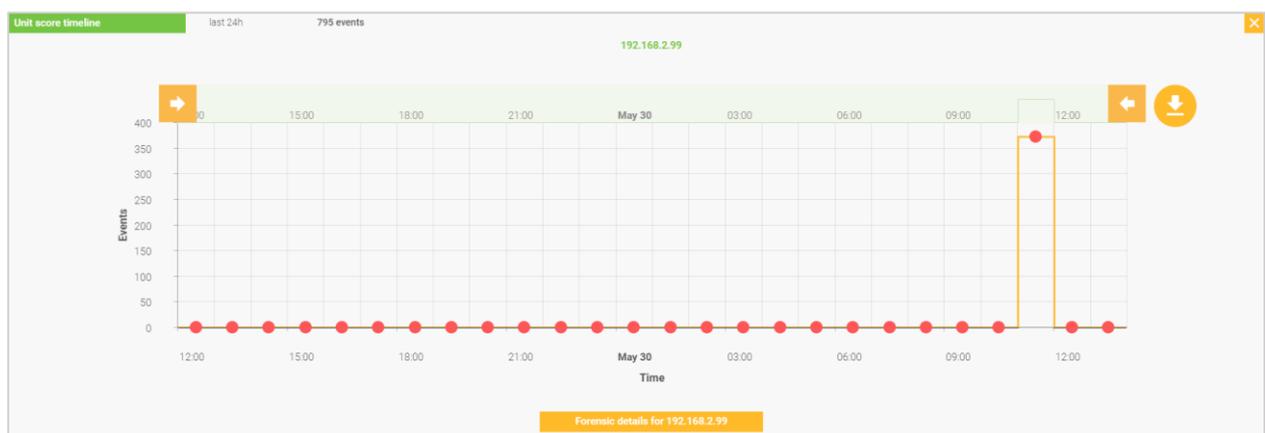
# Top Scored Hosts

The bottom row of the Cybowall dashboard highlights the top scored hosts within the network. This assists with prioritizing which hosts need to be investigated and possible actions taken to ensure they are not putting the network at risk.

The host is identified, together with the number of associated events:



Clicking on the host opens the **Unit score timeline** window, showing when the events occurred:



Click the orange **Forensics details** button to view further details of the events on the **Forensics** tab. See the Forensics section of this guide for additional information.



# Network View

The **Network View** tab of the Cybowall solution provides the opportunity to delve deeper into the hosts connected to the network that Cybowall scans and monitors.

The **Network View** is split into three further tabs; **Windows hosts**, **Other hosts** and **Network map**.

## Windows Hosts

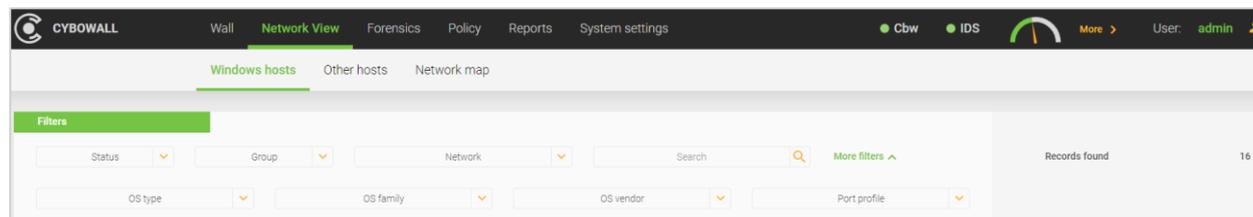
The **Windows hosts** tab shows all Windows workstations and servers to which Cybowall has been able to connect via WMI:

Windows hosts							Download
N	Name	IP address	MAC address	Port profile	Network	Status	
1.	BOYDEM2012	192.168.2.170	04ae52c6b6b5	Windows	192.168.2.0/24 (192.168.2.0/24)	Details ▾	
2.	OONROOM-PC	192.168.2.97	94c69111e021		192.168.2.0/24 (192.168.2.0/24)	Details ▾	
3.	CYBOSUPPORT-PC	192.168.22.23	408d5c0622cc		192.168.22.0/24 (192.168.22.0/24)	Details ▾	
4.	DESKTOP-SUPPORT	192.168.22.37	704d7b32ba8b		192.168.22.0/24 (192.168.22.0/24)	Details ▾	
5.	LAN30SERVER	192.168.30.8	005056b72f04	Windows	192.168.30.0/24 (192.168.30.0/24)	Details ▾	
6.	LENOVO-ALON	192.168.30.23	0050b6202029	Windows	192.168.30.0/24 (192.168.30.0/24)	Details ▾	
7.	NATALIAF-PC	192.168.22.29	1c1b0d609a95		192.168.22.0/24 (192.168.22.0/24)	Details ▾	
8.	PINEDC	192.168.2.215	005056b746aa	Windows	192.168.2.0/24 (192.168.2.0/24)	Details ▾	
9.	PINEX13	192.168.2.7	005056b7b029	Windows	192.168.2.0/24 (192.168.2.0/24)	Details ▾	
10.	SION-LP	192.168.30.12	a402b9705265		192.168.30.0/24 (192.168.30.0/24)	Details ▾	
11.	SUPPORT300-PC	192.168.22.38	704d7b32ba8a	Windows	192.168.22.0/24 (192.168.22.0/24)	Details ▾	

Hosts can be sorted by each column heading (**Name**, **IP Address**, **MAC Address** etc.) by clicking on the appropriate heading.

# Searching for Hosts

Both the **Windows hosts** and **Other hosts** can also be filtered by additional parameters:



The available filters are:

- **Status:** Up or Down – Is the system currently connected to the network?
- **Group:** Host groups can be created to serve as a layer to which policy can be assigned
- **Network:** Search within a specified IP range
- **Search:** Search for a specific host or hosts by Name or IP Address

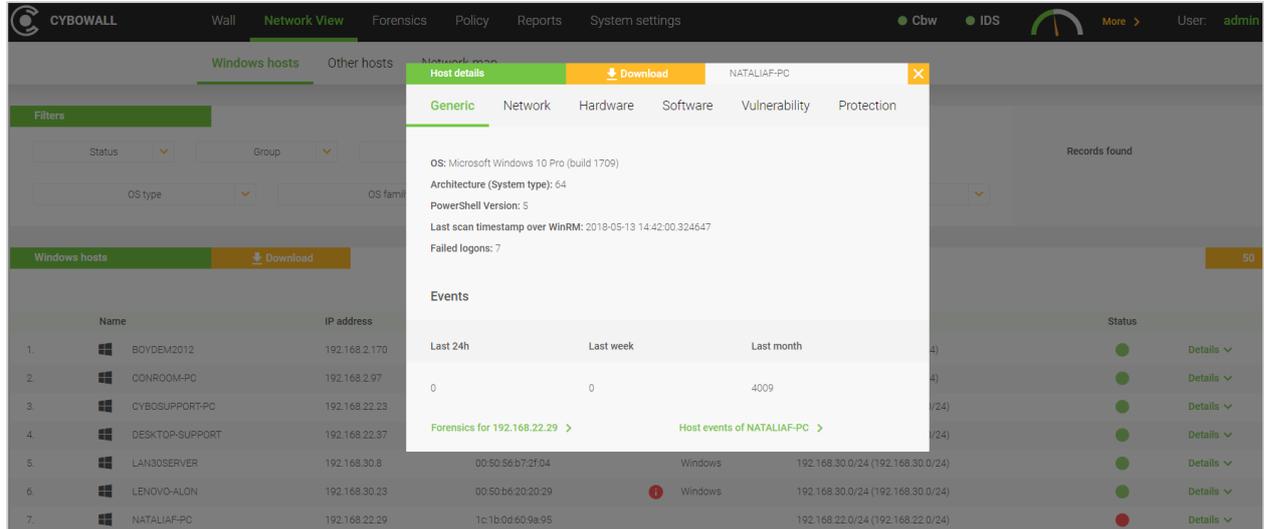
Click on the green **More filters** link for additional filters:

- **OS type:** Operating System – for example General purpose, Printer, Switch
- **OS family:** Operating System – for example Windows, Linux, Comware
- **OS vendor:** Operating system – for example Microsoft, Cisco, HP, VMware
- **Port profile:** for example Windows or Linux. Port profiles can be configured and administered on the **Policy > Port profiles** tab



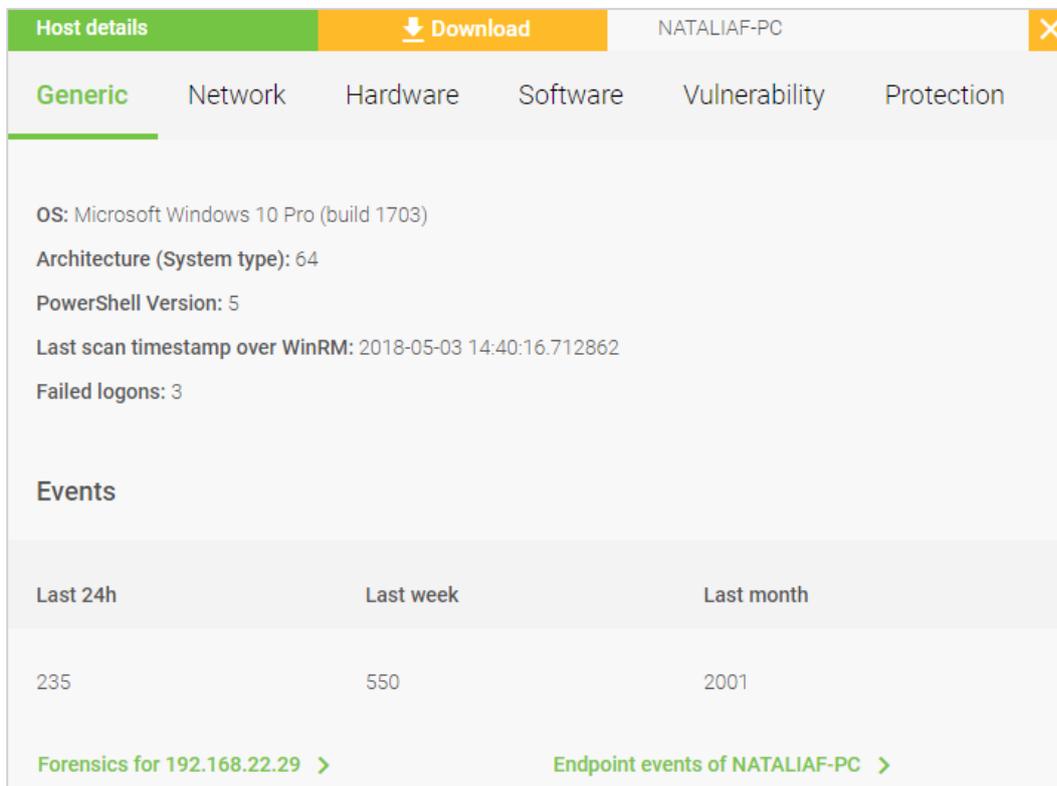
# Windows Host Details

Click on the green **Details** link to the right of each host record to view further information according to the following parameters: **Generic, Network, Hardware, Software, Vulnerability** and **Protection**:



## 1. Host Details: Generic

Provides general information about the host, including information related to the **OS, Architecture (System type), PowerShell Version, Last scan timestamp over WinRM** and **Failed logons**:





Quick links for additional drill down are provided in green at the bottom of this window. These allow for investigation of network and host specific events on the **Forensics** tab of Cybowall.

## 2. Host Details: Network

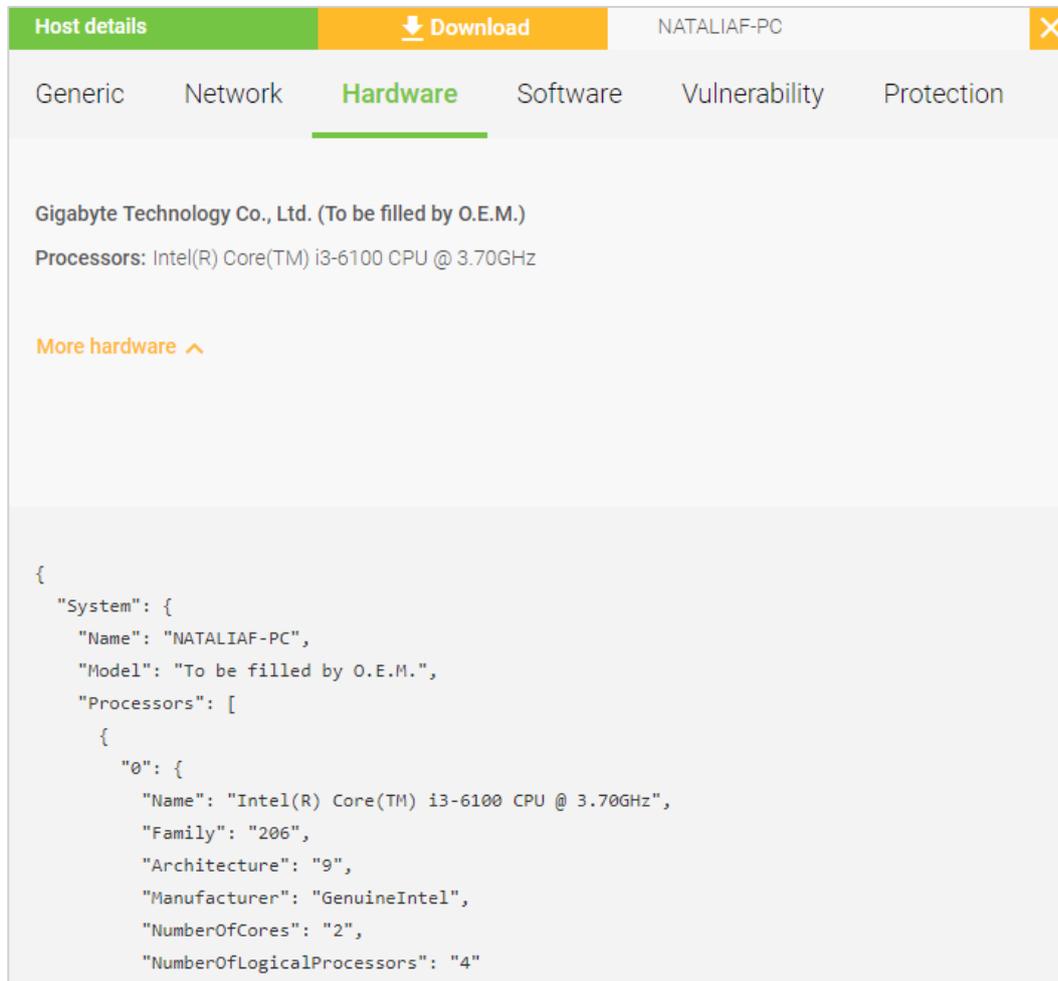
Provides host specific details regarding network connectivity, including MAC address, MAC address provider, Host state discovery engine, total scan time, ports accessible to the host and potential port violations:

Host details		Download	NATALIAF-PC		
Generic	<b>Network</b>	Hardware	Software	Vulnerability	Protection
MAC address: 1c:1b:0d:60:9a:95					
MAC address provider: Giga-byte Technology					
Host state discovered by: arp-response					
Scan time: 30.31ms					
TCP: 80 135 443 3389 5985 7680					
<b>Last port profile violation</b>					
Timestamp			Extra ports		
2018-05-03 14:57:49.37773			TCP: 443, 7680		
<a href="#">Port profiles &gt;</a>					

Click on the green **Port profiles** link at the bottom of this window to configure and administer ports under the **Policy > Port profiles** tab of Cybowall.

