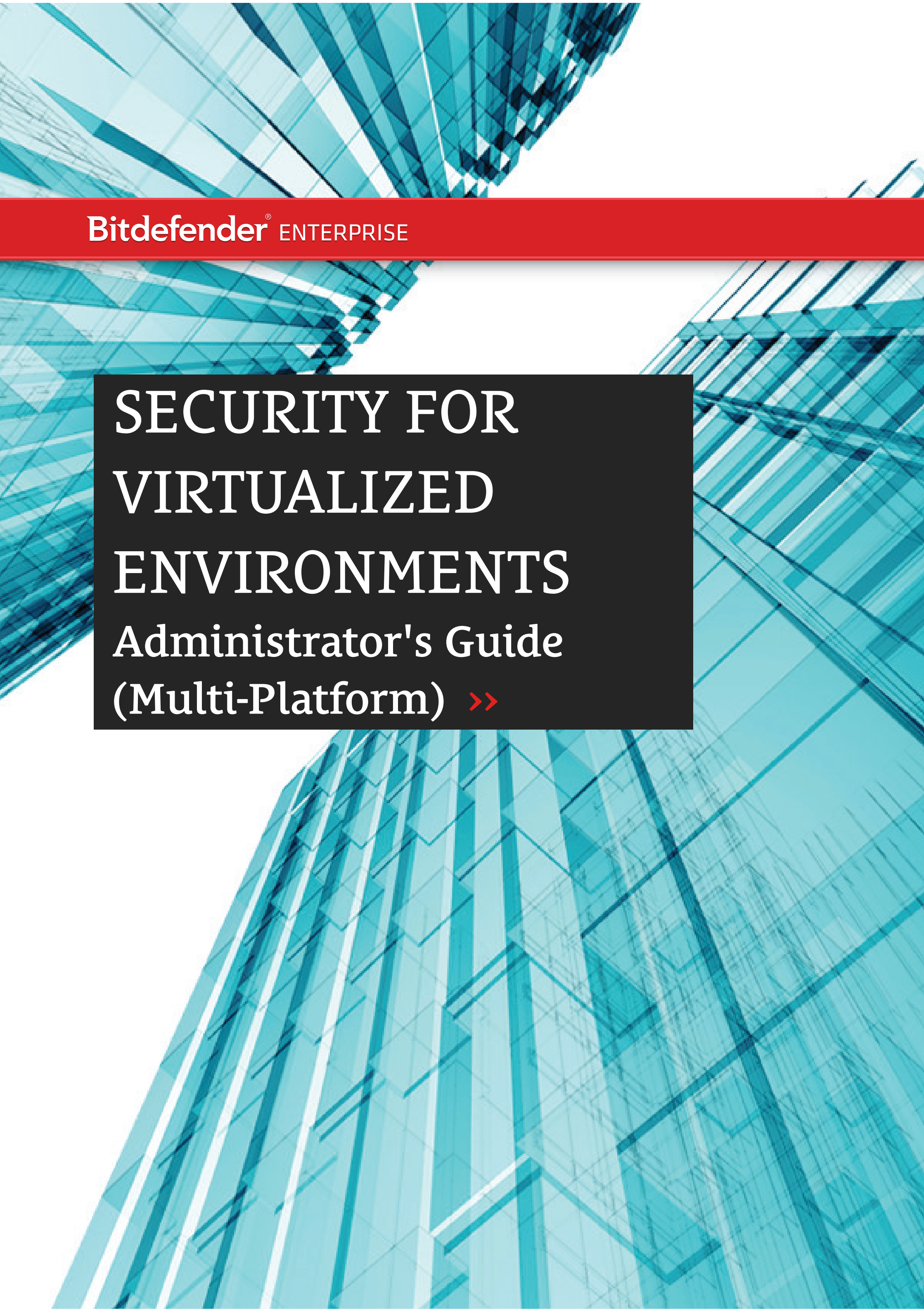


Bitdefender® ENTERPRISE

SECURITY FOR VIRTUALIZED ENVIRONMENTS

Administrator's Guide (Multi-Platform) ››

Security for Virtualized Environments by Bitdefender Administrator's Guide (Multi-Platform)

Publication date 2013.02.01

Legal Notice

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an “as is” basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.

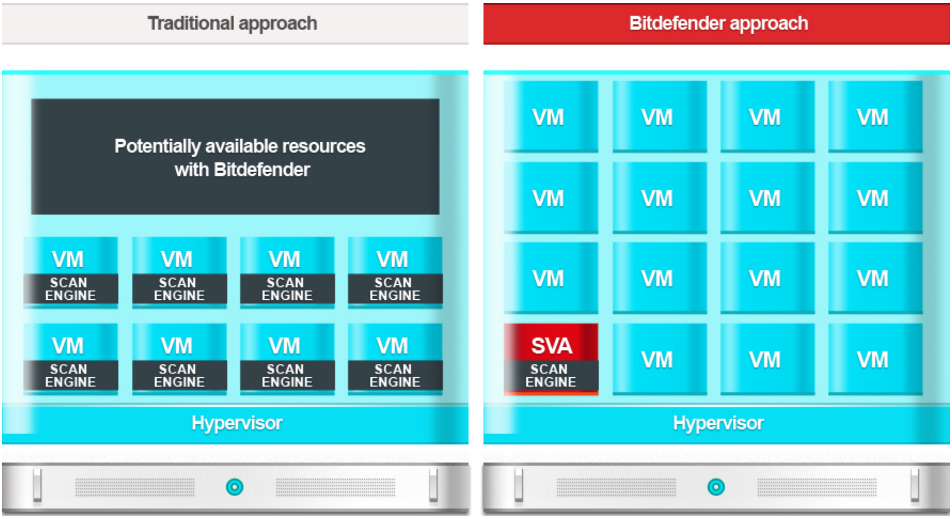
Bitdefender®

Table of Contents

1. About Security for Virtualized Environments

Organizations today look to virtualization technologies to increase the return on investment in datacenter infrastructure. Consolidation of server and end-user workloads onto shared infrastructure has led to cost reductions by deduplication of hardware resources. Virtualization also provides significant operational benefits through near-instant provisioning as organizations create and leverage private and public clouds.

To realize the full potential of virtualized datacenters, organizations must also look to consolidating elements of the workloads themselves, security being an element that must be present across all workloads. In gaining ever-higher consolidation ratios and operational benefits, organizations must not sacrifice security while their valuable brands become increasingly threatened by evermore dedicated, sophisticated, and focused attackers.



Bitdefender Approach

Security for Virtualized Environments (SVE) is the first comprehensive security solution for virtualized datacenters. SVE protects not only Windows servers and end-user systems, but also Linux and Solaris systems. Integrated with VMware vShield and VMware vCenter, its unique architecture also allows it to defend systems running on any system virtualization technology. As organizations increase consolidation ratios, Bitdefender security that has been designed, from day one, to provide highly advanced, proactive, and reliable security in virtualized environments is a cornerstone of building and enhancing datacenter virtualization strategies.

When installed in VMware environments, SVE takes advantage of vShield Endpoint. However, SVE is not dependent on the virtualization technology; it protects environments that are powered by any virtualization technology.

Components

Security Virtual Appliance

Security for Virtualized Environments deduplicates and centralizes much of the scanning functionality to a single, dedicated virtual appliance on each physical host. This hardened Linux scanning virtual appliance deals with the scanning and maintenance (updates, upgrades, RAM, IOPS, etc.) requirements of the antimalware clients.

Security Console

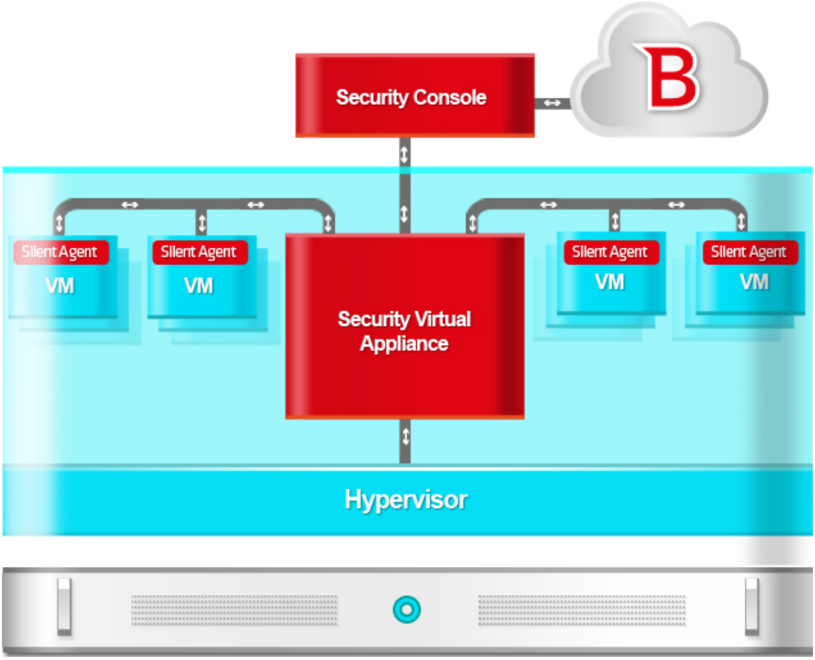
Security Console is a central web interface used for deploying, configuring, monitoring, and reporting on the security status of datacenters and end-user systems. Built on Bitdefender Gravity Architecture, a single Security Console and data store horizontally scale from the smallest to largest deployment with ease.

Security Console is delivered as a virtual appliance. The Security Console appliance also includes **Update Server**, the component handling all product upgrade and signature update tasks. Update Server is the only component that needs access to the Internet in order to communicate with the Bitdefender Cloud.

Silent Agent

Silent Agent is the guest side component that facilitates memory, on-access and on-demand scans. It is a thin application, which also has a secondary role of notifying the user on the local security status.

Silent Agent must be installed on each virtual machine to be protected (different from VMware environments where Security for Virtualized Environments is integrated with vShield Endpoint). The Silent Agent kit is accessible via Security Console.



Components and Operation

2. Installation

2.1. Compatibility and Requirements

Security for Virtualized Environments is delivered within a Security Virtual Appliance running on a hardened Linux Server distribution (2.6 kernel) and is managed by Security Console. Security Console is delivered as a virtual appliance.

Supported Virtualization Platforms

Security for Virtualized Environments supports the following virtualization platforms:

- VMware vSphere 5.1, 5.0, 4.1 with VMware vCenter Server 5.1, 5.0, 4.1
- VMware View 5.1, 5.0
- Citrix XenServer 6.0, 5.6 or 5.5 (including Xen Hypervisor)
- Citrix XenDesktop 5.5 or 5.0 (including Xen Hypervisor)
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2012 or 2008 R2
- Windows Server 2012 or 2008 R2 (including Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor)
- Kernel-based Virtual Machine (KVM)
- Oracle VM 3.0

Important

In VMware environments, you can use Security for Virtualized Environments with VMware vShield Endpoint. For more information, including additional requirements, check the corresponding Security for Virtualized Environments documentation.

Security Console Requirements

The Security Console appliance is a preconfigured virtual machine. This appliance must be installed on one host in your virtualized environment.

You must provision the following resources on the Security Console host:

- Disk space: 15 GB.
- Memory and CPU resource allocation for the Security Console appliance depends on the number of protected virtual machines. The following table lists the recommended resources to be allocated:

Number of protected VMs	RAM	CPUs
<100	2 GB	2 CPUs
100 - 1000	4 GB	2 CPUs
>1000	8 GB	4 CPUs

For better performance, you can allocate more resources if available.

Security Console can be accessed from the following web browsers:

- Internet Explorer 8+
- Mozilla Firefox 4+
- Google Chrome
- Safari
- Opera

Recommended screen resolution: 1024x768 or higher

Security Virtual Appliance Requirements

The Security Virtual Appliance is a preconfigured virtual machine running on a hardened Linux Server distribution (2.6 kernel). The number of necessary Security Virtual Appliance installations depends primarily on the number and type of virtual machines to be protected and on the resources available on hosts. You do not need to install Security Virtual Appliance on each host.

You must provision the following resources for each Security Virtual Appliance:

- Disk space: 8 GB.
- Memory and CPU resource allocation for the Security Virtual Appliance depends on the number and type of VMs running on the host. The following table lists the recommended resources to be allocated:

Number of protected VMs	RAM	CPUs
1-50 VMs	2 GB	2 CPUs
51-100 VMs	2 GB	4 CPUs
101-200 VMs	4 GB	6 CPUs

For better performance, you can allocate more resources if available.

Supported Guest Operating Systems

Security for Virtualized Environments currently protects the following operating systems:

- Windows Server 2012

- Windows Server 2008 / Windows Server 2008 R2
- Windows Server 2003 / Windows Server 2003 R2
- Windows 8
- Windows 7
- Windows Vista
- Windows XP with Service Pack 3 (32-bit) / Service Pack 2 (64-bit)
- Red Hat Enterprise Linux / CentOS 6.2, 6.1, 5.7, 5.6
- Ubuntu 11.04, 10.04
- SUSE Linux Enterprise Server 11
- OpenSUSE 12, 11
- Fedora 16, 15

Note
Protection for Solaris guests is not yet available at the time of this release.

On-access scanning is available for all supported Windows versions. A beta on-access scanning module is also available for specific Linux distributions and kernel versions, as shown in the following table:

Linux Distribution	Kernel Version
Ubuntu 10.04	2.6.32-44
RHEL/CentOS 5.7, 5.6	2.6.18-308
RHEL/CentOS 6.2, 6.1	2.6.32-279

Silent Agent Requirements and Footprint

Silent Agent can be installed on virtual machines running any of the supported operating systems. No specific hardware or software requirements need to be met. As you can see in the following table, Silent Agent uses a minimum of system resources.

Platform	RAM	Disk Space
Windows	20/25* MB	60 MB
Linux	50 MB	70 MB

*20 MB when the Silent Mode option is enabled and 25 MB when it is disabled. When Silent Mode is enabled, the Silent Agent graphical user interface (GUI) is not loaded automatically at system startup, freeing up associated resources.

2.2. Preparing for Installation

For installation, you need the following components:

- A virtual machine template containing Security Virtual Appliance
- A virtual machine template containing Security Console

The Silent Agent installation kit is included in the Security Console appliance. After succesfully deploying and configuring the appliances, you will be able to download the installation kit or remotely install Silent Agent on virtual machines from the Security Console web interface.

To obtain the Security for Virtualized Environments appliances, you must submit your request to evaluate Security for Virtualized Environments via the Bitdefender website or, if you are an existing customer, by contacting your Bitdefender representative. Download links will be emailed to you after your request has been reviewed.

Security Console will be installed on only one host in the virtualized environment. The number of necessary Security Virtual Appliance installations depends primarily on the number and type of virtual machines to be protected and on the resources available on hosts. The default resource allocation settings of Security Virtual Appliance are recommended for up to 100 clients. For more clients, allocate more resources or install additional Security Virtual Appliance instances.

