# Table of contents

1 **Summary** .................................................................................................................. 5  

2 **System requirements** .................................................................................................. 6  
   2.1 Port communication requirements ............................................................................. 7  
      2.1.1 Management server ............................................................................................. 7  
      2.1.2 Hyper-V hosts – Acronis Cloud Security managed .................................................. 8  
      2.1.3 Consoles – Acronis management console, System Center Virtual Machine Manager (SCVMM) plugin, and Azure pack portal ................................................................. 9  
   2.2 Service accounts – permissions .................................................................................. 9  
      2.2.1 Management service account ............................................................................... 9  
      2.2.2 Host service account ............................................................................................ 9  

3 **Installation** .................................................................................................................. 10  
   3.1 Setup launcher application ......................................................................................... 10  
   3.2 Management service ................................................................................................ 11  
      3.2.1 Standalone installation ....................................................................................... 11  
      3.2.2 Configuring for high availability ........................................................................... 20  
   3.3 Host management service ........................................................................................ 21  
      3.3.1 Local .................................................................................................................... 23  
      3.3.2 Remote ................................................................................................................ 28  
   3.4 Management console ................................................................................................ 37  
   3.5 Acronis Cloud Security network manager plugin ..................................................... 42  
   3.6 Acronis AzSec installation ......................................................................................... 45  
   3.7 Silent installation from MSI packages ....................................................................... 48  

4 **Acronis Cloud Security operations** ............................................................................. 48  
   4.1 Adding and removing hosts ....................................................................................... 49  
   4.2 Global administrator and tenants .............................................................................. 51  
      4.2.1 Users management ............................................................................................... 52  
      4.2.2 Configuring tenants ............................................................................................. 55  
      4.2.3 User activity auditing ......................................................................................... 61  
      4.2.4 Collecting usage statistics ................................................................................... 62  
   4.3 Internal events auditing ............................................................................................. 63  
   4.4 Configuring virtual firewall rules .............................................................................. 64  
      4.4.1 User defined security groups ............................................................................... 65  
      4.4.2 User defined rules templates .............................................................................. 67  
      4.4.3 Adding rules ......................................................................................................... 68  
      4.4.4 Editing a rule ....................................................................................................... 85  

Copyright © Acronis International GmbH, 2003-2020
4.16 Syslog server integration ................................................................. 162
4.17 Disaster recovery ........................................................................... 164
  4.17.1 Disaster recovery functionality .................................................. 165
  4.17.2 Configuring disaster recovery ................................................... 165
4.18 Distributed management ................................................................. 167
4.19 Configuring VM settings ................................................................. 171
4.20 Host settings and state ................................................................. 176
4.21 Refreshing the object tree ............................................................... 178
5 Acronis Cloud Security information .................................................. 178
6 Licensing ......................................................................................... 180
  6.1 Core-based licensing overview ......................................................... 180
7 FIPS support ..................................................................................... 181
8 Compatibility with other Acronis products .......................................... 181
9 Acronis Cloud Security log files ......................................................... 182
10 Configuring Acronis Cloud Security network manager plugin .......... 183
11 Uninstall ......................................................................................... 184
12 Appendix – Firewall log reason entry descriptions .......................... 185
  12.1 Action allow reasons ................................................................. 185
  12.2 Action block reasons ................................................................. 185
Index ................................................................................................. 187
1 Summary

Acronis Cloud Security is a unified security and compliance solution designed to specifically address every Hyper-V vulnerability across every virtual resource. With Acronis Cloud Security’s patent-pending technologies, you can automatically and immediately protect every VM. Now Hyper-V users of all sizes can have the industry’s leading security and compliance solution without needing to become a security specialist. With an agentless design and the fastest scans in the industry, Acronis Cloud Security protects your data center virtual infrastructure while reducing resource utilization. There are five basic parts of the solution that protect all of Hyper-V. The virtual firewall, antivirus, intrusion detection system (IDS), network anomalies detection and network traffic scanner. Acronis Cloud Security supports new cutting-edge technologies such as NVGRE and IP rewrite and secures point filtering of virtual machines traffic with its virtual firewall feature. The antivirus component of Acronis Cloud Security solution provides unique, agentless protection of virtual machines that can be arranged either in groups or individually on each separate virtual machine. The active protection feature that protects virtual machine operating system in real time is also available, including anti-ransomware feature\(^1\). Intrusion detection system (IDS) feature allows detection of active attacks, review of the event log and setting the blocking virtual firewall rule on the suspicious IP address. Network traffic scanner allows monitoring of inbound web – http traffic in real time to detect malware that might be downloaded to the virtual machine. Email notifications feature is available to inform administrator about IDS, Antivirus and network traffic scanner events. Acronis Cloud Security also supports multi-user and multi-tenancy that allow delegation of privileges on virtual machines security control so that each owner is able to control security policies in their virtual environment.

\(^1\)Available in the product version with Bit Defender antivirus engine.
2 System requirements

Supported operating systems:

- Management server:
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2016
  - Microsoft Windows 10 x64
  - Microsoft Windows 8.1 x64
  - Microsoft Windows Server 2012 R2

- Hyper-V host:
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2016
  - Microsoft Windows 10 Enterprise with the Hyper-V role enabled
  - Microsoft Windows 10 Professional with the Hyper-V role enabled
  - Microsoft Windows 10 Education with the Hyper-V role enabled
  - Microsoft Windows 8.1 Professional with the Hyper-V role enabled
  - Microsoft Windows Server 2012 R2

- Guest VM:
  - Any Hyper-V supported guest OS

Software prerequisites:

- .NET framework 4.5.2 or higher
- MS SQL Server
- MS PowerShell
- Hyper-V module for PowerShell should be installed. It can be installed from GUI with Add roles and features wizard (can be launched from Server manager). The component path is as follows:


  It can also be installed with following PS command:

  ```powershell
  Install-WindowsFeature -Name Hyper-V-PowerShell
  ```

- Visual C++ redistributable for Visual Studio 2017 should be installed on management server, depending on the antivirus engine version:
  - x64 for Bitdefender antivirus engine (find it at this link: https://aka.ms/vs/15/release/vc_redist.x64.exe).

---

1 The Hyper-V host OS minimal requirements apply if management service is set onto managed Hyper-V host!
- x86 for ThreatTrack antivirus engine (find it at this link: https://aka.ms/vs/15/release/vc_redist.x86.exe).

**Warning!**
Snort application uses MS-DOS SFN (short file names or 8.3) naming convention (read more at https://msdn.microsoft.com/en-us/library/aa365247.aspx#short_vs_long_names). This convention is enabled in the latest versions of MS Windows OS by default. If it is disabled, snort application and, accordingly, IDS feature will not work.

### 2.1 Port communication requirements

The following diagram outlines the Acronis Cloud Security component communication requirements.

![Diagram of Acronis Cloud Security component communication requirements](image)

#### 2.1.1 Management server

Inbound from Hyper-V hosts – Acronis Cloud Security managed:
- TCP 8534 – Antivirus (AV) management endpoint.
- TCP 8790 – Host management endpoint.
- TCP port 8183 – For signature updates of Snort intrusion detection system (IDS) and Bit Defender antivirus if the version with Bit Defender antivirus engine is installed.
Inbound from consoles – Acronis Management console, System Center Virtual Machine Manager (SCVMM) plugin, and Azure Pack portal:

- TCP 8789 – Client.

Outbound to SQL Server database:

- TCP 1433 (default) or other port defined in SQL configuration.

Outbound to Internet:

- TCP 80 – Snort IDS / AV update over HTTP.

Outbound to DHCP server (if applicable):

- UDP 68.

Outbound to DNS server:

- UDP 53.

Outbound to Syslog/Splunk server (if applicable):

- UDP 514.

Outbound to additional Acronis Cloud Security management services (if applicable):

- TCP 8790.

Outbound to Hyper-V hosts:

- TCP 8788, 8533.

Outbound to AV update servers (if applicable):

- TCP 80.

2.1.2 Hyper-V hosts – Acronis Cloud Security managed

5nine.VirtualFirewall.HostManagementService should be installed on each monitored and protected Hyper-V host.

Inbound from Acronis management server:

- TCP ports 8533 – AV management.
- TCP 8788 – Host management.

Outbound to Acronis management server:

- TCP 8534 – Antivirus (AV) management endpoint.
- TCP 8790 – Host management endpoint.
- TCP port 8183 – For signature updates of Snort intrusion detection system (IDS) and Bit Defender antivirus if the version with Bit Defender antivirus engine is installed.

Outbound to Internet:

- TCP 80 – ThreatTrack AV update over HTTP.
2.1.3 Consoles – Acronis management console, System Center Virtual Machine Manager (SCVMM) plugin, and Azure pack portal

Outbound to management server:
- TCP 8789 – Client.

2.2 Service accounts – permissions

2.2.1 Management service account
- WMI access (https://technet.microsoft.com/en-us/library/cc771551(v=ws.11).aspx). Full access to the namespace Hyper-V WMI provider (V2) (ROOT\virtualization\v2) is required.
- SQL database or file access (read/write) – for management service user account only if Windows authentication is used.
- Allow to control Hyper-V (http://blogs.msdn.com/b/virtual_pc_guy/archive/2008/01/17/allowing-non-administrators-to-control-hyper-v.aspx). In most cases this requirement is covered since local administrator’s privileges requirement is already met.

2.2.2 Host service account

Best practice – use the same account for service for the host service account and in the Server settings in the Acronis Cloud Security management console.
- Host service user should have local administrator’s privileges. This requirement is usually met when the user is a member of local administrators group on the Hyper-V host or the Administrators group in the active directory in the case of domain environment.
- If the host is managed remotely from the centralized management console, there should also be an account with similar permissions used in server settings.

For workgroup/mixed domains environment:
- The account for workgroup environment should also have similar permissions for current managed host.
- Managed and management servers should be marked as trusted hosts if workgroup environment is used on several domains environment.
3 Installation

There are three separate components in the full set of Acronis Cloud Security that are installed from either a single setup application or through MSI installer packages for unattended installations:

- **Management service.** This component should be installed on the host(s) or designated VM(s) that will be set as Acronis management servers for the entire Windows Server/Hyper-V environment. Refer to the "Management service" (p. 11) subsection below. There can be several management servers for the given Hyper-V environment, which provides disaster recovery function. Refer to the "Disaster recovery" (p. 164) section below.
- **Host management service.** This component should be installed on each secured/monitored Hyper-V host. Refer to the "Host management service" (p. 21) subsection below.
- **Management console.** This component should be installed on each host/VM that will be used by administrators to operate and control the system security/compliance rules application. Refer to the "Management console" (p. 37) subsection below.

Additionally, the following components are available in Acronis Cloud Security for Hyper-V setup:

- **SCVMM compliance extension (Acronis Cloud Security network manager plugin).** This component is required in certain cases when Microsoft System Center Virtual Machine Manager is used in the environment and the SCVMM-based logical switches are enabled. SCVMM compliance plugin helps to get SCVMM logical switches to compliant state. The "Acronis Cloud Security network manager plugin" (p. 42) subsection below describes SCVMM compliance extension installation process.
- **Acronis Smart Firewall for Azure.** A separate security product designed for Microsoft Azure. The "Acronis AzSec installation" (p. 45) subsection below describes installation process.
- **Acronis Smart Firewall for Azure Web version.** Web version of Acronis Azure Security product.

### 3.1 Setup launcher application

Before installing Acronis Cloud Security for Hyper-V components, first run the single setup launcher application:
Select the left option **Acronis Cloud Security for Hyper-V** to load the **Acronis Cloud Security for Hyper-V** setup.

### 3.2 Management service

Management service must be installed at least on one server (host or designated VM) prior to setting up all other Acronis Cloud Security components. It supports both standalone and clustered (HA) installation scenarios.

#### 3.2.1 Standalone installation

**Warning!**  
Acronis Cloud Security management service uses the same interface with the antivirus management service of another Acronis product – Acronis Manager Standard with Antivirus. Even if they are used to manage different Hyper-V hosts, they still will run into a conflict and the antivirus feature will not work in the case they are running on the same server. Therefore placing of both management services on the same machine is not supported.

To install management service, in the **Acronis Cloud Security for Hyper-V** setup select **Management service** and click **Install**.
Note
If the usage of Federal information processing standard (FIPS) algorithms is enabled in your system, mark the Enable FIPS compliance mode option check box prior to starting the installation to comply with these algorithms. This option can also be reconfigured after the installation, which will require editing configuration files and restarting of management service. Please, refer to the "FIPS support" (p. 181) chapter for detailed information.
The **Acronis Cloud Security management service setup** wizard will open:

Click **Next** to start pre-configuration process.

Select the destination folder for the management service installation.

You can change the default destination folder.
Select or create the new folder and click **OK**. Then click **Next**.

Click **Add** to install the license (.txt) file. The existing license files with current state will be shown in the list:

![License Management Screen]

Set the user that will run management service:

![Service Logon Account Screen]
As a best practice, it is recommended to select the **User** option and enter either local or domain user credentials depending on the environment in which the management service is being installed. The hosts that are added to management console later, will use the user account, management console or host management service are running under, as default credentials. Please refer to "Adding and removing hosts" (p. 49) section for more information. If you select **Local system**, all the hosts must be added with custom credentials, where the user account is entered. Click **Next**.

Select the database server and the authentication method:

- Select the database server from the list. If the database server that you need to connect to is not detected by the installer, you will have to type it manually. The default port is 1433. If your SQL server uses different port, specify this port using the following format: SQLSERVER, port. Example: If the SQL server hostname is SQLSRV and it uses port 1435 instead of standard 1433. Type the following string into the Database Server field: SQLSRV, 1435
- Select the authentication method:
  - **Windows authentication**. Windows user’s credentials entered at the previous step will be used for authentication;
  - **SQL authentication**. SQL Server specified account (sa) will be used for authentication.
    If Local system had been selected at the previous step as an account to run management service, only SQL authentication is possible. Contact your database administrator (DBA) for assistance, if necessary.
If you are doing a fresh installation of Acronis Cloud Security or there is no previously created security admins that exist in your prior database vFirewall in your selected data source, you will be offered to choose whether or not to create a security global admin:

If you choose the option **Create global administrator**, you will be requested to specify the credentials for the new global admin:

- **Select the user type:**
  - **Custom user.** This option lets you create custom users independently from AD. This type is used only within Acronis Cloud Security to identify Acronis Cloud Security application permissions. If you’re working in a mixed environment you should always select this option. You
can set any name and password for this user type.

- **Windows user.** This option applies to a single domain environment only. The user must be registered in active directory (AD).
- Specify the name and, for custom user, password. Windows user's data will be loaded from the domain active directory.
- Enable the roles for the user:
  - **Security Administrator.** This role grants the full permissions on the Hyper-V implementation for the user. The user assigned to this role will act as a global administrator.
  - **Auditor.** A user with this permission will be able to view Cloud Security log records but cannot apply any changes.

The global admin is a user who has full access over Acronis Cloud Security. If you create global admin, you will be able to connect to cloud security management service only under this user (please refer to the “Global administrator and tenants” (p. 51) section below for details). Remember the credentials you have entered to be able to connect to the management service after the installation.

If you choose the option Do not create admin, the installation will proceed without asking to specify user's credentials. In the case you have kept the old database vFirewall from a previous installation in your selected data source and there was at least one admin registered in it, the installer will detect this, and this step will be skipped automatically.

Click **Next.** Select the folder to store vFirewall logs:

Local folder **C:\CloudSecurityLogs** is offered to set by default. Logs for each VM will be kept inside subfolder with the name in the following format: {VM ID (hex string)}. Click **Next.**
Select internal WebAPI endpoint certificate installation option:

- **Self-signed certificate.** Use this option if you use web API on the local machine only, or do not use it at all. The installer will create self-signed certificate during the setup, no other action is required.
- **Existing certificate.** Use this option for other cases. You need to create the certificate in advance and have it saved somewhere in your environment. You will be asked to select the existing
certificate after choosing this option:

Click Next. Then click **Install** to start the management service installation process.

Click **Install** to begin the installation. Click **Back** to review or change any of your installation settings. Click **Cancel** to exit the wizard.
Wait until the following screen appears and then click **Finish** to complete the management service installation process.

Upon completing the installation of the management service, check that the following services are installed and running on your server: **5nine.VirtualFirewall.ManagementService** (display name: **Acronis Cloud Security Management Service**) and **5nine.Antivirus.UpdateService** (display name: **5nine.Antivirus.UpdateService**).