### 3. Host Details: Hardware

Provides host specific details related to hardware, for example vendor details, processors, memory etc. Click on the **More hardware** link and scroll down for further details:



The screenshot shows a web interface for host details. At the top, there is a green header with 'Host details' and a yellow 'Download' button. The host name 'NATALIAF-PC' is displayed in the top right corner. Below the header, there are tabs for 'Generic', 'Network', 'Hardware', 'Software', 'Vulnerability', and 'Protection'. The 'Hardware' tab is selected and highlighted with a green underline. The main content area displays the following information:

Gigabyte Technology Co., Ltd. (To be filled by O.E.M.)  
Processors: Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz

More hardware ^

```
{
  "System": {
    "Name": "NATALIAF-PC",
    "Model": "To be filled by O.E.M.",
    "Processors": [
      {
        "0": {
          "Name": "Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz",
          "Family": "206",
          "Architecture": "9",
          "Manufacturer": "GenuineIntel",
          "NumberOfCores": "2",
          "NumberOfLogicalProcessors": "4"
        }
      }
    ]
  }
}
```



#### 4. Host Details: Software

Provides a list of all software applications installed on the host:

Host details		Download	NATALIAF-PC		X
Generic	Network	Hardware	Software	Vulnerability	Protection
Name					Version
Adobe AIR					22.0.0.153
Adobe Acrobat Reader					18.011.20038
Adobe Refresh Manager					1.8.0
Adobe Shockwave Player					12.2.4.194
Cisco WebEx Meetings					
Common Desktop Agent					1.62.0
Definition Update for					
Dropbox					48.4.58
Dropbox Update Helper					1.3.59.1

This facilitates review and mitigation in relation to the individual host. For example, does company policy permit the installation of Dropbox?

Navigate to the **Software Vulnerability** and **Software Inventory** reports on the **Reports** tab by clicking the green **Software vulnerabilities** and **Software report** links at the bottom of the window.



## 5. Host Details: Vulnerability

Provides continuously updated vulnerability details related to the OS and host specific software applications:

Host details
Download
NATALIAF-PC
✕

Generic
Network
Hardware
Software
Vulnerability
Protection

No Operating system vulnerabilities

**Software vulnerability**

Application	Details	Top score
Adobe Acrobat Reader X 10.1.10 <span style="color: green;">▼</span>	CVE-2015-5115 <span style="color: green;">▼</span>	10
Adobe Shockwave Player 2.0 <span style="color: green;">▼</span>	CVE-2013-5334 <span style="color: green;">▼</span>	10
Cisco Webex Meetings Server <span style="color: green;">▼</span>	CVE-2018-0104 <span style="color: green;">▼</span>	9.3
Google Chrome 0.1.38.1 <span style="color: green;">▼</span>	CVE-2012-1846 <span style="color: green;">▼</span>	10
Imgburn 2.5.0.0 <span style="color: green;">▼</span>	CVE-2011-0403 <span style="color: green;">▼</span>	9.3
Microsoft Excel 2016 <span style="color: green;">▼</span>	CVE-2018-0796 <span style="color: green;">▼</span>	9.3

Click on the green links in the **Software vulnerability** section under **Application** and **Details** to view information related to the nature and severity of the threat, as well as remediation details specific to each vulnerability.

Navigate to the **Software Vulnerability** and **Summary Vulnerability** reports on the **Reports** tab by clicking the **Software vulnerabilities** and **Vulnerability report** links at the bottom of the window.



## 6. Host Details: Protection

Provides a detailed assessment of the host's basic protection including OS updates, Anti-virus protection and host Firewall settings:

Host details
Download
NATALIAF-PC
✕

Generic
Network
Hardware
Software
Vulnerability
Protection

### Anti-virus protection

Anti-virus	Status	DB status	Path
Windows Defender	up	up-to-date	%ProgramFiles%\Windows Defender\MSASCui.exe

### Windows updates

State	Status	Start mode
Running	OK	Manual

### Firewall

Domain profile settings	Public profile settings	Private profile settings
ON	ON	ON

[Protection report >](#)

Click on the **Protection report** link at the bottom to navigate to the **Protection Vulnerability** report on the **Reports** tab of Cybwall.



# Other Hosts

The **Other hosts** tab provides visibility of all other hosts connected to the network, as well as Windows hosts to which Cybowall did not gain WMI access:

	OS type	IP address	MAC address	OS family	Port profile	Network	Status
1.	General purpose	192.168.2.5	00:03:1d:06:d3:ed	Linux	Linux	192.168.2.0/24 (192.168.2.0/24)	Details
2.	General purpose	192.168.2.9	00:18:ae:50:c1:4c	Linux	Linux	192.168.2.0/24 (192.168.2.0/24)	Details
3.	Switch	192.168.2.10	00:1d:b3:cd:81:e0	embedded		192.168.2.0/24 (192.168.2.0/24)	Details
4.	General purpose	192.168.2.50	10:98:36:ab:dd:71	Linux	Linux	192.168.2.0/24 (192.168.2.0/24)	Details
5.	General purpose	192.168.2.53	00:0c:29:5b:7e:5e	Windows	Windows	192.168.2.0/24 (192.168.2.0/24)	Details
6.	General purpose	192.168.2.58	00:50:56:9d:06:88	Linux	Linux	192.168.2.0/24 (192.168.2.0/24)	Details
7.	General purpose	192.168.2.91	00:12:e5:04:74:73	Linux	Linux	192.168.2.0/24 (192.168.2.0/24)	Details
8.	General purpose	192.168.2.99	00:50:56:b7:f3:44	Linux	Linux	192.168.2.0/24 (192.168.2.0/24)	Details

As with the Windows hosts, these hosts can be sorted by each column heading (**Name**, **IP Address**, **MAC Address** etc.) by clicking on the appropriate heading, and can be filtered by additional parameters. See Searching for Hosts under the Windows Hosts section of this guide for further information.

## Other Host Details

Click on the green **Details** link to the right of each host record to view further information about the host.

For **Other hosts**, the available parameters are **Generic** and **Network**. See the explanations under Windows Hosts (sections 1. and 2.) above for further details.



# Generating a Host Specific Report

In the **Details** window, each parameter collected on individual hosts can be downloaded to a PDF by clicking the orange **Download** button and selecting those areas of interest for reporting.

The Default includes **Generic** and **Network**. Alternately select the individual parameters required, or click **Select all** and then click **Download** and Save the PDF:

The screenshot shows the 'Host details' window for 'NATALIAF-PC'. A 'Download' button is visible in the top right corner. A dropdown menu is open, showing the following options:

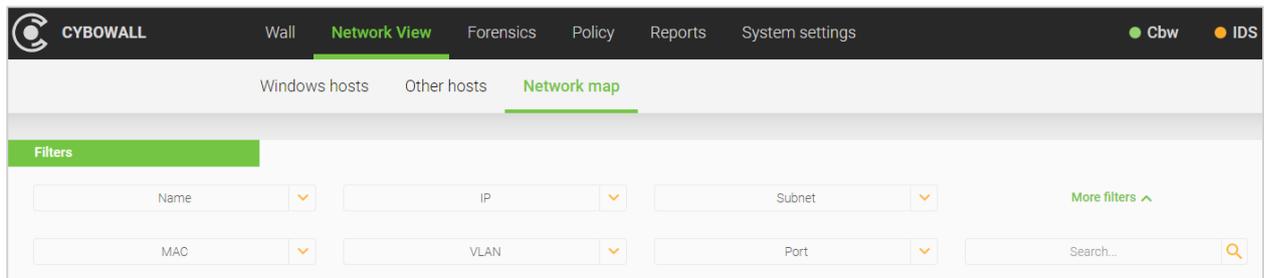
- Generic
- Network
- Hardware
- Software
- Vulnerability
- Protection

Below the menu is a 'Download' button. The background shows the 'Generic' tab selected, with details for OS (Microsoft Windows 10 Pro), Architecture (System type): 64, PowerShell Version: 5, Last scan timestamp over Win, and Failed logons: 0. The 'Events' section shows a table with columns for 'Last 24h', 'Last week', and 'Last month', with values 171, 790, and 2265 respectively. There are also links for 'Forensics for 192.168.22.29' and 'Endpoint events of NATALIAF-PC'.

# Network Map

Cybowall's dynamic network asset map is shown on the **Network map** tab. The network map provides system topology of both traditional and non-traditional hosts, including IoT (Internet of Things) hosts, enabling drill down and investigation of all connected hosts.

The network map can be filtered to focus on specific areas of the network:

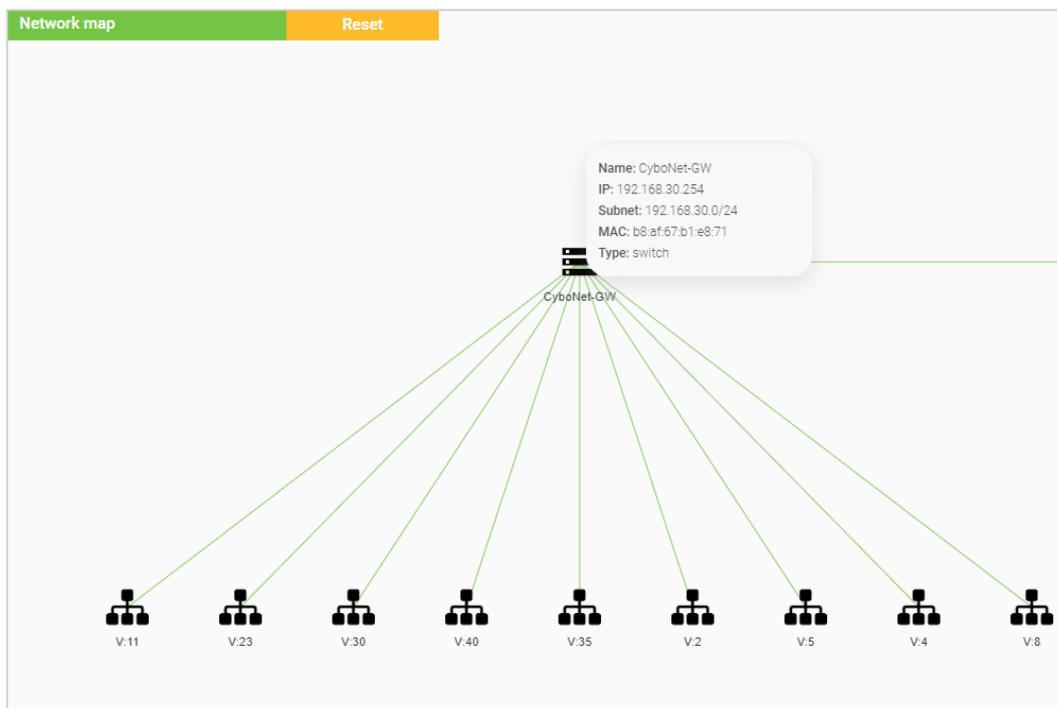


The available filters are host **Name**, **IP** and **Subnet**.

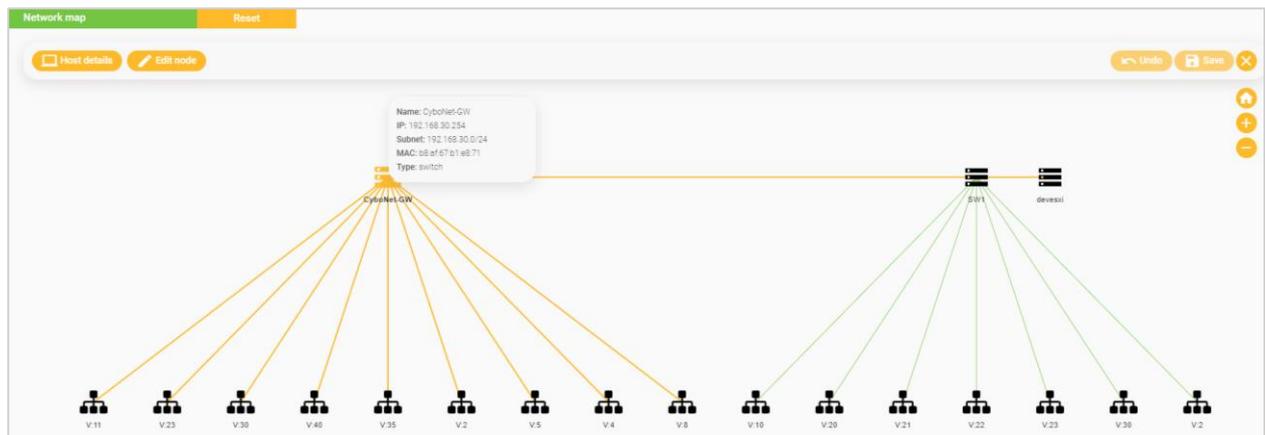
Click on the green **More filters** link for additional filters: **MAC**, **VLAN**, **Port** or conduct a free **Search**.

