The CYRISMA “CyBroker Sensor” is used to scan targets within the LAN subnet where the sensor is installed. Data Sensitivity scans can take place against any UNC file path hosted by a Target and Vulnerability/Baseline scans can take place against Windows, MAC and Linux machines on the local network.

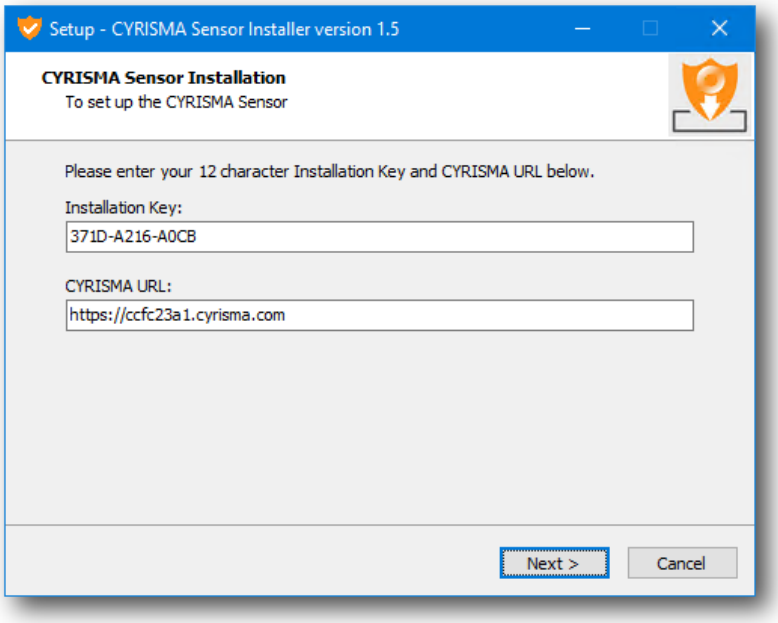
CYRISMA Command Center Web Application receives scan result detail from the Sensor (often referred to as an “Agent”) installed on a workstation or server within your local network. In preparation for Sensor Setup, there are a few requirements to meet first. Please spend a few moments to ensure your Agent Workstation or Server is ready for installation:

- Sensor must be installed on a Windows Server (2012 r2, 2016, 2019) or Windows 10, 11 Workstations.
- Sensor will need to communicate with servers in the cyrisma.com domain. Be sure any web content filters, or firewalls are set to allow communication between the local agent and cyrisma.com. Anti-Virus settings should exempt C:\Cyrisma_Agent. Anti-Spam should allow mail from cyrisma.com.
- Sensor machine needs DotNet 4.7.2. The sensor installer attempts to install this if it is missing, however DotNet installation often requires a reboot, so it is best to install in advance and complete any necessary reboots prior to sensor installation. If needed, you may download DotNet from here: https://portal.dataspotlite.com/jv_dl/dotnet.exe
- The Sensor needs rights on the local network to perform “Agentless” scans of other machines within your network. Create an account with Admin rights on the network and have the credentials available when you are ready to provision agents.

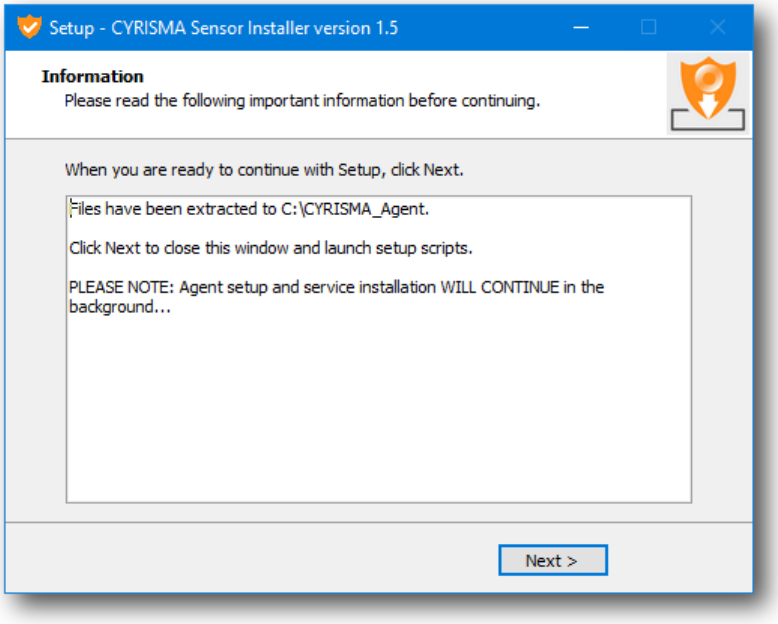
Once you have met the above pre-requisites, log into the Cyrisma Command Center. Go to ADMIN -> Scan Agents. Click Generate (or Regenerate) Windows Installation Key to generate an install key for this instance. Click the email icon if you wish to have the link and instructions emailed to you. From the desktop that will host the agent, use the download link to fetch the agent from: https://msp.cyrisma.com/dl/Cyrisma_Setup.exe.