### 3.2.2 Configuring for high availability

If you are using failover clustering, it is possible to set up Acronis Cloud Security management service for high availability as it supports this standard setup scenario in cluster environments.

In this setup scenario, you will need to install a separate instance of management service onto each server in the failover pair, pointing to the same data source (SQL server). SQL server may also be set for high availability. Installation is done in the same way as described in the previous subsection. From this point you will have to use cluster failover role IP address/FQDN instead of a standalone IP address/FQDN as a management service address when you need to connect to the management service, i.e. when installing Acronis Cloud Security host management service, Acronis Cloud Security for Azure Pack backend service and connecting to the management service from the management console or SCVMM plugin.

When configuring high availability in the failover clustering, you will have to select the **Generic Service** option for Acronis Cloud Security management service and proceed with setup in a standard way.
These are general steps to follow when configuring high availability for Acronis Cloud Security management service:

1. Make sure you have failover pair servers ready and that they meet requirements for Acronis Cloud Security management service installation. Please refer to the ““System requirements” (p. 6)” section above.

2. Install Acronis Cloud Security management service separately onto each server in the failover pair, pointing to the same data source (SQL server). Please refer to the Installation – ““Management service” (p. 11)"–““Standalone installation” (p. 11)” section above. It is recommended to stop 5nine.VirtualFirewall.ManagementService on the first server before proceeding with the installation on the second one.

3. Configure Acronis Cloud Security management service high availability in the standard way using the Generic service option in the failover clustering. Please refer to the following sources for more information about setting up a service for high availability in failover cluster environment and using of the Generic service option:

   **Note**
   Remember that from this moment you will have to use your cluster role IP/FQDN instead of standalone IP/FQDN whenever you connect to Acronis Cloud Security management service.

3.3 Host management service

Before starting host management service setup:

- Confirm that management service is already installed on the host or VM that is selected as a management server in your network.
- Confirm that its service is running (5nine.VirtualFirewall.ManagementService; display name: Acronis Cloud Security Management Service).

To install host management service, in the Acronis Cloud Security for Hyper-V setup select
Host management service:
There are two options available for host management service installation:

- Local installation. With this option host management service will be installed onto the current local server. The ""Local" (p. 23)" section below describes the local installation process.
- Remote installation. With this option host management service will be installed onto any host accessible on the network. The ""Remote" (p. 28)" subsection below describes the remote installation process.
3.3.1 Local

To start host management service installation onto the local host click **Install** in the **Acronis Cloud Security setup** dialog of the single setup application. The **Acronis Cloud Security host management service setup** wizard will open:

![Image of Acronis Cloud Security Host Management Service Setup]

Select the destination folder for the host management service installation. Click **Next** to start the pre-configuration process.
To change the default destination folder, select or create the new folder and click **OK**. Then click **Next**.

Set the user that will run under host management service. Click **Next**.
Note
These credentials are entered for the local host on which the host management service is being installed and may differ from those entered for the remote management server if the program is used in mixed environments.

Specify CBT data storing options and the account for CBT service:

- **Default (auto)**: CBT data will be stored in the program-defined default location (`C:\Program Files\5nine\5nine CBT`);
- **Inplace**: CBT data will be stored together with virtual machine VHD;
- **Dedicated**: CBT data will be stored in the location, specified by user (**Storage path**). The location should be available from the Hyper-V server’s side.

Set the user account for CBT service – **System** or **Windows user**. In the second case, specify credentials.
Specify the management server by entering its fully qualified domain name (FQDN) or IP address. If you set Acronis Cloud Security management service as a highly available clustered service, use cluster role FQDN/IP (please refer to the Installation – “Management service” (p. 11) – “Configuring for high availability” (p. 20) section above). Click **Next**.

Specify if the Snort application should be installed with host management service:

- **Install SNORT**
Snort application is used for IDS feature (please refer to the “IDS” (p. 146) section below) and is included into the single setup application for convenience. You may install it manually at a later time. The original components can be found at www.snort.org.

Click Install to start the host management service installation process.
Wait until the following screen appears and then click **Finish** to complete the host management service installation process.

Server reboot is required to complete the host management service setup. Confirm the system prompt to perform the server reboot immediately or decline to do it at a later time.

### 3.3.2 Remote

With this option you can install host management service onto the multiple hosts simultaneously over the network. To start host management service remote installation click **Remote install** in the **Acronis Cloud Security setup** dialog of the single setup application. The remote installation wizard will open:
Specify the management server by entering its FQDN or IP address into management server path field. If you set Acronis Cloud Security management service as a highly available clustered service, use cluster role FQDN/IP (please refer to the Installation - "Management service" (p. 11) – "Configuring for high availability" (p. 20) section above).

Ensure the management server is accessible by clicking **Test connection**. The corresponding message should appear in the case of successful test. If the connection test is ok, click **Next**.
Add the remote hosts:

Click **Add** to select the host(s) to the list for remote setup of host management service:

Enter the server(s) by typing their FQDN or IP addresses separated by commas. Then select the authentication method (contact your system administrator for the assistance if necessary):

- **Use default credentials.** The current user’s credentials will be used. Use this option if the single domain is used in the environment and the current user granted all necessary rights on the remote server(s), but you will have to separately specify service logon account for each host;
- **Use custom credentials.** Specify the credentials for remote host. Use this option if different credentials should be used on remote host. In the case multiple hosts are added, you will likely need to alter these credentials for each host as applicable in the case you're working in mixed environment and/or different credentials are used on the servers.
Click **Select** to search for the hosts on the network. The **Select Hyper-V servers** dialog will be opened:

![Select Hyper-V servers dialog]

You may also add servers to the list one by one by pressing the **Add** button and enter server name manually in the dialog window above or let Acronis Cloud Security search and add them automatically by pressing the **AD discovery** button, or search them by IP range/subnet mask which can be set in the window below called out by pressing the **IP discovery** button:

![Add Hyper-V Server dialog]

![IP Discovery settings]

31  

Copyright © Acronis International GmbH, 2003-2020
At the end click **OK**. You will see selected hosts appear on the list:

![Remote installation wizard]

Make sure service logon account is properly set. Otherwise Acronis Cloud Security will not allow you to go further.

Right click each host to edit the installation and/or service logon accounts:

- Click **Edit install credentials** to specify/alter the credentials for the host management service installation onto the target host:

  ![Edit install credentials]

- Click **Edit service credentials** to specify/alter the credentials under which **5nine.VirtualFirewall.HostManagementService** (display name **Acronis Cloud Security Host Service**) will be running on the target host:

  ![Edit service credentials]
Then specify/alter the credentials in the dialog that will open:

Check the credentials for all added hosts:

Check **Allow auto-reboot** to let the target host be rebooted automatically after installation. Leave it unchecked to reboot the host manually at a later time. Acronis Cloud Security detects if the virtual firewall driver is already installed on the host and it is up to date (e.g. when the host service reinstallation or upgrade is currently being done). If it is a fresh installation or the driver reset is needed, then either automatic or a manual reboot is necessary. If you are not absolutely sure and able to reboot, it is recommended to check **Allow auto-reboot** to let Acronis Cloud Security automate the reboot process. Click **Next**.
Specify CBT data storing options and the account for CBT service:

- **Default (auto)**: CBT data will be stored in the program-defined default location (C:\Program Files\5nine\5nine CBT);
- **Inplace**: CBT data will be stored together with virtual machine VHD;
- **Dedicated**: CBT data will be stored in the location, specified by user (**Storage path**). The location should be available from the Hyper-V server's side.

Set the user account for CBT service – **System** or **Windows user**. In the second case, specify credentials.
Review the remote setup summary and then click **Finish** to confirm the operation:

The Installation on remote servers dialog will open:

- Right click each server and then click **Start** to evoke the remote installation on each server separately;
- Click **Start all** to evoke the remote installation on all servers simultaneously.
You can interrupt the installation process while it's going:

- Right-click each server and then click **Stop** to interrupt the remote installation on each server separately;
- Click **Stop** in the lower part of the dialog to interrupt the remote installation on all servers simultaneously.

**Note**

It is not generally preferable to interrupt the installation process to avoid possible further application maintenance on the target host(s). Do not use these options without absolute necessity. Prepare and plan the installation well.

At the end of the remote installation process the results will be displayed for each of the remote hosts:

- **Complete.** Remote installation completed successfully.
- **Failed.** Remote installation failed. Additional information for the error that occurred during remote setup will be shown in the **Description** column.

Click **Close**.
Upon completing the installation of host management service, check that the following services are installed and running on the target host(s):

- **5nine.VirtualFirewall.HostManagementService** (display name: *Acronis Cloud Security Host Service*);
- **5nine.Antivirus.Agent** (display name: **5nine.Antivirus.Agent**);
- **59CBTService** (display name: **59CBTService**).

### 3.4 Management console

Before starting the management console setup, make sure management service is already installed on the host or VM that is selected as a management server in your network. It is also preferable to set up host management service prior to management console installation. To install management console, in the *Acronis Cloud Security for Hyper-V* setup select **Management console** and click **Install**.

**Note**

If the usage of Federal information processing standard (FIPS) algorithms is enabled in your system, mark the **Enable FIPS compliance mode** option check box prior to starting the installation to comply with these algorithms. This option can also be reconfigured after the installation, which will require editing configuration files and restarting of management console. Please, refer to the "FIPS support" (p. 181) chapter for detailed information.
Select **Management console** and click **Install**. The **Acronis Cloud Security management console setup** wizard will open. Click **Next:**

![Acronis Cloud Security Management Console Setup](image)

**Welcome to the Acronis Cloud Security Management Console Setup Wizard**

The Setup Wizard will install Acronis Cloud Security Management Console on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

![Next button](image)

Read and accept the EULA (license agreement). Click **Next**.

![Acronis Cloud Security Management Console Setup](image)

**End-User License Agreement**

Please read the following license agreement carefully

![End-User License Agreement](image)

**DATE OF LAST UPDATE: 20 February 2020**

**ACRONIS SOFTWARE LICENSE AGREEMENT**

THIS SOFTWARE LICENSE AGREEMENT (“AGREEMENT” OR “EULA”) GOVERNS THE USE OF THE ACRONIS SOFTWARE (“SOFTWARE”). ACRONIS INTERNATIONAL GMBH (“ACRONIS” OR “LICENSOR”) IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR LEGAL ENTITY (“LICENSEE” OR “YOU”), AND IF APPLICABLE TO YOUR SOFTWARE LICENSE, TO PROVIDE YOU WITH SUPPORT AND MAINTENANCE SERVICES (“SERVICES”), PROVIDED, AND ONLY ON

![I accept the terms in the License Agreement](image)
Select the destination folder and startup options, and then click **Next**.

To change the default destination folder, select or create the new folder and click **OK**.
Specify the management server by entering its FQDN or IP address and user credentials to connect to the management service. If you set Acronis Cloud Security management service as a highly available clustered service, use cluster role FQDN/IP (please refer to the Installation – "Management service" (p. 11) – "Configuring for high availability" (p. 20) section above).

Select one of the following options:

- **Use default credentials** – the current user credentials will be set as default choice to login to management console at startup.
- **Use Windows user credentials** - the specified AD user credentials will be set as default choice to login to management console at startup.
- **Use custom user credentials** – the specified custom user credentials will be set as default choice to login to management console at startup.

**Note**
To install the management console on the server where multiple users with different privileges work, the best practice is to select the option **Use default credentials** so that each time the management console is started the necessary privileges are granted on it. The same applies to tenants’ setup, the user that is currently running the management console instance must match the user, set to connect to the management service in order to get the right privileges. Refer to the "Global administrator and tenants" (p. 51) section.

Click **Next**.
Then click **Install** to start the management console installation process.

![Installation screen](image)

Wait until the following screen appears, and then click **Finish** to complete the management console installation process:

![Completion screen](image)
3.5 Acronis Cloud Security network manager plugin

Acronis Cloud Security network manager plugin should be installed onto SCVMM server when all other Acronis Cloud Security components are set up in the environment managed by SCVMM. SCVMM compliance extension is installed from the Acronis Cloud Security for Hyper-V setup:

Select SC VMM compliance extension and click Install. The Acronis Cloud Security network manager plugin setup wizard will open. Click Next.
Select the destination folder or leave the default path and click Next.

Click Install to start the Acronis Cloud Security network manager plugin installation process.
Wait until the following screen appears, and then click Finish to complete the Acronis Cloud Security network manager plugin installation process.

The installation process is complete, but further steps are required to finalize Acronis Cloud Security network manager plugin configuration and setting up corresponding SCVMM items.
configuration. Refer to the "Configuring Acronis Cloud Security network manager plugin" (p. 183) section below for details.

### 3.6 Acronis AzSec installation

To install Acronis AzSec add-on, complete the Acronis Cloud Security installation first. Please note, you will need a valid license to run Acronis AzSec. To install Acronis AzSec open the setup launcher application, highlight **Acronis Smart Firewall for Azure** and click the **Install** button:
1. Welcome screen:

2. Destination folder – Click **Next** and specify the destination folder for the AzSec application:

3. License file – Then click **Next**, and when prompted specify the location of the AzSec license file that you have received from Acronis via e-mail. If you are installing AzSec as a part of Acronis Cloud Security, you will need to input licenses for both Cloud Security and AzSec add-on.
4. After license is entered, proceed with the installation. You can select to launch AzSec after installation, or launch it thereafter from the status bar or application list.
3.7 Silent installation from MSI packages

It is also possible to install Acronis Cloud Security components silently from the command line. Once a user opens the setup launcher application, the MSI package files can be found in `c:\Users\[USER]\AppData\Local\Temp\5nine\` directory. The MSI can then be copied to another location for future use or used while the launcher application remains open. Once the launcher application is closed the directory and contents will be deleted.

Example - host management service setup:

```powershell
msiexec /i HostManagementServiceSetup.msi /qn /norestart /l* info.log MANAGEMENT_SERVER=[Cloud Security FQDN name] WINLOGIN=[DOMAIN\Administrator] WINPASS=[Password]
```

4 Acronis Cloud Security operations

To configure Acronis Cloud Security, first open its management console using the shortcut to the following application: `C:\Program Files\Acronis\Acronis Security For Hyper-V Management Console\5nine.VirtualFirewall.ManagementConsole.exe`. This shortcut will be available on your desktop by default.

Management console works independently of the place where it is installed. After starting it, you will be advised to specify the management server, which management console will connect to during the current session, tenant (or leave the field empty to connect to the global group) and the user to work under:

- Enter the path to the management server by entering its FQDN or IP address. If you set Acronis Cloud Security management service as a highly available clustered service, use cluster role FQDN/IP (please refer to the "Installation" (p. 10) – "Management service" (p. 11) – "Configuring for high availability" (p. 20) section above).
- Select the user type:
  - **Current user.** The account you are currently logged in under will be used to connect to the management server. Select this option when there are no users has been added yet or if
you’re working in a single domain environment and the current account has the necessary permissions as a global user.

- **Windows user.** The domain account registered in AD will be used to connect to the management server. This option can be selected in the case you are working in the non-mixed environment and available for the members of the global group only.

- **Custom user.** The previously created custom user will be used to connect to the management server. If you are working in the mixed environment you should always select this option once the users and permissions are set. Please refer to the “Users management” (p. 52) of the “Global administrator and tenants” (p. 51) subsection below for the detailed information.

- Enter the tenant name to connect to a tenant or leave the field empty to connect to the global group.

- For the custom user and windows user types enter the name and password in the appropriate fields.

- If you would like the current login information to be saved for the next sessions as a default option so that you don’t have to enter it all over again each time you start management console, check the **Save as default** box.

The **Quick search** field in the left-lower part of the main window will help you to find the necessary VM fast. Just enter the key symbols in it and the VM list will be filtered accordingly.

### 4.1 Adding and removing hosts

To add host(s) for monitoring, select **Hosts** – **Add host** main menu command.
Type the host(s) name in the dialog box below or select them from the list (a separate window titled Select Hyper-V servers will open). Then set the credentials in the dialog box. Contact your network administrator to get the credentials.

To change server credentials in the Server properties dialog box, refer to the "Host settings and state" (p. 176) section below.

Click Select to choose the host.