## Investigating Hosts

Hover over a network asset to view a hoverbox giving details of that particular element – **Name**, **IP**, **Subnet**, **MAC**, **Type**:

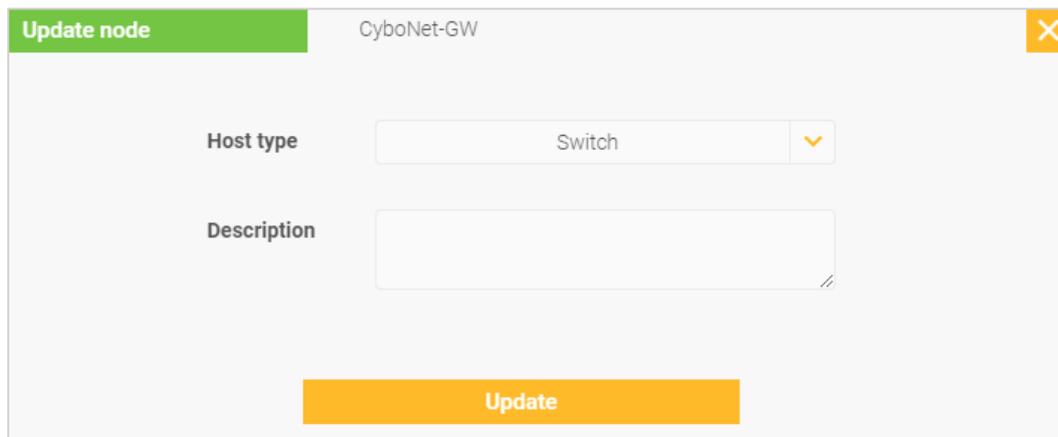


Clicking on a host highlights it and allows it to be edited:



Click on the orange **Host details** button to the left of the section to view the Host details window with all the information Cybowall has collected about that host.

Click the **Edit node** button to confirm or change the **Host type** (select **Host**, **Access Point**, **Switch**, **Router**, **Firewall** or **Gateway** from the dropdown menu) and to add a **Description** in order to customize the map:



**Update node** CyboNet-GW

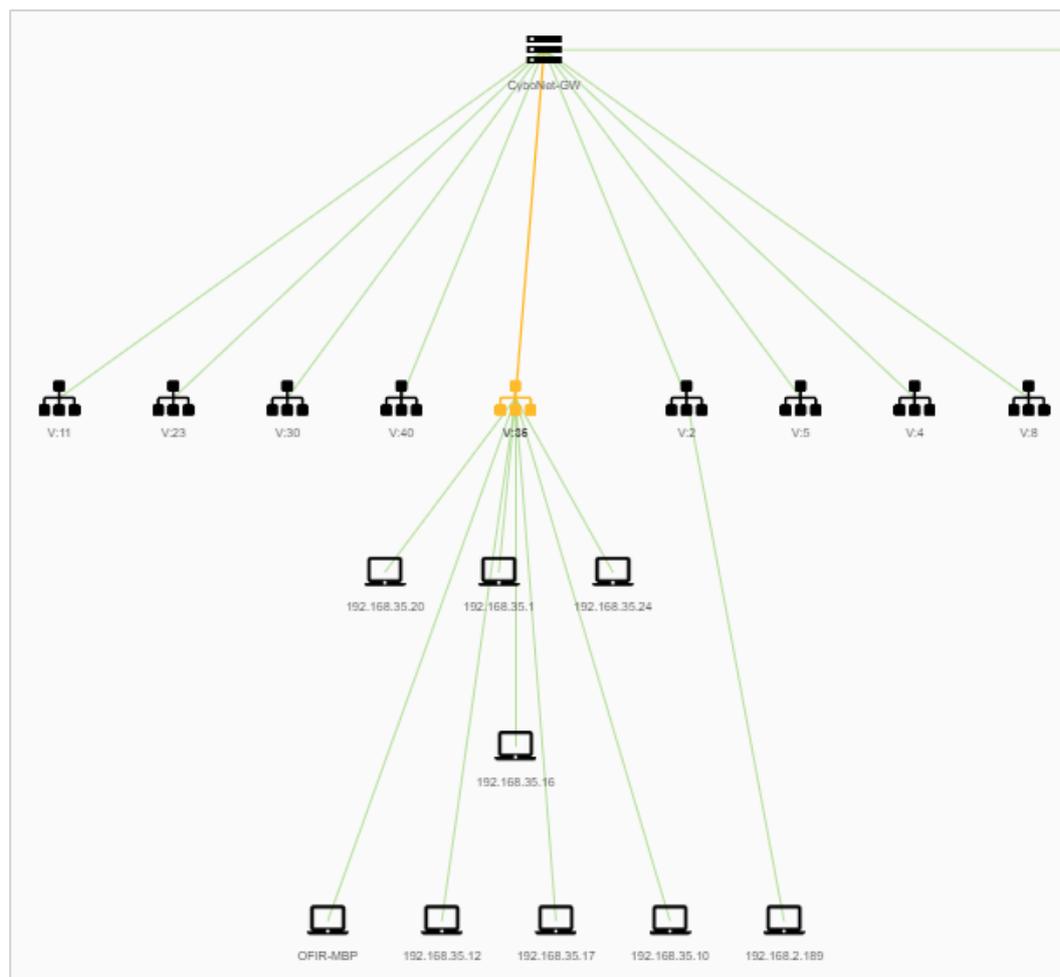
Host type: Switch

Description:

**Update**

Click **Update** to save changes.

Click on a cluster/VLAN to expand it:



Use the orange **plus** and **minus signs** to the right of the **Network map** section to zoom in and out on the map, and click the **home icon** to return to the original scale.

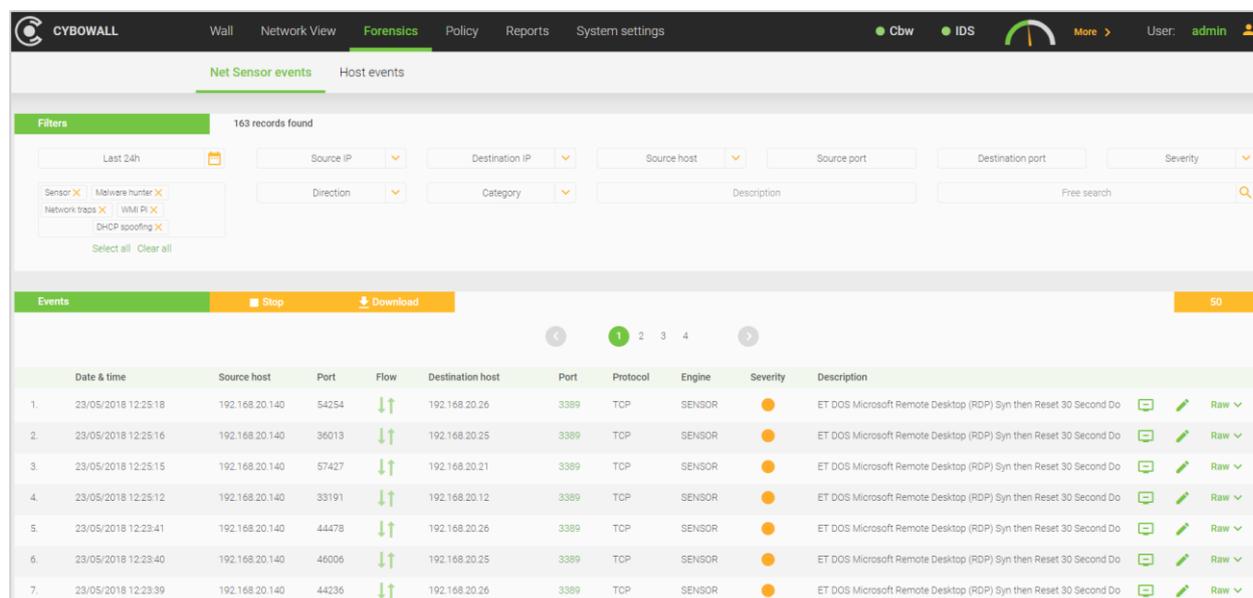
Click the orange **Reset** button next to the **Network map** section heading to reset the network map.

# Network Forensics

The **Forensics** section of Cybowall provides an opportunity to investigate further events occurring within the network. It is split into two tabs; **Net Sensor events** and **Host events**.

## Net Sensor Events

This tab details the events being monitored by various engines within the network Sensor:



The screenshot shows the Cybowall Forensics interface. The top navigation bar includes 'Wall', 'Network View', 'Forensics', 'Policy', 'Reports', and 'System settings'. The 'Forensics' section is active, showing 'Net Sensor events' and 'Host events' tabs. Below the tabs is a filter section with 163 records found. The filter section includes a time range selector (Last 24h), a search bar, and several dropdown menus for Source IP, Destination IP, Source host, Source port, Destination port, Severity, Direction, and Category. Below the filter section is a table of events with columns for Date & time, Source host, Port, Flow, Destination host, Port, Protocol, Engine, Severity, and Description. The table shows 7 events, all of which are ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second DoS attacks.

	Date & time	Source host	Port	Flow	Destination host	Port	Protocol	Engine	Severity	Description
1.	23/05/2018 12:25:18	192.168.20.140	54254	↑↓	192.168.20.26	3389	TCP	SENSOR	●	ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second Do
2.	23/05/2018 12:25:16	192.168.20.140	36013	↑↓	192.168.20.25	3389	TCP	SENSOR	●	ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second Do
3.	23/05/2018 12:25:15	192.168.20.140	57427	↑↓	192.168.20.21	3389	TCP	SENSOR	●	ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second Do
4.	23/05/2018 12:25:12	192.168.20.140	33191	↑↓	192.168.20.12	3389	TCP	SENSOR	●	ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second Do
5.	23/05/2018 12:23:41	192.168.20.140	44478	↑↓	192.168.20.26	3389	TCP	SENSOR	●	ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second Do
6.	23/05/2018 12:23:40	192.168.20.140	46006	↑↓	192.168.20.25	3389	TCP	SENSOR	●	ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second Do
7.	23/05/2018 12:23:39	192.168.20.140	44236	↑↓	192.168.20.26	3389	TCP	SENSOR	●	ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second Do

Events can be sorted by each column heading by clicking on the appropriate heading.

## Searching for Events

Network sensor events can be filtered by additional parameters. The available filters are:

- **Time:** select a time frame to explore network activity
- **Source IP:** the specific IP address inside the network
- **Destination IP:** the IP address outside of the network that communicates with the **Source IP**
- **Source host:** the name of the host that the network traffic originates from
- **Source port:** the port used for a specific event by a host within the network
- **Destination port:** the port communicated with outside the network
- **Severity:** the risk level associated with the type of event – automatically classified by the system
- **Engine:** traffic being monitored by specific Cybowall engines
- **Direction:** the direction of traffic into or out of the network
- **Category:** standard IDS categories



## Organizing and Exporting Events

After selecting the desired filters (if required), relevant network events are presented in list view. Events can be sorted by category heading by clicking the appropriate heading (**Date & time**, **Port**, **Flow** etc.) and the complete list reorders accordingly:

Events		■ Stop	↓ Download			
N	Date & time	Source host	Port	Flow	Destination	
1.	09/05/2018 14:14:38	 80.127.152.30	123	↓↑	192.16	
2.	09/05/2018 13:57:20	 80.127.152.30	123	↓↑	192.16	
3.	09/05/2018 13:40:09	 80.127.152.30	123	↓↑	192.16	
4.	09/05/2018 13:26:43	 80.82.70.118	60000	↓	192.16	

Click the orange **Download** button to export the list (per the filters selected) in **PDF** or **Excel** format for record keeping and/or more detailed analysis.



# Intrusion Detection Categories

The Cybowall solution integrates a configurable out-of-the-box IDS. As Cybowall monitors inbound and outbound traffic flow through the network, it categorizes all abnormal or suspicious activity according to standard IDS classifications. It utilizes five general categories and further identifies activity according to a specific Class-type or sub-category.

This table shows the Class-type or sub-category of network traffic included in each Category type, and broken down further with a more detailed **Description** on the **Forensics** tab of Cybowall:

Category	Class-type
<b>Attempted Attack</b>	<ul style="list-style-type: none"> <li>• Attempted Denial of Service</li> <li>• Detection of a Denial of Service Attack</li> <li>• Web Application Attack</li> <li>• Misc Attack</li> <li>• A Network Trojan was Detected</li> <li>• Denial of Service</li> <li>• Malicious IP Activity was Detected by Cybowall</li> <li>• Malicious URL Activity was Detected by Cybowall</li> <li>• Malicious SSL Fingerprint was Detected</li> </ul>
<b>Suspicious Activity</b>	<ul style="list-style-type: none"> <li>• A Suspicious String Was Detected</li> <li>• Detection of a Network Scan</li> <li>• An Attempted Login Using a Suspicious Username was Detected</li> <li>• Potentially Bad Traffic</li> <li>• A Suspicious Filename was Detected</li> </ul>
<b>Information Leak</b>	<ul style="list-style-type: none"> <li>• Large Scale Information Leak</li> <li>• Potential Corporate Privacy Violation</li> <li>• Information Leak</li> <li>• Attempted Information Leak</li> </ul>
<b>Privilege Gain</b>	<ul style="list-style-type: none"> <li>• Unsuccessful User Privilege Gain</li> <li>• Attempted User Privilege Gain</li> <li>• Attempted Administrator Privilege Gain</li> <li>• Successful User Privilege Gain</li> <li>• Successful Administrator Privilege Gain</li> <li>• Attempt to Login by a Default Username and Password</li> </ul>
<b>Abnormal Activity</b>	<ul style="list-style-type: none"> <li>• Unknown Traffic</li> <li>• Access to a Potentially Vulnerable Web Application</li> <li>• Detection of a Non-Standard Protocol or Event</li> <li>• Generic Protocol Command Decode</li> <li>• A System Call was Detected</li> <li>• Executable Code was Detected</li> <li>• Decode of an RPC Query</li> <li>• A Client was Using an Unusual Port</li> <li>• Misc Activity</li> <li>• Not Suspicious Traffic</li> </ul>



# Updating or Managing IDS Signature Rules

As Cybowall starts to classify activity by Category and then by Class-type, the **Forensics** section also provides the actual **Signature** and **Signature ID** of the event itself by clicking on the green **Edit icon** to the right of the record.

