Vulnerability Management
Quick Start Guide

This guide explains how to get started using the ConnectSecure Vulnerability Management tool. In particular, it explains how to deploy its agents (small software components) on all company/vessel assets and networks you want to monitor for vulnerabilities.

Planning Agent Deployment

You need to install a **LightWeight Agent (LWA)** on every asset (e.g., computer/server) you want to monitor on your network. The LWA works continuously in the background to gather information about that device (and only that device), such as hardware details, installed software and OS versions, and any detected vulnerabilities, and reports this data to the ConnectSecure cloud platform.

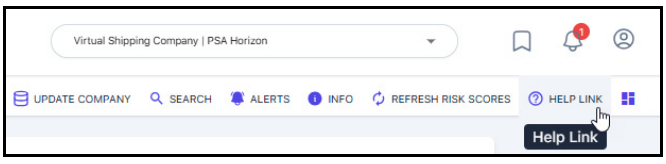
You also need at least one **Probe agent** running on every isolated network segment you want to monitor. The Probe agent scans its mapped network to discover connected devices, including printers and unmanaged computers, and reports any detected network vulnerabilities. In the example shown here, a firewall keeps the OT (Operational Technology) and business LANs separated. Since devices on the OT LAN cannot access devices on the business LAN, and vice-versa, a Probe agent must be configured on at least two endpoint devices – one on each LAN.

Note: *KVH recommends having two Probe agents running on each LAN segment for redundancy.*

In addition, if you have ACL (Access Control List) rules protecting your network, make sure the sites shown here are allowed so ConnectSecure agents can work properly.

For More Information

These instructions only provide basic information. For complete details and advanced configurations, refer to the comprehensive ConnectSecure documentation – select **Help Link** in the ConnectSecure header.

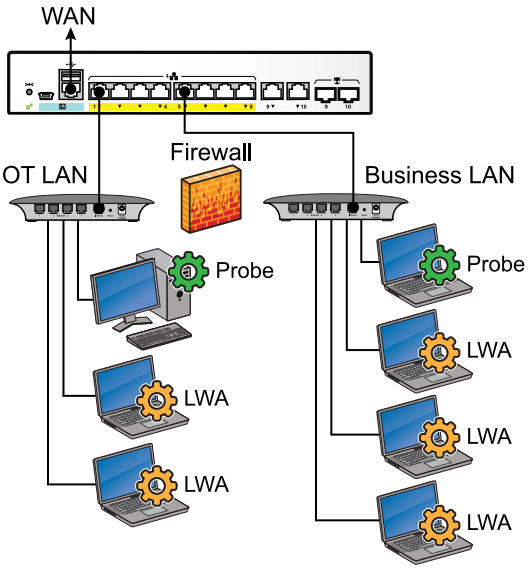


Technical Support

If you have any questions or need technical assistance, please submit a support ticket at the Customer Portal or contact KVH Technical Support 24/7/365:

- Continental USA: 1-866-701-7103
  Worldwide: +1 401-851-3806
- WhatsApp: +1 401-851-3842
- Email: help@kvh.com

Agent Deployment Example



Add to Firewall Allowlist:

149.28.105.81	207.246.64.99
140.82.31.73	149.28.111.222
149.28.99.246	104.207.147.70
144.202.45.22	45.77.118.75
140.82.31.252	149.28.104.10
45.77.119.4	144.202.43.11
45.77.117.23	45.63.105.191

45ee58f3bc4d04c0e1ae971fde066899.r2.cloudflarestorage.com
*.myconnectsecure.com
servicebus1071.myconnectsecure.com
servicebus1072.myconnectsecure.com
servicebus1073.myconnectsecure.com
servicebus1074.myconnectsecure.com
pod107.myconnectsecure.com
pod107.mycybercns.com
https://catalog.s.download.windowsupdate.com
https://catalog.sf.dl.delivery.mp.microsoft.com

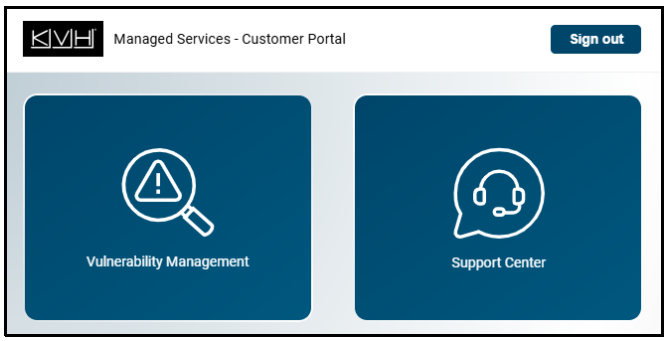
Plus any additional sites required for patching services

Accessing ConnectSecure

ConnectSecure, a cloud-based Vulnerability Management tool, is available via the KVH Managed Services Customer Portal. To access the portal, open a web browser and go to **https://ms.kvh.com**. Then log in with the credentials KVH provided during the onboarding process.