Add servers to the list by clicking Add and entering the server name manually in the dialog box below.
You can let Acronis Cloud Security search and add servers automatically by clicking **AD discovery**. You can also search for them by IP range/subnet mask; click **IP Discovery** to open the window below.

![Add Hyper-V Server](image)

To remove the host from monitoring, select it in the tree and click **Hosts – Remove host**.

### 4.2 Global administrator and tenants

The **User management** feature is designed to set permissions on Acronis Cloud Security objects (virtual machines) and operations performed through the management console. It is crucial to set them appropriately. These permissions are unrelated to users’ permissions that are set in Windows or active directory (AD); they apply users’ rights solely for Acronis Cloud Security objects and operations. The most important users that have to be created (added) in the user management are **global users**, particularly **global administrator**. This user will be able to see all the virtual machines that are managed by Acronis Cloud Security and to perform all the operations through the management console: set global rules, create/delete tenants described below, operate the antivirus feature and set permissions for other users. Before the global administrator is created, there are no permissions set and any user operating management console is considered as global administrator. Once it is set, no other user will be able to do anything until the global administrator grants necessary permissions. It is also possible to add several global administrators; their permissions will be equal. Tenants are the logical groupings of virtual machines, each with its own user management function. It allows setting permissions for non-global users to view and manage.
only designated groups of virtual machines within a single tenant whereas global users view the whole Hyper-V implementation and all tenants.

4.2.1 Users management

Users management is found in the following drop down menu: **Settings - Users management:**

![Users management menu](image1)

All users are managed in the **Users management** dialog box:

![Users management dialog](image2)
To add a user, click **Add**, and then enter the user parameters in the following dialog box:

- Select tenant. The list content depends on how many tenants had been previously created. **Global group** represents global user group membership and it's always present in the list.
- Select the user type:
  - **Custom user**. This option lets you create custom users independently from AD. This type is used only within Acronis Cloud Security to identify permissions. If you're working in a mixed environment you should always select this option. You can set any name and password for this user type. For tenant users this is the only available option.
  - **Windows user**. This option applies to a single domain environment only and available only for global group membership. The user must exist in AD.
- Enter the user name in the **Name** field:
  - For the **Custom user** type enter any name at your wish. E.g., **Admin**. This name will in no way interfere with any of Windows (and/or AD) user names even in the case they are similar; it is solely up to you which one to enter here.
  - For the **Windows user** type enter the domain user name registered in the active directory. You can enter the user name in DOMAIN\User format or just name without specifying the domain - the proper domain will then be added automatically.
- Set the password for the **Custom user** type in the **Password** field and retype it again in the **Confirmation** field.
Note
You can set requirement for stronger passwords. Click **Settings** in the **Users management** dialog box and enable the **Require strong password** option, then click **OK**:

Stricter requirements will apply for the passwords at this point: at least 8 characters length, it must contain one or more uppercase characters, one or more lowercase characters, on or more numeric values and one or more special characters.

- Enable the roles for the user:
  - **Security administrator.** This role grants the full permissions on the Hyper-V implementation for the user. The user assigned to this role will act as a global administrator or a tenant administrator, depending on which group it is assigned to.
  - **Auditor.** A user with this permission will be able to view Cloud Security log records but cannot apply any changes.
- Click **OK** to complete the operation. The newly added user will display in the **Users management** dialog box.

To edit the user, select it in the **Users management** dialog box and click **Edit**:

For custom users you may change password and alter roles. For Windows users you may only alter roles. Click **OK** when operation is complete.

To remove the user, select it in the **Users management** dialog box, click **Remove** and confirm the operation.
4.2.2 Configuring tenants

To configure tenants, navigate to the Tenants entity in the Acronis Cloud Security object tree and use the appropriate context menu items.

Adding tenant

To add the new tenant, right-click Tenants – Add tenant.

Enter parameters for the new tenant in the New tenant dialog box on the Common tab:

- Enter the name for the new tenant in the Name field;
- Click Add and select the virtual machines that are assigned for the new tenant in the Select VMs dialog box, and then click OK:
Type the symbols which a VM name must contain into the Filter field to filter the tree. Those VMs that have been pre-selected will not be filtered off the tree even if they do not match the filtering criteria. Click OK.

- To remove any virtual machine, either deselected it in the Select VMs dialog box or select it in the New tenant dialog box and then click Remove. The effect will be the same.
- Click OK in the New tenant dialog box to apply the changes.

Check and alter tenant permissions as necessary on the Tenant permissions tab:
Here you can determine features that are allowed to be controlled by tenants.

- **Default permissions.** This option is set by default and implies default settings. These settings can be changed on the upper level. Right-click on **Tenants – Edit tenants permissions:**

  ![Tenants Default Permissions]

  Mark permissions that are needed to be allowed for tenants by default. Click OK.

- **Specify manually.** This option allows you to set permissions for the particular tenant. At the end click **OK** in the **New tenant** dialog to apply changes.
Editing tenant

To edit tenant, select the tenant name in the object tree, then right-click it and select from the following options:

- **Edit users and permissions**. Use this menu item to change users and permissions for the selected tenant in the **Users management** window:

  ![Users Management Window]

  It is done in the same way as described in the "Users management" (p. 52) paragraph above.

- **Remove**. Use this menu item to remove the selected tenant. The operation requires confirmation.
Another way to edit tenant membership is to do it directly on the **Virtual machines** tab:
To edit tenant membership, select the target tenant in the object tree on the left, and then click the **Edit members** button on the **Virtual machines** tab. In the **Edit members list** window select the necessary virtual machines to assign them to the tenant or deselect them to remove from it:

Type the characters which a VM name must contain into the **Filter** field to filter the tree. Those VMs that have been pre-selected will not be filtered off the tree even if they do not match the filtering criteria. Click **OK**.

On the **Users** tab you can edit tenant's users:

Here you are able to add, edit or remove users for the selected tenant. It is done in the same way as described in the "Users management" (p. 52) paragraph above.
E.g., editing user is done via the **Edit user** dialog box:

4.2.3 User activity auditing

Acronis Cloud Security audits all user activity. All events are recorded for activities performed in the Acronis Cloud Security management console into the database. The recorded actions are displayed in the **Logged user actions** window that viewed from the **View – User actions log** menu:
No user is able to alter these records in any way. The only action that is available here is filtering the list by the date on which the actions were recorded to get the desired view. To filter the user actions list by date, set the needed date (range from/to) and click the **Update** button.

### 4.2.4 Collecting usage statistics

Cloud Security features usage statistics by tenants is collected on per-month basis and can be exported to a non-editable .dat file to be sent out to Acronis International GmbH. To collect, review and export usage statistics, click the **Help – Collect usage statistics** main menu item:
In the **Usage statistic** window, select the required year and month and click the **Show** button to display data. Information available in statistics: VM name, tenant, user, feature, start and end time the feature has been enabled on VM. Lower row displays the totals per each feature.

Click the **Export** button to save data into the non-editable .dat file and choose the path on your server.

### 4.3 Internal events auditing

Internal audit events are captured for any changes that are sent to a backup management servers and managed Hyper-V hosts. On the backup management servers it writes changes that are sent to the primary management server. To see internal events, select the **View – Internal events audit** menu item:

Click the **Update** button to retrieve the log records matching the filter criteria.

The following filter settings are available:
Dates range for the report – From/To.
Object type – Any, Host, Disaster recovery, Services state, Authentication, Update service, Virtual machine, Common.
Result – Any, Success, Failed.
Operation – depends on the selected object.
Click the Settings button to set the events categories that should be saved into the log and log records retention parameters:

Select categories of internal events that should be saved into log.
Set the number of retention days and maximal events count.
Click Apply to save settings.

4.4 Configuring virtual firewall rules

There are three basic types of virtual firewall rules in Acronis Cloud Security:

- Global rules of default All VMs group. These rules automatically apply to all virtual machines in the Hyper-V implementation.
- Rules of user defined security groups. These rules apply only to those virtual machines to which the group is assigned in the virtual machine settings. Each virtual machine can be a member of several security groups. In addition to virtual machines, firewall rules can also be defined for Hyper-V hosts’ network adapters that are connected to the virtual switch. Please refer to the "Configuring VM settings" (p. 171) section for more information. The "User defined security groups" (p. 65) section below describes how to set up user defined security groups.
- Local rules. These rules apply only to a particular virtual machine or host adapter in which list they were created.

All rules take effect when the virtual firewall protection is enabled. Please refer to the "Configuring virtual firewall" (p. 104) section.

All the rules are created in a similar manner using Acronis Cloud Security features. The type of rule described above is determined depending on what object was selected in the Acronis Cloud Security
object tree prior to creating the new rule. All this is described in the "Adding rules" (p. 68) subsection below.

**Important**

Acronis Cloud Security uses the following approach to prioritize virtual firewall rules:

- All traffic is blocked by default if no rule is added to the protected virtual machine.
- Any allowing rule opens the channel(s) it is set for and lets the corresponding traffic flow.
- Any blocking rule has priority over any allow rule in the case they refer to the same resource(s) and the traffic that matches rule's criteria will be blocked.

### 4.4.1 User defined security groups

Acronis Cloud Security allows creation of multiple security groups in addition to default built-in **All VMs** group. The **All VMs** default group rules apply to all virtual machines with enabled virtual firewall. Rules in other security groups apply to member virtual machines only. Each virtual machine can be a member of several security groups. Setting up security group membership can be done either in the virtual machine settings (Please refer to the "Configuring VM settings" (p. 171) section for more information) or directly on the **Virtual machines** tab, which appears when the security group is selected in the object tree. Security groups are designed to simplify the administration of VM security settings by applying the settings to VMs with common criteria. VMs can be members of multiple security groups. As mentioned above, any blocking rule will take precedence over any allowing rule.

To edit security group membership, select the target security group in the object tree on the left, and then click the **Edit members** button on the **Virtual machines** tab:
In the **Edit members list** window select the necessary virtual machines to include them into the security group or deselect them to remove from it:

Type the symbols which a VM name must contain into the **Filter** field to filter the tree. Those VMs that have been pre-selected will not be filtered off the tree even if they do not match the filtering criteria. Click **OK**.

**Note**

Use this method to edit security group membership for deleted VMs to remove them from the security group. They will be displayed under the **Unknown** branch in the object tree.

Security groups are also available for tenant users who can create their own groups that will apply within a tenant and are available to be altered for this tenant and global administrators only.

To create a new security group, select **Rules – Add global rules group** menu item or right click on the **Global** entity and then click **Add group**.
Then enter the name for the new group in the following dialog box (New VM Group is the default value) and the description (optional). Click OK.

![Specify Settings for Group dialog box](image)

The new group is created and appears in the object tree.

To edit the global rules group, select it in the object tree. Then select Rules – Edit global rules group menu item or Edit group main panel button, or right click on the group and then click Edit:

![Edit global rules group](image)

Enter the new name and/or description in the same dialog box as shown above, and then click OK.

To delete global rules group, select global rules group in the object tree. Then select Rules – Delete global rules group or right click on the group and then click Delete. Confirm the operation.

4.4.2 User defined rules templates

You can create sets of rules as user-defined templates. These templates will then be available when adding rules to a group and/or VMs for convenience and to save time required for setting up (altering) the security plan. User defined rules templates are tenant-specific – they work for each tenant and on the global level independently and are available only on the level (and in tenant) they were created. Templates are a stored collection of rules, the rules added to a template will not take effect until this template is applied to a group or a VM. Altering template content – adding, changing and/or removing rules - will not affect those objects (groups and/or VMs) to which the template had been previously applied. Re-applying the template to the object will add the whole set of its rules over again, even if some of them (or all) are already present in the VM's/group's rules list – that way the same rule may be doubled, which will not cause any issues in their functioning.

To create a new template, right click the Templates entity and then click Add template:
Then enter the name for the new template in the following dialog box (New Template is the default value) and the description (optional). Click OK.

The new template is created and appears in the object tree.

To edit the rules template, right click on the template and then click Edit:

Enter the new name and/or description in the same dialog box, and then click OK.

To delete rules template, right click on the template and then click Delete. Confirm the operation.

The next subsection will describe how to add rules into templates, groups and VMs’ rule lists.

4.4.3 Adding rules

To add Acronis Cloud Security virtual firewall rules, select one of the following entities in the object tree:

- All VMs default group to create a global virtual firewall rule that will apply to all virtual machines and Hyper-V hosts. The global administrator is the only user that is able to do this.
- Previously created user-defined security group. The rules will be created within this group.
- Previously created template under the Templates entity to create the rule in the template. Please refer to the "User defined rules templates" (p. 67) subsection above.
- Virtual machine or a host to create a local rule. This rule will apply to this virtual machine or a host only.
Then use the **Rules** menu items or the similar main panel buttons (not all of the panel buttons duplicate main menu functionality).

Adding ARP/L2 rule

To add the ARP/L2 rule, select the **Add ARP/L2 rule** item of the **Rules** menu. The **Add ARP/L2 rule** dialog box will open:

![Add ARP/L2 rule dialog box](image)

Fill out all the parameters on the **Common** tab:
- **Name.** Enter the name that will help you identify the rule.
- **Description.** Enter the description for the rule (optional);
- **Action.** Select action for the rule to apply to corresponding network traffic – allow or block actions are only applicable for ARP/L2 rule.

**Note**

Acronis Cloud Security blocks all traffic by default when the virtual machine is set on firewall protection. However, in certain cases you may need to use both type of rule’s action with multiple rules to create a proper set.

- **Direction.** Set the traffic direction in respect of the target VM(s):
  - **Any** – to apply the rule in both directions;
  - **Inbound** – to apply the rule for inbound traffic only;
  - **Outbound** – to apply the rule for outbound traffic only.
- **Frame type (hex).** Enter the frame type to identify L2 protocol. By default there are two values available from the list: ARP (0806) and RARP (0835). Type the necessary number for the L2 protocol. ARP protocol will let you additionally specify remote IP addresses to limit rule action to.
- **Remote IPs.** Enter remote IP addresses to/from which the ARP traffic is sent/received, using spaces and comma as delimiters. Empty field assumes any address. This option basically applies to ARP traffic. For the majority of the other L2 protocols, e.g. for PPPoE protocol, this option is not applicable and will be disabled.
- **Remote VMs.** Select remote virtual machines to/from which the traffic is sent/received. Empty field assumes any remote VM. This option basically applies to ARP traffic. For the majority of L2 protocols, e.g. for PPPoE protocol, this option is not applicable and will be disabled.

To select remote virtual machines from a list, click the button to the right of the **Remote VMs** field and check the box to the left of the field containing their names and check the machines you want to add:
Type the symbols which an object name must contain into the Filter field to filter the tree. Those objects that have been pre-selected will not be filtered off the tree even if they do not match the filtering criteria. Click OK.

- **Remote MACs.** Enter remote MAC addresses to/from which the ARP/L2 traffic is sent/received. Empty field assumes any MAC address.

**Note**
Parameters Remote IPs, Remote VMs and Remote MACs work independently from each other and do not interfere with each other. I.e. if you select the remote virtual machine into the remote VMs list and enter IP address from another server into remote IPs field as well, the rule will apply to both remote systems.

Fill out all the parameters on the Advanced tab:
Packet type. Select the address type:
- **Any.** The rule will apply to any MAC address type.
- **Broadcast.** The rule will apply to broadcast MACs only (FF:FF:FF:FF:FF:FF).
- **Unicast.** The rule will apply to unicast MACs only.
- **Multicast.** The rule will apply to multicast MACs only (0x:01:00:5E:00:00:xx).

**VLAN ID.** Enter the VLAN number to add VLAN tagging option to the rule. The rule will apply to the frames with specified VLAN ID only. You have the following options to select from the list as well:
- **Any** (default option) – the rule will apply to any frame regardless of VLAN tagging.
- **No** – the rule will apply only to frames without VLAN tagging.

**Local address.** Enter the IP address or a subnet address using this notation: x.x.x.x/y.y.y.y, where x.x.x.x – network address in the decimal format; y.y.y.y – subnet mask in the decimal format, e.g., 192.168.0.0/255.255.255.0. When this address is specified, local VM address that the rule is applied will be checked to match it. If local VM address does not match the entered value, the traffic will be blocked. Since ARP/L2 rule usually applies to multiple virtual machines or a group, it is important to have all these virtual machines in the same subnet to be able to use this parameter properly. In this case you may enter a subnet address instead of a single IP address – the rule will apply to VMs which local address is in this subnet. If VMs are in different networks/subnets, the rule will only apply to the VM(s), which local address matches the IP address or subnet specified in the rule. It is not currently possible to enter IP ranges or multiple IP addresses here. Therefore either omit using it for multiple virtual machines/groups from different networks, or use it in the rules that apply for each VM or a subnet (group) individually.