You must ensure the following:

- Each of the installed appliances must use either a reserved IP address assigned by DHCP or a static IP address. Appliances are by default configured to obtain IP addresses using DHCP.
- The Security Console appliance must have Internet access because it downloads and distributes updates for all product components. It must also be accessible from all machines in the virtualized environment.
- Security Virtual Appliance instances must have network connectivity with the Security Console appliance and with all machines that use their scanning services.
- Configure the local firewall on virtual machines to allow connectivity with the other Security for Virtualized Environments components on the following ports:
  - `7081` - the communication port between Silent Agent and Security Virtual Appliance.
  - `7083` - the Secure Sockets Layer (SSL) communication port between Silent Agent and Security Virtual Appliance.
  - `8082` - the communication port between Silent Agent and Security Console.
  - `7074` - the Update Server port on the Security Console appliance.
- For continuous protection, installed appliances must always be on.

2.3. Installation Steps

You must complete these steps in order to install all Security for Virtualized Environments components:

1. Deploy Security Console on one host from your virtualized environment.

   Power it on. Configure this VM so that is has access to the Internet for product updates, and also can be accessed by the Bitdefender Silent Agents and Security Virtual Appliances.

2. Deploy Security Virtual Appliance on hosts as needed. The number of necessary Security Virtual Appliance installations depends primarily on the number and type of virtual machines to be protected and on the resources available on hosts. The default resource allocation settings of Security Virtual Appliance are recommended for up to 100 clients. For more clients, allocate more resources or install additional Security Virtual Appliance instances.

   Power on all installed appliances. These VMs need network connectivity with associated Bitdefender Silent Agents and with Security Console.

3. Appliances are by default configured to obtain IP addresses using DHCP. Configure the DHCP Server to reserve IP addresses for all of the installed appliances. Otherwise, you must configure each of them to use a static IP address. See next step for static IP configuration.

4. Set up installed appliances from their CLI console. For more information, refer to "Setting Up SVE Appliances" (p. 9).

5. Connect to Security Console via HTTPS and set up your company account. For more information, refer to "Setting Up Your Company Account" (p. 11).

6. Install Silent Agent on the instances you want to protect. For installation instructions, refer to "Installing Silent Agent on VMs" (p. 14).

7. Create and assign policies to virtual machines to configure protection settings and to direct them to the preferred Security Virtual Appliance instance. For more information, refer to "Security Policies" (p. 43).

   Note

   In a virtualized environment with multiple Security Virtual Appliance installations, the agent will initially use the default Security Virtual Appliance configured in the Security Console company account. As soon as a policy is applied on the virtual machine, the agent will use the Security Virtual Appliance configured through the policy settings. Use the policy to direct the agent to the preferred Security Virtual Appliance instance. For more information, refer to "Recommended Setup with Multiple SVAs" (p. 22).

It is recommended to first group virtual machines (by Security Virtual Appliance instance, physical host, or other criteria) and then assign group policies. For more information, refer to "Using Groups" (p. 37).

2.4. Setting Up SVE Appliances

Security Console and Security Virtual Appliance have command-line interfaces that allow configuring basic settings, including network settings.

Default login credentials are the same for both appliances:

- User name: `administrator`
- Password: `admin`

2.4.1. Security Console Setup

The Security Console configuration script allows you to configure the appliance with static network settings. If you have created an IP reservation for the appliance on the DHCP server, you do not need to run the configuration script.

To configure Security Console with static network settings:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client). Alternatively, you can connect to the appliance via SSH.
2. Log in using the default credentials.
3. Obtain root privileges by running the `sudo su` command and then entering the `admin` password.
4. Run the `sc-setup` command.
5. Enter the network settings: IP address, network mask, gateway, DNS servers.
6. Type `Y` and press Enter to save the changes.

   Note
   If you are connected to the appliance via a SSH client, changing the network settings will immediately terminate your session.

7. Make sure the appliance has the designated IP address in place. You can check the IP configuration by running the following command:

```
$ ifconfig eth0
```

2.4.2. Security Virtual Appliance Setup

The Security Virtual Appliance configuration script allows you to configure the appliance with the Security Console and update server addresses and static network settings. Before you set up Security Virtual Appliance, make sure the Security Console appliance is configured with the designated IP address.

To set up Security Virtual Appliance:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client). Alternatively, you can connect to the appliance via SSH.
2. Log in using the default credentials.
3. Obtain root privileges by running the `sudo su` command and then entering the `admin` password.

    Important

    To successfully run the Security Virtual Appliance configuration script, Security Virtual Appliance must have network connectivity with the Security Console appliance. If no DHCP server is available in the local network, you must manually configure the network settings of Security Virtual Appliance before running the configuration script. You can assign a temporary IP address and gateway address to the appliance by running the following commands:

    ```
    $ sudo ifconfig eth0 <IP address> netmask <subnet mask>
    ```

    ```
    $ sudo route add default gw <gateway IP address>
    ```

    Use the configuration script afterwards to configure all necessary network settings.

4. Run the `sva-setup` command.
5. Enter the IP address or hostname of the Security Console machine.
6. Enter the IP address or hostname of the local update server. Since the local update server runs on the Security Console machine, you must enter the IP address or hostname of that machine.
7. Optionally, you can configure the appliance with static network settings. If you have created an IP reservation for the appliance on the DHCP server, skip this configuration by pressing Enter.

    a. Type `Y` and press Enter to continue.

    b. Enter the network settings: IP address, network mask, gateway, DNS servers.

    c. Type `Y` and press Enter to save the changes.

    Note

    If you are connected to the appliance via a SSH client, changing the network settings will immediately terminate your session.

8. Make sure the appliance has the designated IP address in place. You can check the IP configuration by running the following command:

```
$ ifconfig eth0
```

2.4.3. Changing Administrator Password

To prevent unauthorized access to the CLI of the Bitdefender appliances, it is recommended to change the default password for the administrator account. Password changing procedure is the same for both appliances.

To change the password:

1. Access the appliance console in vSphere Client. Alternatively, you can connect to the appliance via SSH.
2. Log in using the default credentials.
3. Run the `passwd` command.
4. Enter the current password (default `admin`).
5. Enter the new password. Make sure to choose a strong password that you can easily remember. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).
6. Enter the new password again.

2.5. Setting Up Your Company Account

Once you have deployed the Security for Virtualized Environments appliances, you must connect to Security Console via HTTPS and set up your company account.

To set up your company account:

1. Open your web browser.

   Note
   Requirements:
   - Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari or Opera
   - Recommended screen resolution: 1024x768 or higher

2. Enter the IP address of the Security Console VM (using https). A login page is displayed.
3. Log in with the default credentials:
   - User name: `default@company.com`
   - Password: `default`
4. Read and confirm that you agree with the terms of service. If you do not agree with these terms, you cannot use the service.

5. Provide all the necessary information to configure your company account.

    a. Under **Account Details**, configure your company account details.

    - **Full name.**
    - **Email.** This is your login and contact email address. Reports and important security notifications are sent to this address. Email notifications are sent automatically whenever important risk conditions are detected in the network.
    - **Password.** Set the login password. The password must have between 8 and 128 characters and it must contain at least one upper case character, one lower case character and one digit or special character.
    - **Company name.**

    b. Under **Default Silent Agent Settings**, configure the default settings to be included in the Silent Agent kit and in the default policy.

    - **Security Console Address.** Enter the IP address of the Security Console VM. Silent Agent uses this address to communicate with Security Console.
    - **Security Virtual Appliance Address.** Enter the IP address of the Security Virtual Appliance instance that Silent Agent connects to by default. If you have deployed multiple Security Virtual Appliance instances, you will use policies to direct agents to the appropriate Security Virtual Appliance instance. For more information, refer to "Recommended Setup with Multiple SVAs" (p. 22).
    - **Use SSL.** Select this option if you want to secure communication between Silent Agent and the Security Virtual Appliance using Secure Sockets Layer (SSL). Take into account that activating SSL encryption for the Silent Agent - Security Virtual Appliance traffic will slightly impact performance.

        Note
        Communication between Silent Agent and Security Console is always encrypted using SSL, regardless of how you configure this option.

        The Silent Agent - Security Virtual Appliance communication port depends on the use of SSL encryption:

        – The port used for SSL-secured communication is `7083`.

        – The port used for unsecured communication is `7081`.

    c. Under **Proxy Settings**, select **Use Proxy** if the Security Console machine connects to the Internet via a proxy server. You must configure the following settings:

    - Address of the proxy server.
    - Port number used by the proxy server.
    - Username recognized by the proxy.
    - Valid password for the previously specified username.

Note

Security Console does not support proxy servers that use Active Directory authentication. A workaround for the NTLM authentication method is described in this KB article.

d. Under **SMTP Settings**, you can configure Security Console to send email reports and notifications using an external mail server instead of the built-in postfix mail server. If you do not specify any settings, Security Console uses the built-in mail server.

- **IP/ Hostname.** Enter the IP address or hostname of the mail server that is going to send the emails.
- **Port.** Enter the port used to connect to the mail server.
- **Username.** If the SMTP server requires authentication, enter a recognized username / email address.
- **Password.** If the SMTP server requires authentication, enter the password of the previously specified user.
- **From Name.** Enter the name that you want to appear in the From field of the email (sender's name).
- **From Email.** Enter the email address that you want to appear in the From field of the email (sender's email address).

Note

Security Console does not support encrypted connection (SSL, TLS) to the mail server.

e. Under **License**, you can check current license details. For more information, refer to "Licensing and Registration" (p. 30).

f. Under **Settings**, configure the account settings according to your preferences.

- **Timezone.** Choose from the menu the timezone of the account. The console will display time information according to the selected timezone.
- **Language.** Choose from the menu the console display language.
- **Logo.** You can change the default cloud-shaped Security Console logo with your company logo. This will allow you to customize PDF report layout. To change the logo, click **Custom** and load the logo image file from your computer. The following restrictions apply:
  - Logo dimensions: 81x41 pixels.
  - Supported file formats: PNG and JPG.

g. Click **Submit** to save the changes.

2.6. Installing Silent Agent on VMs

To protect virtual machines with Security for Virtualized Environments, you must install Silent Agent (the client software) on each of them. Silent Agent manages protection on the local VM. It sends scan requests to the Security Virtual Appliance, which performs the actual scan. It also communicates with Security Console to receive the administrator's commands and to send the results of its actions.

Before you install Silent Agent:

- Make sure all previous steps in the Security for Virtualized Environments installation procedure have been completed. For more information, refer to "Installation Steps" (p. 7).
- Prepare for installation as described in "Preparing for Installation" (p. 14).

There are two installation methods:

- **Local installation.** Use the installation link from Security Console to download and install Silent Agent locally on individual virtual machines. For more information, refer to "Local Installation" (p. 15).

  Important
  Local installation is currently the only installation method available for Linux VMs.

- **Remote installation.** Once installed on a virtual machine, Silent Agent automatically detects Windows virtual machines visible in the local network. The Security for Virtualized Environments protection can then be installed on detected virtual machines remotely from the console. Remote installation is performed in the background, without the user knowing about it. For more information, refer to "Remote Installation" (p. 16) and "How Network Discovery Works" (p. 17).

2.6.1. Preparing for Installation

Prepare for installation on virtual machines as follows:

1. Make sure the virtual machines run a supported guest operating system. For some VMs, you may need to install the latest operating system service pack available.
2. Uninstall (not just disable) any existing antimalware software from the virtual machines. Running other security software simultaneously with Security for Virtualized Environments may affect their operation and cause major problems with the system.
3. The installation requires administrative privileges. For remote installation, make sure to have administrative credentials for all virtual machines at hand.

4. The Security Console virtual appliance must be powered on and accessible from the virtual machines. Installation files are downloaded from the Security Console virtual machine.

2.6.2. Local Installation

Local installation can be performed by yourself, by logging on to each virtual machine, or you can ask for help the users of the virtual machines. It requires locally running a small installation file, which you can download from Security Console. The installation file comes in two versions (Windows and Linux).

Important
Local installation is currently the only installation method available for Linux instances.

To obtain or distribute the download links for local installation:

1. Connect to Security Console using your **company account**.
2. Go to the **Computers > Installation Area** page.
3. Click the **Link** button and choose **View**. The window that appears provides you with the download links for the Window web installer and the Linux installation script. Use the link to download a small installation file, which then you can run on the local computer to install protection. You can also copy the file to a network share accessible from the virtual machines.
4. Another option is to send users within the organization's network email invites with the installation link, asking them to download and install protection on their computer. To email the link, click the **Link** button and choose **Send by Email**. Email invites are to be sent to Windows users only, as they contain only the Windows web installer link.

To manually install Silent Agent on a Windows virtual machine:

1. Download the Silent Agent Windows web installer from Security Console.
2. Locate the downloaded installation file and double-click it. The web installer downloads the full installation package from the Security Console appliance and then starts the installation.
3. Wait for the installation to complete. The latest versions of the application files are downloaded and installed, and the Bitdefender services are started. This step can take a couple of minutes.

   The installation window closes automatically once installation is completed.

To manually install Silent Agent on a Linux virtual machine:

1. Download the Silent Agent Linux installation script from Security Console.

   If you have the download link, run the following command in a terminal:

```
$ wget --no-check-certificate <download link>
```

The downloaded file is named `downloader`.

2. Grant execute permission to current user on the `downloader` file.

```
$ chmod u+x downloader
```

3. Run `downloader` as root. The script downloads the full installation package from the Security Console instance and then starts the installation.

```
$ sudo ./downloader
```

Installation will normally complete in less than a minute.

2.6.3. Remote Installation

To make deployment easier, Security for Virtualized Environments includes an automatic network discovery mechanism based on which Silent Agent can be installed on Windows virtual machines remotely from Security Console. Detected computers are displayed as **unmanaged computers** on the **Computers** page. For detailed information on network discovery, refer to "How Network Discovery Works" (p. 17).

To enable network discovery and remote installation, you must have Silent Agent already installed on at least one virtual machine in the network. This machine will be used to scan the network and install Silent Agent on unprotected machines.

Note
Once the first Silent Agent is installed, it may take a few minutes for the rest of the network computers to become visible in the Security Console.

Note
Each target machine must have the admin$ administrative share enabled for the installation to work.

To remotely install protection on virtual machines:

1. Connect to Security Console using your **company account**.
2. Install protection manually on a virtual machine in the network. Wait a few minutes after installation while Silent Agent detects computers in the local network.
3. Go to the **Computers > View Computers** page. This is where you can view protected virtual machines and the computers detected in local networks where Silent Agent has

been installed. Physical computers might also be detected if they are connected to the virtual network.

