Windows Agent & Syslog Agent Installation Guide

A step-by-step guide to installing and managing the Cerulean Agent on your Windows servers and workstations.

Overview

The Cerulean Agent provides automated data collection and configuration services for your end points and lays the framework for Securus360's autonomous response capabilities. The Cerulean Agent includes several enhancements and remote support capabilities not included in previous Securus360 Management Agent versions.

Additionally, the Cerulean Agent no longer includes Sysmon64, minimizing its footprint on your Windows machines while enhancing Securus360's monitoring capabilities.

Relevant Agent Versions

This guide covers the installation process for the Cerulean Agent, starting with version 2304.3.2.

Supported Operating Systems

The agent supports the following Windows operating systems:

- Windows 8.1 and newer
- Windows Server 2012/R2 and newer

 +1 (949) 266-6900 | support@securus360.com
100 Spectrum Center Drive, Suite 900, Irvine, CA 92618, USA | www.securus360.com

Windows Agent & Syslog Agent Installation Guide

Minimum System Requirements

The agent is specially designed to use minimal system resources; the requirements for the agent are simply those of the operating system installed. Special consideration should be made to virtual machine infrastructure such that the actual allocation of resources meets the operating system / user load requirements. Specifically, shared computing environments such as VDI desktops or Terminal Server / Services should have adequate resources to handle the user load. (E.g. enough physical resources that each user has sufficient resources allocated to their session.) Securus360 cannot guarantee the complete functionality of the agent if resources do not meet recommended levels.

Networking Requirements

The Cerulean Agent, and its associated data collection services, securely sends data over the internet to the Securus360 Cloud. To allow this, the following ports should be configured for outbound traffic on all devices and environment firewalls, routers, etc.

- TCP Outbound Port 443
- TCP Outbound Port 9243

Anti-Virus Configuration

The Cerulean Agent performs administrative actions on your devices that some anti-virus systems may identify as malicious. To prevent anti-virus systems from quarantining or otherwise impeding the agent from performing its responsibilities, please be sure to whitelist the related files and services.

- C:\Program Files\Cerulean*
- C:\Program Files\Elastic\Agent*
- C:\Program Files\Elastic\Agent\elastic-agent.yml
- C:\Program Files\Elastic\Agent\fleet.enc
- C:\Program Files\Elastic\Agent\data\elastic-agent-*\logs\elastic-agent-json.log
- C:\Program Files\Elastic\Agent\data\elastic-agent-*\logs\default*-json.log*
- C:\Program Files\Elastic\Endpoint\elastic-endpoint.exe

 +1 (949) 266-6900 | support@securus360.com
100 Spectrum Center Drive, Suite 900, Irvine, CA 92618, USA | www.securus360.com

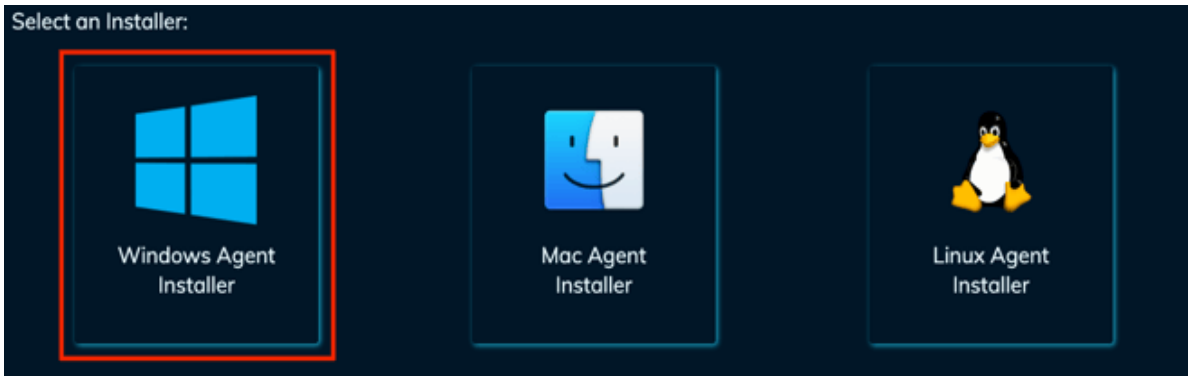
Windows Agent & Syslog Agent Installation Guide

Download the Installer

When downloading the Cerulean Agent installer, you will receive a ZIP file containing two files: windows_installer3.exe and config.json. Both items will be important for the installation process.