Click on the green **Raw** link on the far right to view the raw data logs for further investigation:

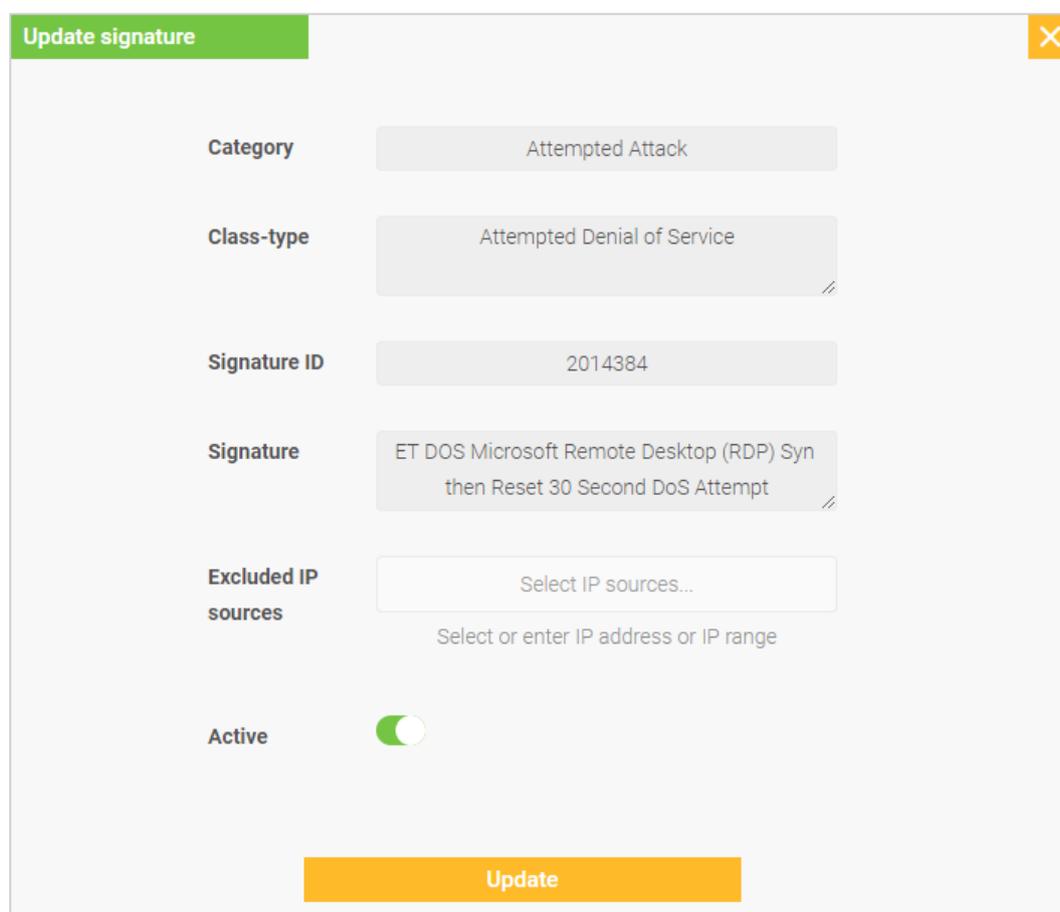
Details of event	26/05/2018 22:58:07	X
<b>Generic</b>		
<pre>{   "id": 4,   "content": {     "alert": {       "gid": 1,       "rev": 8,       "action": "allowed",       "category": "Attempted Denial of Service",       "severity": 2,       "signature": "ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second DoS Attempt",       "signature_id": 2014384     },     "proto": "TCP",     "src_ip": "192.168.20.140",     "dest_ip": "192.168.20.12",     "flow_id": 1867884436347465,     "in_iface": "eth1",     "src_port": 64941,     "dest_port": 3389,     "timestamp": "2018-05-26T22:58:07.219937+0300",     "event_type": "alert"   },   "creation_ts": {     "sec": 1527364687,     "usec": 219937   } }</pre>		

As events are tracked, it is important that organizations fine tune and customize the IDS rules based on specific network needs and baseline operating procedures.

The IDS rules can be managed and modified from the **Forensics** tab by clicking on the green **Edit icon** to the right of each event record:

Description			
ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second Do			Raw v
ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second Do			Raw v

The following window opens:



The **Update signature** window provides options to fine tune the existing IDS rules:

- **Excluded IP sources:** excludes this specific host within the network from being flagged when this specific IDS signature is identified with the host. If selected, this event is no longer tracked and reported on by Cybowall.
- **Active:** enables a more general deactivation of a specific signature-based rule within Cybowall. Once a signature is deactivated, it is no longer tracked and reported on by Cybowall until reactivated on the **Policy > IDS** tab of the Cybowall solution.

Clicking on the green **desktop icon** to the right of the event **Description** automatically adds the host IP to be excluded:

**Update signature** ✕

**Category** Attempted Attack

**Class-type** Attempted Denial of Service

**Signature ID** 2014384

**Signature** ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second DoS Attempt

**Excluded IP sources** 192.168.20.140 ✕ Select IP sources...  
Select or enter IP address or IP range

**Active**

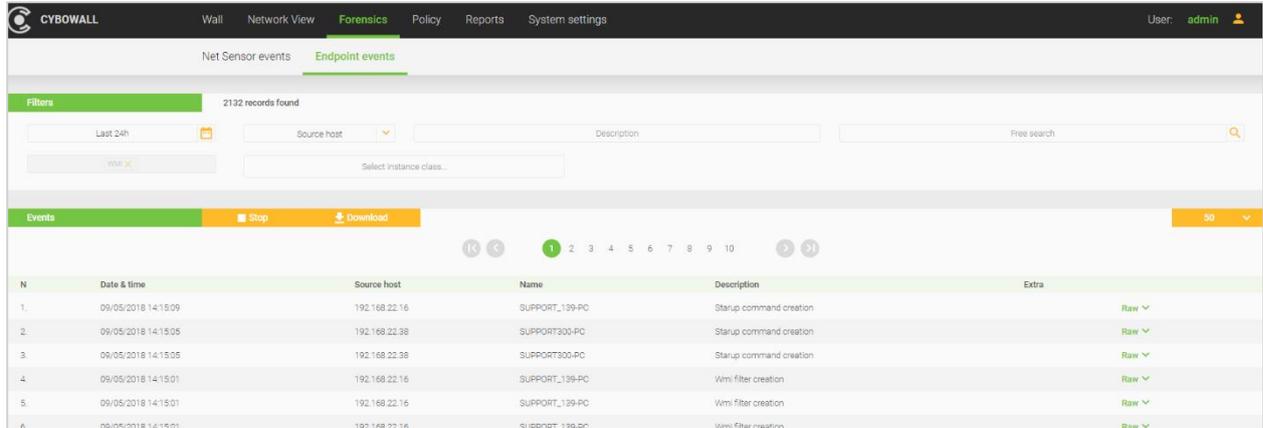
**Update**

See the Policy – IDS section of this guide for further information about the IDS management interface.

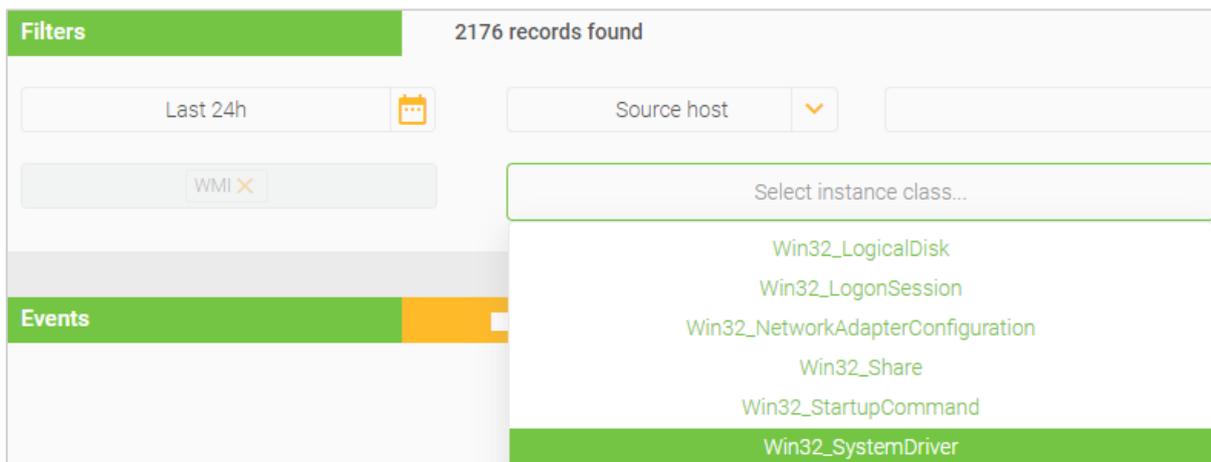


# Host Events

The **Host events** tab details events occurring directly on the hosts and being tracked by WMI.



It provides an immediate WMI level events list that can be filtered by **Date & time**, **Source host** or **Select instance class** (for WMI Class-types):



The WMI Class-types detailed in the table below monitor and manage system hardware and features:

WMI Class-type	Description
Win32_LogicalDisk	<ul style="list-style-type: none"> <li>A data source that resolves to an actual local storage device on a computer system running Windows</li> </ul>
Win32_LogonSession	<ul style="list-style-type: none"> <li>The logon session/sessions associated with a user logged on to a computer system running Windows</li> </ul>
Win32_NetworkAdapterConfiguration	<ul style="list-style-type: none"> <li>The attributes and behaviors of a network adapter</li> </ul>
Win32_Share	<ul style="list-style-type: none"> <li>A shared resource on a computer system running Windows</li> </ul>
Win32_StartupCommand	<ul style="list-style-type: none"> <li>A command that runs automatically when a user logs onto the computer system</li> </ul>
Win32_SystemDriver	<ul style="list-style-type: none"> <li>The system driver for a base service</li> </ul>



Further information can be viewed in the **Details of event** window by clicking the green **Raw** link to the right of each record:

```
Details of event 27/05/2018 12:54:01 X
Generic
{
  "id": 19,
  "content": {
    "ip": "192.168.30.23",
    "ts": "131718884414494611",
    "name": "LENOVO-ALON",
    "event": {
      "Name": "OneDriveSetup",
      "User": "PINEAPP\\wmi",
      "Caption": "OneDriveSetup",
      "Command": "C:\\Windows\\SysWOW64\\OneDriveSetup.exe /thfirstsetup",
      "UserSID": "S-1-5-21-162655134-940351046-1175432655-4667",
      "Location": "HKU\\S-1-5-21-162655134-940351046-1175432655-4667\\SOFTWARE\\Microsoft\\Windows\\C",
      "EventClass": "__InstanceCreationEvent",
      "Description": "OneDriveSetup",
      "subscription": "cbw_StartupCommandCreation",
      "InstanceClass": "Win32_StartupCommand"
    },
    "subts": "1523952812.11842"
  },
  "creation_ts": {
    "sec": 1527414841,
    "usec": 449461
  }
}
```



# Policy

The **Policy** tab provides customization options for Cybowall. It enables Cybowall to be configured according to the needs of the organization.

It is split into further tabs, including: **Network scanner**, **Port profiles**, **WMI**, **Malware hunter** and **IDS**.

## Network Scanner

The **Network scanner** tab allows the networks being scanned to be customized.

The networks that appear under the **Networks** section are added via **System settings > Network devices**. They are enabled/disabled and additionally configured on this tab:

Name	Address range	Risk factor	Malware hunter	Default gateway	DNS servers	DHCP servers	Protected	Whitelisted	Enabled
1.	192.168.2.0/24	192.168.2.0/24	1	Normal			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.	192.168.10.0/24	192.168.10.0/24	1	Normal			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.	192.168.22.0/24	192.168.22.0/24	1	Normal	192.168.22.254	192.168.2.215	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.	192.168.30.0/24	192.168.30.0/24	1	Normal			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

To edit the settings of a particular network, click the **Edit icon** to the right of the relevant network.

The **Update network** window opens:

Update network ✕

**⚠ Important** If you need to change *IP range* field, you should delete it and create a new one with all corresponding network definitions in **System settings / Network devices / VLAN access interface list**. Please note that deleting the network is *an irreversible operation* and will cause all hosts and statistic related to this *IP range* to be deleted.

IP address and subnet mask (CIDR notation)	<input type="text" value="172.16.100.0/24"/>
Network name	<input type="text" value="172.16.100.0/24"/>
Default gateway	<input type="text" value="192.168.0.254"/>
DNS servers	<input type="text" value="8.8.8.8"/> <span>+</span>
DHCP servers	<input type="text" value="192.168.0.254"/> <span>+</span>
Network risk factor	<input type="text" value="1"/>
Malware hunter profile	<input type="text" value="Normal"/> <span>▾</span>
Status	<input checked="" type="checkbox"/>

Update

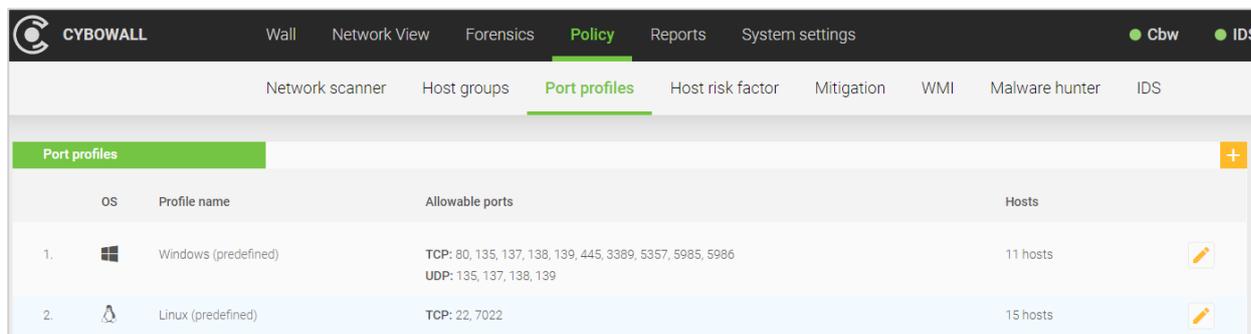
The following customizations are possible:

- **Network name:** provide a custom name for the network
- **Default gateway:** choose an alternate default gateway
- **DNS servers:** add additional DNS servers by clicking the orange + icon
- **DCHP servers:** add additional DNS servers by clicking the orange + icon
- **Network risk factor:** change the risk factor
- **Malware hunter profile:** select **Normal** or **Aggressive**
- **Enabled:** enable or disable monitoring on that network

# Port Profiles

A port profile is a set of ports allowed for a specific profile. If a host has opened a port beyond the defined port profile set, it is considered suspicious behavior.