4. Click the **Show** menu located above the table (to the left) and choose **Unmanaged Computers**. In this way, only detected computers that are not currently protected by Security for Virtualized Environments are displayed.
5. If you have organized computers into groups, select the desired group from the left-side pane. To view all of your computers, right-click the root group and choose **View all computers**.
6. Select the check boxes corresponding to the virtual machines on which you want to install protection.
7. Click **Tasks** and choose **Install** from the menu. The Installation Options window will appear.
8. Provide the administrative credentials required for remote authentication on selected virtual machines.

   Enter the user name and password of an administrator account for each of the selected computers. If computers are in a domain, it suffices to enter the credentials of the domain administrator. Use Windows conventions when entering the name of a domain user account (for example, `domain\user` or `user@domain.com`).
9. Click **Install Silent Agent**. A confirmation window will appear.
10. You can view and manage the task on the **Computers > View Tasks** page.

2.6.4. How Network Discovery Works

Security for Virtualized Environments relies on the **Microsoft Computer Browser service** to perform network discovery. The Computer Browser service is a networking technology used by Windows-based computers to maintain updated lists of domains, workgroups, and the computers within them and to supply these lists to client computers upon request. Computers detected in the network by the Computer Browser service can be viewed by running the **net view** command in a command prompt window.

> **Important**
>
> Security for Virtualized Environments does not use network information from Active Directory or from the network map feature available in Windows Vista and later. Network map relies on a different network discovery technology: the Link Layer Topology Discovery (LLTD) protocol.

Security for Virtualized Environments is not actively involved in the Computer Browser service operation. Silent Agent only queries the Computer Browser service for the list of workstations and servers currently visible in the network (known as the browse list) and then sends it to Security Console. Security Console processes the browse list, appending newly detected computers to its **Unmanaged Computers** list. Previously detected computers are not deleted after a new network discovery query, so you must manually exclude & delete computers that are no longer on the network.

The initial query for the browse list is carried out by the first Silent Agent installed in the network.

- If Silent Agent is installed on a workgroup computer, only computers from that workgroup will be visible in Security Console.
- If Silent Agent is installed on a domain computer, only computers from that domain will be visible in Security Console. Computers from other domains can be detected if there is a trust relationship with the domain where Silent Agent is installed.

Subsequent network discovery queries are performed regularly every hour. For each new query, Security Console divides the managed computers space into visibility areas and then designates one Silent Agent in each area to perform the task. A visibility area is a group of computers that detect each other. Usually, a visibility area is defined by a workgroup or domain, but this depends on the network topology and configuration. In some cases, a visibility area might consist of multiple domains and workgroups.

If a selected Silent Agent fails to perform the query, Security Console waits for the next scheduled query, without choosing another Silent Agent to try again.

For full network visibility, Silent Agent must be installed on at least one computer in each workgroup or domain in your network. Ideally, Silent Agent should be installed on at least one computer in each subnetwork.

More about the Microsoft Computer Browser Service

Quick facts about the Computer Browser service:

- Works independent of Active Directory.
- Runs exclusively over IPv4 networks and operates independently within the boundaries of a LAN group (workgroup or domain). A browse list is compiled and maintained for each LAN group.
- Typically uses connectionless server broadcasts to communicate between nodes.
- Uses NetBIOS over TCP/IP (NetBT).
- Requires NetBIOS name resolution. It is recommended to have a Windows Internet Name Service (WINS) infrastructure up and running in the network.
- Is not enabled by default in Windows Server 2008 and 2008 R2.

For detailed information on the Computer Browser service, check the Computer Browser Service Technical Reference on Microsoft Technet.

Network Discovery Requirements

In order to successfully discover all the computers (servers and workstations) that will be managed from Security Console, the following are required:

- Computers must be joined in a workgroup or domain and connected via an IPv4 local network. Computer Browser service does not work over IPv6 networks.
- Several computers in each LAN group (workgroup or domain) must be running the Computer Browser service. Primary Domain Controllers must also run the service.
- NetBIOS over TCP/IP (NetBT) must be enabled on computers. Local firewall must allow NetBT traffic.
- File sharing must be enabled on computers. Local firewall must allow file sharing.
- A Windows Internet Name Service (WINS) infrastructure must be set up and working properly.
- For Windows Vista and later, network discovery must be turned on (**Control Panel > Network and Sharing Center > Change Advanced Sharing Settings**).

  To be able to turn on this feature, the following services must first be started:
  - DNS Client
  - Function Discovery Resource Publication
  - SSDP Discovery
  - UPnP Device Host
- In environments with multiple domains, it is recommended to set up trust relationships between domains so that computers can access browse lists from other domains.

Computers from which Silent Agent queries the Computer Browser service must be able to resolve NetBIOS names.

Note
The network discovery mechanism works for all supported Windows operating systems, provided the requirements are met.

2.6.5. Enabling Support for On-access Scanning on Linux VMs

The Linux version of Silent Agent includes a beta on-access scanning module that works with specific Linux distributions and kernel versions. On-access scanning support can be enabled manually on each virtual machine.

On-access scanning requires the DazukoFS loadable kernel module. DazukoFS is a stackable file system that enables third-party applications to control file access on Linux systems. For more information, go to http://www.dazuko.org.

The Silent Agent installation package includes and automatically installs DazukoFS. Once installed, DazukoFS must be mounted on top of all directories that you want to be scanned in real-time.

Important

Silent Agent is exclusively compatible with the DazukoFS version included in the installation package. If DazukoFS is already installed on the system, remove it prior to installing Silent Agent.

To enable on-access scanning support on a Linux virtual machine with Silent Agent installed:

1. Load the DazukoFS kernel module.
2. Mount the directories to be monitored using DazukoFS.

Once support is enabled, on-access scanning can be managed remotely from Security Console using policies.

Important

For DazukoFS and on-access scanning to work, the SELinux policy must be either disabled or set to **permissive**. To check and adjust the SELinux policy setting, edit the `/etc/selinux/config` file.

Load DazukoFS Module

During Silent Agent installation, DazukoFS is set to load automatically at boot time. To load the module immediately after installation, you must either restart the virtual machine or run the following command:

```
# modprobe /lib/modules/`uname -r`/kernel/fs/dazukofs/dazukofs.ko
```

Note

If the DazukoFS package shipped with Silent Agent is not compatible with the system's kernel version, the module will fail to load. In such case, you can either update the kernel to the supported version or recompile the DazukoFS module for your kernel version. You can find the DazukoFS package in the Silent Agent installation directory:
`/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`
For more information on compiling and loading DazukoFS for an unsupported kernel version, refer to this KB article.

To check if DazukoFS is loaded, run the following command:

```
# lsmod | grep dazukofs
```

If the module is loaded, the command outputs a line starting with `dazukofs`.

Note
To unload the DazukoFS kernel module, you must first unmount monitored directories and then make sure to stop the Bitdefender services.
To stop the Bitdefender services, run this command:

```
# /opt/BitDefender/bin/bd stop
```

After unloading the module, restart the Bitdefender services using this command:

```
# /opt/BitDefender/bin/bd start
```

Manage Monitored Directories

Mount using DazukoFS all directories that you want to be scanned. DazukoFS monitors the entire directory tree under a mounted directory.

Important
If you mount a directory from a DazukoFS-monitored directory tree using another file system, on-access scanning will no longer work for that directory tree. Therefore, make sure to mount DazukoFS over a directory tree only after mounting all other file systems required.

To mount a directory using DazukoFS, run the following command:

```
# mount -t dazukofs <directory_path> <directory_path>
```

For example, to enable on-access scanning for the home directory, the command is:

```
# mount -t dazukofs /home /home
```

Note
You cannot mount DazukoFS over the root file system (/).

To check the list of directories mounted using DazukoFS, run the following command:

```
# mount | grep dazukofs
```

The command outputs each mounted directory on a separate line.

To stop monitoring a specific directory, run the following command:

```
# umount <directory_path>
```

2.6.6. Creating a VM template with Silent Agent

Starting with Security for Virtualized Environments version 1.2.4, Silent Agent automatically detects when it is running on a machine created from a template and creates a unique instance ID. Consequently, no special configuration is required in order to include Silent Agent on a virtual machine template.

To create a virtual machine template with Silent Agent:

1. Create the virtual machine that is to be used to create the template.
2. Prepare the system (for example, install the necessary software).
3. Install Silent Agent on the virtual machine by downloading and running the installation file from Security Console. For more information, refer to "Local Installation" (p. 15).
4. Check that the virtual machine is displayed in Security Console as managed. Go to the **Computers > View Computers** page.
5. Shut down the machine and save it as template.

2.7. Recommended Setup with Multiple SVAs

The number of necessary Security Virtual Appliance installations depends on the following:

- Number of virtual machines and virtualization type (VDI or server virtualization)
- Resources available on hosts
- Network topology and connectivity between hosts and between virtual machines
- Failure prevention requirements

It is important to note that Silent Agent is configured by default to use the Security Virtual Appliance specified in the Security Console company account. In environments with multiple Security Virtual Appliance installations, you can redirect specific Silent Agent instances to a different Security Virtual Appliance using policies. When you create a policy, you can specify the following:

- Virtual machines or groups to which the policy will apply (policy target).
- Security Virtual Appliance instances to which the agents included in the policy target can connect. Settings can be configured in the **General > Advanced** policy section. You can change the existing Security Virtual Appliance address or add the addresses of other Security Virtual Appliance instances. Silent Agent selects one of the specified Security Virtual Appliance instances based on assigned priority, availability and current load (normal, overload, underload).

The recommended approach is to configure policies with the addresses of all available Security Virtual Appliance instances and rely on the load balancing mechanism to automatically distribute agents. Set the preferred Security Virtual Appliance for selected Silent Agent instances with priority 1.

To learn how to use policies, refer to "Security Policies" (p. 43).

3. Getting Started

Security for Virtualized Environments can be configured and managed using Security Console, a central web-based interface.

By using Security Console, you can do the following:

- Manage your license.
- Install protection on virtual machines.
- Visualize the entire network (managed virtual machines, unprotected computers detected in the network).
- Find out detailed information about a managed virtual machine.
- Remotely run tasks on virtual machines (install, uninstall, scan).
- Assign policies to managed virtual machines in order to configure and manage protection.
- Monitor protection.
- Obtain centralized easy-to-read reports regarding the managed virtual machines.
- Check and manage quarantined files remotely.
- Create and manage user accounts for other company employees.
- Check user activity log.

3.1. Connecting to Security Console

Access to Security Console is done via user accounts.

To connect to Security Console:

1. Requirements:
   - The Security Console virtual appliance must be powered on, connected to Internet and accesible from your computer.
   - Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari or Opera
   - Recommended screen resolution: 1024x768 or higher
2. Open your web browser.
3. Go to the IP address of the console host (using https).
4. Enter the email address and password of your account.
5. Click **Login**.

Note

If you have forgotten your password, use the password recovery link to receive a new password. You must provide the email address of your account.

The first time you log in to the console, you will be prompted to read and confirm that you agree with the terms of service. If you do not agree with these terms, you cannot use the service.

3.2. Security Console Overview

Security Console is organized so as to allow easy access to all the features.

Use the menu bar in the upper area to navigate through the console.

Dashboard

View easy-to-read charts providing key security information concerning your network. For more information, refer to "Monitoring Dashboard" (p. 32).

Computers

Install protection, manage computers and run tasks remotely. For more information, refer to "Managing Computers (Virtual Machines)" (p. 35).

Policies

Create, apply and manage security policies. For more information, refer to "Security Policies" (p. 43).

Reports

Get security reports concerning the managed computers. For more information, refer to "Using Reports" (p. 63).

Quarantine

Remotely manage quarantined files. For more information, refer to "Quarantine" (p. 71).

Accounts

Manage your account details and preferences. Create and manage user accounts for other company employees. For more information, refer to "User Accounts" (p. 74).

Log

Check the user activity log. For more information, refer to "User Activity Log" (p. 77).

In the upper-right corner of the console, you can find the following links:

- **User name.** Click your user name to manage your account details and preferences.
- **Help and Support.** Click this link to find help and support information.
- **Logout.** Click this link to log out of your account.

3.3. Configuration and Management Guidelines

Here are some guidelines to help you get started:

1. Go to the **Accounts > My Account** page to manage your account details. It is recommended that you change the default login password. You can customize the PDF report layout by loading your company logo.
2. Go to the **Computers > Installation Area** page and install Silent Agent (the client software) on virtual machines. For installation instructions, refer to "Installing Silent Agent on VMs" (p. 14).
3. If you manage a larger number of computers (tens or more), organize them into groups to manage them more efficiently:
   a. Go to the **Computers > View Computers** page.
   b. Create groups in the left-side pane by right-clicking the root group (or a group you have created) and selecting **Create group**.
   c. Click the root group, then select computers and drag and drop your selection to the desired group.
4. The protection settings on computers are automatically configured according to the default security policy. To check the default protection settings, go to the **Policies > View Policies** page and click the default policy name.

   You cannot edit the default policy. To change the default protection settings:

   a. Go to the **Policies > New Policy** page and create a new policy.
   b. Configure the policy settings as needed.
5. Later on, to manage and monitor protection, do the following:
   - Check the **Dashboard** page regularly to see real-time information on the Security for Virtualized Environments protection.
   - Go to the **Reports > New Report** page to create the reports you need. It is recommended to create scheduled reports for the report types you need regularly. To view a generated report, go to the **Reports > View Reports** page and click the report name.
   - Use the tasks on the **Computers > View Computers** page to scan protected VMs, install protection remotely on unmanaged VMs or completely remove protection.

3.4. Changing Default Login Password

It is recommended that you change the default login password. It is also advisable to change your login password periodically.

To change the login password:

1. Go to the **Accounts > My Account** page.
2. Type a new password in the corresponding fields (under **Account Details**).
3. Click **Submit** to save the changes.

3.5. Managing Your Account

To check and change your account details and settings:

1. Go to the **Accounts > My Account** page.
2. Under **Account Details**, correct or update your account details.
   - **Full name.**
   - **Email.** This is your login and contact email address. Reports and important security notifications are sent to this address. Email notifications are sent automatically whenever important risk conditions are detected in the network.
   - **Password.** To change your login password, type a new one in the corresponding fields.
   - **Company name.**
3. **Company account only!** Under **Default Silent Agent Settings**, configure the default settings to be included in the Silent Agent kit and in the default policy.
   - **Security Console Address.** Enter the IP address of the Security Console VM. Silent Agent uses this address to communicate with Security Console.
   - **Security Virtual Appliance Address.** Enter the IP address of the Security Virtual Appliance instance that Silent Agent connects to by default. If you have deployed multiple Security Virtual Appliance instances, you will use policies to direct agents to the appropriate Security Virtual Appliance instance. For more information, refer to "Recommended Setup with Multiple SVAs" (p. 22).
   - **Use SSL.** Select this option if you want to secure communication between Silent Agent and the Security Virtual Appliance using Secure Sockets Layer (SSL). Take into account that activating SSL encryption for the Silent Agent - Security Virtual Appliance traffic will slightly impact performance.