Note: *If you are a KVH Airtime customer, use the email address and password you use to log into KVH Manager.*

Once you are logged in, select **Vulnerability Management** to launch ConnectSecure. From there, you can download its agent installers.

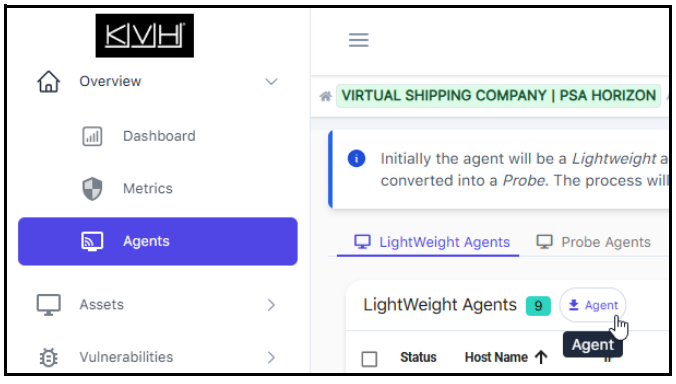


Installing LightWeight Agents (LWAs)

IMPORTANT!
If you are unable to install an agent, please contact KVH Technical Support. With your help, KVH may install it for you over a secure remote desktop connection.

1. In the ConnectSecure header, select the company and/or vessel you want to monitor.

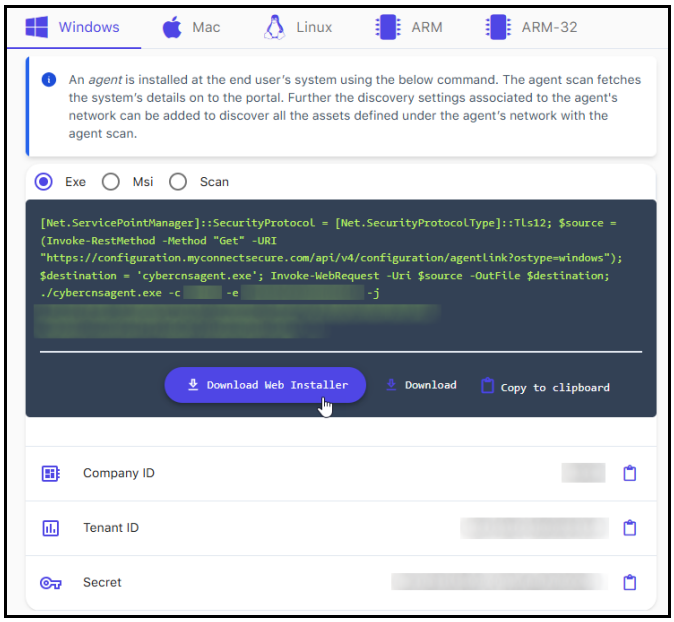
2. Select **Overview > Agents** from the main menu.



3. Under Lightweight Agents, select **Download Agent**.

4. Choose the operating system and installation type (Exe, Msi, or Scan) that applies to the endpoint device. Then select **Download Web Installer** to download the agent to your computer.

Note: *This agent is specific to your selected company/site. It cannot be installed anywhere else.*

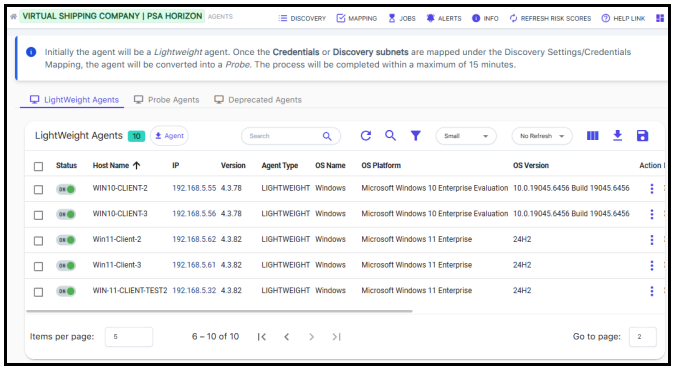


Note: *If an RMM (Remote Monitoring and Management) tool is deployed on your network, you can push the LWA to multiple endpoint devices using the displayed PowerShell/ Terminal script.*

5. Find the file in your Downloads folder. The filename is **cybercns_webinstaller_XXXXXX.exe**, where XXXXXX is your company ID.