Specify the time frame and the days in a week on which only the rule should be in action. Time
period will only apply if at least one day of a week is marked. Leave all days unmarked to let the rule always be in action.

At the end click **OK**. The rule will be created and added to the selected VM or a group and will be displayed in the main window.

**Adding IP rule**

To add the IP rule, select the **Add IP rule** item of the **Rules** menu. The **Add rule** dialog box will open:

![Add Rule dialog box](image)

Fill out all the parameters on the **Common** tab:

- **Name**. Enter the name that will help you identify the rule. E.g., LLMNR inbound that refers to link-local multicast name resolution inbound;
- **Description**. Enter the description for the rule (optional);
- **Action**. Select action for the rule to apply to corresponding network traffic. The following options are available for IP rule:
  - **Allow** – allow all packets including SPI.
  - **Allow (no SPI)** – allow direct packets only, SPI packets will be filtered.
  - **Block** – block all packets.
- **Direction**. Set the traffic direction in respect of the target VM(s):
- **Any** – to apply the rule in both directions;
- **Inbound** – to apply the rule for inbound traffic only (SPI packets will be excluded if allow action is set);
- **Outbound** – to apply the rule for outbound traffic only (SPI packets will be excluded if allow action is set).

SPI packets are normally allowed through Acronis Cloud Security virtual firewall when the certain traffic is set to be passed through it. E.g., the RDP inbound allowing rule on TCP port 3389 will let corresponding outbound SPI packets from TCP port 3389 to the remote private TCP port on the remote host that initiate RDP session in the case allow action is set. It will be considered as TCP established connection and will be displayed in connections table for the target VM. In certain situations such connections will be dropped by timeout, which results in losing the current session. Using allow (no SPI) action you can set two separate rules for inbound and outbound traffic to avoid such issues.

In the given example it will look like:

- **Allow (no SPI), Inbound**, TCP local ports: 3389, remote ports empty: (Any);
- **Allow (no SPI), Outbound**, TCP local ports 3389, remote ports empty (Any);

Such sessions are not recognized by Acronis Cloud Security virtual firewall as established TCP connections and will not be displayed in the connections table for the target virtual machine, while the sessions themselves will be allowed and will not be dropped by timeout unlike SPI-based TCP connections.

- **Protocol**. Select the protocol that is used to send the certain traffic type. You have the following options:
  - **Any** – any IP protocol.
  - **TCP** – TCP protocol.
  - **UDP** – UDP protocol.
  - **GRE** – GRE protocol.
- **ICMP** or **ICMPv6** – ICMP (ICMPv6) protocol. The following additional options are available for this protocol:

  ![Add Rule](image)


  Enter the required number(s) divided by commas (spaces will be added automatically). Leave the field empty to allow all types of ICMP messages.
You can use the dialog box to select the necessary ICMP message types by clicking the **Edit** button next to the **ICMP message types** field:

Check the boxes against the necessary types (the **Select all** and **Clear** buttons will select all types and clear the selection accordingly) and then click **OK**. The selected types will appear in the **ICMP message types** field.

- **Local ports** (if applicable). Enter the local ports through which the traffic flows. Empty field assumes any local port.
- **Remote ports** (if applicable). Enter the remote ports through which the traffic flows. Empty field assumes any remote port.
- **Remote IPs**. Enter remote IP addresses to/from which the traffic is sent/received. Empty field assumes any address.
- **Remote VMs**. Select remote virtual machines to/from which the traffic is sent/received. Empty field assumes any remote VM.
- **Remote MACs**. Enter remote MAC addresses to/from which the traffic is sent/received. Empty field assumes any address.
Fill out all the parameters on the **Advanced** tab:

- **Address type.** Select the address type to which the traffic is sent:
  - **Any.** All address types will be considered by the rule.
  - **Broadcast.** Only broadcast traffic will be considered by the rule. E.g. the one that is sent to the IPv4 addresses like x.x.x.255 for the subnet mask like 255.255.255.0 (VLSM broadcast addresses are also considered, they depend on the subnet mask length each time).
  - **Unicast.** Only traffic that is sent to a single receiver will be considered. E.g. the one that is sent to the IPv4 single host address like 192.168.1.10 with the subnet mask of 255.255.255.0.
  - **Multicast.** Only multi-recipient traffic will be considered. E.g. in IPv4 the target addresses must be within the following range: 224.x.x.x – 239.x.x.x.
    
    Note. Certain types of traffic are unicast, multicast or broadcast by their nature. E.g. RDP connection on port 3389 is the unicast type. Link local multicast name resolution on port 5355 is the multicast type. You have to be aware of it when setting this parameter so that the rule applies correctly unless you choose to set it to **Any**.

- **VLAN ID.** Enter the VLAN number to add VLAN tagging option to the rule. The rule will apply to the packets with specified VLAN ID only. You have the following options to select from the list as well:
  - **Any** (default option) – the rule will apply to any packet regardless of VLAN tagging.
  - **No** – the rule will apply only to packets without VLAN tagging.
Local address. Enter the IP address or a subnet address using this notation: x.x.x.x/y.y.y.y, where x.x.x.x - network address in the decimal format; y.y.y.y - subnet mask in the decimal format, e.g., 192.168.0.0/255.255.255.0. When this address is specified, local VM address that the rule is applied will be checked to match it. If local VM address does not match the entered value, the traffic will be blocked. If the rule applies to multiple VMs that are in different networks/subnets, the rule will only apply to the VM(s), which local address matches the IP address or subnet specified in the rule. It is not currently possible to enter IP ranges or multiple IP addresses here. Therefore either omit using it for multiple virtual machines/groups from different networks, or use it in the rules that apply for each VM or a subnet (group) individually.

- Specify the time frame and the days in a week on which only the rule should be in action. Time period will only apply if at least one day of a week is marked. Leave all days unmarked to let the rule always be in action.

- Mark the Authorization required option to enable authorization in the rule. If this option is enabled, the rule will only apply to authorized addresses. Please refer to the "Authorization" (p. 85) subsection below for details on how to set up authorization from remote computers when using the rules with this option.

At the end click OK. The rule will be created and added to the selected VM and will be displayed in the main window.

Pre-defined rule templates

There are pre-defined rule parameters sets (templates) implemented in Acronis Cloud Security that help you fill out the dialog box with necessary values to create rules for some common scenarios (e.g., HTTP access; remote access through RDP, Telnet or SSH). These templates already contain the necessary values to be entered in the dialog box, i.e., protocol, TCP/UDP port number etc. Select the desired template, and choose the right direction, action and remote VMs/IP addresses for which the rule will apply.

To use the rule template click the Templates button in the Add rule dialog box. The dialog box below shows the template list with the most commonly used scenarios placed at the top of the list and marked as Popular:
- Select the desired scenario by using a left-click.
- Select the direction (inbound/outbound)
- Click Apply. The Add rule dialog box will show parameters applicable for the selected scenario.

**Note**
Be accurate when choosing the direction of the traffic you wish to allow or block. It is important to set this parameter correctly; the assigned TCP/UDP port (local or remote) depends on the set direction. Otherwise, the rule you created will not work properly. For example, if you wish to create the HTTP rule on the VM-web client, set the *outbound* direction; if you wish to create the same rule on the VM that is a web server, set the *inbound* direction. Acronis Cloud Security template will assign the HTTP port 80 to remote for VM-client and local for VM-server in order to set the TCP segment analysis properly. Contact your network expert if assistance is needed.

For example, let’s see how it will work for the HTTP rule, allowing traffic on the VM – web client.
Select the template row with the name **HTTP**: 

![Rule templates dialog box](image)
Make sure you have selected the **Outbound** direction (**Inbound** is the default).

Click **Apply**. The **Add rule** dialog box fields will be automatically filled in with the selected rule template:
Adding rules for multiple virtual machines

To add the ARP/L2 or IP rule for multiple VMs, use the corresponding Rules menu command or main panel button. The Add ARP/L2 rule for multiple VMs or Add rule for multiple VMs dialog windows will open accordingly:
Type the symbols which an object name must contain into the Filter field to filter the tree. Those objects that have been pre-selected will not be filtered off the tree even if they do not match the filtering criteria. Fill out the rule parameters.
Click **OK**. The corresponding message will appear after successfully adding multiple rules.

**Adding default gateway rule**

To add the default gateway rule, select the **Add default gateway rule** item of the **Rules** menu. The **Default gateway rule** dialog box will open:
You have two options:

- **Add rules to virtual machines global rules** – the rule being created will be added to global VM rules list (the All VMs group) and will apply to all VMs set on virtual firewall.
- **Add rules to selected virtual machines** – the rule being created will be added to the rules lists only for those VMs that were chosen. Type the symbols which a VM name must contain into the Filter field to filter the tree. Those VMs that have been pre-selected will not be filtered off the tree even if they do not match the filtering criteria.

Click **OK**. The following rules with the characteristics shown below will be automatically created and then added to the necessary places as described above:

1. Default gateway IP Rule
   - **Name**: Default gateway IP Rule
   - **TypeOfRule**: IP, Any
   - **Type**: Any
   - **Action**: Allow
   - **Protocol**: Any
   - **Remote IPs**: 192.168.1.1 (as it's entered in the example given here)

2. Default gateway L2 Rule
   - **Name**: Default gateway ARP rule
   - **TypeOfRule**: ARP
- **Type**: Any
- **Action**: Allow
- **Protocol**: 0806
- **Remote IPs**: any

### 4.4.4 Editing a rule

To edit a rule, select it in the list, then click the **Edit rule** on the top menu panel. Then change the rule settings in the appropriate dialog box just as when adding a rule.

### 4.4.5 Removing a rule

To remove a rule, select it in the list, then click the **Remove rule** on the top menu panel. Confirm the operation. The rule will disappear from the list.

### 4.4.6 Authorization

When the **Authorization required** option is enabled in the IP rule's parameters, this rule will only apply to authorized addresses. Any remote address that the rule is intended to be active for should be authorized using special application that arrives with Acronis Cloud Security installation package. It is also necessary to have custom users created in Acronis Cloud Security users list, which will be required during authorization.

---

**Note**


To setup authorization follow the steps below:

1. Ensure that you have properly configured and installed the security certificates on the management server. To use authorization feature, two certificates should be installed on the management server:
   - Pfx-certificate (should be installed for **Local machine**);
   - Authorization certificate **AuthCert.cer** should be placed into this location on the management server: `C:\ProgramData\Acronis\Acronis Cloud Security for Hyper-V\AuthCert.cer`. Acronis Cloud Security management service should be restarted after copying the certificate into this location.
   - These certificates will be used for SSL communication between the server and the client.

2. Ensure that you have appropriate custom users created in Acronis Cloud Security (please refer to the "Global administrator and tenants" (p. 51) - "Users management" (p. 52) section for details). Currently it is not required to grant those users permissions, it is enough just to have them in the...
users list. If the target virtual machine is in the global group, then the custom user should be created in the global group. If the target virtual machine is assigned to a tenant, then the custom user should be created in that tenant. In the case your rule is created in the security group and/or applies for multiple VMs, which may be assigned to different tenants and some just be in the global group, then you should have custom users in each tenant and/or global group accordingly.
3. On the remote computer that the rule should be active towards, run the `5ninecli.exe` application that arrived with Acronis Cloud Security installation package:

![Access Client](image)

- Enter the management server IP address into the **Host** field.
- Enter the custom user’s name into the **Login** field.
- Enter the custom user’s password.
- Enter the tenant’s name into the **Tenant** field. Leave it empty if you are connecting to global group.
- Enter virtual machine ID into the **VM Id** field. This value can be retrieved in the **Virtual machine settings** dialog window (please refer to the "Configuring VM settings" (p. 171) section for details):

![Virtual Machine Settings](image)

**Note**

In the case third party needs to get authorization, Cloud Security administrator will have to provide the above data to this person along with the `5ninecli.exe` application.
Click the **Connect** button. If authorization is successful, you will see the following information:

At this point the IP address of the computer, which the authentication has been initiated from, is authorized and the rule will apply. Do not close the application unless you want to interrupt the authorization and your session. Clicking on the **Disconnect** button will also interrupt the session and the rule will be no longer in action.

### 4.4.7 Common scenarios

To help you set the most commonly used virtual firewall rules, see the explanations listed below for which rules to use to allow or block the necessary type of traffic to or from the target virtual machine. We presume that the target VM is set on virtual firewall.

**RDP**

To allow remote desktop connection to the VM, the following rules must be added:
- ARP rule allowing any ARP traffic on the VM

![Add ARP/L2 Rule](image)

- **Name:** ARP all VMs
- **Description:**
- **Action:** Allow
- **Direction:** Any
- **Frame type (hex):** 0806 (ARP)
- **Remote IPs (example):**
  - 192.168.0.1
  - 192.168.1.0/255.255.255.0
  - 192.168.2.0-192.168.2.255
- **Remote VMs (example):**
  - Test2003, VM1, VM3
- **Remote MACs:**  

[Screen shot of Add ARP/L2 Rule dialog box]
- IP rule allowing inbound TCP traffic on the local port 3389

![Add Rule dialog window](image)

**Ping traffic**

To allow ping to/from VM, the following rules must be added:

- ARP rule allowing any ARP traffic on the VM
- IP rule allowing ICMP traffic on the VM
Leaving the ICMP message types field blank assumes any types of ICMP message, while 0 and 8 types covers echo request and reply messages to ping the host.

**HTTP**

To allow HTTP access on the VM, the following rules must be added:

- ARP rule allowing any ARP traffic on the VM
- Default gateway rule to the network default gateway IP address as it is set on your IP configuration. This will automatically add IP and ARP rules to default gateway on the target VM.
- If the default gateway and the DNS Server have different IP addresses, an additional IP rule for
DNS should be created allowing outbound UDP traffic on remote port 53.
IP rule allowing outbound TCP traffic on remote port 80 to allow HTTP access:

DHCP

To allow dynamic host configuration function on the VM, the following rules must be added:
- IP rule allowing inbound UDP traffic on local port 68 for DHCP client

<table>
<thead>
<tr>
<th>Common</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>DHCPC</td>
</tr>
<tr>
<td>Description:</td>
<td>Dynamic Host Configuration Protocol Client; Filter</td>
</tr>
<tr>
<td>Action:</td>
<td>Allow</td>
</tr>
<tr>
<td>Direction:</td>
<td>Inbound</td>
</tr>
<tr>
<td>Protocol:</td>
<td>UDP</td>
</tr>
<tr>
<td>Local Ports (example 80,8080-8088,443)</td>
<td>68</td>
</tr>
<tr>
<td>Remote Ports (example 80,8080-8088,443)</td>
<td></td>
</tr>
<tr>
<td>Remote IPs (example 192.168.0.1, 192.168.1.0/255.255.255.0, 192.168.2.0-192.168.2.255)</td>
<td></td>
</tr>
<tr>
<td>Remote VMs</td>
<td></td>
</tr>
<tr>
<td>Remote MACs</td>
<td></td>
</tr>
</tbody>
</table>
IP rule allowing outbound UDP traffic on remote port 67 for request to DHCP server

This is necessary when the VM gets its IP configuration dynamically through DHCP server, when resolving IP configuration issues if they take place on the target VM and when you have to renew the VM’s IP configuration through DHCP.

IIS

To allow the necessary access on the VM that is a Web server, the following rules must be added:

- ARP rule allowing any ARP traffic on the VM;
- IP rule allowing TCP traffic on local port 80 to allow HTTP access to the web server:

![Add Rule](image)

**MS SQL Server**

To allow the necessary access on the VM that is a Web server, the following rules must be added:

- ARP rule allowing any ARP traffic on the VM;
- IP rule allowing TCP traffic on local port 1433:
Note
If a VM is MS SQL client, you should create a rule allowing TCP traffic on remote port 1433 so that the VM-client is able to communicate with VM – MS SQL server.

4.4.8 Applying user defined rules templates

To apply a user defined rules template, select one of the following entities in the object tree:

- **All VMs** default group to apply a template to all virtual machines. The global administrator is the only user that is able to do this.
- Previously created user-defined security group to apply a template to the members of this group.
- Virtual machine to apply a template to a single VM.