     Note
     Communication between Silent Agent and Security Console is always encrypted using SSL, regardless of how you configure this option.

     The Silent Agent - Security Virtual Appliance communication port depends on the use of SSL encryption:

     – The port used for SSL-secured communication is `7083`.

     – The port used for unsecured communication is `7081`.

4. **Company account only!** Under **Proxy Settings**, select **Use Proxy** if the Security Console machine connects to the Internet via a proxy server. You must configure the following settings:
   - Address of the proxy server.
   - Port number used by the proxy server.
   - Username recognized by the proxy.
   - Valid password for the previously specified username.

   Note

   Security Console does not support proxy servers that use Active Directory authentication. A workaround for the NTLM authentication method is described in this KB article.

5. **Company account only!** Under **SMTP Settings**, you can configure Security Console to send email reports and notifications using an external mail server instead of the built-in postfix mail server. If you do not specify any settings, Security Console uses the built-in mail server.
   - **IP/ Hostname.** Enter the IP address or hostname of the mail server that is going to send the emails.
   - **Port.** Enter the port used to connect to the mail server.
   - **Username.** If the SMTP server requires authentication, enter a recognized username / email address.
   - **Password.** If the SMTP server requires authentication, enter the password of the previously specified user.
   - **From Name.** Enter the name that you want to appear in the From field of the email (sender's name).
   - **From Email.** Enter the email address that you want to appear in the From field of the email (sender's email address).

   Note

   Security Console does not support encrypted connection (SSL, TLS) to the mail server.

6. **Company account only!** Under **License**, you can check current license details. For more information, refer to "Licensing and Registration" (p. 30).
7. Under **Settings**, configure the account settings according to your preferences.
   - **Timezone.** Choose from the menu the timezone of the account. The console will display time information according to the selected timezone.
   - **Language.** Choose from the menu the console display language.

- **Logo.** You can change the default cloud-shaped Security Console logo with your company logo. This will allow you to customize PDF report layout. To change the logo, click **Custom** and load the logo image file from your computer. The following restrictions apply:
  - Logo dimensions: 81x41 pixels.
  - Supported file formats: PNG and JPG.

8. Click **Submit** to save the changes.

3.6. Working with Table Data

Tables are frequently used throughout the console to organize data into an easy-to-use format. You may find this information useful:

- Tables can span several pages (only 10 entries are displayed per page by default). To move through the pages, use the navigation buttons at the bottom of the table. To change the number of entries displayed on a page, select an option from the menu next to the navigation buttons.
- To easily find what you are looking for, use the search boxes or the filtering options below the column headers.
- You can also click column headers to sort data by a specific column. Click the column header again to change the sorting order.

To make sure the latest information is being displayed, click the ⟳ **Refresh** button in the bottom-left corner of the table.

4. Licensing and Registration

Security for Virtualized Environments comes with a 30 day free trial period during which you can test the product and decide if it is the right solution for your organization. To continue using the product after the trial period expires, you must purchase a license key and use it to register the product.

Important

If you do not register your product, malware signature updates, product upgrades and antimalware scans will no longer function.

The multi-platform version of Security for Virtualized Environments is licensed per virtual machine. To purchase a license, contact a Bitdefender reseller or contact us by email at enterprisesales@bitdefender.com. Please write your email in English in order for us to be able to assist you promptly.

4.1. Finding a Reseller

Our resellers will assist you with all the information you need and help you choose the best licensing option for you.

To find a Bitdefender reseller in your country:

1. Go to http://enterprise.bitdefender.com/partners.
2. Go to **Partner Locator**.
3. The contact information of the Bitdefender partners should be displayed automatically. If this does not happen, select the country you reside in to view the information.
4. If you do not find a Bitdefender reseller in your country, feel free to contact us by email at enterprisesales@bitdefender.com. Please write your email in English in order for us to be able to assist you promptly.

4.2. Checking Current License Details

To view your license details:

1. Connect to Security Console using your **company account**.
2. Go to the **Accounts > My Account** page.
3. Under **License**, you can check the current license details.

4.3. Registering Your Product

To register your product or to change the current license key:

1. Connect to Security Console using your **company account**.
2. Go to the **Accounts > My Account** page.
3. Under **License**, click the available link. The **License Information** page will be displayed. If the product has already been registered with a license key, you can see the license details.
4. Enter the license key in the corresponding field.
5. Click **Change Key**.

5. Monitoring Dashboard

Each time you connect to Security Console, the **Dashboard** page is displayed automatically. The dashboard is a status page consisting of 7 portlets, which provide you with a quick security overview of all protected virtual machines.

Dashboard portlets display various security information using easy-to-read charts, thus allowing you to quickly identify any issues that might require your attention. Each dashboard portlet includes a detailed report in the background, accessible with just one click on the chart.

Some portlets offer status information, while other report on security events in the last period.

You can check and configure the reporting period of a portlet by clicking the ▼≡ button on its title bar.

5.1. Dashboard Portlets

The dashboard consists of the following portlets:

Network Status

Provides you with detailed information on the overall network security status. Computers are grouped based on these criteria:

- Unmanaged computers do not have Security for Virtualized Environments protection installed and their security status cannot be assessed. Unmanaged computers are detected automatically by the Security for Virtualized Environments agents installed on protected virtual machines. They can represent not only virtual machines, but also physical computers (if they are connected to the virtual network).
- Offline computers normally have Security for Virtualized Environments protection installed, but there is no recent activity from Silent Agent. The security status of offline computers cannot be accurately assessed because status information is not current. For more information, refer to "About Offline Computers" (p. 36).
- Protected computers have Security for Virtualized Environments protection installed and no security risks have been detected.
- Vulnerable computers have Security for Virtualized Environments protection installed, but specific conditions prevent proper protection of the system. The report details show you which security aspects need to be addressed.

Computer Status

Provides you with various status information concerning the computers on which the Security for Virtualized Environments protection is installed.

- Protection update status
- Antimalware protection status
- License status
- Network activity status (online/offline)

You can apply filters by security aspect and status to find the information you are looking for.

Top 10 Most Infected Computers

Shows you the top 10 most infected computers in the network over a specific time period.

Top 10 Detected Malware

Shows you the top 10 malware threats detected in the network over a specific time period.

Malware Activity

Provides you with overall and per computer details about the malware threats detected in the network over a specific time period. You can see:

- Number of detections (files that have been found infected with malware)
- Number of infections solved (files that have been successfully disinfected or isolated in the local quarantine folder)
- Number of infections blocked (files that could not be disinfected, but to which access has been denied; for example, an infected file stored in some proprietary archive format)

Computer Malware Status

Helps you find out how many and which of the protected computers have been affected by malware over a specific time period and how the threats have been dealt with. Computers are grouped based on these criteria:

- Computers with no detections (no malware threat has been detected over the specified time period)
- Computers with resolved malware (all detected files have been successfully disinfected or isolated in the local quarantine folder)
- Computers with blocked malware (some of the detected files have been denied access to)

Notifications

This portlet, which by default is minimized, informs you of existing security risks in the virtualized environment. Notifications are also sent to you by email.

5.2. Managing Portlets

The dashboard is easy to configure based on individual preferences.

You can minimize portlets to focus on the information you are interested in. When you minimize a portlet, it is removed from the dashboard and its title bar appears at the bottom of the page. The remaining portlets are automatically resized to fit the screen. All minimized portlets can be restored at any time.

To manage a portlet, use the buttons on its title bar:

↻ The refresh option will re-load data for each portlet.

▾≡ Click this button to configure portlet options. Some portlets include data from a specific time period.

▬ Minimize the portlet to the bottom of the page.

⧉ Restore a minimized portlet.

6. Managing Computers (Virtual Machines)

To view information on the computers (virtual machines) in your virtualized environment and to manage their security, go to the **Computers > View Computers** page. Besides the virtual machines protected by Security for Virtualized Environments, you can also view other VMs detected in the virtual network. Physical computers might also be detected if they are connected to the virtual network.

From the **View Computers** page, you can do the following:

- Organize virtual machines into groups to manage their security more efficiently. This is recommended if you manage a larger number of VMs (tens or more).
- Check system and protection details.
- View and change security policy settings.
- Remotely run tasks on virtual machines to scan them, to install or remove the Security for Virtualized Environments protection. To find out more, refer to "Running and Managing Tasks" (p. 60).
- Create quick reports in order to obtain various security information about specific virtual machines.

The page consists of two panes:

- Left-side pane helps you organize virtual machines into groups.
- Right-side pane contains a table displaying the virtual machines and useful information about them:
  - VM name and IP address.
  - Operating system installed on the VM.
  - Update status of the Security for Virtualized Environments protection.
  - When the VM has last been seen.

Note
It is important to monitor the **Last Seen** field as long inactivity periods might indicate a communication issue or a disconnected computer.

The icon next to the name of each computer informs you about that computer:

🖥 Virtual machine on which the Security for Virtualized Environments protection is installed.

🖥 Virtual or physical computer on which the Security for Virtualized Environments protection has not been installed yet, detected in the virtual network by protected VMs.
🖥 Computer you have excluded from management.

6.1. About Managed, Unmanaged and Excluded Computers

Computers are organized into three main categories:

- **Managed Computers** - VMs on which the Security for Virtualized Environments protection is installed.
- **Unmanaged Computers** - detected computers on which the Security for Virtualized Environments protection has not been installed yet.

> **Note**
>
> Once installed on a VM, Silent Agent automatically detects computers visible in the local network. Unmanaged computers will be available on the **View Computers** page as they are detected. Physical computers might also be detected if they are connected to the virtual network.

- **Excluded Computers** - computers that you have excluded from management.

Use the **Show** menu located above the table (to the left) to choose the computer categories to be displayed.

6.2. About Offline Computers

Offline computers normally have Security for Virtualized Environments protection installed, but there is no recent activity from Silent Agent. Computers are considered to be offline if Silent Agent is inactive for more than 1 minute.

Possible reasons why computers appear offline:

- Computer is shut down, sleeping or hibernating.

> **Note**
>
> Computers normally appear online even when they are locked or the user is logged off.

- Silent Agent has been manually uninstalled from the computer. In such cases, you must manually delete the computer from the **Computers > View Computers** page.
- Silent Agent cannot communicate with Security Console. The communication port is `8082`. Communication might be blocked by the local firewall or by a network firewall or router.

- Silent Agent might not be working properly.

To find out for how long computers have been inactive:

1. Go to the **Computers > View Computers** page.
2. Check the **Last Seen** field. To easily find the information you need, choose **Offline** from the corresponding menu and then sort computers by inactivity period by clicking the column header.

You can ignore shorter periods of inactivity (minutes, hours) as they are likely the result of a temporary condition. For example, the computer is currently shut down.

Longer inactivity periods (days, weeks) usually indicate a problem with the computer.

6.3. Listing Security Virtual Appliance Machines

To view the Security Virtual Appliance machines deployed in your environment:

1. Go to the **Computers > View Computers** page.
2. Click the **Show** menu located above the table (to the left) and choose **Security Virtual Appliances**.

You can only view information about the existing Security Virtual Appliance machines. There are no quick tasks or reports available for Security Virtual Appliance.

If the **Update** column displays the **pending** status, an update is available for the corresponding Security Virtual Appliance machine. Security Virtual Appliance can only be updated manually from the virtual machine console. To find out more information, search for the release notes of the available update on the Bitdefender Support Center.

6.4. Using Groups

If you manage a larger number of virtual machines (tens or more), you will probably need to organize them into groups. Organizing VMs into groups helps you manage them more efficiently. A major benefit is that you can use group policies to meet different security requirements.

Groups are displayed in the left-side pane of the **View Computers** page. Initially, there is only the root group named after your company. All VMs on which you have installed the Security for Virtualized Environments protection, as well as those detected in the network, are automatically placed in this group. You can organize your VMs by creating groups under the root group and then moving VMs to the appropriate group.

Important

Please note the following:

- A group can contain both VMs and other groups.

- When selecting a group in the left-side pane, you can view all VMs except those placed into its sub-groups. To view all VMs included in the group and in its sub-groups, right-click the group and choose **View all computers**.

Before you start creating groups, think of the reasons why you need them and come up with a grouping scheme. For example, you can group VMs based on one or a mix of the following criteria:

- Host computer or virtual network they are part of.
- Organization structure (Sales, Marketing, Quality Assurance, Software Development, Management etc.).
- Security needs (Desktops, Laptops, Servers etc.).
- Location (Headquarter, Local Offices, Remote Workers, Home Offices etc.).

Creating Groups

To divide your virtualized environment into groups:

1. Right-click the root group in the left-side pane and choose **Create group**. A new group (named **New Group**) will appear under the parent group in the tree menu.
2. Rename the newly created group.
3. Follow the previous steps to create additional groups.
4. Move VMs from the root group to the appropriate group.

To create sub-groups:

1. Right-click the group into which the new sub-group is to be included and select **Create group**. A new group (named **New Group**) will appear under the parent group in the tree menu.
2. Rename the newly created group.

Renaming Groups

To rename a group, right-click it, select **Rename group** and enter the new name.

Moving Groups

Groups can be moved anywhere inside the group hierarchy. To move a group, drag and drop it from the current location to the new one.

Moving VMs to Another Group

To move VMs from the current group to another group:

1. Select the check boxes corresponding to the VMs you want to move.
2. Drag and drop your selection to the desired group in the left-side pane.

Deleting Groups

You can only delete empty groups (which contain no computers).

To delete a group:

1. Move all the computers in the group to other groups. If the group includes sub-groups, you can choose to move entire sub-groups rather than individual computers.
2. Right-click the group and select **Delete group**. You will have to confirm your action by clicking **Yes**.

6.5. Searching and Sorting Computers

Depending on the number of VMs, the computers table can span several pages (only 10 entries are displayed per page by default). To move through the pages, use the navigation buttons at the bottom of the table. To change the number of entries displayed on a page, select an option from the menu next to the navigation buttons.

If there are too many entries, you can use the search boxes or the menus under the column headers to filter displayed data. For example, you can search for a specific computer or choose to view only the offline computers.

You can also click column headers to sort data by a specific column. For example, if you want to order computers by name click the **Computer Name** heading. If you click the heading again, the computers will be displayed in reverse order.

When using groups, select a group in the left-side pane to view the computers it contains. Please note that computers placed in sub-groups are not displayed by default. To view all computers included in the group and in its sub-groups, right-click the group and choose **View all computers**.

6.6. Checking System and Protection Details

From the **View Computers** page, you can find various information on any computer:

- General computer details, such as its name, IP address or operating system.
- Security policy settings.
- License and update status of the Security for Virtualized Environments protection.
- Antimalware protection status (enabled or disabled).
- Information concerning malware detected on the computer.
- Latest scan log.

To get system and protection details:

1. Go to the **Computers > View Computers** page.
2. If you have organized virtual machines into groups, select the desired group from the left-side pane. To view all of your VMs, right-click the root group and choose **View all computers**.
3. Click the name of the VM you are interested in. The computer details page is displayed. Click available links for more details.