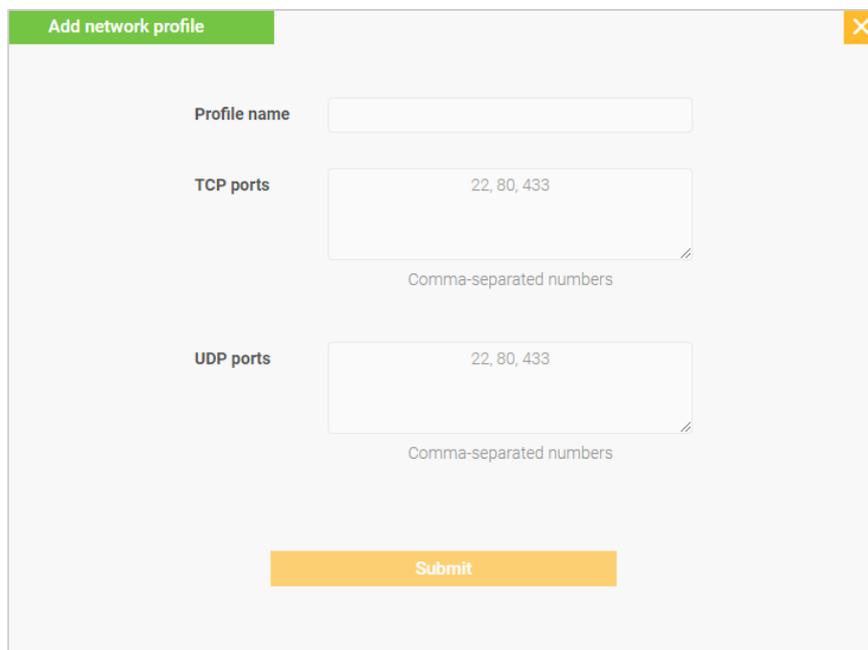
There are two default (predefined) port profiles; one for Windows and one for Linux:



OS	Profile name	Allowable ports	Hosts
1.	 Windows (predefined)	TCP: 80, 135, 137, 138, 139, 445, 3389, 5357, 5985, 5986 UDP: 135, 137, 138, 139	11 hosts 
2.	 Linux (predefined)	TCP: 22, 7022	15 hosts 

## Creating Port Profiles

To create a custom profile, click the orange + icon to the right of the **Port profiles** section. The **Add network profile** window opens:



**Add network profile** 

**Profile name**

**TCP ports**   
Comma-separated numbers

**UDP ports**   
Comma-separated numbers

**Submit**

Add a **Profile name**, enter the allowed **TCP ports** and/or **UDP ports** (separated by commas) and **Submit**.

To edit a port profile, click the orange **Edit icon** to the right of the profile in the **Port profiles** section.

# Assigning Port Profiles

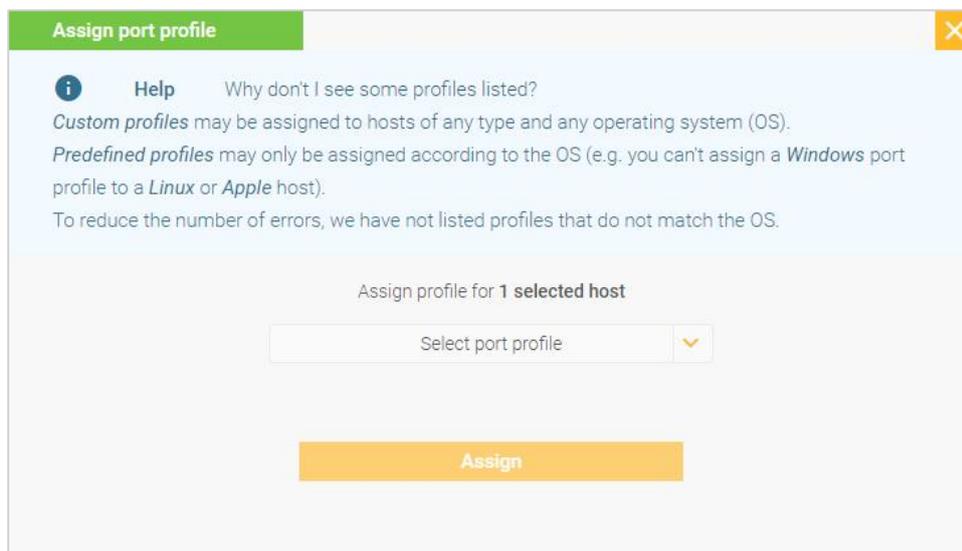
Profiles are assigned to hosts in the **Network hosts** section.

In the left hand column, select the individual host or hosts. Click the orange **Assign profile** button next to the section name:



All	Address	Name	OS family	Network	Status	Profile
<input type="radio"/>	192.168.2.5		Linux	192.168.2.0/24 (192.168.2.0/24)	<span style="color: green;">●</span>	Linux
<input checked="" type="radio"/>	192.168.2.7	PINEX13	Windows	192.168.2.0/24 (192.168.2.0/24)	<span style="color: green;">●</span>	Windows

The **Assign port profile** window opens. Choose the relevant port profile for the host under **Select port profile**:



### Assign port profile

**Help** Why don't I see some profiles listed?  
*Custom profiles* may be assigned to hosts of any type and any operating system (OS).  
*Predefined profiles* may only be assigned according to the OS (e.g. you can't assign a *Windows* port profile to a *Linux* or *Apple* host).  
To reduce the number of errors, we have not listed profiles that do not match the OS.

Assign profile for **1 selected host**

Select port profile

**Assign**

Once a port profile has been assigned, it is reflected in the **Dashboard > Risk assessment** and **Dashboard > Network Visibility** sections of Cybowall, in the **Network View > Details** window and in the **Host Analysis > Host health** and **Vulnerability > Open Ports Reports**.

# WMI

WMI access is configured on this tab. It allows Cybwall to query the various hosts on the network with minimal interference.

**\*Note:** The WMI account requires Admin level privileges at the domain level.

To set a WMI account, click the orange **Update** button in the **Domain settings** section:

Name	IP address	Network	Status	WMI subscriptions
1. BOYDEM2012	192.168.2.170	192.168.2.0/24 (192.168.2.0/24)	●	Subscription details ▾
2. OONROOM-PC	192.168.2.97	192.168.2.0/24 (192.168.2.0/24)	●	Subscription details ▾
3. CYBOSUPPORT-PC	192.168.22.23	192.168.22.0/24 (192.168.22.0/24)	●	Subscription details ▾
4. DESKTOP-SUPPORT	192.168.22.37	192.168.22.0/24 (192.168.22.0/24)	●	Subscription details ▾

Enter the company **Domain**, **User** name and **Password**, and click the **Save** button:

Click the **Test WMI connection** button on the right. The following window opens:

Enter the IP address of a host in the network being scanned, and click **Test**.



If the test is successful, Cybowall displays **Successful WMI connection**:

Domain settings	Update	
✓ Successful WMI connection		
Domain	User	Password

If not successful, ensure the **User** name and **Password** are correct and check that the GPO was correctly configured and deployed. See the Cybowall Configuration Guide for further details.

# Malware Hunter

The behavior of the malware hunter tool can be customized on this tab by specifying which file types to look for and in which locations.

Cybowall has two predefined profiles which are shown in the **Malware hunter profiles** section – **Normal** and **Aggressive**:

Malware hunter profiles			
N	Name	Extensions	Paths
1.	Normal	*.dll, *.exe, *.bmp, *.jpeg, *.jpg	C:\Program Files
2.	Aggressive	*.apk, *.bat, *.bin, *.cgi, *.pl, *.com, *.exe...	C:\ProgramFiles, C:\ProgramFiles(x86)...

It is possible to edit the existing profiles, though it is preferable to create custom profiles.

## Editing Malware Hunter Profiles

To edit the existing malware hunter profiles in the **Malware hunter profiles** section, click the orange **Edit icon** to the right of the relevant profile. The **Update malware hunter profile** window opens:

**Update malware hunter profile**

**Profile name** Normal

**Extensions** \*.dll, \*.exe, \*.bmp, \*.jpeg, \*.jpg

**Paths** C:\Program Files

[Back to factory defaults](#)

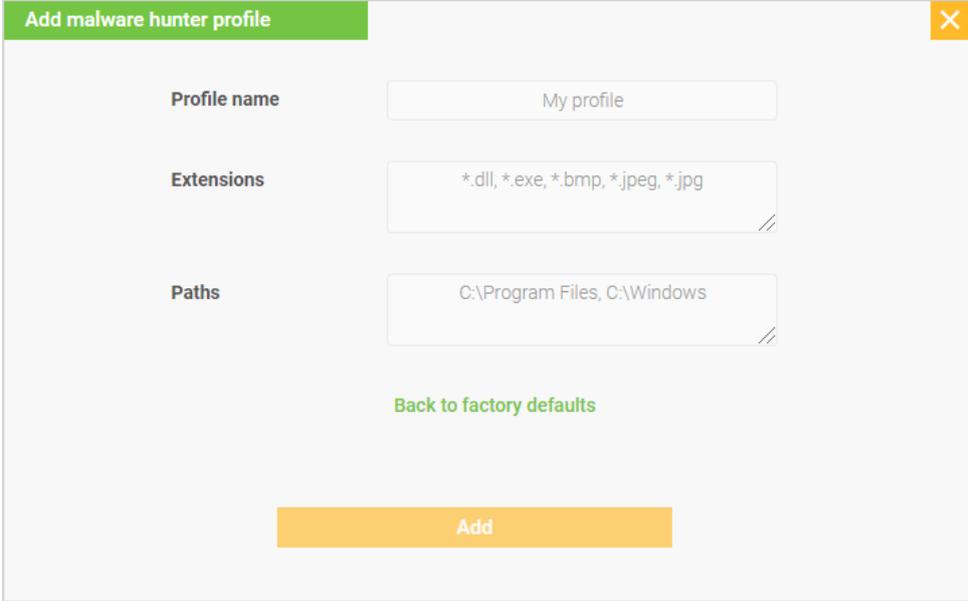
**Update**

Edit the **Extensions** and/or **Paths** as required, and click **Update**.

To return to the default settings, click the green **Back to factory defaults** link.

# Creating Malware Hunter Profiles

To create a new malware hunter profile, click the orange + icon to the top right of the **Malware hunter profiles** section. The **Add malware hunter profile** window opens:



The screenshot shows a dialog box titled "Add malware hunter profile" with a close button in the top right corner. The dialog contains three input fields:

- Profile name:** My profile
- Extensions:** \*.dll, \*.exe, \*.bmp, \*.jpeg, \*.jpg
- Paths:** C:\Program Files, C:\Windows

Below the input fields, there is a green link labeled "Back to factory defaults" and an orange "Add" button at the bottom center.

Input a **Profile name**, desired **Extensions** (file types) and **Paths**, and click **Add**.

# IDS

An IDS monitors and inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack. It provides alerts regarding suspicious activity and known threats.

Organizations deploy IDS solutions to gain visibility into potentially malicious activities, detect security breaches and aid in mitigating damage to their environments.

The **IDS** tab in Cybowall provides the option to choose from existing IDS profiles or to customize the behavior of the IDS:

IDS profiles		Switch	Update IDS rules		Update
Profile	Description		Last update check		Last update completed
Silent	Attempted Attack		21 minutes ago		20 minutes ago
<b>Regular</b>	Attempted Attack, Suspicious Activity, Privilege Gain				
Aggressive	Attempted Attack, Suspicious Activity, Information Leak, Privilege Gain, Abnormal Activity				
Custom	Extended management				

## Selecting IDS Profiles

In order to select an existing IDS profile, click the orange **Switch** button at the top of the **IDS profiles** section. The **Switch IDS profile** window opens:

Switch IDS profile
✕

**IDS profile**

Silent

Regular

Aggressive

Custom

Under **IDS profile**, select the profile option required; **Silent**, **Regular**, **Aggressive** or **Custom** (to customize the configuration). Click the orange **Switch** button.

If **Custom** is selected, choose the required options to filter signatures, enable/disable popular signatures in the network and excluding specific IP addresses/entire ranges.

# Editing IDS Signatures

To edit a signature, click the **Edit icon** to the right of the signature in the **Popular signatures** section:

Filters						Signatures found
Select class-type...		Enter signature...			0	
Popular signatures						
N	ID	Signature	Events	Enabled	Excluded IP sources	
1.	2001972	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)	125	<input checked="" type="checkbox"/>		
2.	2523112	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 557	81	<input checked="" type="checkbox"/>		
3.	2023882	ET INFO HTTP Request to a *.top domain	19	<input checked="" type="checkbox"/>		
4.	2023883	ET DNS Query to a *.top domain - Likely Hostile	10	<input type="checkbox"/>	192.168.2.215	
5.	2016538	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download	6	<input checked="" type="checkbox"/>		
6.	2025535	ET CURRENT_EVENTS Observed Coin-Hive In Browser Mining Domain (coin-hive.com in TLS SNI)	4	<input checked="" type="checkbox"/>		
7.	2402000	ET DROP Dshield Block Listed Source group 1	3	<input checked="" type="checkbox"/>		
8.	2403328	ET DNS Active Threat Intelligence Poor Reputation IP group 29	3	<input checked="" type="checkbox"/>		
9.	2025106	ET INFO DNS Query for Suspicious .ml Domain	1	<input checked="" type="checkbox"/>		
10.	2025536	ET CURRENT_EVENTS Observed Malicious SSL Cert (Coin-Hive In Browser Mining)	1	<input checked="" type="checkbox"/>		
Total			253			

The **Update signature** window opens:

Update signature
✕

**Category**

**Class-type**

**Signature ID**

**Signature**

**Excluded IP sources**   
Select or enter IP address or IP range

**Active**

Update

To exclude IP addresses, enter an IP address in the **Exclude IP sources** field and **Enter**. Continue adding IP addresses as required.



If networks were added under **System settings > Network devices**, these can be selected in the **Exclude IP sources** field.

Set the **Active** slider to deactivate or activate (green) a signature.