Then click **Rules – Add rule using template** main menu item or **Use template** main panel button. The **Add rule using template** window will appear:
Select the necessary template from the Template list. You will see the set of rules added into the template in the field next to the template description.

If necessary, alter remote system parameters for the rules: Remote IPs, Remote VMs and/or Remote MACs.

**Note**

The rules may already contain remote system parameters in themselves. If you set the new ones here before applying the template – they will overwrite those that had been set in the rules. This will happen at this time only, when the template is applied to the object. Template itself will keep its previous settings.

Click OK to apply the selected template. The rules will be added to the object's rules list.

### 4.4.9 Exporting rules

Acronis Cloud Security virtual firewall rules can be exported into xml file. This operation is possible from the following objects: virtual machine, user-defined template, security group. The object must have the rules created in advance. To export virtual firewall rules into the .xml file, select the target object in the object tree, then select the Rules - Export main menu command or right click on it and select the Export rules context menu command:
Then, choose the path and type the name to save the .xml file on the disk and click Save:

4.4.10 Importing rules

Exported rules can be imported back to Acronis Cloud Security from the .xml file. This operation is possible for the same objects as the export operation: virtual machine, user-defined template, security group. To import virtual firewall rules from the .xml file, select the target object in the object tree, then select the Rules - Import main menu command or right click on it and select the Import rules context menu command:

Then, choose the .xml file, which had been previously saved on the disk, and click Open:
The rules from the .xml file will be applied to the selected object.

4.5 Deep packet inspection

Acronis Cloud Security provides Deep packet inspection (DPI) on HTTP and DNS packets. When DPI is enabled, it allows the data portion of the network packet to be examined and either allow or deny the packets based on DPI rules configured for HTTP and DNS traffic, even after the network packet was allowed using virtual firewall rules. Note that rules are order-specific.

4.5.1 Configuring DPI

Select the Deep packet inspection entity from the tree view on the left hand side of the console window. Click the Add rule button to configure DNS or HTTP rules.
Name: Rule name to be displayed in list

Description: Option field for clarification of the rule

Action: The action drop down selection list has two settings

- **Block** – Deny the packet if it matches the defined criteria
- **Allow** – Permit the packet if it matches the defined criteria

URL string: The URL string which HTTP DPI rules will be evaluated against. This string can contain wild cards, for example *UnwantedSite.com will match any host before the unwantedsite.com domain such as ww1.unwantedsite.com or ww2.unwantedsite.com

User agent string: The UserAgent string dynamically returns a different value depending on the browser and platform versions. The User-Agent string contains information about the user agent originating the request and is used for statistical data, protocol violations and tailored responses based on characteristics or limitations of a browser and platform. Allow rules can be configured for supported browser and platform combinations and block rules can be set for unsupported or known suspicious and malicious tags.

Examples of known malicious or suspicious user agent strings:
- Fake antivirus – malicious:
  - Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; AntivirXP08; .NET CLR 1.1.4322)

- Adware and Spyware – Sends data back to a remote host
  - Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; PeoplePal 7.0; .NET CLR 2.0.50727)
  - Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; FunWebProducts; .NET CLR 1.1.4322; .NET CLR 2.0.50727)


- **Scan mode:** Specifies DNS and or HTTP packet inspection

- **Monitored HTTP ports:** Specifies the port or ports for HTTP packet inspection. Port 80 is set by default but other ports can be added in a comma delimited list. Note that HTTPS traffic cannot be inspected.
In the **DPI rule properties** window the **Advanced** tab allows rules to be enforced based on time and days of the week.
Rules can be removed by highlighting the rule in the list and clicking the **Remove rule** button. Existing rules can also be modified by highlighting the desired rule and clicking the **Edit** button. The order of the rules can also be changed by selecting a rule and either choosing the **Move up** or **Move down** menu options.

### 4.6 Configuring virtual firewall

To configure virtual firewall select **Settings – vFirewall** menu item:

Specify which VMs or Hyper-V host adapters will be set on virtual firewall protection in the **Enforce configured firewall rules** dialog box:
Check the boxes for the VMs or host adapters that you want to remove from monitoring. Type the symbols which a VM name must contain into the Filter field to filter the tree. Those VMs that have been pre-selected will not be filtered off the tree even if they do not match the filtering criteria. Click OK. Then confirm to the system warning – only traffic allowed by the rules will go through from this moment on these VMs.

To set a particular VM or Hyper-V host's virtualized adapters on the virtual firewall protection, select the necessary VM, click the vFirewall context menu item and confirm to the system warning. Use the same context menu item to remove the VM from virtual firewall protection.

For Hyper-V hosts there is also the test function, which temporarily enables virtual firewall and then automatically disables it. This is implemented to check if there are no network issues while the host is under virtual firewall protection and all firewall rules are configured as required. It is recommended to use this function prior to enable the virtual firewall on Hyper-V host's adapters normally. To test virtual firewall action on the host, select the target host in the object tree, then make sure all rules are configured, right click on the host and select the Test firewall settings context menu command:
Confirm the action. The virtual firewall will be enabled for three minutes and then automatically turned off. If during this time no issues were observed, you may enable the virtual firewall on the host normally.

### 4.7 Virtual firewall logs

In the latest versions of Acronis Cloud Security virtual firewall logs are stored on management server's local disk (as set by default) instead of database. The path to store virtual firewall logs is set during installation of management service (as described in the “Installation” (p. 10) – “Management service” (p. 11) section above). Default location is `C:\CloudSecurityLogs`. Logs for each VM will be stored inside subfolder with the name in the following format: `{VM ID (hex string)}`. There is also an option to cancel sending virtual firewall logs to the management server as described below.

#### 4.7.1 Virtual firewall logs settings

To change virtual firewall log settings, open the **View – Log settings** main menu:

- Enable the **Convert log time to local** option to display events in the local time zone (time on management server);
- Enable the **Do not send firewall log to the central management service** option to cancel sending virtual firewall logs to the management server. You will not be able to view logs in this case and they will not be written into the configured location storage saving the disk space and reducing management service workload, but still will be exported to the external syslog in the case it's configured. Please refer to the "Syslog server integration" (p. 162) section for more information.
- Enable the **Track obsolete records purge events** option to start tracking obsolete virtual firewall log records purging events. The events will be written in the internal audit events log (see the "Internal events auditing" (p. 63) section above).
Enable **Track log review events** option to start tracking virtual firewall log review events. The events will be written into the user actions log (see the "User activity auditing" (p. 61) section above).

Click **OK** to store settings.

### 4.7.2 Viewing virtual firewall logs

To view current virtual firewall log records for the selected virtual machine, click **Load log** on the **Firewall** tab of the program main window. The log records will display in the lower part of the main window:

**Note**

The **Do not send firewall log to the central management service** option must not be checked in virtual firewall log settings to be able to view the new log records in the management console.

The resulting vFirewall log entries can be filtered by selecting the **Enable filter** menu item which will drop down the filter settings.
Filtering options:

- **Direction**: Any, Inbound or Outbound
- **Action**: Any, Allow or Block
- **Source address**: IP Address
- **Target address**: IP Address
- **Type**: Any, IP, ARP or L2
- **Protocol**: If IP is selected for type than GRE, ICMP, ICMPv6, IGMP, TCP or UDP
- **Start date**: Starting date of range
- **End date**: End date of range
- **Source port**: Port number for the source
- **Target port**: Port number for the target

Each column in the list can be sorted by clicking on the desired one. There is also a right click menu for each column that allows further customization on sorting, grouping, choosing columns to add and remove. Column order can be changed by dragging and dropping.
You can create context rule directly from this log. To do so, select the necessary record and then use the **Add rule** context menu item. You will be offered to add the new firewall rule of the opposite action to the selected record, e.g. if it was blocked packet, you will be offered to add the corresponding allowing rule:

![Add Rule dialog box](image)

As it’s shown on the screen capture, you are advised to allow inbound traffic from certain IP address on certain UDP port in accordance with the firewall log record the rule creation was initiated from. You are still able to alter the rule parameters in the standard way as it is described above in the "Configuring virtual firewall rules" (p. 64) section.

You may also export the virtual firewall logs to the .xls file. Right-click any of the events and then select the **Export to file** context menu item:
Then select the destination folder to save the file and click **Save**:

4.8 **Antivirus**

There are the following antivirus features, represented in Acronis Cloud Security:

- Agentless antivirus:
  - Immediate anti-malware scans
  - Recurrent anti-malware scans by user-defined schedules
  - Delayed one-time anti-malware scans
- Active protection. Agent-based real time virtual machine protection, including on-access file control.
- Anti-ransomware. Agent-based protection against malicious processes (programs), as a part of active protection feature. Available in Acronis Cloud Security version with Bit Defender antivirus engine only.
- Network traffic scanner. Agentless protection for http traffic. It is described in the "Network traffic scanner" (p. 156) section. Malicious files that were downloaded via http and have been detected by network traffic scanner then can be quarantined either by agentless anti-malware scan or active protection agent. In the last case it will be done immediately upon downloading such file.
Antivirus is controlled on the Antivirus tab of the main Acronis Cloud Security window:
Active protection agent activity with both agent and signature version information is shown on the **Active protection** tab:

![Active protection tab](image)

See the "Active protection" (p. 137) section below for a description of the controls that are used to operate the active protection agent and view the results.

### 4.8.1 Antivirus and active protection settings

Acronis Cloud Security antivirus function depends on pre-defined settings. You can change these settings if you are working under a user with sufficient privileges. That means the user must be set with Security administrator role enabled. Please, refer to the “Global administrator and tenants” (p. 51) section above for more information.

To alter antivirus and active protection settings select the **Settings – Antivirus** menu item. All settings are done in the **Antivirus settings** window.

**Antivirus updates**

Acronis Cloud Security with Bit Defender antivirus has centralized mechanism to get the antivirus definitions. All antivirus databases are collected on the management server, and then distributed to each Hyper-V host. This process is managed by the separate service – **5nine.Antivirus.UpdateService**. This service installs along with **5nine.Antivirus.ManagementService**. In order for AV updates to work properly, Internet access should be opened on the management server and connections should be allowed on TCP local ports 8183 and 8939 through which hosts will receive definitions. Refer to the "System requirements" (p. 6) section above.

To view antivirus updates open the **General** tab:
Here you can do the following:

- Check the last definitions update info per each host;
- Manually evoke immediate definitions update by clicking the Update button for a particular host or the Update all button to perform update for all hosts;
Configure the proxy server by clicking the **Proxy Settings** button:

![Proxy Settings dialog box](image)

- Configure workload orchestration. Set the maximum number of concurrent anti-malware scan jobs and active protection auto-installation jobs per host. It depends on the Hyper-V host performance. The default value is 8.
- Set the antivirus definitions update frequency: frequency in hours and the period of a day.
- Set the full definitions update schedule. To control/limit antivirus definitions full update workload, which may affect Hyper-V host performance, you may set the frequency schedule and define conditions to perform full update: full update frequency (number of incremental update events to happen to run the full update next time), or a period (daily, weekly, monthly), and the size of definitions on the disk that must be reached to perform full definitions update. Whichever of these conditions will be met first, full definitions update will be evoked. This helps to spread the full updates in time and optimize the load on Hyper-V hosts.

Acronis Cloud Security uses antivirus definitions update VM spreading algorithm for active protection agents to reduce load. The main idea of this approach is to split VMs on each Hyper-V host into portions (considering update interval and update safe period settings – **Definitions update frequency**) and update them portion by portion every 10 minutes.

**Policies**

Policies allow you to specify antivirus security configurations for desired groupings of VMs. Depending on organizational policies and standards, some virtual machines may require different antivirus exclusions while others may require different active protection operational modes.
Antivirus policy configurations for selected VMs includes enabling active protection state and mode, exclusions, scanned extensions, blocked and allowed threats. Support different configurations for multi-tenant and diversified environments.

Configuring policies

To configure antivirus policies open the Policies tab in the Antivirus settings window. Click the Add policy menu item to create a new policy. Enter the name of the file (and the policy) that the configurations will be saved to.

Virtual machines

Select the desired VMs for the policy to be applied.

Active protection and quarantine settings

To set parameters for the virtual machines real time anti-malware protection and active protection agent behavior options, select the Policies – Active protection tab:
Check the Enabled box in the Settings block to enable active protection on virtual machines; this is the default setting. Active protection will be immediately activated on those virtual machines where active protection agent is installed. Refer to the "Active protection" (p. 137) section for more information. If you need to disable active protection, deselect this box and active protection agent will immediately stop working.

Select the action to be taken against the malicious items detected during agentless antivirus scans:

- **Move to quarantine** (set by default) – all detected items will be moved to quarantine folder.
- **Try disinfecting and quarantine on fail** – antivirus engine will try to clear just the harmful code from each infected file, leaving then the cleared file in its original location and, in the case of failure to do so, move it to quarantine folder.

**Note**
Active protection agent always moves malicious items to quarantine.

Move the On access slider to one of the three positions:

- **Execution only** – the least resource consuming, but also the least secure. Active protection agent will scan files when they attempt to execute. Malware could already be copied to the virtual machine and will not be caught by active protection until the malware attempts to execute if protection is enabled as described above.
- **High risk extensions only** – active protection will scan files with the known extensions (shown to the right) whenever these files are touched. Active protection will also scan any file that attempts to execute if protection is enabled as described above.
- **All touched files** – active protection will scan any file each time it is touched. Active protection will also scan any file that attempts to execute if protection is enabled as described above. This mode is the most resource consuming, but also the most secure.

Review the known extensions in **AP known/Admin known** lists. Check the boxes of each extension to enable or disable active protection. The same operations are made on the Extensions tab as described below. The Modify button will take you there.
Exclusions

The **Exclusions** tab allows you to specify the files and folders (with destinations if needed) on the host that will be excluded from anti-malware protection and allowed on your system:

![Exclusions Tab](image)

**Note**

The files, destinations and folders can be added to the exclusions list either from the host file system or the VM internal file system, as it works for both VM and host. If you add entries from the VM internal file system, you can only type them directly into the dialog boxes as described below. If you add them from the host file system, you can either type them in directly or browse for them as described below.
To add a file, destination or folder to the exclusions list, click *Add* and use the appropriate selection:

- **Add file** – select and add a single file to the exclusions list. Enter the file name directly or click the *Browse* button to search for the file.

  ![Exclusions File Dialog](image)

- **Add file with path** – select and add a single file with its destination to the exclusions list. Enter the full path to the file directly or click the *Browse* button to search for the file.

  ![Exclusions File with Path Dialog](image)

- **Add folder** – select and add a folder to the exclusions list. Enter the path to the folder directly or click the *Browse* button to search for the file.

  ![Exclusions Folder Dialog](image)

To remove a file, destination or a folder from the exclusions list, select it and then click the *Remove* button.
Extensions

The Extensions tab allows you to specify the file name extensions that will either be included or excluded from the anti-malware active protection. It will also determine whether or not the files of all the kinds should be included in the regular anti-malware scan.

There is a set of pre-defined known extensions on this tab. You can apply changes to it by:

- Clearing the check box to the left of each extension to exclude this file type from the anti-malware active protection and regular anti-malware scans;
- Checking the box to the left of each extension to include this file type in the anti-malware active protection and regular anti-malware scans;
- Adding the new admin known extension for a certain file type. To add the extension, click Add and fill in the dialog box as shown below.

- Enter the extension in the Extension field.
- Check the Enable box to enable active protection for the files with this extension. Leave the box empty to disable active protection.
- Click OK.
- Select the extension and click the Remove button to remove it from the list of known extensions.
Check the **Scan all files (full and incremental)** box to include all file types in regular anti-malware scans. Leave it clear to let the internal antivirus mechanism decide which files to scan. Click **OK** in the **Antivirus settings** window when all the settings are complete.

**Always blocked**

On the **Always blocked** tab set the paths and/or files that will always be treated as malicious during the AV scan:

![Always blocked](image)

**Note**

The files, destinations and folders can be added to the **always blocked** list either from the host file system or the VM internal file system, as it works for both VM and host. If you add entries from the VM internal file system, you can only type them directly into the dialog boxes as described below. If you add them from the host file system, you can either type them in directly or browse search for them as described below.