6.7. Checking and Changing Security Settings

Security settings on virtual machines are managed using policies. For more information, refer to "Security Policies" (p. 43).

To view the security settings applied on a particular virtual machine:

1. Go to the **Computers > View Computers** page.
2. If you have organized virtual machines into groups, select the desired group from the left-side pane. To view all of your VMs, right-click the root group and choose **View all computers**.
3. Click the name of the VM you are interested in.
4. Check the **Active policy** field. Click the policy name to view its settings.
5. If the default policy is active, you cannot change security settings. You must create a new policy and assign it to the VM.

   If you have already assigned a new policy to the VM, you can change security settings as needed. Please note that any change you make will also apply to all other VMs on which the policy is active.

6.8. Creating Quick Reports

To create quick reports from the **View Computers** page:

1. Click the **Show** menu located above the table (to the left) and choose **Managed Computers**.
2. If you have organized virtual machines into groups, select the desired group from the left-side pane. To view all of your VMs, right-click the root group and choose **View all computers**.
3. Select the check boxes corresponding to the VMs to be included in the report.
4. Click **Reports** and choose the report type from the menu. Activity reports will only include data from the last week.

6.9. Excluding Computers from Management

Silent Agent automatically detects all computers visible in the local network. Detected computers are displayed in Security Console as unmanaged so that you can remotely install protection on them. Physical computers might also be detected if they are connected to the virtual network.

If you do not plan to manage some of the detected computers, you can move them to the **Excluded Computers** list. In this way, you will not be bothered about them.

To exclude detected computers from management:

1. Go to the **Computers > View Computers** page.
2. Click the **Show** menu located above the table (to the left) and choose **Unmanaged Computers**.
3. Select the check boxes corresponding to the virtual machines you want to exclude.
4. Click the **Tasks** button in the upper-right corner of the page and choose **Exclude**.

If protection is manually installed on an excluded virtual machine, it will be moved automatically to the **Managed Computers** list.

To view excluded computers:

1. Go to the **Computers > View Computers** page.
2. From the menu above the table, choose **Excluded Computers**.
3. If you want to restore an excluded computer, you must delete it from the console. Click the **Tasks** button in the upper-right corner of the page and choose **Delete**.

6.10. Deleting Computers from Console

There are several situations when you may want to delete computers from the console:

- To clean up the Managed Computers list of duplicate entries or inactive computers. For example, when reinstalling the operating system on a virtual machine without first removing Silent Agent, you must manually delete the corresponding entry from the list.
- To clean up the Unmanaged Computers list of duplicate entries or inactive computers.
- To restore an excluded computer.

If the deleted computer is still connected to the network, it will eventually be detected and displayed as unmanaged in the console.

To delete managed virtual machines:

1. Go to the **Computers > View Computers** page.
2. Click the **Show** menu located above the table (to the left) and choose **Managed Computers**.

3. If you have organized virtual machines into groups, select the desired group from the left-side pane. To view all of your VMs, right-click the root group and choose **View all computers**.
4. Select the check boxes corresponding to the VMs you want to delete.

> **Note**
>
> - Check the **Last Seen** field to identify VMs inactive for a long time.
> - Search or sort computers by name to identify duplicate entries or VMs that have been permanently disconnected from the network.

5. Click the **Tasks** button in the upper-right corner of the page and choose **Uninstall Silent Agent**. Protection will be uninstalled from selected VMs and they will be deleted from the console.

To delete excluded computers:

1. Go to the **Computers > View Computers** page.
2. From the menu above the table, choose **Excluded Computers**.
3. Select the check boxes corresponding to the computers you want to delete.
4. Click the **Tasks** button in the upper-right corner of the page and choose **Delete**.

To delete unmanaged computers:

1. You must first exclude from management the unmanaged computers you want to delete.
2. Delete excluded computers as described previously.

7. Security Policies

Once installed, the Security for Virtualized Environments protection can be configured and managed from Security Console using security policies. A policy specifies the security settings to be applied on target virtual machines.

Immediately after installation, virtual machines are assigned the default policy, which is preconfigured with the recommended protection settings. The default policy is intended to be used as a template for creating new policies.

Because the default policy cannot be edited, you must create at least one new policy in order to change protection settings on virtual machines. If you manage a larger number of virtual machines (tens or more), you may want to create several policies to apply different settings based on security requirements.

This is what you need to know about policies:

- There is a single default policy template, which allows configuring all protection settings. Some of the policy settings are not available for Linux and are indicated as such in this documentation.
- Policies are pushed to target virtual machines immediately after creating or modifying them. Settings should be applied on virtual machines in less than a minute (provided they are online). If a virtual machine is not online, settings will be applied as soon as it gets back online.
- Policies can be assigned either to individual virtual machines or to groups of virtual machines. The policy target cannot be a mix of virtual machines and groups.
- Several policies can be assigned at a given moment to a virtual machine. However, there will always be only one active policy: the one that was last created or modified.
- On-access scanning options only have effect on Windows machines and on the specific Linux machines on which on-access scanning support is enabled.

To view and manage security settings and policies, go to the **Policies > View Policies** page. Existing policies are displayed in the table. For each policy, you can see:

- Policy name.
- Policy target (virtual machines or groups the policy applies to).
- How many of the target virtual machines comply with the policy.
- User who created the policy.
- Time when the policy was last modified.

7.1. Creating New Policies

To create a new policy:

1. Go to the **Policies > New Policy** page.
2. Enter a suggestive name for the policy. When choosing a name, consider the purpose and target of the policy.
3. Choose a policy template from the menu. The new policy will be initialized with the settings of the template policy.
4. Configure the policy target (virtual machines to which the policy will apply). You can choose one of the following options:
   - **Groups.** Select this option to apply the policy to groups of managed virtual machines. Click the corresponding link and choose the desired groups.

     Note
     The policy will apply automatically to any virtual machine that is later added to a selected group.

   - **Computers.** Select this option to apply the policy to individual virtual machines. Click the corresponding link and choose the desired virtual machines.
5. Click **Submit** to create the policy and to go to the policy page.
6. Next, configure the policy settings. For detailed information, refer to "Configuring Policy Settings" (p. 44).
7. Click **Save** to save changes and apply protection settings to the target virtual machines. The new policy will be displayed on the **View Policies** page.

7.2. Configuring Policy Settings

Policy settings can be initially configured when creating the policy. Later on, you can change them as needed anytime you want.

Important
You cannot edit the default policy. Changes will not be saved. To change protection settings, create a new policy.

To change the settings of a policy:

1. Go to the **Policies > View Policies** page.
2. Click the policy name. This will open the policy page.
3. Configure the policy settings as needed. Settings are organized into the following categories:

- Summary
- General
- Antimalware

You can select the settings category using the menu on the left-side of the page.

Important

Some of the policy settings are not available for Linux:

- **General.** The scan server settings on the Advanced tab and the proxy settings on the Update tab apply to both Windows and Linux. All other configuration options in this category are available only for the Windows version of Silent Agent.
- **Antimalware.** On-access scanning options only have effect on Windows machines and on the specific Linux machines on which on-access scanning support is enabled.

4. Click **Save** to save changes and apply them to the target virtual machines. To leave the policy page without saving changes, click **Cancel**.

7.2.1. Summary

The Summary page contains general policy details:

- **Policy name.** You can rename the policy by entering the new name in this field.
- **Specified target.** If you want to change the policy target, click the link and select the new target.
- **Complying.** This field indicates how many of the target virtual machines are compliant with the policy.

7.2.2. General

General settings help you manage user interface display options, update preferences, password protection and other settings of Silent Agent.

The settings are organized under the following tabs:

- Display
- Advanced
- Update

Important

The scan server settings on the Advanced tab and the proxy settings on the Update tab apply to both Windows and Linux. All other configuration options in this category are available only for the Windows version of Silent Agent.

Display Tab

In this section you can configure the user interface display options. Silent Agent has a minimal user interface, which only allows users on the virtual machines to check protection status and events.

- **Silent Mode.** When Silent Mode is enabled, the Silent Agent graphical user interface (GUI) is not loaded automatically at system startup, freeing up associated resources. At the same time, the Silent Agent icon B is not displayed in the Windows notification area (also known as the system tray). The notification area icon allows users to open the main program window and access product information. Even if the notification area icon is not available, users can still access the main program window from the Windows Start menu.
- **Technical Support Information.** Fill in the fields to customize the technical support and contact information available in Silent Agent. Users can access this information from the Silent Agent window by clicking the i icon in the lower-right corner (or, alternatively, by right-clicking the B Silent Agent icon in the system tray and selecting **About**).

Advanced Tab

In this section you can configure general settings and the uninstall password.

- **Remove events older than {30} days.** Silent Agent keeps a detailed log of events concerning its activity on the computer. By default, events are deleted from the log after 30 days. If you want to change this interval, choose a different option from the menu.
- **Submit crash reports to Bitdefender.** Select this option so that reports will be sent to Bitdefender Labs for analysis if Silent Agent crashes. The reports will help our engineers find out what caused the problem and prevent it from occurring again. No personal information will be sent.
- **Password configuration.** To prevent users with administrative rights from uninstalling protection, you must set a password.

  To set the password, or to change the current password, select **Enable password** and enter the desired password. To remove password protection, select **Disable password**.
- **Scan Servers.** Silent Agent is configured by default to use the Security Virtual Appliance specified in the Security Console company account. In environments with multiple Security Virtual Appliance installations, you must specify the Security Virtual Appliance instances Silent Agent can connect to. You can change the existing Security Virtual Appliance address or add the addresses of other Security Virtual Appliance instances.

  Silent Agent selects one of the specified Security Virtual Appliance instances based on assigned priority, availability and current load (normal, overload, underload).

- If the Security Virtual Appliance with priority 1 is initially unavailable, or becomes unavailable later on, Silent Agent attempts to connect to the Security Virtual Appliance with priority 2 and so on, until it finds a Security Virtual Appliance that is available.
- If the selected Security Virtual Appliance instance repeatedly reports being overloaded, Silent Agent reinitiates the selection process, attempting to connect to a Security Virtual Appliance instance having a normal load. If no such instance is available, Silent Agent connects to a Security Virtual Appliance instance that is underloaded or less overloaded (if any).
- If the selected Security Virtual Appliance instance repeatedly reports being underloaded, Silent Agent searches for and connects to a Security Virtual Appliance instance having a normal load (if any).

Note
The load balancing mechanism helps improve performance, quickly recover in case of Security Virtual Appliance failures and save resources on hosts on which Security Virtual Appliance is underloaded.

To add a Security Virtual Appliance:

1. Enter the IP address or name of the Security Virtual Appliance in the edit field.
2. If you want to secure communication between Silent Agent and the Security Virtual Appliance using Secure Sockets Layer (SSL), select **Use SSL**. Take into account that activating SSL encryption for the Silent Agent - Security Virtual Appliance traffic will slightly impact performance.

   The Silent Agent - Security Virtual Appliance communication port depends on the use of SSL encryption:

   - The port used for SSL-secured communication is `7083`.
   - The port used for unsecured communication is `7081`.
3. Click the ✚ **Add** button.
4. Use the Up/Down icons in the **Action** column to set the priority of the Security Virtual Appliance. If the first scan server is unavailable, agents will try the second one and so on.

Important
Set the preferred Security Virtual Appliance for selected Silent Agent instances with priority 1.

To remove a Security Virtual Appliance from the list, click the corresponding ✖ **Remove** button.

Update Tab

In this section you can configure the Silent Agent update settings. Updates are very important as they allow countering the latest threats.

- **Update interval (hours).** Silent Agent automatically checks for, downloads and installs product updates every hour (default setting). Automatic updates are performed silently in the background.

  To change the automatic update interval, choose a different option from the menu. Please note that automatic update cannot be turned off.

  > **Note**
  >
  > Although the scan itself is performed in the Security Virtual Appliance, which is updated automatically on a regular basis, Silent Agent has a reduced set of signatures that are used for pre-scan operations (such as extracting files from archives). The local signature files of the agent are updated automatically together with those on the Security Virtual Appliance, regardless of how you configure this setting. All updates are delivered via the Security Console Appliance, so there is no increase in Internet traffic.

- **Postpone reboot.** Some updates require a system restart to install and work properly. By selecting this option, the program will keep working with the old files until the computer is restarted, without informing the user. Otherwise, a notification in the user interface will prompt the user to restart the system whenever an update requires it.

  If you choose to postpone reboot, you can set a convenient time when the virtual machines will reboot automatically if (still) needed. This option can be very useful for virtualized servers. Select **If needed, reboot after installing updates** and specify when it is convenient to reboot (daily or weekly on a certain day, at a certain time of day).

- **Enable proxy.** Select this option if virtual machines connect to the Internet through a proxy server. There are two options to set the proxy settings:
  - **Import proxy settings from default browser.** Silent Agent can import proxy settings from the most popular browsers, including the latest versions of Internet Explorer, Mozilla Firefox and Opera.
  - **Use custom proxy settings.** If you know the proxy settings, select this option and then specify them:
    - **Server** - type in the IP of the proxy server.
    - **Port** - type in the port used to connect to the proxy server.
    - **User name** - type in a user name recognized by the proxy.
    - **Password** - type in the valid password of the previously specified user.

7.2.3. Antimalware

Security for Virtualized Environments protects virtual machines against all kinds of malware threats (viruses, Trojans, spyware, rootkits, adware and so on). Antimalware protection has two components:

- On-access scanning: prevents new malware threats from entering the system.
- On-demand scanning: allows detecting and removing malware already residing in the system.

Based on the settings configured in the policy, the agent installed on the virtual machine decides what files need to be scanned and sends scan requests to the Security Virtual Appliance. The actual scan is performed in the Security Virtual Appliance, using both signature-based and heuristic detection methods. The scan result is returned to the agent, which takes the appropriate action based on policy settings and instructions received from the Security Virtual Appliance.

By default, when a virus or other malware is detected, Silent Agent will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection. Disinfection instructions are obtained from the Security Virtual Appliance. Files that cannot be disinfected are moved to quarantine in order to contain the infection. When a virus is in quarantine it cannot do any harm because it cannot be executed or read. Quarantined files are stored locally on the virtual machines, but they can be viewed and managed remotely from the Quarantine page.

Advanced users can configure scan exclusions if they do not want specific files or file types to be scanned.

The settings are organized under the following tabs:

- On-access
- On-demand
- Exclusions
- Quarantine

Important
On-access scanning options only have effect on Windows machines and on the specific Linux machines on which on-access scanning support is enabled.

On-access Tab

On-access scanning prevents new malware threats from entering the system by scanning files as they are accessed (opened, moved, copied or executed).

To configure on-access scanning:

1. Use the switch to turn on-access scanning on or off. If you turn off on-access scanning, virtual machines will be vulnerable to malware.