## Customizing the IDS

It is possible to fine tune the behavior of the IDS with regard to all signatures by choosing the **Custom** IDS profile. This provides a number of options for customization:

Categories		Class-types				Signatures			
Category	Enabled	N	Class-type	Events	Enabled	N	Signature	Events	Enabled
Attempted Attack	<input checked="" type="checkbox"/>	1.	Misc Attack	97	<input checked="" type="checkbox"/>	1.	ET_VOIP_INVITE Message Flood TCP	0	<input checked="" type="checkbox"/>
Suspicious Activity	<input checked="" type="checkbox"/>	2.	A Network Trojan was Detected	5	<input checked="" type="checkbox"/>	2.	ET_VOIP_REGISTER Message Flood TCP	0	<input checked="" type="checkbox"/>
Information Leak	<input type="checkbox"/>	3.	Attempted Denial of Service	0	<input checked="" type="checkbox"/>	3.	ET_VOIP_Multiple Unauthorized SIP Responses TCP	0	<input checked="" type="checkbox"/>
Privilege Gain	<input type="checkbox"/>	4.	Denial of Service	0	<input type="checkbox"/>	4.	ET_VOIP_INVITE Message Flood UDP	0	<input checked="" type="checkbox"/>
Abnormal Activity	<input type="checkbox"/>	5.	Detection of a Denial of Service AT...	0	<input checked="" type="checkbox"/>	5.	ET_VOIP_REGISTER Message Flood UDP	0	<input checked="" type="checkbox"/>
		6.	Malicious IP Activity was Detected...	0	<input type="checkbox"/>	6.	ET_VOIP_Multiple Unauthorized SIP Responses UDP	0	<input checked="" type="checkbox"/>
		7.	Malicious SSL Fingerprint was Det...	0	<input type="checkbox"/>	7.	ET_WEB_SERVER Possible Cherokee Web Server GET A...	0	<input checked="" type="checkbox"/>
		8.	Malicious URL Activity was Detect...	0	<input type="checkbox"/>	8.	ET_SCADA_RealWin SCADA System Buffer Overflow	0	<input checked="" type="checkbox"/>
		9.	Web Application Attack	0	<input checked="" type="checkbox"/>	9.	ET_TFTP_TFTPGUI Long Transport Mode Buffer Overflow	0	<input checked="" type="checkbox"/>
						10.	ET_WEB_SERVER_PHP Large Subnormal Double Preci...	0	<input checked="" type="checkbox"/>

Under **Categories**, five categories – **Attempted Attack**, **Suspicious Activity**, **Information Leak**, **Privilege Gain** and **Abnormal Activity** – can be enabled or disabled by clicking the **Edit icon** to the right of each category and clicking the **Active** slider:

Update category
✕

**Category** Attempted Attack

**Excluded IP sources** Select IP sources...  
Select or enter IP address or IP range

**Active**

Update

Exclude IP addresses or ranges by entering them in the **Excluded IP sources** field.

Selecting a **Category** displays the **Class-types** relevant to that category.



Click the **Edit icon** to enable/disable a Class-type and to customize the **Excluded IP sources**.

Select a **Class-type** to display the **Signatures** applicable to that Class-type:

Categories		Class-types			Signatures		
Category	Enabled	Class-type	Events	Enabled	Signature	Events	Enabled
Attempted Attack	<input checked="" type="checkbox"/>	1. Misc Attack	17	<input checked="" type="checkbox"/>	1. ET EXPLOIT ExtremeZ-IP File and Print Server Multiple ...	0	<input type="checkbox"/>
Suspicious Activity	<input checked="" type="checkbox"/>	2. A Network Trojan was Detected	0	<input checked="" type="checkbox"/>	2. ET EXPLOIT ExtremeZ-IP File and Print Server Multiple ...	0	<input type="checkbox"/>
Information Leak	<input type="checkbox"/>	3. Attempted Denial of Service	0	<input checked="" type="checkbox"/>	3. ET EXPLOIT Borland ViaBroker Smart Agent Heap Over...	0	<input type="checkbox"/>
Privilege Gain	<input type="checkbox"/>	4. Denial of Service	0	<input checked="" type="checkbox"/>			
Abnormal Activity	<input type="checkbox"/>	5. Detection of a Denial of Service At...	0	<input type="checkbox"/>			
		6. Malicious IP Activity was Detected...	0	<input type="checkbox"/>			
		7. Malicious SSL Fingerprint was Det...	0	<input type="checkbox"/>			
		8. Malicious URL Activity was Detect...	0	<input type="checkbox"/>			
		9. Web Application Attack	0	<input checked="" type="checkbox"/>			

Click the **Edit icon** to the right of each **Signature** to enable/disable signatures and to exclude IP addresses and ranges.



## Custom Signatures

Cybowall provides the option to introduce custom signatures to the system.

Click the orange + icon to the right of the **Custom signatures** section at the bottom of the IDS tab:

Custom signatures											+
SID	Source IP	Port	Flow	Destination IP	Port	Description	URL	Class-type	Enabled	Excluded IP sources	

The **Add custom signature** window opens. Complete the fields and **Add**:

### Add custom signature

**Source IP**   
Select or enter IP address or IP range, or leave it empty

**Source port**   
Enter port number or leave it empty

**Flow**  ▾

**Destination IP**   
Select or enter IP address or IP range, or leave it empty

**Destination port**   
Enter port number or leave it empty

**Description**

**URL**

**Class-type**  ▾

**Excluded IP sources**   
Select or enter IP address or IP range

**Active**

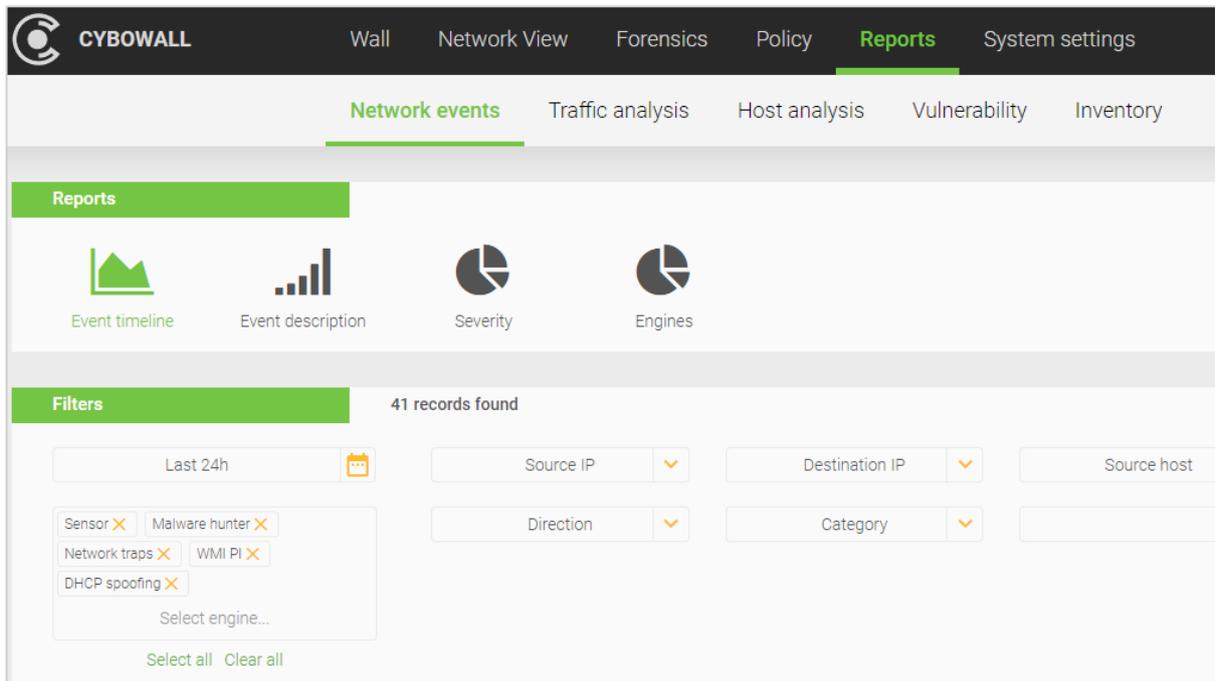
**Add**

# Reports

The **Reports** tab of Cybwall allows the information collected by Cybwall to be presented in relevant and easy to digest report formats.

These reports help the organization to investigate and remediate issues identified, report information to internal and external stakeholders, and meet compliance and audit requirements.

Cybwall's **Reports** section is broken down further into five tabs; **Network events**, **Traffic analysis**, **Host analysis**, **Vulnerability** and **Inventory**:



The screenshot shows the Cybwall Reports interface. At the top, there is a navigation bar with the following tabs: Wall, Network View, Forensics, Policy, Reports (highlighted), and System settings. Below this, there is a sub-navigation bar with the following tabs: Network events (highlighted), Traffic analysis, Host analysis, Vulnerability, and Inventory. The main content area is titled 'Reports' and contains four report types: Event timeline (represented by a line graph icon), Event description (represented by a bar chart icon), Severity (represented by a pie chart icon), and Engines (represented by a pie chart icon). Below the report types, there is a 'Filters' section with the text '41 records found'. The filters include: 'Last 24h' (with a calendar icon), 'Source IP' (dropdown), 'Destination IP' (dropdown), 'Source host', 'Direction' (dropdown), and 'Category' (dropdown). There is also a 'Sensor' section with a list of selected sensors: Malware hunter, Network traps, WMI PI, and DHCP spoofing. Below the sensor list, there is a 'Select engine...' dropdown and 'Select all' and 'Clear all' buttons.

## Selecting Report Criteria

On the **Network events**, **Traffic analysis**, **Host analysis** and **Inventory** tabs, reports can be filtered by relevant criteria and the report period chosen.

To select the time period to be shown in the report, click the orange calendar icon or click on 'Last 24h'.



The calendar window opens. Choose the relevant dates from the calendar (Custom Range) or quick choices are shown in the left hand column, for example, 'Last 7 days' or 'Last year':

The screenshot shows a 'Filters' panel with '177 records found'. It includes a 'Last 24h' button, a date range selector (2018-05-06 10:37:04 to 2018-05-07 10:37:04), and a calendar view for April and May 2018. The calendar grid shows dates from 25th of April to 9th of May. The 6th and 7th of May are highlighted in green. There are also buttons for 'Apply' and 'Cancel'.

## Available Reports

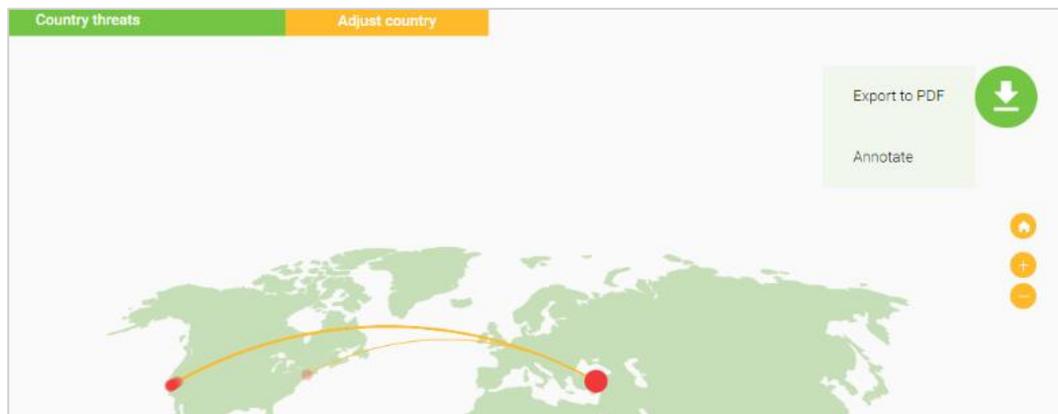
The following reports are available on the **Reports** tab of Cybowall:

Tab	Report Title	Report Description
Network events	Event timeline	Network events and when they occurred
	Event description	IDS event categories and signatures
	Severity	Events categorized by severity rating
	Engines	Events discovered by Cybowall engine
Traffic analysis	Threat source	Network events by threat source country
Host analysis	Host health	Individual host risk assessment
	Host details	Host inventory
	Asset summary	Asset summary by OS type
	Operating system	Breakdown by OS family
	WMI events	Network events discovered by WMI
	Active hosts	Events timeline of active hosts
Vulnerability	Summary	Summary of vulnerability severity ratings
	Open ports	Open ports inventory
	Protection	Summary of host protection measures
	Default credentials	Details of default and weak credentials
Inventory	Software	Breakdown of vulnerabilities by application

# Exporting and Annotating Reports

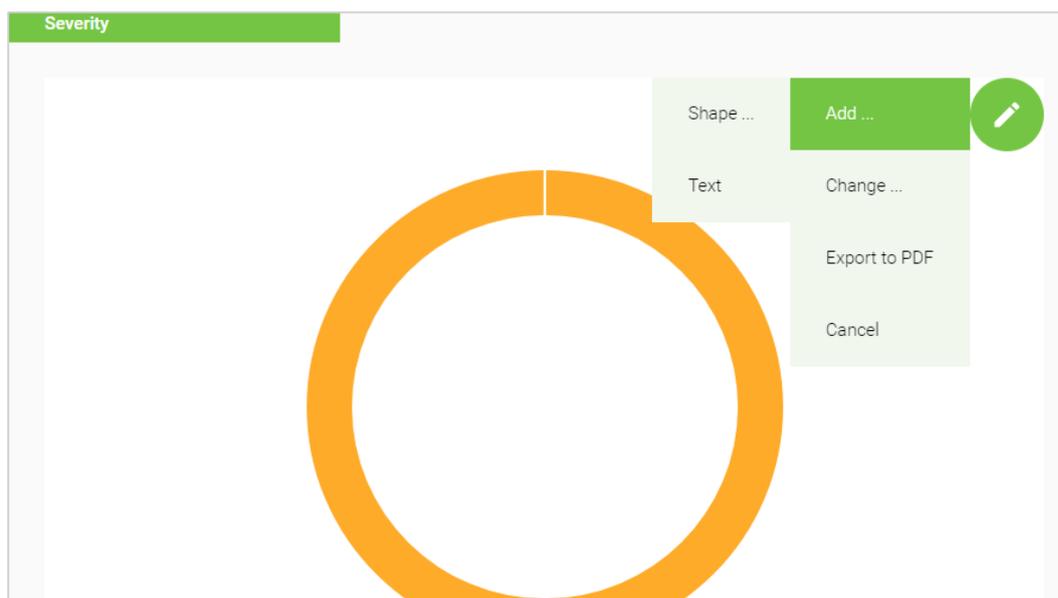
To enable review and record keeping, reports can be exported to PDF. They can also be annotated to highlight particular aspects or follow-up actions etc. before being exported.