6. Copy and run the installer on every endpoint device you want ConnectSecure to monitor. Be sure to download and install the correct agent for each device's operating system.

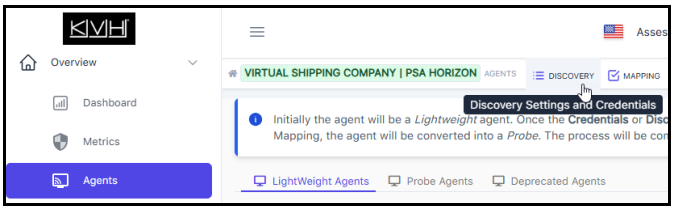
7. All your installed LightWeight agents will appear in the ConnectSecure portal.



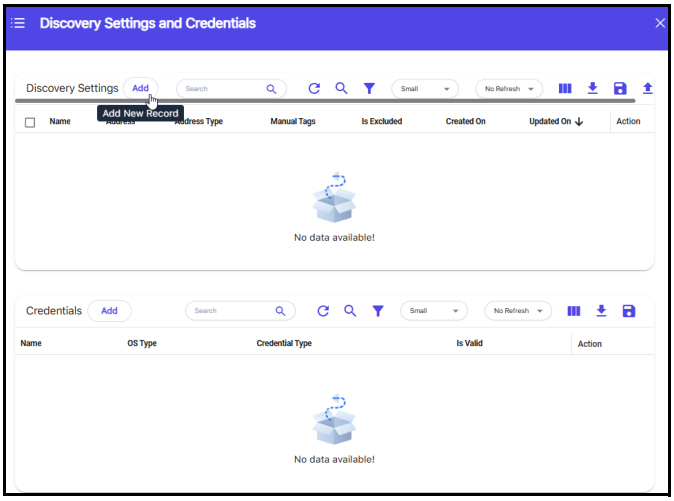
Configuring Discovery Settings and Credentials

Before configuring Probe agents, you need to provide some details about the network(s) you want the Probe agent to scan, along with any administrator credentials required to access the devices on them.

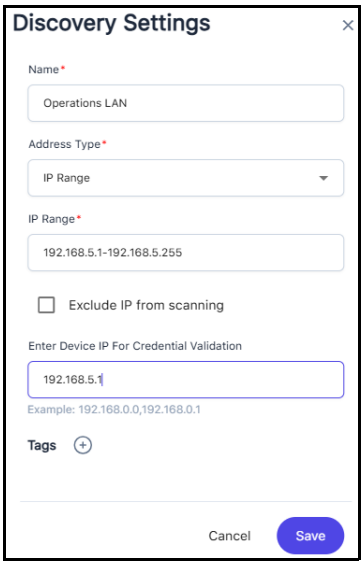
1. Select **Overview > Agents** from the main menu. Then select **Discovery** (Discovery Settings and Credentials).



2. In the Discovery Settings section, select **Add**.

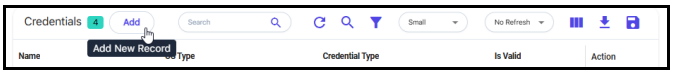


3. Enter the network's details and assign it a descriptive name. You can specify the network using static IP, CIDR, domain, or IP range format. Then select **Save**.

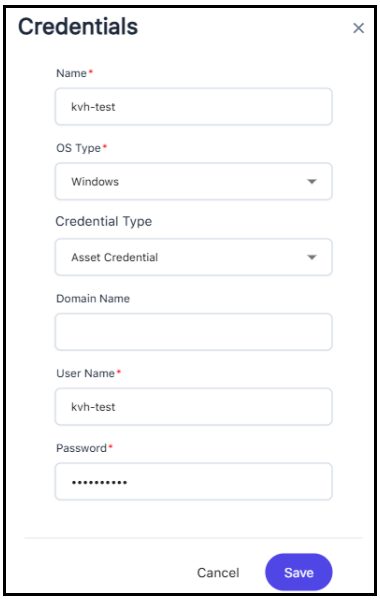


4. Repeat steps 2-3 to add each additional network you would like to include in a scan.

5. In the Credentials section, select **Add**.



6. Enter any admin credentials required to permit deep scanning of devices found on the network. Assign the credential a descriptive name. Then select **Save**.