2. Choose the protection level that best suits your security needs. For a quick configuration, drag the slider along the scale to a predefined protection level. Use the description on the right side of the scale to guide your choice.
3. Advanced users can configure the scan settings in detail by selecting the **Custom** check box and clicking the corresponding button.

Custom options. The scan settings are organized under two tabs, as follows:

- **File Types.** You can set Silent Agent to scan all accessed files (regardless of their file extension), application files only or specific file extensions you consider to be dangerous. Scanning all accessed files provides best protection, while scanning applications only can be used for better system performance.

  Note

  Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "List of Application File Types" (p. 83).

  If you want only specific extensions to be scanned, choose **User defined extensions** from the corresponding menu and enter the extensions (separated by semicolons ";") in the corresponding field.

- **Archives.** Select **Scan inside archives** if you want to enable on-access scanning of archived files. Scanning inside archives is a slow and resource-intensive process, which is therefore not recommended for real-time protection. Archives containing infected files are not an immediate threat to system security. The malware can affect the system only if the infected file is extracted from the archive and executed without having on-access scanning enabled.

  If you decide on using this option, you can configure the following optimization options:

  - **Limit archive size to {10} MB.** You can set a maximum accepted size limit of archives to be scanned on-access. Select the corresponding check box and type the maximum archive size (in MB).
  - **Maximum archive depth (levels).** Select the corresponding check box and choose the maximum archive depth from the menu. For best performance choose the lowest value, for maximum protection choose the highest value.

  Note

  Packed files and ZIP archives under 256 KB are scanned automatically even if the **Scan inside archives** option is disabled.

- **Miscellaneous.** Select the corresponding check boxes to enable the desired scan options.

  - **Scan only new or changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.

  - **Deferred scanning.** Select this option to prioritize the scanning of files accessed for read operations over those accessed for write operations. This is intended to optimize the scan process.
  - **Scan for keyloggers.** Keyloggers record what you type on your keyboard and send reports over the Internet to a malicious person (hacker). The hacker can find out sensitive information from the stolen data, such as bank account numbers and passwords, and use it to gain personal benefits.

- **Scan Actions.** Depending on the type of detected file, the following actions are taken automatically:
  - **Infected files.** Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Silent Agent can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

    If an infected file is detected, Silent Agent will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

    > **Important**
    > For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

  - **Suspect files.** Files are detected as suspicious by the heuristic analysis. Because B-HAVE is a heuristic analysis technology, Silent Agent cannot be sure that the file is actually infected with malware. Suspect files cannot be disinfected, because no disinfection routine is available.

    When a suspect file is detected, users will be denied access to that file in order to prevent a potential infection.

  Though not recommended, you can change the default actions. The following actions are available:

  Disinfect
  Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.

  Move to quarantine
  Move detected files from their current location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the Quarantine page of the console.

  Delete
  Delete detected files from the disk, without any warning. It is advisable to avoid using this action.

  Deny access
  Deny access to detected files.

On-demand Tab

In this section you can configure antimalware scan tasks that will run regularly on the target virtual machines, according to the schedule you specify. Scans are performed silently in the background, without the user knowing about them.

Though not mandatory, it is recommended to schedule a comprehensive system scan to run weekly on all computers. Scanning computers regularly is a proactive security measure that can help detect and block malware that might evade real-time protection features.

Managing Scan Tasks

The Scan Tasks table informs you of the existing scan tasks, providing important information on each of them:

- Task name and type.
- Time when the task was first run.
- Schedule based on which the task runs regularly (recurrence).
- Actions you can take on the scan task.

You can easily configure the default scan task to run as needed. **Full System Scan** checks the entire system for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others. The scan options of the default scan task are preconfigured and you cannot change them.

Besides the default scan task (which you cannot delete or duplicate), you can create as many custom scan tasks as you want. A custom scan task allows you to choose the specific locations to be scanned and to configure the scan options.

To create and configure a new task, click **Add Task** and choose the type of task you want to create. To change the settings of an existing task, click the name of that task. Refer to the following topic to learn how to configure the task settings.

To remove a task from the list, click the corresponding ✖ **Remove** button.

Configuring Scan Tasks

The scan task settings are organized under three tabs: General - set task name, execution schedule and scan target; Options - choose a scan profile for quick configuration of the scan settings; Advanced - configure scan settings in detail. The Options and Advanced tabs are available for custom scan tasks only. The Advanced tab can be accessed only after selecting the **Custom** check box on the Options tab.

Options are described hereinafter from the first tab to the last:

- **Task Details.** Choose a suggestive name for the task to help easily identify what it is about. When choosing a name, consider the scan task target and possibly the scan settings.

- **Scheduler.** Use the scheduling options to configure the scan schedule. You can set the scan to run every few hours, days or weeks, starting with a specified date and time.

  Please consider that virtual machines must be on when the schedule is due. A scheduled scan will not run when due if the virtual machine is turned off, hibernating or in sleep mode, or if no user is logged on. In such situations, the scan will be postponed until next time.

- **Target.** Add to the list all the locations you want to be scanned on the target virtual machines.

  To add a new file or folder to be scanned:

  1. Choose from the menu either a predefined location or the **Specific paths** option.
  2. Specify the path to the object to be scanned in the edit field.
     – If you have chosen a predefined location, complete the path as needed. For example, to scan the entire `Program Files` folder, it suffices to select the corresponding predefined location from the menu. To scan a specific folder from `Program Files`, you must complete the path by adding a backslash (\) and the folder name.

       Note
       For more information, refer to “Using System Variables” (p. 83).

     – If you have chosen **Specific paths**, enter the full path to the object to be scanned. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target VMs.
  3. Click the ✚ **Add** button.

  To edit an existing location, click it. To remove a location from the list, click the corresponding ✖ **Remove** button.

- **Scan Options.** For a quick configuration of the scan options, choose one of the predefined scan profiles. Drag the slider along the scale to the profile that best suits your security needs. Use the description on the right side of the scale to guide your choice.

  Based on the selected profile, the scan options on the **Advanced** tab are automatically configured. However, if you want to, you can configure them in detail. To do that, select the **Custom** check box and then go to the **Advanced** tab.

- **Scan Operations.**
  – **Run the task with low priority.** Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
  – **Shut down computer when the task is finished.** This option may be useful when you run scans during off-working hours.

- **File Types.** Use these options to specify which types of files you want to be scanned. You can set Silent Agent to scan all files (regardless of their file extension), application files only or specific file extensions you consider to be dangerous. Scanning all files provides best protection, while scanning applications only can be used to perform a quicker scan.

  Note

  Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "List of Application File Types" (p. 83).

  If you want only specific extensions to be scanned, choose **User defined extensions** from the corresponding menu and enter the extensions (separated by semicolons ";") in the corresponding field.

- **Archives.** Archives containing infected files are not an immediate threat to system security. The malware can affect the system only if the infected file is extracted from the archive and executed without having real-time protection enabled. However, it is recommended to use this option in order to detect and remove any potential threat, even if it is not an immediate threat.

  Note

  Scanning archived files increases the overall scanning time and requires more system resources.

  – **Scan inside archives.** Select this option if you want to check archived files for malware. If you decide on using this option, you can configure the following optimization options:

    - **Limit archive size to {10} MB.** You can set a maximum accepted size limit of archives to be scanned. Select the corresponding check box and type the maximum archive size (in MB).

    - **Maximum archive depth (levels).** Select the corresponding check box and choose the maximum archive depth from the menu. For best performance choose the lowest value, for maximum protection choose the highest value.

    Note

    Packed files and ZIP archives under 256 KB are scanned automatically even if the **Scan inside archives** option is disabled.

  – **Scan email archives.** Select this option if you want to check email archives for malware.

- **Miscellaneous.** Select the corresponding check boxes to enable the desired scan options.

  – **Scan memory.** Select this option to scan programs running in the system's memory.

  - **Scan cookies.** Select this option to scan the cookies stored by browsers on the virtual machine.
  - **Scan for rootkits.** Select this option to scan for rootkits and objects hidden using such software.
  - **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
  - **Ignore commercial keyloggers.** Select this option if commercial keylogger software is installed on the target VMs. Commercial keyloggers are legitimate computer monitoring software whose most basic function is to record everything that is typed on the keyboard.

- **Scan Actions.** Depending on the type of detected file, the following actions are taken automatically:
  - **Infected files.** Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Silent Agent can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

    If an infected file is detected, Silent Agent will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

    Important
    For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

  - **Suspect files.** Files are detected as suspicious by the heuristic analysis. Because B-HAVE is a heuristic analysis technology, Silent Agent cannot be sure that the file is actually infected with malware. Suspect files cannot be disinfected, because no disinfection routine is available.

    Scan tasks are configured by default to ignore suspect files. You may want to change the default action in order to move suspect files to quarantine. Quarantined files are sent for analysis to Bitdefender Labs on a regular basis. If malware presence is confirmed, a signature is released to allow removing the malware.
  - **Rootkits.** Rootkits represent specialized software used to hide files from the operating system. Though not malicious in nature, rootkits are often used to hide malware or to conceal the presence of an intruder into the system.

    Detected rootkits and hidden files are ignored by default.

  Though not recommended, you can change the default actions. You can specify a second action to be taken if the first one fails and different actions for each category. Choose from the corresponding menus the first and the second action to be taken on each type of detected file. The following actions are available:

Disinfect

Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.

Move to quarantine

Move detected files from their current location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the Quarantine page of the console.

Delete

Delete detected files from the disk, without any warning. It is advisable to avoid using this action.

Take no action

No action will be taken on detected files. These files will only appear in the scan log.

Exclusions Tab

In this section you can configure scan exclusion rules. Exclusions can apply to on-access scanning or on-demand scanning, or to both. Based on the object of the exclusion, there are four types of exclusions:

- **File exclusions:** the specified file only is excluded from scanning.
- **Folder exclusions:** all files inside the specified folder and all of its subfolders are excluded from scanning.
- **Extension exclusions:** all files having the specified extension are excluded from scanning.
- **Process exclusions:** any object accessed by the excluded process is also excluded from scanning.

Important

Scan exclusions are to be used in special circumstances or following Microsoft or Bitdefender recommendations. For an updated list of exclusions recommended by Microsoft, refer to this article. If you have an EICAR test file that you use periodically to test antimalware protection, you should exclude it from on-access scanning.

Use the switch to turn exclusions on or off.

To configure an exclusion rule:

1. Select the exclusion type from the menu.
2. Depending on the exclusion type, specify the object to be excluded as follows:
   - **Extension exclusions.** Enter the file extension you want to exclude. Before you exclude extensions, document yourself to see which are commonly targeted by malware and which are not.

- **File, folder and process exclusions.** You must specify the path to the excluded object on the target virtual machines.
    a. Choose from the menu either a predefined location or the **Specific paths** option.
    b. If you have chosen a predefined location, complete the path as needed. For example, to exclude the entire `Program Files` folder, it suffices to select the corresponding predefined location from the menu. To exclude a specific folder from `Program Files`, you must complete the path by adding a backslash (\) and the folder name. For process exclusions, you must also add the name of the application's executable file.

        > **Note**
        > For more information, refer to “Using System Variables” (p. 83).

    c. If you have chosen **Specific paths**, enter the full path to the object to be excluded. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target VMs.

3. Select the types of scanning the rule will apply to. Some exclusions may be relevant for on-access scanning only, some for on-demand scanning only, while others may be recommended for both.
4. Click the ✚ **Add** button. The new rule will be added to the list.

To remove a rule from the list, click the corresponding ✖ **Remove** button.

Quarantine Tab

In this section you can configure the quarantine settings. You can set Silent Agent to automatically perform the following actions:

- **Delete files older than {30} days.** By default, quarantined files older than 30 days are automatically deleted. If you want to change this interval, choose a different option from the menu.
- **Send quarantined files to Bitdefender for further analysis.** Keep this option selected to automatically send quarantined files to Bitdefender Labs. The sample files will be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

  By default, quarantined files are automatically sent to Bitdefender Labs every hour. If you want to change this interval, choose a different option from the menu.
- **Rescan quarantine after malware signatures update.** Keep this option selected to automatically scan quarantined files after each malware signatures update. Cleaned files are automatically moved back to their original location.

7.3. Monitoring Policy Execution

To check if a policy has been applied on the target virtual machines:

1. Go to the **Policies > View Policies** page.
2. Check the status in the **Complying** column. You can see how many of the target virtual machines are compliant.
3. Click the link to open a window with more details. All virtual machines that have been assigned the policy are displayed in a table. You can check the compliance status for each target machine.

   Note

   If there are too many entries, you can use the search boxes or the menus under the column headers to filter displayed data. You can also click column headers to sort data by a specific column. To move through the pages, use the navigation buttons at the bottom of the table.

7.4. Checking and Changing Policy Assignments

Policies can be assigned either to individual virtual machines or to groups of virtual machines.

To check and change policy assignments:

1. Go to the **Policies > View Policies** page.
2. Click the policy name. This will open the policy page.
3. Assigned virtual machines or groups are listed in the **Specified targets** field. Click the link to see more details and change current assignments. Please note that you cannot change the target type (virtual machines or groups).
4. To change the current assignments, follow these steps:
   a. Depending on the target type, proceed as follows:
      - If the policy has originally been assigned to groups, select the new groups you want the policy to apply to.
      - If the policy has originally been assigned to virtual machines, you must select the new virtual machines you want the policy to apply to. First of all, clear the **Display only the selected computers** check box in the upper-left corner of the window. Next, select the check boxes corresponding to the desired virtual machines.

      Note

      If there are too many entries, you can use the search boxes or the menus under the column headers to filter displayed data. You can also click column headers to sort data by a specific column. To move through the pages, use the navigation buttons at the bottom of the table.

b. Click **Change** to save the new target.

c. Click **Save** to apply policy changes.

7.5. Renaming Policies

Policies should have suggestive names so that you or other administrator can quickly identify them.

To rename a policy:

1. Go to the **Policies > View Policies** page.
2. Click the policy name. This will open the policy page.
3. Enter a new name for the policy.
4. Click **Save** to apply policy changes.

7.6. Deleting Policies

If you no longer need a policy, delete it. Once the policy is deleted, the virtual machines to which it used to apply will be assigned the policy of the parent group. If no other policy applies, the default policy will be enforced eventually.

To delete a policy:

1. Go to the **Policies > View Policies** page.
2. Select the corresponding check box.
3. Click the **Delete** button in the upper-right corner of the page. You will have to confirm your action by clicking **Yes**.

8. Running and Managing Tasks

From the **View Computers** page, you can remotely run a number of administrative tasks on VMs. This is what you can do:

- Install protection on detected VMs.
- Scan managed VMs for malware.
- Remove protection from VMs.

Note
Remote installation and removal tasks are available for Windows VMs only.

Tasks can be monitored and managed from the **Computers > View Tasks** page.

8.1. Installing Protection on Unmanaged VMs

Once you have installed the Security for Virtualized Environments agent on a virtual machine, it will automatically detect computers in the local network. The Security for Virtualized Environments protection can then be installed on those computers remotely from the console. Remote installation is performed in the background, without the user knowing about it.