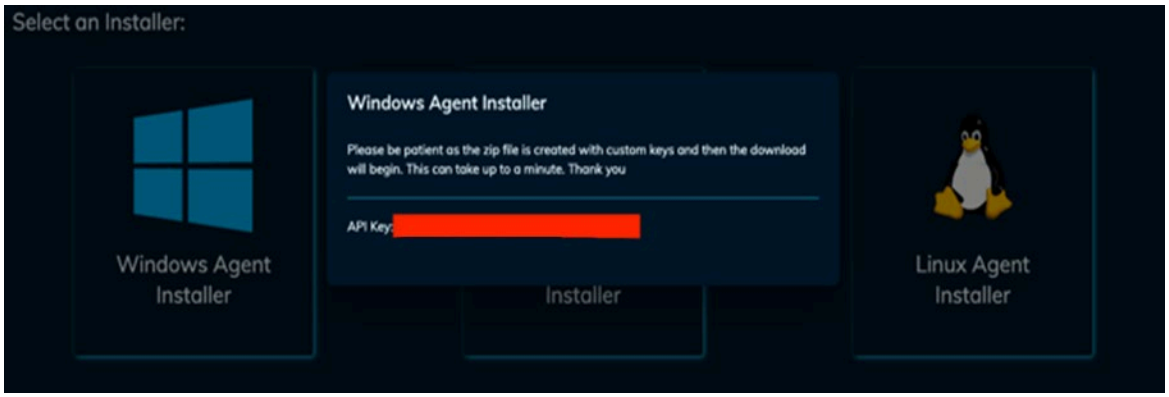
1. Open a web browser and navigate to the **Securus360 Portal**
2. Select **Agent** from the management section of the navigation menu

3. Click on the **Windows Agent Installer** tile



 +1 (949) 266-6900 | support@securus360.com
100 Spectrum Center Drive, Suite 900, Irvine, CA 92618, USA | www.securus360.com

4. Take note of the **API Key** provided on the corresponding pop-up



Installing the Agent

The Cerulean Agent can be installed locally on your Windows machine or deployed via your RMM (see note below). This section covers local installations.

1. **Unzip** the file collected in the previous section
2. Right click on **windows_installer3.exe** and select **Run as administrator**

Optionally, the install can also be completed from a command prompt:

1. Open an administrative Command prompt
2. Navigate to the directory containing the installer executable
3. Run the following command:

```
windows_installer3.exe install
```

Note: If you wish to deploy this via RMM (i.e. InTune, SCCM, etc.) please contact support@securus360.com directly for further instructions.

Windows Agent & Syslog Agent Installation Guide

Confirm Installation Success

There are a couple of different methods to confirm the installation of the agent. Most importantly, you will want to verify that the following services are present on the machine on the machine with the status and startup type reflected below:

- Cerulean Agent
  - Status: Running
  - Startup Type: Automatic
- Cerulean Updater
  - Status: N/A
  - Startup Type: Manual
- Elastic Agent
  - Status: Running
  - Startup Type: Automatic

- Elastic Endpoint
  - Status: Running
  - Startup Type: Automatic

Optionally, you can confirm installation by checking for the agent file located at:

- C:\Program Files\Cerulean\cerulean-agent.exe

 +1 (949) 266-6900 | support@securus360.com
100 Spectrum Center Drive, Suite 900, Irvine, CA 92618, USA | www.securus360.com

Windows Agent & Syslog Agent Installation Guide

Manage Your Installation

In addition to the installation commands above, the Cerulean Agent has several helpful built-in options available to you as well. When operating from an elevated command prompt, you can utilize the following commands and flags to achieve the listed actions. Additionally, you can add the command **help** to see these commands during the installation, uninstallation, or troubleshooting processes:

```
windows_installer3.exe help
```

Available General Commands:

- help
  - Help about any command
- install
  - Installs the Cerulean Agent onto the system
- repair
  - Repair a Cerulean Agent installation
- uninstall
  - Uninstalls the Cerulean Agent

Available General Flags:
**Note: All flags must be added after one of the commands listed above.*

- -h
  - help for windows_installer3.exe
- -v
  - Verbose output
- -i
  - Places agent into image mode, ment for Golden Image usage
- -s
  - Places agent into syslog mode **(use install -s)**

Agent Deployment

If you are leveraging an RMM for deployment of the Cerulean Agent, utilize the following command:

```
windows_installer3.exe install -a YOURAPIKEYHERE -u
https://agentapi.agileblue.com
```


 +1 (949) 266-6900 | support@securus360.com
100 Spectrum Center Drive, Suite 900, Irvine, CA 92618, USA | www.securus360.com

Windows Agent & Syslog Agent Installation Guide

Installing the Syslog Agent

Overview

The Securus360 SOC leverages Syslog Collection to monitor network devices such as firewalls, switches, routers, and some third-party apps which support Syslog Forwarding. To collect syslog data, you must choose a dedicated Syslog Server on which to install the Monitoring Agent with an additional command switch to designate the device as your Syslog Agent.

Minimum System Requirements

- Virtual (or physical) machine with high up-time (typically a server)
- 2 CPU / 4GB RAM / 120GB (Virtual) Disk

Step-by-Step

1. Download the Installer

To download the installer, open a web browser and navigate to https://portal.securus360.com/ and log in. Then select *Agent* from the navigation bar and choose the installer corresponding to the Operating System (OS) of the intended Syslog Agent.
Note: More detailed instructions for this can be found above

2. Install the Syslog Agent

Run the following command from an elevated (administrative) command prompt:

```
windows_installer3.exe install -s
```

3. Notify Support

6

Once the agent has been installed on the designated Syslog Server, please notify Securus360 support (support@securus360.com). The Securus360 team will then provide the next steps for Syslog Collection of your respective devices.

(Note: To uninstall either the Agent or Syslog Agent, simply use the *uninstall* switch from an elevated command prompt. For example: *windows_installer3.exe uninstall)*