Click on the orange **download arrow**. It turns green and shows two options; **Export to PDF** or **Annotate**:



To export directly, click **Export to PDF**. Choose the location where the report should be saved, and click **Save**.

To first annotate the report, click **Annotate**. Annotations can be made with the cursor. Hover over the green circle again and it changes to an **Edit icon**:



The following options are available:

- Add: Shape or Text
- **Change: Mode, Color, Size or Opacity** of the annotations

After annotation, the report can be printed or downloaded as a PNG, JPG, SVG or PDF file.



A number of the inventory/list style reports can be downloaded by clicking the orange **Export to PDF** button:

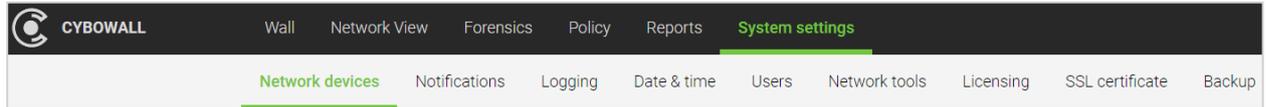
Host health		Export to PDF		16 records		10	
Name	Anti-virus	Firewall	Ports not in profile	Windows updates	Vulnerabilities	Wireless access	
1.  BOYDEM2012							
2.  ZOOM							

Choose the location where the report should be saved, and click **Save**.



# System Settings

The **System settings** section provides configuration options for Cybowall. It is split into the following tabs: **Network devices**, **Notifications**, **Date & time**, **Users**, **Network tools**, **Licensing**, **SSL certificate** and **Backup**:

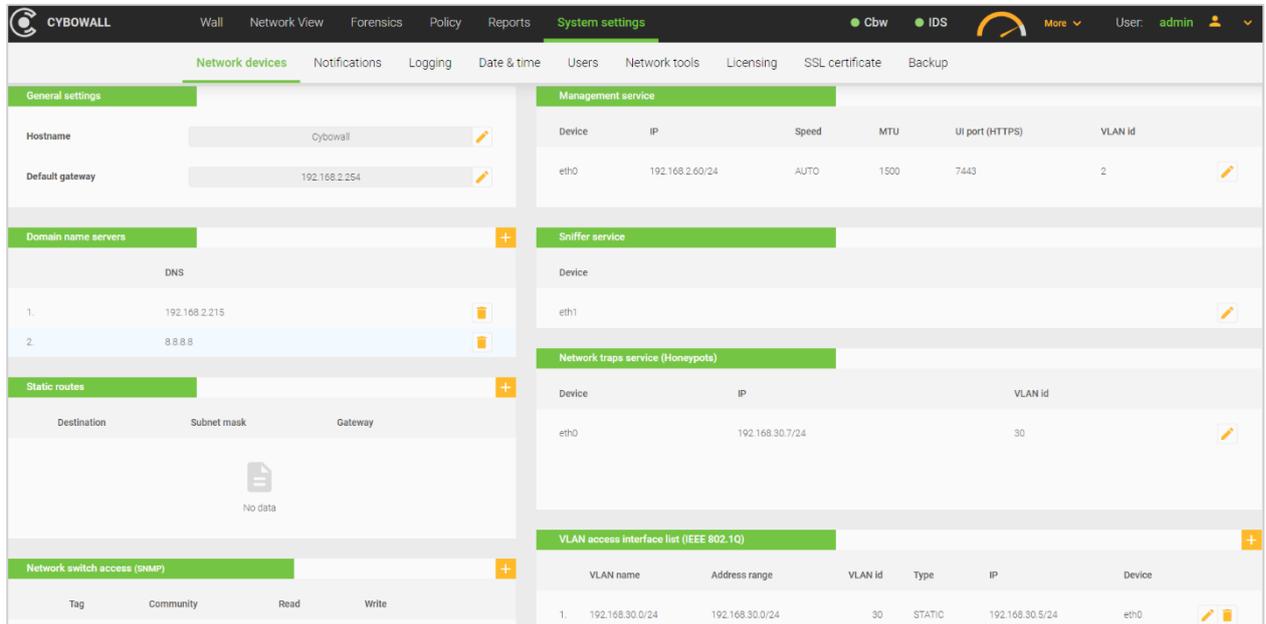


For detailed instructions on configuring Cybowall, consult the [Cybowall Configuration Guide](#).

## Network Devices

The **Network devices** tab provides network configuration options for Cybowall. It also enables the IP address of the network trap (honeypot) to be defined, and more.

After Cybowall has been installed, accessed via the browser and the license key entered, navigate to **Network devices** to configure the solution:





## General Settings

The Cybowall **Hostname** and **Default gateway** address are configured in the **General settings** section (the **Default gateway** is configured via the CLI during installation, but can be changed here).

Clicking the **Edit icon** to the right of the relevant field, update the information and click the orange **check mark** that appears in the edit mode:

General settings	
Hostname	Cybowall <input type="checkbox"/> <input type="checkbox"/>
Default gateway	192.168.2.254 <input type="checkbox"/>

## Domain Name Servers

DNS server addresses can be added or edited in the **Domain name servers** section.

Click the orange **+** icon to the top right of the section. An empty **New DNS** field appears at the bottom of the section. Input the IP address of the DNS server and click the orange **+** icon to the right of the field to add it:

Domain name servers		+
DNS		
1.	192.168.2.215	<input type="checkbox"/>
2.	8.8.8.8	<input type="checkbox"/>
New DNS	<input type="text"/>	+

New DNS servers can be added multiple times. The default DNS server displayed is for Google (8.8.8.8).

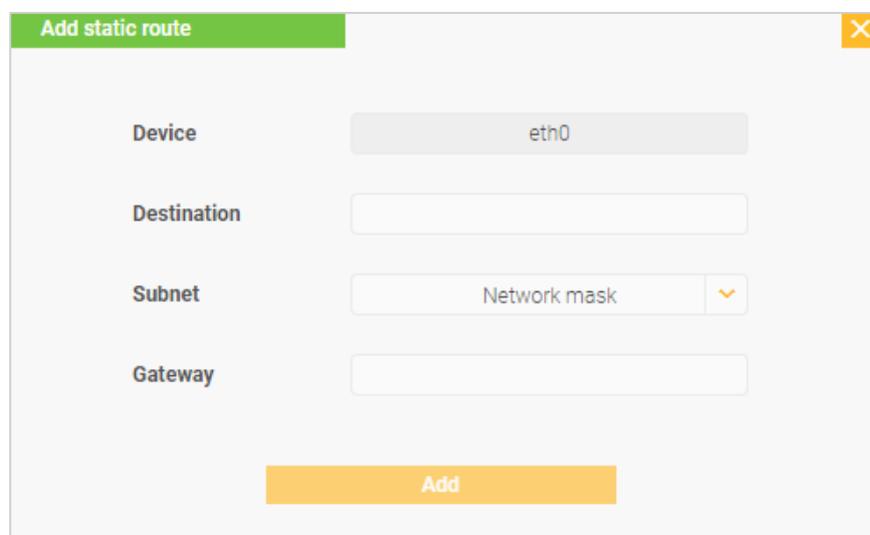
## Static Routes

The **Static routes** section allows static routes to hosts in different networks to be configured, without passing through the default gateway.

To configure a static route, click the orange + icon to the top right of the section, and complete the following fields:

- **Device:** choose a network interface
- **Destination:** add the destination IP address
- **Subnet:** add the required subnet mask (in CIDR notation)
- **Gateway:** add the default gateway

Click **Add**:



The screenshot shows a modal window titled "Add static route" with a close button (X) in the top right corner. The form contains four input fields:

- Device:** A dropdown menu with "eth0" selected.
- Destination:** An empty text input field.
- Subnet:** A dropdown menu with "Network mask" selected and a small orange arrow icon to its right.
- Gateway:** An empty text input field.

At the bottom center of the form is a large orange button labeled "Add".

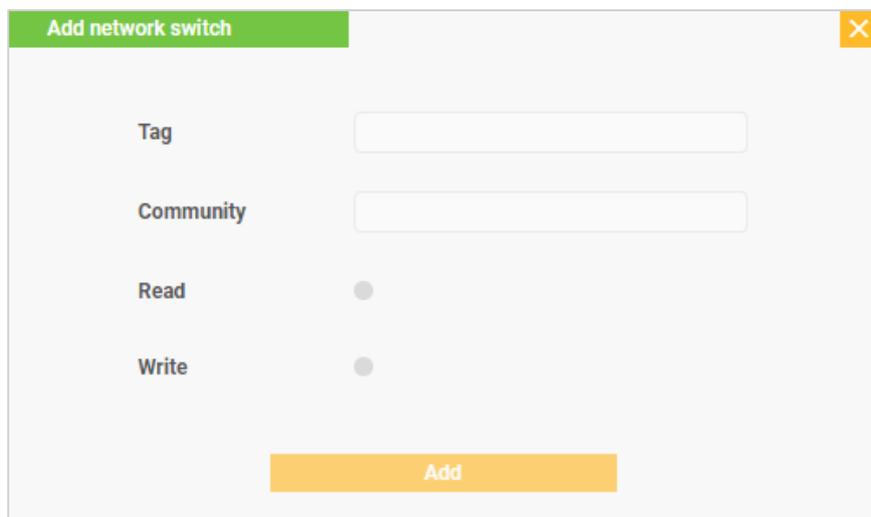
## Network Switch Access

Access to network devices is configured in the **Network switch access (SNMP)** pane.

Click the orange + icon to the top right of the section, and complete/select the following fields:

- **Tag:** add a name/description for the switch
- **Community:** add the passphrase for the switch
- **Read:** allow read privileges
- **Write:** allow write privileges

Click **Add**:



The screenshot shows a modal window titled "Add network switch" with a close button (X) in the top right corner. The form contains the following fields:

- Tag:** A text input field.
- Community:** A text input field.
- Read:** A radio button.
- Write:** A radio button.

At the bottom center of the form is an orange "Add" button.

## Management Service

The management service configuration is edited in the **Management service** section.

The initial information is based on the setup performed in the CLI during installation. To edit the configuration, click the **Edit icon** to the right of the section and edit the relevant fields:

### Update management interface ✕

Device	<input type="text" value="eth0"/> <span>▼</span>
Select the network interface to configure (the interface used for "Sniffer service" will <b>not</b> be available here)	
IP address and subnet mask (CIDR notation)	<input type="text" value="192.168.100.7/24"/>
Please enter a valid IP address and subnet mask using a CIDR notation	
MTU	<input type="text" value="1500"/>
From 68 to 1500	
UI port (HTTPS)	<input type="text" value="7443"/>
From 1024 to 65535	
Speed	<input type="text" value="AUTO"/> <span>▼</span>
VLAN id	<input type="text" value="100"/>
From 1 to 4094	

**Note:** Add a **VLAN id** only in a tagged network environment, where VLAN IDs are in use. See the Cybwall Configuration Guide for further information.

## Sniffer Service

The **Sniffer service** section enables the interface used by the sniffer service (IDS) to be changed.

Click the **Edit icon** to the right of the section and select the relevant interface from the dropdown, then click the checkmark, to approve.



Sniffer service	
Device	
eth1	
Device	<input type="text"/>
	<input checked="" type="checkbox"/> <input type="checkbox"/>
	eth0
	eth1

**Note:** Do not select the interface used by the management service. Additionally, the chosen interface needs to be connected to a port which was configured for port mirroring.

## Network Traps

The **Network traps service (honeypots)** section enables the configuration of the Cybowall network trap.

Click the **Edit icon** to the right of the section. The **Update network traps interface** window opens. Enter/select the following:

- **Device:** select the network interface
- **IP address and subnet mask (CIDR notation)**
- **VLAN id:** for a **Tagged** environment only

Click **Update**:

**Update network traps interface** ✕

**Device**  ▼  
Select the network interface to configure (the interface used for "Sniffer service" will **not** be available here)

**IP address and subnet mask (CIDR notation)**   
Please enter a valid IP address and subnet mask using a CIDR notation

**VLAN id**   
From 1 to 4094

**Update**

## VLAN Access

The **VLAN access interface list (IEEE 802.1Q)** section provides an interface for adding additional networks to be monitored by Cybowall.

To add networks, click the orange + icon to the top right of the section and complete the following:

- **Device selection:** select the network interface to work with
- **IP address type:** **Static (Manual)** or **DHCP** (currently only Static is supported)
- **IP address and subnet mask (CIDR notation):** enter a valid IP address (that is not in use and is within the required network) and the subnet mask – using a CIDR notation
- **Tagged / Untagged:** select the network type – refer to the Cybowall Configuration Guide for explanations
- **VLAN id:** for a **Tagged** network environment, enter the VLAN id for that network

Click **Add**:

**Add VLAN access interface** ✕

**Device selection**  ▼  
Select the network interface to configure  
(the interface used for "Sniffer service" will not be available here)

**IP address type** Static (Manual) DHCP  
DHCP is only allowed to be configured for fully-configured VLANs, go to Policy / Network scanner to configure the VLAN in full first

**IP address and subnet mask (CIDR notation)**   
Please enter a valid IP address and subnet mask using a CIDR notation

**Tagged / Untagged** Tagged Untagged  
Is this VLAN tagged (for IEEE 802.1Q access) or untagged (native VLAN)?

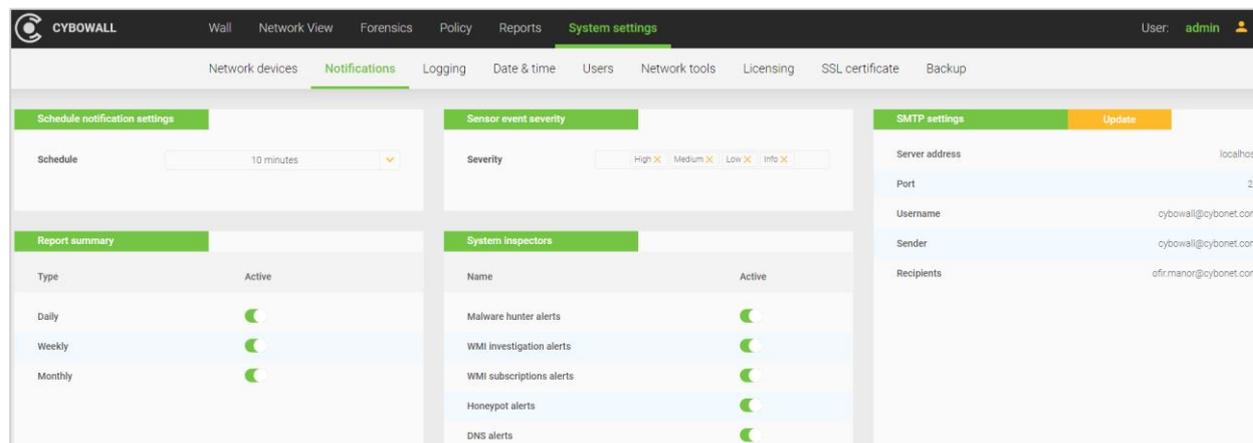
**VLAN id**   
What is the VLAN id for this? (check your network equipment settings to be sure please)

**Add**

To edit or delete an existing VLAN, click the **Edit/Delete icon** to the right hand side of each VLAN record in the **VLAN access interface list (IEEE 802.1Q)** section.