Warning

Before installation, be sure to uninstall existing antimalware software from VMs. Installing Security for Virtualized Environments over existing security software may affect their operation and cause major problems with the system.

To remotely install the Security for Virtualized Environments protection on one or several detected VMs:

1. Go to the **Computers > View Computers** page.
2. Click the **Show** menu located above the table (to the left) and choose **Unmanaged Computers**.
3. If you have organized VMs into groups, select the desired group from the left-side pane. To view all of your VMs, right-click the root group and choose **View all computers**.
4. Select the check boxes corresponding to the VMs on which you want to install protection.
5. Click **Tasks** and choose **Install** from the menu. The Installation Options window will appear.

6. Provide the administrative credentials required for remote authentication on selected virtual machines.

   Enter the user name and password of an administrator account for each of the selected computers. If computers are in a domain, it suffices to enter the credentials of the domain administrator. Use Windows conventions when entering the name of a domain user account (for example, `domain\user` or `user@domain.com`).
7. Click **Install Silent Agent**. A confirmation window will appear.
8. You can view and manage the task on the **Computers > View Tasks** page.

8.2. Scanning Managed VMs

There are two ways to scan VMs protected by Security for Virtualized Environments:

- You can create scheduled scan tasks using the policy.
- Run an immediate scan task from the console.

To remotely run a scan task on one or several VMs:

1. Go to the **Computers > View Computers** page.
2. Click the **Show** menu located above the table (to the left) and choose **Managed Computers**.
3. If you have organized VMs into groups, select the desired group from the left-side pane. To view all of your VMs, right-click the root group and choose **View all computers**.
4. Select the check boxes corresponding to the VMs you want to scan.
5. Click **Tasks** and choose **Scan** from the menu.
6. Click **Request Scan**. A confirmation window will appear.
7. You can view and manage the task on the **Computers > View Tasks** page.

8.3. Uninstalling Protection from VMs

To remotely uninstall the Security for Virtualized Environments protection from one or several VMs:

1. Go to the **Computers > View Computers** page.
2. Click the **Show** menu located above the table (to the left) and choose **Managed Computers**.
3. If you have organized VMs into groups, select the desired group from the left-side pane. To view all of your VMs, right-click the root group and choose **View all computers**.
4. Select the check boxes corresponding to the VMs you want to uninstall protection from.
5. Click **Tasks** and choose **Uninstall Protection** from the menu.

6. Click **Uninstall**. A confirmation window will appear.
7. You can view and manage the task on the **Computers > View Tasks** page.

8.4. Viewing and Managing Tasks

The tasks you have created can be viewed and managed on the **Computers > View Tasks** page. You can see the existing tasks and details about them:

- Task name.
- Execution progress on the target VMs.
- When the task was created.

8.4.1. Checking Execution Status and Results

Tasks will start running immediately on online VMs, but they will take some time to complete (more or less, depending on the task).

To check if a task has run on the target VMs:

1. Go to the **Computers > View Tasks** page.
2. Find the task in the list and check the **Progress** field. You can see on how many of the target VMs the task has run.
3. To access the task report, which provides details on the task execution, click the task name.

The task report consists of a Summary page and a Details page.

8.4.2. Deleting Tasks

Once a task has run and you no longer need the task report, it is best to delete it.

To delete one or several tasks:

1. Go to the **Computers > View Tasks** page.
2. Select the check boxes corresponding to the tasks you want to delete.
3. Click the **Delete** button located above the table. A confirmation window will appear.

9. Using Reports

Security Console allows you to create and view centralized reports on the security status of the protected virtual machines. The reports can be used for multiple purposes, such as:

- Monitoring and ensuring compliance with the organization's security policies.
- Checking and assessing the security status of the virtual network.
- Identifying security issues, threats and vulnerabilities.
- Monitoring security incidents and malware activity.
- Providing upper management with easy-to-interpret data on VM security.

Several different report types are available so that you can easily get the information you need. The information is presented as easy-to-read pie charts, tables and graphics, allowing you to quickly check the virtual network security status and identify security issues.

Reports can consolidate data from the entire virtual network or from specific VM groups only. In this way, from a single report, you can find out:

- Statistical data regarding all or groups of protected virtual machines.
- Detailed information for each protected virtual machine.
- The list of VMs that meet specific criteria (for example, those that have antimalware protection disabled).

All generated reports are available in Security Console for a default period of 90 days, but you can save them to your computer or email them. Available formats include Portable Document Format (PDF) and comma-separated values (CSV).

9.1. Available Report Types

This is the list of available report types:

Update Status

Shows you the update status of the Security for Virtualized Environments protection installed on selected computers. Using the available filters, you can easily find out which clients have updated or have not updated in a specific time period.

Computer Status

Provides you with various status information concerning selected computers on which Security for Virtualized Environments protection is installed.

- Protection update status
- License status

- Network activity status (online/offline)
- Antimalware protection status

You can apply filters by security aspect and status to find the information you are looking for.

Malware Activity

Provides you with overall and per computer details about the malware threats detected over a specific time period on selected computers. You can see:

- Number of detections (files that have been found infected with malware)
- Number of infections solved (files that have been successfully disinfected or isolated in the local quarantine folder)
- Number of infections blocked (files that could not be disinfected, but to which access has been denied; for example, an infected file stored in some proprietary archive format)

Protection Module Status

Informs you of the status of the antimalware protection on selected computers. The protection status can be Enabled or Disabled. The report details also provide information on the update status.

You can apply filters by status to find the information you are looking for.

Top 10 Most Infected Computers

Shows you the top 10 most infected computers over a specific time period from selected computers.

Top 10 Detected Malware

Shows you the top 10 malware threats detected over a specific time period on selected computers.

Network Status

Provides you with detailed information on the overall network security status. Computers are grouped based on these criteria:

- Unmanaged computers do not have Security for Virtualized Environments protection installed and their security status cannot be assessed. Unmanaged computers are detected automatically by the Security for Virtualized Environments agents installed on protected virtual machines. They can represent not only virtual machines, but also physical computers (if they are connected to the virtual network).
- Offline computers normally have Security for Virtualized Environments protection installed, but there is no recent activity from Silent Agent. The security status of offline computers cannot be accurately assessed because status information is not current. For more information, refer to "About Offline Computers" (p. 36).
- Protected computers have Security for Virtualized Environments protection installed and no security risks have been detected.

- Vulnerable computers have Security for Virtualized Environments protection installed, but specific conditions prevent proper protection of the system. The report details show you which security aspects need to be addressed.

Computer Malware Status

Helps you find out how many and which of the selected computers have been affected by malware over a specific time period and how the threats have been dealt with. Computers are grouped based on these criteria:

- Computers with no detections (no malware threat has been detected over the specified time period)
- Computers with resolved malware (all detected files have been successfully disinfected or isolated in the local quarantine folder)
- Computers with blocked malware (some of the detected files have been denied access to)

Executive

Allows you to export the charts from the dashboard portlets to a PDF file.

9.2. Creating Reports

To create a report:

1. Go to the **Reports > New Report** page.

> **Note**
> If you are on the **View Reports** or **Scheduled Reports** page, just click the **New** button located above the table.

2. Select the desired report type from the menu. For more information, refer to "Available Report Types" (p. 63).
3. Enter a suggestive name for the report. When choosing a name, consider the report type and target, and possibly the report options.
4. Configure the report target. Select one of the available options and click the corresponding link to choose the groups or the individual virtual machines to be included in the report.
5. Configure report recurrence (schedule). You can choose to create the report immediately, daily, weekly (on a specific day of the week) or monthly (on a specific day of the month).
6. Configure the report options.
   a. For most report types, when you create an immediate report, you must specify the reporting period. The report will only include data from the selected time period.
   b. Several report types provide filtering options to help you easily find the information you are interested in. Use the filtering options to obtain only the desired information. For example, for an **Update Status** report you can choose to view only the list of

protected VMs that have updated (or, on the contrary, that have not updated) in the selected time period.

> **Note**
>
> When you view the report in the console, all information will be available, regardless of the selected options. If you download or email the report however, only the report summary and selected information will be included in the PDF file. Full report details will only be available in CSV format.

c. To receive the report by email, select the corresponding option.

7. Click **Generate** to create the report.
   - If you have chosen to create an immediate report, it will be displayed on the View Reports page. The time required for reports to be created may vary depending on the number of managed VMs. Please wait for the requested report to be created. Once the report has been created, you can view the report by clicking its name.
   - If you have chosen to create a scheduled report, it will be displayed on the Scheduled Reports page.

9.3. Viewing and Managing Generated Reports

To view and manage generated reports, go to the **Reports > View Reports** page. This page is automatically displayed after creating an immediate report.

> **Note**
>
> Scheduled reports can be managed on the Reports > Scheduled Reports page.

You can see the generated reports and useful information about them:

- Report name and type.
- When the report was generated.

To sort reports by a specific column, simply click the header of that column. Click the column header again to change the sorting order.

Each report is marked with one of the following icons to inform you whether the report is scheduled or not:

Indicates a one-time only report.

Indicates a scheduled report.

To make sure the latest information is being displayed, click the **Refresh** button in the bottom-left corner of the table.

9.3.1. Viewing Reports

To view a report:

1. Go to the **Reports > View Reports** page.
2. Click the name of the report you want to view. To easily find the report you are looking for, you can sort reports by name, type or creation time.

All reports consist of a Summary page and a Details page.

- The Summary page provides you with statistical data (pie charts and graphics) for all target VMs or groups. At the bottom of the page, you can see general information about the report, such as the reporting period (if applicable), report target etc.
- The Details page provides you with detailed information for each managed VM. For some reports, you may need to click a pie chart area on the Summary page in order to see details.

Use the tabs in the upper-left corner of the report to view the desired page.

9.3.2. Searching Report Details

The report details are displayed in a table that consists of several columns providing various information. The table can span several pages (only 10 entries are displayed per page by default). To browse through the details pages, use the buttons at the bottom of the table.

To easily find what you are looking for, use the search boxes or the filtering options below the column headers.

To sort report details by a specific column, simply click the header of that column. Click the column header again to change the sorting order.

9.3.3. Saving Reports

By default, generated reports are available in Security Console for 90 days. After this period, they are deleted automatically.

If you need reports to be available for longer time periods, you can save them to your computer. The report summary and selected report information will be available in PDF format, whereas full report details will be available in CSV format.

To save the report you are viewing to your computer:

1. Click the **Export** button in the upper-right corner of the report page. A download window will appear.
2. Download the `.zip` archive to your computer. Depending on your browser settings, the file may be downloaded automatically to a default download location.

9.3.4. Printing Reports

To print a report, you must first save it to your computer.

9.3.5. Emailing Reports

To email the report you are viewing:

1. Click the **Email** button in the upper-right corner of the report page. A window will appear.
2. If you want to, you can change the report name.
3. Enter the email addresses of the people you want to send the report to, separating them by semicolons (;).
4. Click **Send Email**.

9.3.6. Automatic Deletion of Reports

By default, generated reports are available in Security Console for 90 days. After this period, they are deleted automatically.

To change the automatic deletion period for generated reports:

1. Go to the **Reports > View Reports** page.
2. Click the link at the bottom of the table.
3. Select the new period from the menu.
4. Click **OK**.

9.3.7. Deleting Reports

To delete a report:

1. Go to the **Reports > View Reports** page.
2. Select the report.
3. Click the **Delete** button located above the table.

9.4. Managing Scheduled Reports

When creating a report, you can choose to configure a schedule based on which the report will be automatically generated (at regular time intervals). Such reports are referred to as scheduled reports.

Generated reports will be available on the **Reports > View Reports** page for a default period of 90 days. They will also be emailed to you if you have selected this option.

To manage scheduled reports, go to the **Reports > Scheduled Reports** page. You can see all scheduled reports and useful information about them:

- Report name and type.
- Schedule based on which the report is automatically generated.
- When the report was last generated.

9.4.1. Viewing Last Report Generated

From the **Reports > Scheduled Reports** page, you can easily view the most recently generated report by clicking the link in the **Last Report Generated** column.

9.4.2. Renaming Scheduled Reports

Reports generated by a scheduled report are named after it. Renaming a scheduled report will not affect the reports generated previously.

To rename a scheduled report:

1. Go to the **Reports > Scheduled Reports** page.
2. Click the report name.
3. Change the report name in the corresponding field. Choose a suggestive name for the report to help easily identify what it is about. When choosing a name, consider the report type and target, and possibly the report options.
4. Click **Submit** to save changes.

9.4.3. Editing Scheduled Reports

To change the settings of a scheduled report:

1. Go to the **Reports > Scheduled Reports** page.
2. Click the report name.
3. Change report settings as needed. You can change the following:
   - **Report name.** Choose a suggestive name for the report to help easily identify what it is about. When choosing a name, consider the report type and target, and possibly the report options. Reports generated by a scheduled report are named after it.
   - **Report target.** The selected option indicates the type of the current report target (either groups or individual virtual machines). Click the corresponding link to view the current report target. To change it, click any of the two links and select the groups or VMs to be included in the report.
   - **Report recurrence (schedule).** You can set the report to be automatically generated daily, weekly (on a specific day of the week) or monthly (on a specific day of the

month). Depending on the selected schedule, the report will only include data from the last day, week or month, respectively.

- **Report options.** You can choose to receive the report by email. Most reports provide filtering options to help you easily find the information you are interested in. When you view the report in the console, all information will be available, regardless of the selected options. If you download or email the report however, only the report summary and selected information will be included in the PDF file. Full report details will only be available in CSV format.

4. Click **Submit** to save changes.

9.4.4. Deleting Scheduled Reports

When a scheduled report is no longer needed, it is best to delete it. Deleting a scheduled report will not delete the reports it has generated automatically to that point.

To delete a scheduled report:

1. Go to the **Reports > Scheduled Reports** page.
2. Select the report.
3. Click the **Delete** button located above the table.

10. Quarantine

Security for Virtualized Environments can isolate the malware-infected files and the suspicious files in a secure area named quarantine. When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

Quarantined files are stored locally on the virtual machines. To make your life easier, quarantine content is managed automatically.

By default, quarantined files are automatically sent to Bitdefender Labs in order to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

In addition, quarantined files are scanned after each malware signature update. Cleaned files are automatically moved back to their original location.

Security Console provides detailed information on all quarantined items, so that you can easily monitor unresolved threats and malware outbreaks. To check and manage quarantined files, go to the **Quarantine** page.

Information about quarantined files is displayed in a table. You are provided with the following information:

- Name given to the malware threat by the Bitdefender security researchers.
- Path to the infected or suspicious file on the virtual machine it was detected on.
- Virtual machine the threat was detected on.
- Time when the file was quarantined.
- Pending action requested by administrator to be taken on the quarantined file.