To add a file, destination or folder to the always blocked list, click **Add** and use the appropriate command:

- **Add file** – select and add a single file to the always blocked list. Enter the file name directly or click the **Browse** button to search for the file.
- **Add file with path** – select and add a single file with its destination to the always blocked list. Enter the full path to the file directly or click the **Browse** button to search for the file.

![Always Blocked File with Path Dialog](image)

- **Add folder** – select and add a folder to the always blocked list. Enter the path to the folder directly or click the **Browse** button to search for the folder.

![Always Blocked Folder Dialog](image)

To remove a file, destination or folder from the always blocked list, select it and then click the **Remove** button.
Allowed threats

On the **Allowed threats** tab you can manage the malicious and suspected files that have been allowed in the system – restored from quarantine (please refer to the "Quarantine" (p. 142) subsection below).

To remove the threat from the allowed threats list, select it and click the **Remove** button.

Anti-ransomware

On the **Anti-ransomware** tab you can manage anti-ransomware feature (please refer to the "Anti-ransomware" (p. 145) paragraph below for the general description of the feature):
On the **Protecting paths** tab you need to add folders to protect against malicious processes. These folders must be created before they are added here. Otherwise, restart of the active protection agent service on VMs will be required. Click the **Add** button to select and add the folder to the protected list. Enter the path to the folder directly or click the **Browse** button to search for the folder:

![Protecting Path Folder Dialog](image)

If you want to remove the folder from the protected list, select it and click the **Remove** button.

On the **Trusted processes** tab you can add any processes to the *trusted* list so the anti-ransomware feature ignores them when it is in action:

![Antivirus Settings](image)

**Note**

Anti-ransomware feature activates when all the settings are completed and active protection agent is installed on a particular VM and synced. All processes, started prior to activating the anti-ransomware feature will be also ignored. The same effect will take place when the AP agent is restarted – all processes that were running before active protection agent's service gets started will be considered as *trusted*. This should be noted before taking action of restarting the AP agent.
To add the process with or without child processes to the trusted list, click the **Add – Process with children/Process w/o children** buttons correspondingly:

Then enter the full path to the process file directly or click the **Browse** button to search for the file:

If you want to remove the process from the trusted list, select it and click the **Remove** button.

**Active protection auto installation and update**

Acronis Cloud Security provides optional ability to auto-install active protection agent onto VMs. This feature is configured on the **Active protection** tab of the **Antivirus settings** window:

On the **General** tab this option can be enabled or disabled. If enabled, all VMs will be checked for AP installation status at the configured intervals and, if any of VMs do not have AP installed, auto-installation of the active protection agent will occur on such VMs, followed by auto-reboot of these VMs, as it's normally required for AP agent installation.
Note
The maximum concurrent number of auto-installation jobs, counted in total by the number of VMs that require AP installation, is limited and configurable, just like the maximum concurrent number of the agentless anti-malware scan jobs. The same workload orchestration setting is used to control this limit, which is located on the General tab of the Antivirus settings window:

To enable active protection agent auto-installation and set the interval to check its status on VMs, do the following:

- Mark the Enabled check box.
- Set the number of minutes through which the AP installation state on VMs will be checked and set the time period of the day to perform auto-installation procedure.

On the Auto install exclusions tab, you can exclude VMs that you do not want to check for active protection state and auto-install the AP agent in the case it’s absent on these VMs:

Mark the check boxes of the VMs in the tree that you need to exclude from active protection auto-installation process.

On the Update definitions exclusions tab you can exclude VMs that you do not want to automatically update active protection definitions:
This is implemented to let administrators control the load on the system, caused by definitions updates and exclude VMs from the automatic updates. Mark the check boxes of the VMs in the tree that you need to exclude from auto-update of the active protection definitions.

Click the **Apply changes** button in the bottom of the **Antivirus settings** window when all settings are done and then **OK** to close the window.

### 4.8.2 Creating antivirus jobs

There are two options to initiate the agentless anti-malware scan job:

- Quick start the anti-malware scan with the default policy.
- Create the antivirus job via the antivirus wizard.

**Quick starting anti-malware scan with default policy**

To quickly start the anti-malware scan with the default policy, simply select the target (VM or a host) in the object tree, right-click on it and select the **Av scan with default policy** context menu command:

This will immediately launch the scan, using the default policy.
Creating antivirus job via the antivirus wizard

To create the antivirus job via the antivirus wizard, run the **Antivirus wizard** by selecting the **Create job** drop down menu on the upper left side of the **Antivirus jobs** or **AV scheduled jobs** tabs and select which job to start: **Scan host** or **Scan VMs**.

Enter the name of the job and click **Next**.
Then select the objects to be scanned:

Mark objects to include in the job. Use filter for convenience. If you wish all VMs on the host(s), including newly created VMs, to be automatically included in the already created schedule in the future, avoiding the necessity to manually edit the job each time new VMs are created, enable the option **Scan all virtual machines (auto include new)**. Click **Next**.
Select file types for the scan:

Here you have two options:

- **Scan all files** – all files on the virtual machine will be checked.
- **Allow me to control exactly what is scanned** (default option) – only certain types of files which extensions are added to the list will be checked. There is the default list of file types which is recommended to be used. However, you are able to edit it by adding or removing file extensions from this list. Push the Add or Remove buttons to add or remove the extensions.

Add the file extension and its description in the dialog below, and then click **OK**.
To edit the already added extension, find it in the list, then click the **Edit** button and do the same actions as above in the **Edit extension** dialog:

To include the files without extensions in the scanning process, enable the **Scan files with no extensions** option (disabled by default). To restore the default settings click the **Restore defaults** button.

Set the location(s) in the host/guest OS that will be excluded from the scan and specify if the full scan should be done forcefully:

- Check the **Full scan** box to force full scan regardless of CBT data. If it's left clear, then CBT data will be taken into account and the scan type will be set in accordance with it for each VM – full scan for the first time scan and incremental for subsequent scans.
- Set the log level as required: select the **Standard** or **Maximum** option in the **Log level** list box. It will determine, less or more detailed the antivirus job will be logged.
Click the **Add** button to add the new location and enter the path manually in the following dialog:

![Exclusion dialog]

Click **OK**.

- Click the **Edit** button and do the same action as above for editing the existing location.
- Click the **Remove** button to remove the existing location from the exclusions list.

Click **Next**.

Set the location(s) in the host/guest OS that will be treated as malicious during the AV scan:

![Antivirus Wizard dialog]

- Click the **Add** button to add the new location and enter the path.
- Click the **Edit** button and do the same action as above for editing the existing location.
- Click the **Remove** button to remove the existing location from the block list.

Click **Next**.
Set the job schedule:

- Run Job Immediately
- Delayed Run: 1/28/2020 3:00:00 AM
- Create Recurrent Job:
  - Daily every 1 day
- Weekly every Sunday
- Monthly at 1 day

Review all settings and submit the new job:

Job Name: Schedule 1 VMs
Create Recurrent Daily Job
Start at: 1:00:00 AM
Run each 1 days
LogLvl: Standard
Scan Exclusions: C:\Program Files (x86)\Exsvnr\Log

Press 'Finish' button to create job
The job will appear in the **Antivirus jobs** tab if the job runs immediately and in the AV scheduled jobs tab if it is scheduled or deferred job.

All currently active and already completed jobs are shown in the **Antivirus jobs** tab for the particular VM that is selected in the tree. If the host is selected in the tree, then all host scanning jobs and all jobs for VMs seating on the host and ever been scanned will be shown. To filter jobs by date select the corresponding **Show** filter options:

- **Last day** (default) – to show jobs occurred in the last day;
- **Last 7 days** – to show jobs occurred in the last 7 days;
- **Last 30 days** – to show jobs occurred in the last 30 days.

To view the log of the particular antivirus job, double click it:

To export the log into the .txt file, click the **Export** button at the bottom of the **View log** window.

The default path to save files is: `C:\Program Files\Acronis\Acronis Cloud Security Management Console\Exports\yyyyMMdd_hh.mi.ss_AvScanLog.txt`. 
When the job is currently in progress, completeness percentage will be available with ability to pause, resume or stop (interrupt) the scan:

- To pause the scan, select the job that currently in progress and click the **Pause** button.
- To resume the paused scan, select the job on pause and click the **Resume** button.
- To interrupt the scan, select the job that currently in progress and click the **Stop** button.

All deferred and scheduled jobs are displayed in the **AV scheduled jobs** tab:

- To edit the existing job, select the job and click the **Edit** button – the same **Antivirus wizard** will be opened as when creating the new job.
- To create the new job, click the **Create job** button and select the necessary item – **Scan VMs** or **Scan host**. Then follow the procedure described above.
- To remove the job, select it and click the **Remove** button.

**Note**

Each time a malware is found on the virtual machine during any regular scan, the threats are moved to the designated quarantine folder inside guest OS. This requires rebooting of the target virtual machine. If malware is found on a particular virtual machine, the VM gets the **reboot required** status. It is then up to user when to reboot the target virtual machine. Please refer to the "Quarantine" (p. 142) and "Reboot action" (p. 144) subsections below for more information.

Email notifications are available to inform admins about malware events detected during agentless antivirus scan. Please refer to the "Notifications" (p. 159) subsection below for details.

### 4.8.3 Antivirus status

The full antivirus status view is available for all VMs:
On the **Antivirus – Summary** tab when the host is selected in the object tree (will display all VMs that are currently seating on the selected host):

If any of VMs requires reboot, the corresponding link (**Reboot now**) will appear in the **Reboot action** column. Click this link if you need to immediately perform the reboot on the VM.
In the **Virtual machine status** window. Use the **View – Antivirus status** menu item to open this window (will display all VMs that are currently seating on the selected host):

<table>
<thead>
<tr>
<th>Last Scan</th>
<th>Name</th>
<th>Job Status</th>
<th>AP Status</th>
<th>Message</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>testVM2</td>
<td>Need to scan</td>
<td>Agent status unknown</td>
<td>Not scanned</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCVMM</td>
<td>Need to scan</td>
<td>Agent status unknown</td>
<td>Not scanned</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCVMM-LIB</td>
<td>Scanning</td>
<td>Agent running. Active protection status unknown</td>
<td>Scanning...</td>
<td></td>
</tr>
<tr>
<td>1/20/2020 6:08:22 AM</td>
<td>test1VM1</td>
<td>Infected</td>
<td>Agent status unknown</td>
<td>44 infected items found</td>
<td>1/20/2020 3:51:36 AM</td>
</tr>
<tr>
<td></td>
<td>Envine Web Portal</td>
<td>Need to scan</td>
<td>Agent status unknown</td>
<td>Not scanned</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DEV-DCNODE1</td>
<td>Need to scan</td>
<td>Agent status unknown</td>
<td>Not scanned</td>
<td></td>
</tr>
</tbody>
</table>

Here you can get the following information:

- Last scan date and time.
- VM name.
- Antivirus job status.
- Active protection status.
- Message – last scan brief result (if it has ever occurred).
- Signature – timestamp.

From this window, using standard controls in the top menu, you can change page layout settings, print the report, or export data to MS Word, MS Excel or PDF file formats.
4.8.4 Antivirus events history

To review antivirus events history, use the View – Antivirus events main menu command. You may filter events in the Antivirus notifications window:

To filter events, set start and end period, then click the Filter button. Upper field will display the list of VMs that had malware events during the selected period. Select a VM to view its events in a middle field. Select event to view its status message.

4.8.5 Active protection

Active protection controls your system in real time by using the active protection agent. This agent should first be installed separately on each virtual machine that needs protection. Go to the Antivirus – Active protection tab of Acronis Cloud Security's main window.

Acronis Cloud Security detects the presence of the active protection agent on a particular virtual machine. There is an ability to automatically detect and install the active protection agent on VMs except ones that are marked as exclusions (please refer to the "Active protection auto installation and update" (p. 124) paragraph above).

If there is no active protection agent installed on the virtual machine, the Install agent button will be available on the Active protection tab:
If the agent is already installed on the virtual machine, the **Remove agent** button will appear on the **Active protection** tab instead. In addition you can also update the virus definitions used by active protection agent:

![Active Protection Tab](image)

**Note**

Make sure there are no other active protection agents or antivirus software active on virtual machines as problems and conflicts may occur.

- To install the active protection agent on the virtual machine, click the **Install agent** button on the **Active protection** tab. Acronis Cloud Security will evoke AP agent installation onto the current virtual machine.
- To remove the active protection agent from the virtual machine, click the **Remove agent** on the **Active protection** tab. Acronis Cloud Security will evoke AP agent uninstall from the current virtual machine.

**Note**

Each time you click the **Install agent** or **Remove agent** buttons, the current virtual machine gets the *reboot required* status. The reboot is required to install and remove active protection agent software to/from the guest OS. It is then up to user when to reboot the target virtual machine. Please refer to the "Reboot action" (p. 144) subsection for more information.

- To force the AP definitions update, click the **Update AP definitions** button. Normally, AP definitions are updated automatically. In some cases, you may need to force the update on a particular VM, e.g., if it’s excluded from automatic definitions updates (please refer to the "Active protection auto installation and update" (p. 124) paragraph above).

Click the **Refresh** button to immediately get the current active protection agent and signatures status.
Active protection integrity control

Active protection integrity control is intended to ensure active protection agent components and databases are consistent and have not been altered outside of a regular update process. To start the active protection integrity control job run the **Antivirus wizard** by selecting the **Create job** drop down menu on the upper left side of the **Antivirus jobs** tab and select the **Active protection integrity control** item.
Name the job and click **Next**. Then select the entities to be checked:

Mark objects to include into the job. Use filter for convenience. Click **Next**.
Set the job schedule:

Review all settings and submit the new job:
The job will appear in the Antivirus jobs tab if the job runs immediately and in the AV scheduled jobs tab if it is scheduled or deferred job. As a result there will be report and corresponding job status informing if a VM successfully passed the check.

4.8.6 Quarantine

All threats that are found and caught by the active protection agent or during agentless anti-malware scan are moved to the designated quarantine folder, located on each virtual machine at the following destination:

- For agentless antivirus: `C:\5nine.QAR`;
- For AP agent, depends on AV engine:
  - Bitdefender AV engine: `C:\Program Files (x86)\5nine\5nine ActiveProtection\Quarantine`
  - ThreatTrack AV engine: `C:\ProgramData\5nine, Inc\AntiMalware\Quarantine`

All quarantine events are displayed on the Antivirus jobs tab in the lower part of the main window:

To filter events click the Enable filter button:

- **Event time**: Date range to display desired events
- **Action**: All actions or any of the selected actions:
  - **All**
  - **Unquarantine**
  - **Quarantined files delete**
  - **Quarantine Pending**
  - **Quarantine Delete**
  - **Quarantine Failed**
  - **Duplicated**

- **Event type**:
  - **All** – to display all events;
  - **Antivirus** – display agentless antivirus events;
  - **ActiveProtection** – to display active protection agent events.
You can control the threats that are moved to the quarantine folder. You can take the following actions:

- **Restore.** This action restores the file back to its original location (or cancels disinfect action). Those files will be added to the *allowed threats* list and remain in the allowed state in the system until they are removed from the allowed list as described above (please refer to the "Antivirus and active protection settings" (p. 112) subsection). To restore the quarantined or disinfected threat, select it, and then click the **Restore** button.

- **Remove from quarantine.** This action permanently deletes the threat from the quarantine folder. To remove a threat from quarantine, select it, and then click the **Remove from quarantine** button.

You also can control the threats that are pending quarantine before they get treated:

- **Cancel quarantine.** This action immediately interrupts processing the selected file and leaves it at its original location.

- **Remove file.** This action permanently deletes the threat from its original location without moving it to quarantine as it’s scheduled. The action will be done upon reboot of the guest OS.

You may also track the treatment history of any threat. Double click on the wanted record to view the actions that had been done with the particular threat:

To export events to the .xls file, right-click on any of the events and then select the **Export to file** context menu item:
Then select the destination folder to save the file and click **Save**:

![Save File Dialog](image)

### 4.8.7 Reboot action

Reboot action is required on the virtual machine in the following cases:

- To move threats that were detected by the agentless anti-malware scan to quarantine folder or disinfect files or delete them from the original location, depending on the action;
- To remove threats from quarantine or restore threats;
- To install active protection agent into guest OS.

Acronis Cloud Security will prompt you each time the reboot action is required and it is up to you when to do it. You will see the current reboot status for each VM in the lower status bar that is displayed on the **Reboot action** tab of the Acronis Cloud Security main window, and be able to control it:

![Reboot Action Tab](image)
Click the **Refresh** button to immediately update current information of what actions are required VM reboot. This information is also updated automatically.