You may also install an agent on several hosts or on all windows machines within the environment.

Put the install package on the host machine and execute it from there. You will need the Installation Key and the URL of the instance to pair with this agent. Double click the installer to enter your key and url:



Hit next to see the EULA, then Next to begin file extraction. Once file extraction is complete, you will see:



Click next to close the installer window. **The installer will run in the background to complete the installation process.** When the installer finishes, it will pop a momentary indicator announcing the Sensor installation is complete.

If using a Software deployment package manager, the agent can also be deployed using the Command Line:

```
Cyrisma_Setup /verysilent /key=nnnn-nnnn-nnnn /url=https://ccNNNNNN.cyrisma.com
```

In addition, when using the command line option, you may also include the alternate parameter: **`/role=sensor.`**

This option will install the optional packet capture driver if this agent will be used to perform unauthenticated scans of an IP subnet.

The Agent will now contact the Command Center for final approval and provisioning. To complete the Approval and Provisioning process, return to Command Center -> Admin -> Scan Agent, and at the bottom, go to New Agent. Select the agent in the provisioning window. If this agent is going to be used as a sensor to scan the network, please select “No” to “Run as System” and enter the network credentials of your network service account that you have set up previously.

If local security policies prevent you from creating an endpoint protection exclusion for c:\Cyrisma_Agent, please exclude the following files specifically:

Working with the CYRISMA Agent and Endpoint Protection

The CYRISMA Agent will operate in two different modes:

- Local Scanning – The Agent service is running as “System” and relies on these rights to access the local machine for all scan types.

- Network Scanning – The Agent service is running using a previously defined “Service Account” and the agent is being provided account and credential detail at scan time (Using previously defined credentials or Scan Alternate Credentials) and relies on these access rights to perform scanning duties on the network or with machines visible on the network.

Some endpoint protection suites immediately suspect the Agent or parts of the agent and attempt to block or quarantine the agent or its actions. In addition, some of the duties of a CYRISMA agent may include TCP scanning of other machines on the network to assess open ports and depending on the port profile, even attempt remote access of the machine to collect Operating System, Share Level and Security Software details.

These scans may look like a threat to some of the endpoint protection suites and in such a case, the IP address of the agent host machine will need to be allowed to perform its duties. This could mean firewall rule changes or otherwise allowing the agent machine access to the network.

Keep in mind that CYRISMA is not intended to evade detection, compete with, or replace endpoint security suites and when endpoint protection intercedes and blocks CYRISMA, that simply means that the endpoint protection suite is acting as intended and must be configured to allow CYRISMA to operate.

Such configuration generally means including CYRISMA in the Endpoint Protection Allow list or list of Exclusions in Endpoint Security scans.

If your Security Policies allow Exclusion by directory, you can simply exclude the C:\CYRISMA_Agent folder.

If your policy does not allow exclusion by directory, here is a short list of executables that are often detected as a threat and can be added to the exclusion policy:

EXECUTABLE	PURPOSE
C:\CYRISMA_Agent\DataSpotliteAgent.exe	Main executable running as a service
C:\CYRISMA_Agent\App\psexec.exe	Provides remote collection of target attributes
C:\CYRISMA_Agent\App\atexec.exe	Secondary method to collect remote target attributes
C:\CYRISMA_Agent\App\cytcp.exe	TCP Port Scanning
C:\CYRISMA_Agent\App\fileconv.exe	Read data from files and prepare for sensitivity scanning
C:\CYRISMA_Agent\bin\pscopy.exe	Agent management and agent upgrades
C:\CYRISMA_Agent\App\7z.exe	Compresses scan results