To make sure the latest information is being displayed, click the ⟳ **Refresh** button in the bottom-left corner of the table. This may be needed when you spend more time on the page.

10.1. Navigation and Search

Depending on the number of managed VMs and the nature of infections, the number of quarantined files can be sometimes large. The table can span several pages (only 10 entries are displayed per page by default).

To move through the pages, use the navigation buttons at the bottom of the table. To change the number of entries displayed on a page, select an option from the menu next to the navigation buttons.

If there are too many entries, you can use the search boxes under the column headers to filter displayed data. For example, you can search for a specific threat detected in the network or for a specific virtual machine. You can also click column headers to sort data by a specific column.

10.2. Restoring Quarantined Files

On particular occasions, you may need to restore quarantined files, either to their original location or to an alternate location. One such situation is when you want to recover important files stored in an infected archive that has been quarantined.

To restore one or more quarantined files:

1. Go to the **Quarantine** page.
2. Check the list of quarantined files and select the check boxes corresponding to the ones you want to restore.
3. Click the **Restore** button in the upper-right corner of the page.
4. Choose the location where you want the selected files to be restored (either the original or a custom location on the target virtual machine).

   If you choose to restore to a custom location, you must enter the path in the corresponding field. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target VMs. For more information, refer to "Using System Variables" (p. 83).
5. Click **Restore** to request the file restore action. You can notice the pending action in the **Action** column.
6. The requested action is sent to the target VMs immediately or as soon as they get back online. Once a file is restored, the corresponding entry will disappear from the Quarantine table.

10.3. Automatic Deletion of Quarantined Files

By default, quarantined files older than 30 days are automatically deleted. This setting can be changed by editing the policy assigned to virtual machines.

To change the automatic deletion interval for quarantined files:

1. Go to the **Policies > View Policies** page.
2. Find the policy assigned to the VMs on which you want to change the setting and click its name.
3. Go to the **Antimalware > Quarantine** section.
4. Select the desired automatic deletion period from the menu.
5. Click **Save** to save changes.

10.4. Deleting Quarantined Files

If you want to delete quarantined files manually, you should first make sure the files you choose to delete are not needed. Use these tips when deleting quarantined files:

- A file may actually be the malware itself. If your research leads you to such a situation, you can search the quarantine for the specific threat and delete it from quarantine.
- You can safely delete:
  - Unimportant archive files.
  - Infected setup files.

To delete one or more quarantined files:

1. Go to the **Quarantine** page.
2. Check the list of quarantined files and select the check boxes corresponding to the ones you want to delete.
3. Click the **Delete** button in the upper-right corner of the page. You can notice the pending action in the **Action** column.
4. The requested action is sent to the target VMs immediately or as soon as they get back online. Once a file is deleted, the corresponding entry will disappear from the Quarantine table.

11. User Accounts

Security for Virtualized Environments can be configured and managed from the Security Console **company account** created after installation. This is your company administrator account.

To allow other company employees access to Security Console, you can create additional user accounts from your company account. User accounts can be used to limit access to the Security Console features or to specific groups of virtual machines.

You can create two types of accounts:

Administrator
Administrator accounts offer full access to all areas of the console, allowing users full control over Security for Virtualized Environments. You can allow access to the entire virtualized environment or to a specific VM group only.

Reporter
Reporter accounts offer limited access to the console features. Users can only view the dashboard, reports and activity log sections, without being able to view or change the VM or security configuration. You can allow access to the entire virtualized environment or to a specific VM group only.

To create and manage user accounts, go to the **Accounts > Users** page.

Existing accounts are displayed in the table. For each account, you can see:

- Name of the account owner.
- Email address of the account (used to log in to Security Console and also as a contact address). Reports and important security notifications are sent to this address. Email notifications are sent automatically whenever important risk conditions are detected in the network.
- VM group that the user is in charge of.
- User role (administrator / reporter).

11.1. Creating User Accounts

Create user accounts to delegate administrative or reporting responsibility to other people.

To create a user account:

1. Go to the **Accounts > Users** page.
2. Click the **New** button in the upper-right corner of the page.

3. Under **Account Details**, fill in the account details.
   - **Full name.** Enter the full name of the account owner.
   - **Email.** Enter the user's email address (which will be used by the user to log in to Security Console). Login information will be sent to this address immediately after creating the account.
   - **User role.** Select the user role:
     - **Administrator** - has administrative rights over the assigned virtual machines.
     - **Reporter** - has limited access to the console, being able only to monitor and create reports on the security of the assigned virtual machines.
   - **Group.** Choose the VM group that the user will be in charge of. The rest of the virtual network will be invisible to the user. By default, the user can see the entire virtual network.
4. Under **Settings**, you can configure the account settings.
   - **Timezone.** Choose from the menu the timezone of the account. The console will display time information according to the selected timezone.
   - **Language.** Choose from the menu the console display language.
5. Click **Submit**. The new account will appear in the user accounts list.

11.2. Editing Accounts

Edit accounts to keep account details up to date or to change account settings.

To edit a user account:

1. Go to the **Accounts > Users** page.
2. Click the user's name.
3. Change account details and settings as needed.
4. Click **Submit** to save the changes.

11.3. Deleting Accounts

Delete accounts when they are no longer needed. For example, if the account owner is no longer with the company.

To delete an account:

1. Go to the **Accounts > Users** page.
2. Select the account from the list.
3. Click the **Delete** button in the upper-right corner of the page.

11.4. Resetting Login Passwords

Accounts owners who forget their password can reset it by using the password recovery link on the login page. You can also reset a forgotten login password by editing the corresponding account from the console.

To reset the login password for a user:

1. Go to the **Accounts > Users** page.
2. Click the user's name.
3. Type a new password in the corresponding fields (under **Account Details**).
4. Click **Submit** to save the changes. Be sure to inform the account owner of the new password.

12. User Activity Log

Security Console logs all the operations and actions performed by users. Logged events include the following:

- Logging in and logging out
- Creating, editing, renaming, deleting user accounts
- Creating, editing, renaming, deleting policies
- Creating, editing, renaming, deleting reports
- Deleting, restoring quarantined files
- Deleting or moving computers between groups
- Creating, moving, renaming, deleting groups

To examine the user activity records, go to the **Log** page.

Recorded events are displayed in a table. The table columns provide you with useful information about the listed events:

- Name of the user who performed the action.
- Type of user account.
- Action that caused the event.
- Type of console object affected by the action.
- Specific object affected by the action.
- IP address the user connected from.
- Time when the event occurred.

To easily find what you are looking for, use the search boxes or the filtering options below the column headers. To sort events by a specific column, simply click the header of that column. Click the column header again to change the sorting order.

To view detailed information about an event, select it and check the section under the table.

To make sure the latest information is being displayed, click the ⟳ **Refresh** button in the bottom-left corner of the table.

13. Getting Help

Bitdefender strives to provide its customers with an unparalleled level of fast and accurate support. If you experience any issue with or if you have any question about your Bitdefender product, go to our online Support Center. It provides several resources that you can use to quickly find a solution or an answer. Or, if you prefer, you can contact the Bitdefender Customer Care team. Our support representatives will answer your questions in a timely manner and they will provide you with the assistance you need.

Note
You can find out information about the support services we provide and our support policy at the Support Center.

13.1. Bitdefender Support Center

Bitdefender Support Center, available at http://enterprise.bitdefender.com/support, is the place where you will find all the assistance you need with your Bitdefender product.

You can use several resources to quickly find a solution or an answer:

- Knowledge Base Articles
- Bitdefender Support Forum
- Product Documentation

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

Knowledge Base Articles

The Bitdefender Knowledge Base is an online repository of information about the Bitdefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the Bitdefender support and development teams, along with more general articles about virus prevention, the management of Bitdefender solutions with detailed explanations, and many other articles.

The Bitdefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their way into the Bitdefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The Bitdefender Knowledge Base for business products is available any time at http://enterprise.bitdefender.com/support.

Bitdefender Support Forum

The Bitdefender Support Forum provides Bitdefender users with an easy way to get help and to help others. You can post any problem or question related to your Bitdefender product.

Bitdefender support technicians monitor the forum for new posts in order to assist you. You may also get an answer or a solution from a more experienced Bitdefender user.

Before posting your problem or question, please search the forum for a similar or related topic.

The Bitdefender Support Forum is available at http://forum.bitdefender.com, in 5 different languages: English, German, French, Spanish and Romanian. Click the **Business Protection** link to access the section dedicated to business products.

Product Documentation

Product documentation is the most complete source of information about your product.

You can check and download the latest version of documentation for Bitdefender business products at Support Center > Documentation.

13.2. Asking for Assistance

You can contact us for assistance through our online Support Center:

1. Go to http://enterprise.bitdefender.com/support/contact-us.html.
2. Use the contact form to open an email support ticket or access other available contact options.

13.3. Contact Information

Efficient communication is the key to a successful business. During the past 10 years Bitdefender has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

13.3.1. Web Addresses

Sales Department: enterprisesales@bitdefender.com
Support Center: http://enterprise.bitdefender.com/support
Documentation: documentation@bitdefender.com
Local Distributors: http://enterprise.bitdefender.com/partners

Partner Program: partners@bitdefender.com
Media Relations: pr@bitdefender.com
Job Opportunities: jobs@bitdefender.com
Virus Submissions: virus_submission@bitdefender.com
Spam Submissions: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Web site: http://enterprise.bitdefender.com

13.3.2. Local Distributors

The Bitdefender local distributors are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters.

To find a Bitdefender distributor in your country:

1. Go to http://enterprise.bitdefender.com/partners.
2. Go to **Partner Locator**.
3. The contact information of the Bitdefender local distributors should be displayed automatically. If this does not happen, select the country you reside in to view the information.
4. If you do not find a Bitdefender distributor in your country, feel free to contact us by email at enterprisesales@bitdefender.com. Please write your email in English in order for us to be able to assist you promptly.

13.3.3. Bitdefender Offices

The Bitdefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

United States

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Phone (sales&technical support): 1-954-776-6262
Sales: sales@bitdefender.com
Web: http://www.bitdefender.com
Support Center: http://www.bitdefender.com/businesshelp

Germany

Bitdefender GmbH

Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Phone (office&sales): +49 (0)2301 91 84 222
Phone (technical support): +49 (0)2301 91 84 444
Sales: vertrieb@bitdefender.de
Website: http://www.bitdefender.de
Support Center: http://www.bitdefender.de/businesshelp

UK and Ireland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Phone (sales&technical support): +44 (0) 8451-305096
Email: info@bitdefender.co.uk
Sales: sales@bitdefender.co.uk
Website: http://www.bitdefender.co.uk
Support Center: http://www.bitdefender.co.uk/businesshelp

Spain

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1° 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Phone (office&sales): (+34) 93 218 96 15
Phone (technical support): (+34) 93 502 69 10
Sales: comercial@bitdefender.es
Website: http://www.bitdefender.es
Support Center: http://www.bitdefender.es/businesshelp

Romania

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest, Sector 6
Fax: +40 21 2641799
Phone (sales&technical support): +40 21 2063470
Sales: sales@bitdefender.ro
Website: http://www.bitdefender.ro

Support Center: http://www.bitdefender.ro/businesshelp

United Arab Emirates

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Phone (sales&technical support): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Sales: sales@bitdefender.com
Web: http://www.bitdefender.com/world
Support Center: http://www.bitdefender.com/businesshelp

A. Appendices

A.1. List of Application File Types

The antimalware scanning engines included in the Bitdefender security solutions can be configured to limit scanning to application (or program) files only. Application files are far more vulnerable to malware attacks than other types of files.

This category includes files with the following extensions:

`386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp`

A.2. Using System Variables

Some of the settings available in the console require specifying the path on the target virtual machines. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target VMs.

Here is the list of the predefined system variables:

`%ALLUSERSPROFILE%`

The All Users profile folder. Typical path:

`C:\Documents and Settings\All Users`

`%APPDATA%`

The Application Data folder of the logged-in user. Typical path:

- Windows XP:

`C:\Documents and Settings\{username}\Application Data`

- Windows Vista/7:

  `C:\Users\{username}\AppData\Roaming`

`%HOMEPATH%`
The user folders. Typical path:

- Windows XP:

  `\Documents and Settings\{username}`

- Windows Vista/7:

  `\Users\{username}`

`%LOCALAPPDATA%`
The temporary files of Applications. Typical path:

`C:\Users\{username}\AppData\Local`

`%PROGRAMFILES%`
The Program Files folder. A typical path is `C:\Program Files`.

`%PROGRAMFILES(X86)%`
The Program Files folder for 32-bit applications (on 64-bit systems). Typical path:

`C:\Program Files (x86)`

`%COMMONPROGRAMFILES%`
The Common Files folder. Typical path:

`C:\Program Files\Common Files`

`%COMMONPROGRAMFILES(X86)%`
The Common Files folder for 32-bit applications (on 64-bit systems). Typical path:

`C:\Program Files (x86)\Common Files`

`%WINDIR%`
The Windows directory or SYSROOT. A typical path is `C:\Windows`.

Glossary

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive Web pages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the Web page. ActiveX controls are often written using Visual Basic.

Active X is notable for a complete lack of security controls; computer security experts discourage its use over the Internet.

Adware

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory.

Every time you boot your system from that point on, you will have the virus active in memory.

Browser

Short for Web browser, a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Command line

In a command line interface, the user types commands in the space provided directly on the screen using command language.

Cookie

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

Disk drive

It's a machine that reads data from and writes data onto a disk.

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

Download

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

E-mail

Electronic mail. A service that sends messages on computers via local or global networks.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

False positive

Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Guest Operating System

An isolated operating system that runs inside another operating system (the host) within a virtualized environment.

Heuristic

A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

Host Operating System

An operating system inside of which other operating systems (the guests) run by virtualization.

Hypervisor

A program that allows multiple operating systems to run concurrently on a single computer.

IP

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Java applet

A Java program which is designed to run only on a web page. To use an applet on a web page, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the web page is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from applications in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Mail client

An e-mail client is an application that enables you to send and receive e-mail.

Malware

Malware is the generic term for software that is designed to do harm - a contraction of 'malicious software'. It is not yet in universal usage, but its popularity as a general term for viruses, Trojan Horses, worms, and malicious mobile code is growing.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

Non-heuristic

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

Packed programs

A file in a compression format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

Path

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Polymorphic virus

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Report file

A file that lists actions that have occurred. Bitdefender maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

Rootkit

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

Spam

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited e-mail.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Startup items

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or application programs can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right-click an icon to view and access the details and controls.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

Bitdefender has it's own update module that allows you to manually check for updates, or let it automatically update the product.

Virtual appliance

A virtual machine image containing a pre-configured operating system and an application packaged together to facilitate the installation and configuration of the application in a virtualized environment.

Virtual machine

An isolated software environment that emulates a physical computer on which an operating system and applications can run.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Virus definition

The binary pattern of a virus, used by the antivirus program to detect and eliminate the virus.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.