If there are such actions, then the following reboot options will be possible and the corresponding buttons will appear:

- Immediate reboot of the target VM. To evoke it, click the **Reboot now** button. Selected virtual machine will be rebooted immediately.

- Delayed (scheduled) reboot of the target VM. To set the delayed reboot, click the **Reboot scheduler** button.

Then set the date and time when you would like the target VM to be rebooted and click **OK** in the **Reboot scheduler** dialog:

![Reboot Scheduler Dialog](image)

The selected virtual machine will be rebooted automatically at this time.

### 4.8.8 Anti-ransomware

Anti-ransomware is a part of active protection feature. It is available in the Acronis Cloud Security version with Bitdefender AV engine only. This feature actively protects virtual machine against malicious processes by preventing them from an execution of unwanted/unauthorized actions with the files and folders inside the guest OS. To use anti-ransomware protection on the particular VM, active protection agent must be installed into the guest OS (please, refer to the “Active protection” (p. 137) paragraph above). Anti-ransomware protection monitors the registered paths, which should be created in advance (or exist) in the guest file system, and prevents malicious processes from executing actions/making changes in these folders. There are processes, which are marked as trusted in the antivirus engine by the provider (mostly standard Microsoft desktop applications and the other commonly used and well-known tools like Notepad, Notepad++, Paint etc.) and the anti-ransomware feature does not apply any action against such programs. There is also the configurable custom list of trusted processes, in which certain programs can be included by the security administrator so the anti-ransomware feature ignores them. These settings are described above in the “Antivirus and active protection settings” (p. 112) – “Configuring policies” (p. 115) – “Anti-ransomware” (p. 122) paragraph.

Anti-ransomware events are displayed on the **Antivirus – Anti ransomware** tab of Acronis Cloud Security’s main window:
It shows the target object, event time, the process with the path and blocked path. The filter is available to display the events by the required date range:

You may copy the particular path into the clipboard by clicking the **Copy path** button in the upper-left corner of the tab.

## 4.9 IDS

The Intrusion Detection System (IDS) allows detection\(^1\) of intrusion attacks, review of the event log and setting the blocking virtual firewall rule on the suspicious IP address.

### 4.9.1 Enabling IDS

IDS feature is disabled on all virtual machines and host network adapters by default. To enable IDS on the virtual machines or for Hyper-V hosts’ network adapters that are connected to the virtual switch, open the **IDS settings** dialog window using the **Settings – IDS** main menu item:

---

\(^1\)Detection of intrusion attacks is done through IDS – Snort ® ([www.snort.org](http://www.snort.org)) – third-party freely distributed application that is able to determine whether certain inbound traffic is considered as an intrusion with Snort for Business rule subscription included.
On the **Enable IDS** tab check the boxes against the VMs or host network adapters on which IDS should be enabled. Type the symbols which a VM name must contain into the **Filter** field to filter the tree. Those VMs that have been pre-selected will not be filtered off the tree even if they do not match the filtering criteria. Click **OK**.

### 4.9.2 IDS updates

IDS updates are set on the **Updates** tab:
The following operations are available:

- Check the last definitions update info per each host;
- Manually evoke immediate definitions update by clicking the Update button for a particular host or the Update all button to perform update for all hosts;
Configure the proxy server by clicking the **Proxy settings** button:

![Proxy Settings Window]

- Set the automatic definitions update frequency in minutes (the default period is 120 minutes).

### 4.9.3 Viewing IDS logs

The IDS log is displayed on the **IDS** tab. To view IDS events, click the **Load log** button in the left-upper corner.
Check the **Enable filter** box to turn on the filter so that only IDS events matching filter parameters will be displayed.

Set the start date for IDS events in the **From** field and the end date in the **To** field. Use the calendar feature for convenience.

Set event priority in the **Priority** field. Select the priority **1, 2, 3** or **Any** (for all priorities) from the list.

Each column in the list can be sorted by clicking on the desired one. There is also a right click menu for each column that allows for further customization on sorting, grouping choosing columns to add and removing. Column order can be changed by dragging and dropping.
Email notifications are available to inform admins about possible intrusions – IDS events. Please refer to the “Notifications” (p. 159) subsection below for details.

4.9.4 Block suspicious IP address

To block the traffic flow from the suspicious address, right-click the event and select the **Add rule** command. You will be offered to create the blocking virtual firewall rule with pre-defined parameters:
As it’s shown on the picture, you are advised to block all IP traffic from the address-aggressor and it is strongly recommended to leave these default settings. However, you are still able to alter the rule parameters in the standard way as it is described above in the “Configuring virtual firewall rules” (p. 64) section.

4.9.5 Exporting log

To export the log into the .xls file, right-click any event and select the Export to file command.
Then select the destination folder and type the file name to save. Click **Save**:

![Save As dialog box](image)

### 4.10 Network anomalies

Network anomalies detection is intended to determine whether traffic on a particular VM differs from normal level. Acronis Cloud Security automatically analyzes network statistics on monitored VMs for the period of last week, then splits the data for the last day by hours and sends notifications if the traffic skew factor is equal to or greater than 1.4. The following parameters are measured: the amount of traffic, packet size, the number of packets.

This feature is configurable for particular VMs. To enable network anomalies detection on VMs, go to **Settings – Network anomalies** main menu:
Select VMs to enable the network anomalies detection feature on, and click OK.
To view network anomalies report, select VM in the object tree, go to the **Network anomalies** tab and click the **Load log** button. Use filter to set the time period if necessary.

![Network anomalies report](image)

### 4.11 Acronis AzSec and Acronis Cloud Security integration

If you also have purchased Acronis AzSec, additional functionality will be available in the Acronis AzSec console when Acronis Cloud Security is also installed. A statistics tab will be shown with inbound and outbound network traffic for the specified time range gathered from the Azure
firewall logs.

4.12 Network traffic scanner

The network traffic scanner allows detection of malware that might be downloaded to the virtual machine with http inbound traffic and review the event log.

4.12.1 Enabling network traffic scanner

Network traffic scanner feature is disabled on all virtual machines by default. To enable network traffic scanner on the virtual machines, open the **Antivirus settings** dialog window using the **Settings – Antivirus** menu item:
On the Traffic scanner tab check the boxes against the VMs on which IDS should be enabled. Type the symbols which a VM name must contain into the Filter field to filter the tree. Those VMs that have been pre-selected will not be filtered off the tree even if they do not match the filtering criteria. Click OK.

### 4.12.2 Viewing network traffic scanner logs

The network traffic scanner log is displayed on the Network traffic scanner tab:

Events normally appear in the log automatically. Click the Refresh button to facilitate retrieving of the fresh events.

Email notifications are available to inform admins about http malware events. Please refer to the "Notifications" (p. 159) subsection below for details.

### 4.13 Connections table

The list of current connections is displayed for each virtual machine (the virtual firewall must be turned on):

Click the Update button to get the current connections list for the selected virtual machine.

You can set certain connection parameters to filter the list in the way you want it to be displayed, e.g. to find the exact TCP session in the connections table. Set the connection parameters you need to see and click the Update button:
The connections table will be filtered.

**Note**
In the current version of Acronis Cloud Security the connections table feature can be used in observation mode only.

### 4.14 Network statistics

Network statistics are displayed on the VM level for each VM separately, on the **Statistics** tab:

Display options available:
- **Traffic** – displays traffic in Mb;
- **Packets** – displays packets amount;
- **Packet size** – displays packets size in bytes.
Traffic types are distinguished by a color (bytes in – blue, bytes out – green, bytes blocked in – purple, bytes blocked out – pink).

Export format options available: Excel, PDF, MS Word. Or the report can be printed out right from the console with possibility to adjust page parameters – use print/page setup buttons to set up page parameters to print.

Use the calendar in the Report date field to set the date for network statistic report.

### 4.15 Notifications

Acronis Cloud Security has two types of notifications: console notifications and email notifications. Console notifications give immediate online information about various events to administrator who has the management console opened on the computer. Email notifications are sent offline to specified emails to inform those whom required.

#### 4.15.1 Console notifications

Console notifications appear under the **Notifications** entity in the object tree:

To drag the attention, the corresponding branch is highlighted with the bold font when the fresh/unread events appear. Console notifications include the following security events:

- Network anomalies events.
- Antivirus events.
- IDS events.
- Internal events.
- Virtual firewall events.

When the root branch **Notifications** is selected in the object tree, the total counts are displayed on the right side of the management console:
Select the branch you need to review to see the details of the certain type of events. Example, antivirus events:

The notifications will be erased immediately after watching when the navigation is moved to another object in the management console and the corresponding counter will be reset to 0 until the new events appear.

4.15.2 Email notifications

Email notifications are sent for the following security events:

- IDS.
- Antivirus.
- Network traffic scanner.
- Network anomalies.
- Host components state.

To set up email notifications, open the Email notifications window with Settings – Email notifications menu item:
Set the notifications parameters:

- Check the **Enable notifications** box to enable email notifications.
- Select which security events must be sent via email notifications:
  - Check the **Intrusion detection system** box to include IDS events into email notifications.
  - Check the **Antivirus** box to include antivirus events into email notifications.
  - Check the **Network traffic scanner** box to include inbound http traffic events into email notifications.
  - Check the **Network anomalies** box to include network statistics anomalies into email notifications. Acronis Cloud Security automatically analyzes network statistics on monitored VMs for the period of last week, then splits the data for the last day by hours and sends notifications if the traffic skew factor is equal to or greater than 1.4. The following parameters are measured: the amount of traffic, packet size, the number of packets. Notification shows virtual machine with detected traffic anomaly and the hour of the day during which this anomaly had been detected.
  - Check the **Host components state** box to include host components state events to email notifications.
- Set the notification period (select value between 1 min – 24 hours from the list). The default value is 1 minute.
- Specify the SMTP server address and port.
- Check the **Enable SSL** box in the case SSL authentication is required to access the SMTP server. Then set the login and password for the user (SMTP administrator).
- Specify the sender’s email address.
- Specify the recipients’ email addresses separated by semicolon.
Click **OK** to save the settings and close the **Email notifications** window.
4.16 Syslog server integration

Acronis Cloud Security supports integration with external Syslog server. To let virtual firewall, IDS, agentless antivirus and active protection events be sent to an external Syslog server, call out the **Syslog server settings** dialog box with **Settings – Syslog** menu item, enable syslog server logging and set the IP address where it’s running:

- Enable syslog server logging to turn this option on.
- Enable RFC5424 header if necessary\(^1\).
- Type the syslog server IP address.

---

\(^1\)Some external syslog servers require RFC5424 standard header support (e.g., Splunk ® syslog server), whereas the others do not (e.g., SolarWinds ® syslog server) and won’t function if this option is enabled. Contact your system administrator to determine if your external syslog server requires RFC5424 header support!
Example of external syslog server function with Acronis Cloud Security (Splunk® syslog server is shown):

The above screen capture shows IDS events appearing in the Splunk event log loaded from Acronis Security IDS event log.

If you have Syslog configured and are also running Acronis AzSec you can export the Azure firewall logs saved with Acronis AzSec from the Acronis Cloud Security Tools – Import Azure firewall log menu:
Then select the desired logs from the directory where the logs were saved in Acronis AzSec:

Log is forwarded to Microsoft Operations Management Suite (OMS) from Acronis Cloud Security.

Target Syslog server requires OMS agent configured to forward syslog messages to the OMS Log Analytics platform

See the following link for more information: [Syslog Collection in Operations Management Suite](#).

### 4.17 Disaster recovery

Having multiple management servers installed on different servers (host(s) and/or VMs) in Windows Server/Hyper-V environment instead of using just a single one on a single server, provides disaster recovery. Management server that is currently taking control over the environment is a primary management server. The other one(s) are backup management server(s). When the primary management server becomes unavailable, the next backup management server takes over the control. It is also possible to switch the management servers manually.

After the installation of Acronis Cloud Security components, there is only one active management server – the one that had been installed and specified during host management service and management console installation (refer to the "Installation" (p. 10) section above). With just a single management server the product will function in the ordinary mode without disaster recovery. The following subsections below describe disaster recovery functionality and setting it up.
4.17.1 Disaster recovery functionality

Multiple management servers running management service instances are connected to their own separate data source each, having separate database vFirewall.

Management servers exchange and replicate the following data:

- Managed Hyper-V hosts list and settings.
- Virtual firewall rules and VMs’ monitoring statuses.
- Antivirus and active protection settings and VMs’ antivirus statuses (for scheduled scans).
- Global security groups and tenants.
- Syslog server integration settings.
- Notifications settings.
- VM connections table (the feature is not replicated but works independently from management server and VM connections are displayed similarly no matter which management server is currently taking control).
- Management servers list itself.

The data is replicated in real time from any of the management servers, to which the management console is connected when applying the changes, no matter whether it is a primary or a backup one.

Management servers do not exchange the following data:

- Virtual Firewall and IDS log records.
- Antivirus, active protection (including quarantine) and anti-ransomware log records and unfinished jobs.
- User’s actions.

That data remains at the management server at which it occurred. Log recording will start on the management server the moment it becomes the primary server and stops recording when the other one takes control.

**Important**

In the current version of Acronis Cloud Security, Antivirus, Active protection and Anti-ransomware functions are not replicated between management servers! This means that any action – install/remove AP agent into guest OS, run agentless anti-malware scan and subsequent reboot actions must be completed with the management server they had been evoked without switching to the other one. In the case management servers were switched before completing the reboot action, you will have to set the first management server back to complete them.

4.17.2 Configuring disaster recovery

To set up disaster recovery, do the following:

- Install the additional management service instances onto other host(s) and/or designated virtual machines as you chose to be backup management servers. This is done in the similar
way as when installing the first instance of management service (refer to the "Installation" (p. 10) – "Management service" (p. 11) section above). The recommended number of management servers is 2-3 servers in general case. It depends on available resources at the data center. Note that each one should connect to its own separate data source (SQL instance).

- Go to the management console connected to the first management service and select the 
  **Settings – Management servers list** item from the menu:

- In the **Management servers list** dialog box edit the management servers list:

- Click the **Add** button to add another management server to the list:

  Type the hostname, FQDN or IP address of the management server and click **OK**.

- Select the management server and click the **Move up** button to bring the target server to the one position up. The top one will become the primary management server and will immediately take over the control. The second one will take over the control if the top one becomes unavailable, etc.
Select the management server and click the **Move down** button to bring the target server to the one position down.

Select the management server and click the **Remove** button to remove it from the list. Click **OK** in the **Management servers list** dialog box to complete the disaster recovery setup operation.

### 4.18 Distributed management

The distributed management service is a new feature in Acronis Cloud Security that allows multiple concurrent management services to run in an environment providing greater scalability. Administrators can choose to group their Hyper-V hosts to specific management services based on location, workload, logical or any desired criteria. This feature is designed to improve performance at scale for the largest deployments of Hyper-V, many of which are distributed across multiple data centers.

This feature expands on Cloud Security’s existing capability for multiple management servers for high availability and disaster recovery. Configurations are distributed and synchronized between all of the management services for resiliency. Should a management service become unavailable, the host group will then use the next available management service with all of the existing configurations.

The administrator can associate each host group with a specific management service from the available list. Once configured the resulting hosts will communicate with the specified instance of the management service to receive notifications, get configurations and send logging data.

If the management service associated with the current host group is not available – host group will use first available management service from the servers list (as it was implemented earlier for DR scenario). This feature allows significant reducing and distributing management service load, thus improving performance for large size distributed environments (speed of applying rules changes, loading logs etc. increase by several times for large distributed deployments).

It is also especially useful for geographically distributed environments. Admin can configure to use local management service instead of remote server. But at the same time all settings will be distributed to all servers. Majority of communication between Cloud Security components is logs transfers. In this configuration it will use faster local connections instead of WAN which will also reduce cost.

From user experience there are no significant changes except the speed of operations for large distributed environments as it avoids overloading the management service.