# Notifications

This tab allows for the configuration of an SMTP server, and enables alerts and reports to be configured so that they are sent to designated users/email accounts according to pre-defined frequencies:



## Schedule Notification Settings

The **Schedule notification settings** section allows the interval between the sending of alert emails to be configured.

## Report Summary

The **Report summary** section enables Daily, Weekly and Monthly reports to be activated/de-activated in order to customize the reports received.

## Sensor Event Severity

The **Sensor event severity** section enables the selection of the severity level of events (**High**, **Medium**, **Low**, **Info**) to which a user is alerted.

## System Inspectors

The **System inspectors** section enables the selection of the types of events to which a user is alerted: **Malware hunter alerts**, **WMI investigation alerts**, **WMI subscriptions alerts**, **Honeygot alerts**, **DNS alerts**.

## SMTP Settings

The **SMTP settings** section provides an interface for configuring which email server sends out the Cybwall alerts and reports.

To configure this, click the orange **Update** button to the right of the section heading and enter the following information:

- **Server address:** the address of the mail/SMTP server
- **Port:** the relevant port (usually port 25)
- **Username:** the username of the account with access to the SMTP server
- **Password:** the password of the account added in the **Username** field
- **Sender:** the email address displayed as the sender of Cybwall alerts and reports
- **Recipients:** the email addresses to which Cybwall sends alerts and reports

Click **Update**:

**Update SMTP settings** ✕

<b>Server address</b>	<input type="text" value="192.168.2.7"/>
<b>Port</b>	<input type="text" value="25"/>
<b>Username</b>	<input type="text" value="username"/>
<b>Password</b>	<input type="password"/>
<b>Sender</b>	<input type="text" value="cybwall@cybonet.com"/>
<b>Recipients</b>	<input type="text" value="idan@cybonet.com"/>

**Update**



# Date and Time

The **Date & time** tab enables the correct date and time, time zone and Network Time Protocol (NTP) server to be set up for Cybowall:

Date & time settings	Update
Time	16:38:53
Date	05/31/2018
Time zone	Asia/Jerusalem
NTP server	pool.ntp.org

Click the orange **Update** button to the right of the **Date & time settings** section heading to enter the correct: **Time**, **Date**, **Timezone** and the required **NTP server**.

# Users

The **Users** tab provides the option to manage Cybowall users. The default user is admin:

Users				
	Login	Full name	Permissions	Enabled
1.	admin	admin	Full access	<input checked="" type="checkbox"/> 

Click the **Edit icon** to the right in order to edit the user, change the user's password, and enable/disable the user's account.

To add a user, click the orange **+** icon. The **Add user** window opens:

### Add user

**Login**

**Full name**

**Password**

**Confirm password**

Permissions	Read	Write
Wall	<input type="checkbox"/>	<input type="checkbox"/>
Network View	<input type="checkbox"/>	<input type="checkbox"/>
Forensics	<input type="checkbox"/>	<input type="checkbox"/>
Policy	<input type="checkbox"/>	<input type="checkbox"/>
Reports	<input type="checkbox"/>	<input type="checkbox"/>
System settings	<input type="checkbox"/>	<input type="checkbox"/>

**Enabled**

**Add**

Create the user **Login**, **Full name**, **Password** and designate the user **Permissions (Read/Write** – as applicable) by Cybowall tab.

Click on the **Enabled** slider to enable/disable the user, and click **Add**:



# Network Tools

The **Network tools** tab consists of two sections:

- **ARP table:** all hosts detected (on the left)
- **System routing table:** displays the list of routes to the monitored networks (on the right)

To sort the sections by category, click on the relevant column heading:

The screenshot shows the CYBOWALL interface with the 'Network tools' tab selected. It displays two tables: the ARP table on the left and the System routing table on the right.

ARP table					System routing table									
Address	HW-type	MAC	Flags	Interface	Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Interface		
192.168.2.130	ether	b8:2a:72:d0:c2:28	C	eth0.2	1.	0.0.0.0	192.168.2.254	0.0.0.0	UG	0	0	0	eth0.2	
192.168.2.91	ether	00:12:e5:04:74:73	C	eth0.2	2.	169.254.0.0	0.0.0.0	255.255.0.0	U	1003	0	0	eth1	
192.168.30.100	ether	00:50:56:b7:72:88	C	eth0.30	3.	169.254.0.0	0.0.0.0	255.255.0.0	U	1101	0	0	eth0.2	
192.168.2.20	ether	00:50:56:b7:c4:c0	C	eth0.2	4.	169.254.0.0	0.0.0.0	255.255.0.0	U	1102	0	0	eth0.22	
192.168.2.150	ether	00:e0:00:00:b9:81	C	eth0.2	5.	169.254.0.0	0.0.0.0	255.255.0.0	U	1103	0	0	eth0.23	
192.168.23.36	ether	1c:1b:0d:08:24:84	C	eth0.23	6.	169.254.0.0	0.0.0.0	255.255.0.0	U	1104	0	0	eth0.30	
172.18.0.10	ether	02:42:ac:12:00:0a	C	br-1c73f85bd615	7.	172.17.0.0	0.0.0.0	255.255.0.0	U	0	0	0	docker0	
192.168.2.170	ether	d4:ae:52:c5:b6:b5	C	eth0.2	8.	172.18.0.0	0.0.0.0	255.255.0.0	U	0	0	0	br-1c73f85bd615	
192.168.30.254	ether	b8:af:67:b1:e8:6f	C	eth0.30	9.	192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0.2	
192.168.23.32	ether	1c:1b:0d:e6:4a:93	C	eth0.23	10.	192.168.22.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0.22	

# Licensing

The **Licensing** tab provides information regarding the Cybowall license and is used to add a license key to Cybowall:

License information	Update
Install date	28-05-2018
End date	27-07-2018
License type	Renewal
Key	A3FTJ-81ACA-QACIV-K3NIJ-Q74H5-QQVHE-ULUEL
Serial number	502630
Model	8118

To add a new license key, click the orange **Update** button to the right of the **License Information** section heading. The **Update product license** window opens.

Enter the license key received following registration on the CYBONET website in the **New license key** field and click **Update**:

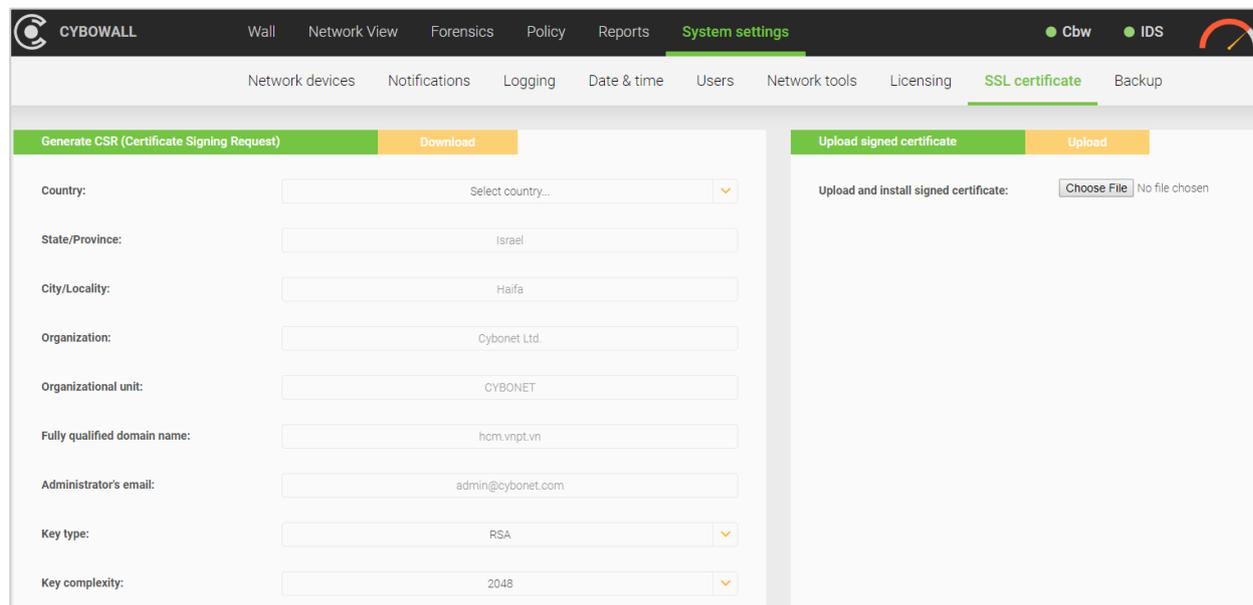
**Update product license** ✕

New license key

**Update**

# SSL Certificate

The **SSL certificate** tab enables a certificate file to be prepared and downloaded:



The screenshot shows the 'System settings' page in the Cybonet interface, specifically the 'SSL certificate' tab. The page is divided into two main sections: 'Generate CSR (Certificate Signing Request)' and 'Upload signed certificate'.

**Generate CSR (Certificate Signing Request) section:**

- Country:** Select country... (dropdown menu)
- State/Province:** Israel
- City/Locality:** Haifa
- Organization:** Cybonet Ltd.
- Organizational unit:** CYBONET
- Fully qualified domain name:** hcm.vnpt.vn
- Administrator's email:** admin@cybonet.com
- Key type:** RSA (dropdown menu)
- Key complexity:** 2048 (dropdown menu)

**Upload signed certificate section:**

- Upload and install signed certificate:** Choose File No file chosen

The **Generate CSR (Certificate Signing Request)** section is comprised of the following fields:

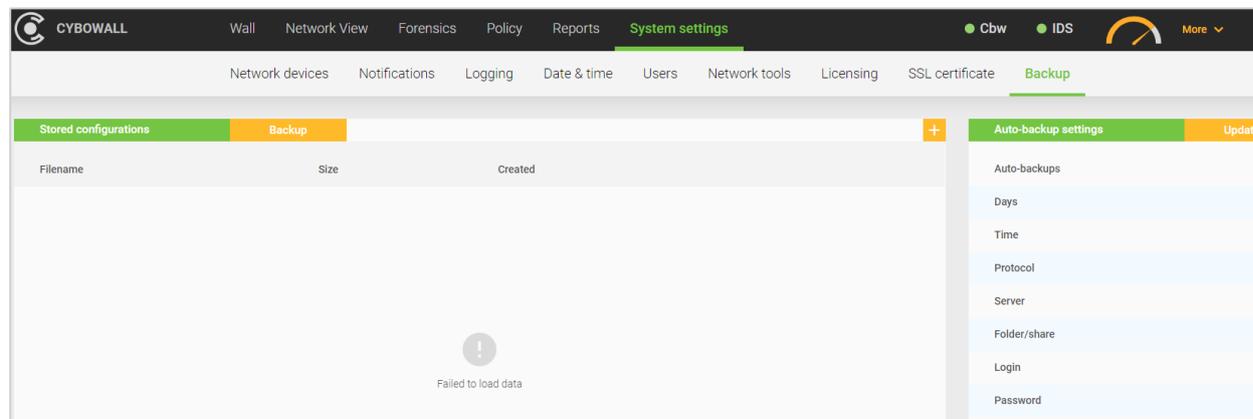
- **Country**
- **State/Province**
- **City/Locality**
- **Organization**
- **Organizational unit**
- **Fully qualified domain name**
- **Administrator's email**
- **Key type:** RSA/DSA
- **Key complexity:** 2048/4096

Once signed in the organization's Certificate Authority, the certificate can be uploaded back into Cybonet in the **Upload signed certificate** section to the right.

Click on **Choose File**, browse for the certificate file and click **Open**.

# Backup

The **Backup** tab allows the Cybowall configuration information to be backed up and restored:



To configure the backup, click the orange **Update** button in the in the **Auto-backup settings** section and complete the following fields:

- **Days:** which day(s) of the week to perform backups
- **Time:** the hour of the day to perform backups
- **Protocol:** FTP or SAMBA
- **Server:** the Hostname or IP address of the server where the backup should be saved
- **Folder:** the folder on the server where the backup should be saved
- **Login:** the username of a login account to the backup server
- **Password:** the password of the login account
- **Auto-backups:** activate/deactivate automatic backups

Click **Update**.

After backups have been configured, the current configuration can be backed up at any time. Click the orange **Backup** button to the right of the **Stored configurations** section heading to start a manual backup.



# Revision History

Date	Description	Section



## About CYBONET

CYBONET, formerly PineApp, was originally established as an email security solutions company. Since 2002, CYBONET has been providing easy to deploy, flexible and scalable security solutions that empower organizations of all sizes to actively safeguard their networks in the face of today's evolving threats. CYBONET's product suite includes our new Cybwall solution for network visibility, vulnerability management and breach detection, our flagship PineApp Mail Secure for comprehensive email security, and our carrier-grade Outbound Spam Guard (OSG). With a continued emphasis on developing and delivering high quality solutions, and in conjunction with our valued partner community, CYBONET is dedicated to security. For further details, please contact [info@cybonet.com](mailto:info@cybonet.com) [www.cybonet.com](http://www.cybonet.com)