To arrange grouping hosts for distributed management, the new command **Add hosts group** appears now in the **Hosts** menu of management console:
<table>
<thead>
<tr>
<th>Hosts</th>
<th>Rules</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Host</td>
<td>Remove Host</td>
<td>Add Hosts Group</td>
</tr>
</tbody>
</table>
The **Host group properties** dialog window is used to create and edit host groups:

![Host Group properties dialog window]

A host can be added into a single group only, their appearance depends on this when adding – those that are already added into a group will not be displayed:

![Select hosts dialog window]
The object tree gets the new structure when hosts are added into groups:

To map management servers to host groups, the new controls are implemented in the DR server's settings:
The **Hosts map** button opens the **Management servers map** window where mapping is configured:

![Management Servers Map](image)

Management servers are listed on the left side. Selecting the server will display host groups it mapped to. There can be several host groups mapped to a single management server, but not the opposite. When adding host groups they are displayed corresponding to their availability – only those that have not been mapped will appear:

![Select objects](image)

Once mapping is done, the management process will occur in the corresponding manner as described above.

**4.19 Configuring VM settings**

To change virtual machine settings, select the necessary virtual machine in the tree on the left. Then click the **VM settings** button on the top menu panel or use the **VM settings** context menu item.
The following dialog will display:

On the **Common** tab you can manually define the VM IP address, set logging parameters such as retention length in days, log records count and bandwidth – allowed send/receive limits for the virtual machine service.

The **VM name** field displays the virtual machine name. The **VM ID** field displays the virtual machine ID – this parameter will be needed for authorization in the case virtual firewall rules with authorization are used (please refer to the "Configuring virtual firewall" (p. 104) – "Authorization" (p. 85) section for detailed information).

Check the **Define IP manually** box to set the VM IP address for Acronis Cloud Security manually. In most cases you don't have to do this, because normally the IP address is detected automatically by Acronis Cloud Security. However, there are certain situations when this option is needed, such as with non-Windows OS based VMs, when Acronis Cloud Security is unable to automatically detect VM IP
configuration. In the cases like this it is necessary to manually determine IP address so that Virtual Firewall rules work for this kind of virtual machines.

Enter a single IP v4 or IP v6 IP address (as applicable), which are assigned to the VM, in the IP Addresses field – only single value is accepted. If Acronis Cloud Security gets the IP addresses from the VM IP network settings automatically, you will see them in this field when this dialog box opens – there is no need to define them manually in this case.

**Note**
The IP address that is set here manually does not affect actual IP settings on a virtual machine. It is only used by Acronis Cloud Security to analyze the virtual machine traffic and properly apply virtual firewall rules in the case it is unable to automatically detect it.

Set virtual firewall logging parameters on the **Firewall** tab:

Select the logging level from the list.

- **Filtered** – only filtered VM events will be recorded to the log.
- **Allowed** – only allowed VM events will be recorded to the log.
- **All** (default) – all VM events except SPI packets will be recorded to the log.
- **No logging** – neither of the VM events will be recorded to the log.
- **Allowed and SPI** – allowed VM events and allowed SPI packets will be recorded to the log.
- **All and SPI** – all VM events including SPI packets will be recorded to the log. It is the maximal logging level.

Enter the number of days to keep the log records in the **Log retention days** field.

Enter the maximum number of records that will be added to the log in the **Log records count** field.

Set the log size and retention for the IDS logs on the **IDS** tab in the same way.
Set the log size and retention for the antivirus logs on the **Antivirus** tab:

![Antivirus Log Configuration](image)

Set the log size and retention for the network anomalies logs on the **Anomalies** tab:

![Anomalies Log Configuration](image)

Set bandwidths allowed send/receive limits:

- Enter the maximum (in Kbps) allowed send bandwidth limit in the **Allowed send bandwidth (Kbps)** field.
- Enter the maximum (in Kbps) allowed receive bandwidth limit in the **Allowed receive bandwidth (Kbps)** field.

Tick the **Packet integrity check** box to enable CRC check in the packets towards the VM. If this option is enabled, any traffic allowed by any rule for this virtual machine will be put to CRC check. If the sum is incorrect or corrupted the packet will be dropped. Some network devices might not be compatible with this option and therefore normal traffic will be blocked if CRC check is enabled. In such cases it is recommended to leave this option disabled.
On the **Member of** tab you can determine to which user defined security groups a VM will be assigned:
To add a new security group, click **Add**. In the **Select VM groups** dialog box select the necessary groups and click **OK** to add the selected groups to the VM:

![Select VM Groups dialog box]

You may select several groups by holding the **Shift** or **Control** buttons pressed on your keyboard while doing the selection:

![Select VM Groups dialog box with selected groups]

All the groups created by any user will be seen here if you work under the global administrator. If you work under a tenant user, only those groups created by this tenant's users will be displayed and available to be assigned to the VM.

The rules of the assigned security groups will then be applied to the VM. Please refer to the "Configuring virtual firewall rules" (p. 64) section above for details of how the user defined security groups and virtual firewall rules are set.

### 4.20 Host settings and state

To change host settings, first select the necessary host in the tree, then use the **Settings** context menu item.

The **Server properties** dialog box will open:
Set the authentication parameters as described in the "Adding and removing hosts" (p. 49) section above.

Acronis Cloud Security displays current state and recent history for each managed Hyper-V host. This information is shown on the Host state tab when the host is selected in the object tree:

The upper field shows current host state. The following components on the host are monitored: services 5nine.Antivirus.Agent, 5nine.VirtualFirewall.HostManagementService, 59CBTService; and the Hyper-V virtual switch filtering extension 5nine vFW extension (filtering driver).

The lower field shows the recent history for each component if there were problems and the moment they had gone.
4.21 Refreshing the object tree

To refresh or change the view (list or tree), go to the **View** menu and select the **Refresh** command:

![Object Tree Menu]

5 Acronis Cloud Security information

To get the Acronis Cloud Security version/user license information, use the **Help – About** menu item:

![Help Menu]

The **About Acronis Cloud Security** window will show the Acronis Cloud Security version info.
and the licensing information (also refer to the “Licensing” (p. 180) section below):
6 Licensing

Acronis Cloud Security is available in three editions based on the size of the virtualized environment being secured:

- Standard Edition: A single license covers 6 VMs – Min 16 cores & 2 CPUs
- Enterprise Edition: A single license covers 20 VMs - Min 16 Cores & 2 CPUs
- Datacenter Edition: A single license covers unlimited VMs - Min 16 Cores & 2 CPUs

If you need a greater number of virtual machines to be monitored and protected by Acronis Cloud Security, you are able to purchase additional licenses for the required virtual machines.

The license is also time limited. When it's expired, virtual firewall will be turned off automatically and scheduled antivirus scans will be disabled on those VMs that have been set on virtual firewall and/or scheduled antivirus scans.

You can get information about currently and previously installed licenses, installation and expiration dates, total VMs amount allowed by the license and number of VMs currently in use in the About Acronis Cloud Security window as described in the “Acronis Cloud Security information” (p. 178) section above.

Open the Licensing dialog with Help – Install license menu item to install the new license:

![Licensing dialog](image)

Then, browse to the license .txt file or copy-paste/Manually type the path to it and click OK.

**Note**
When updating the license in the environment with disaster recovery or HA set, you will have to install the new license onto each of management servers separately.

6.1 Core-based licensing overview

- All physical cores in the server must be licensed. Servers are licensed based on the number of processor cores (CPUs) in the physical server.
- A minimum of 16 core licenses is required for each server.
- A minimum of 8 core licenses is required for each physical processor.
- Additional 2 core packs can be purchased for servers with higher core densities.
7 FIPS support

Acronis Cloud Security supports Federal information processing standard (FIPS) algorithms to comply with security standards, usually present in government organizations. If such standards are used and Windows Server has this security option enabled on the machines where Acronis Cloud Security management service and management console are installed, the corresponding settings should be configured either before Acronis Cloud Security installation (with the corresponding option on the main screen of the setup application – preferable way) or after the installation. Second way will require editing configuration files of both components and restarting of the services. Same thing will be required if FIPS is getting disabled in Windows Server where Acronis Cloud Security is already installed and has this mode enabled.

To change FIPS compliance mode on the installed product, need to change the following configuration files:

- For the management server: C:\Program Files\5nine\5nine Cloud Security Management Service\5nine.VirtualFirewall.ManagementService.exe.Config.
- For the management console: C:\Program Files\5nine\5nine Cloud Security Management Console\5nine.VirtualFirewall.ManagementConsole.exe.Config.

In the appSettings section of these configuration files, edit the FIPSCompliantMode key value from false to true (or vice versa):

```
<appSettings>
  ...
  <add key="FIPSCompliantMode" value="true" />
  ...
</appSettings>
```

The value true will enable FIPS compliance mode, the value false will disable it. This setting should match the corresponding security setting configured in Windows Server on the machine, where the corresponding component is installed.

After saving changes in the configuration files, the management console and management service will need to be restarted to apply FIPS compliance mode.

8 Compatibility with other Acronis products

Acronis Cloud Security is compatible with Acronis Cloud Manager and Acronis Manager Standard (version without antivirus feature). Acronis Cloud Security is incompatible with Acronis Manager Standard with antivirus. Acronis Cloud Security uses the same services for antivirus feature on managed hosts as Acronis Manager Standard with antivirus – 5nine.Antivirus.Agent and 59CBTService. These services will conflict if they are managed by both products on the same host. Acronis Cloud Security management service and Acronis Manager Standard with Antivirus management service also use the same programmatic interface and also cannot be placed on the same machine as they will also run into a conflict resulting in a failure of the antivirus feature. Therefore it is recommended to use Acronis Manager Standard without
antivirus or Acronis Cloud Manager (for large deployments) in the environments that are protected by Acronis Cloud Security, which will cover anti-malware functionality instead of Acronis Manager Standard with Antivirus. In the case there are separate hosts in the data center that are not designated to be managed by Acronis Cloud Security, it is possible to use Acronis Manager Standard with Antivirus on these hosts, making sure the antivirus management service is not placed on the same machine with Acronis Cloud Security management service.

9 Acronis Cloud Security log files

Acronis Cloud Security writes the following log files that are used to troubleshoot the product and contains information of its activity:

<table>
<thead>
<tr>
<th>Log file name</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management server file system</td>
<td>C:\ProgramData\Snine\Snine Cloud Security for Hyper-V\Logs\Management Service\</td>
<td>Contains information related to central management service activity</td>
</tr>
<tr>
<td>YYYY-MM-DD ManagementServiceLog.txt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Starter.log</td>
<td>C:\Program Files\Snine\Snine Cloud Security for Hyper-V Management Service\Logs\</td>
<td>Contains information related to recurrent agentless anti-malware scans</td>
</tr>
<tr>
<td>YYYY-MM-DD.txt</td>
<td>C:\ProgramData\Snine\Snine Update Service\Logs\</td>
<td>Contains information related to antivirus update service activity</td>
</tr>
<tr>
<td>{VM ID}</td>
<td>C:\CloudSecurityLogs\(default)</td>
<td>Virtual firewall logs</td>
</tr>
<tr>
<td>Host/VM(s) file system where management console is installed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>YYYY-MM-DD ManagementConsoleLog.txt</td>
<td>C:\ProgramData\Snine\Snine Cloud Security for Hyper-V\Logs\Management Console\</td>
<td>Contains information related to activity on management console</td>
</tr>
<tr>
<td>Managed host file system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>YYYY-MM-DD HostServiceLog.txt</td>
<td>C:\ProgramData\Snine\Snine Cloud Security for Hyper-V\Logs\Host Service\</td>
<td>Contains information related to host management service activity</td>
</tr>
<tr>
<td>vFWFilteringPlatform.log (hidden)</td>
<td>C:\ProgramData\Snine\Snine Cloud Security for Hyper-V\</td>
<td>Contains information related to virtual firewall rules applicability</td>
</tr>
<tr>
<td>vFWFilteringPlatform.log (hidden)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Snine.Antivirus.AgentService.log</td>
<td>C:\ProgramData\Snine\Snine Cloud Security for Hyper-V\</td>
<td>Contains information about</td>
</tr>
<tr>
<td>Log file name</td>
<td>Location</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Antivirus Agent\Logs\</td>
<td><strong>Antivirus</strong> agent\Logs\ (including anti-malware scans tracking) and active protection agent activity on the current host and its virtual machines.</td>
<td></td>
</tr>
<tr>
<td>Guest file system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>log.txt</td>
<td>C:\Program Files (x86)\5nine\5nine ActiveProtection\Logs\</td>
<td>Contains information related to active protection agent activity for Bit Defender antivirus engine.</td>
</tr>
<tr>
<td>APAgentSvcLog.csv</td>
<td>C:\ProgramData\5nine, Inc\5nine Hyper-V Agent\Logs\</td>
<td>Contains information related to 5nine.AP.Agent service activity for ThreatTrack antivirus engine.</td>
</tr>
<tr>
<td>SBAMSvcLog.csv</td>
<td>C:\ProgramData\5nine, Inc\AntiMalware\Logs\</td>
<td>Contains information related to SBAMSvc service activity for ThreatTrack antivirus engine.</td>
</tr>
<tr>
<td>SBAMThreatEngineLog.csv</td>
<td>C:\ProgramData\5nine, Inc\AntiMalware\Logs\</td>
<td>Contains information related to threat engine activity for ThreatTrack antivirus engine.</td>
</tr>
</tbody>
</table>

### 10 Configuring Acronis Cloud Security network manager plugin

This section is only applicable to those environments that are running under Microsoft System Center Virtual Machine Manager with enabled SCVMM-based logical switches where it is necessary to get those switches to compliant state with Acronis Cloud Security filtering extension.

Upon installation of Acronis Cloud Security network manager plugin, do the following actions on your SCVMM server to complete Acronis Cloud Security network manager plugin configuration:

1. Restart SCVMM service. Re-open SCVMM management console, make sure you do it with administrative privileges *(Run as administrator)*.
2. Go to Settings – Configuration Providers. Check that 5nine Cloud Security network management provider is present in configuration providers list.
3. Create Network service in SCVMM:
   - Go to Fabric – Networking – Network service – (right click) Add network service;
   - Name the network service (e.g. Cloud Security filtering service);
   - Select 5nine Software, Inc – CloudSecurity manager;
- Enter credentials. The best way is to add current domain user account that has all necessary permissions;
- Connection string: localhost;
- Host group: check All hosts
4. Go to Fabric – Networking – Logical switches:
   - Right-click on the logical switch – Properties;
   - Select Extensions;
   - Check the box against the new 5nine Cloud Security filtering extension.
   - Click OK.
5. Check that logical switch extensions order in SCVMM console and Hyper-V manager match for each Hyper-V host. Alter the order if necessary by using the Move up/Move down buttons.
6. Go to Fabric – Networking – Logical switches:
   - Select Hosts on the main pane;
   - Select logical switches that are in the Not compliant state.
   - Remediate the logical switches that are in the Not compliant state.
   - Wait until the state of logical switch becomes Compliant.

Note
You might have to refresh the hosts that do not run Acronis Cloud Security host management service (in the case you have those in your environment) when the remediate action is completed to get the logical switches to the compliant state on such hosts!

11 Uninstall

To uninstall Acronis Cloud Security components from your servers, use the same Acronis Cloud Security for Hyper-V setup application as when installing the product:
Select the necessary component, click **Uninstall** and confirm the operation.

## 12 Appendix – Firewall log reason entry descriptions

The following is a list of possible entries and their descriptions in the firewall log for the **Reason** column. Please see the "Virtual firewall logs" (p. 106) section for more information about the firewall log.

### 12.1 Action allow reasons

- **Empty** – connection allowed by firewall rule.
- **New** – packet allowed and new entry was added into SPI table.
- **SPI** – packet allowed by SPI.

### 12.2 Action block reasons

- **Filtered** – packet was blocked by existing rule with block action.
- **NoRule** – packet was blocked as there was no rule allowing this packet.
- **BadSize** – bad packet size, either it was corrupted or is being used for some attack.
- **UnknownPacket** – packet blocked as IP version is different from IPv4 or IPv6, probably corrupt.
- **InvalidState** – blocked packet as invalid packet connection phase detected by SPI.
- **LowMemory** – packet blocked as firewall is unable to handle it due to insufficient free memory.
- **NullScan** – packet blocked, null scan attack.
- **FinScan** – packet blocked, fin scan attack.
- **XmasScan** – packet blocked, Xmas scan attack.
- **InvalidFlags** – packet blocked because of invalid TCP flags.
- **BadCRC** – bad packet CRC.
- **Dns** – packet was blocked by DPI rule with DNS conditions.
- **Http** – packet was blocked by DPI rule with HTTP conditions.