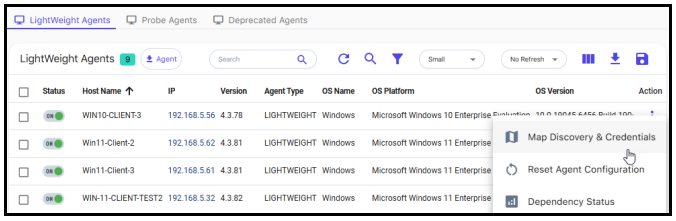


7. Repeat steps 5-6 to add any additional credentials. For example, you might add SNMP credentials for network devices, such as a router, switch, or network appliance like the CommBox Edge.

Converting an LWA to a Probe Agent

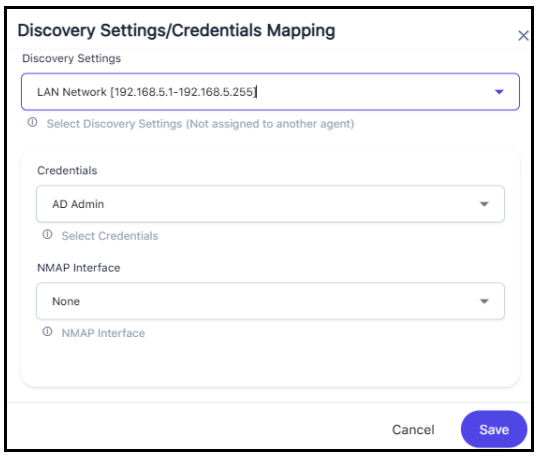
To add a Probe agent to a network, you simply convert an installed Lightweight Agent (LWA) to a Probe agent.

1. Select **Overview > Agents** from the main menu.
2. Under LightWeight Agents, select the **Action** menu next to the LWA you want to convert into a Probe agent. Then select **Map Discovery & Credentials**.



3. Under Discovery Settings/Credentials Mapping, select the network(s) that the Probe should scan, and select any credentials it might need to access devices on them. Then select **Save**.

Note: *Make sure the agent's device has access to the network(s) you designate.*

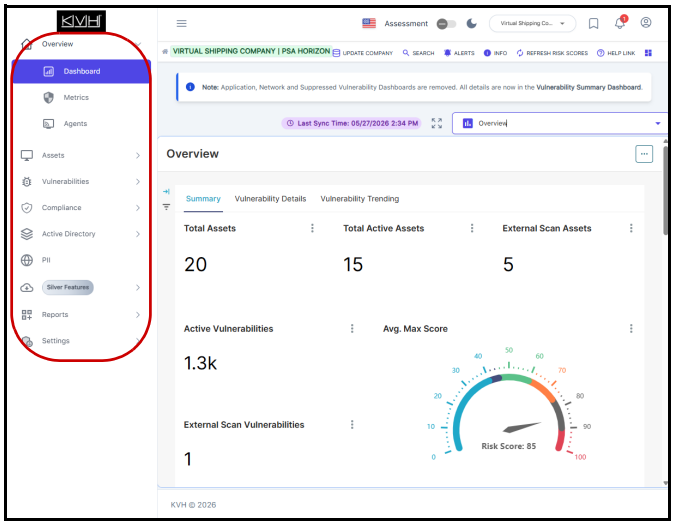


4. Repeat this process for any other LightWeight agents you want to convert into Probe agents. KVH recommends setting up two Probe agents on each LAN segment.

Note: *It might take up to 15 minutes for the conversion process to complete.*

Exploring the ConnectSecure Portal

Once you have installed and configured your agents, you can view their scan results in a variety of ways by selecting the desired option from the main menu.



- **Dashboard**: Select from an extensive library of built-in dashboards or create your own custom dashboard to display detected security problems, vulnerabilities, asset health metrics, and compliance gaps at a glance
- **Metrics**: Total vulnerabilities categorized by severity, along with risk and compliance scores
- **Assets**: View technical details for all assets reported by LightWeight agents and discovered by Probe agents, view detected problems and suggested remediations, and manage application/OS patches
- **Vulnerabilities**: Consolidated list of detected problems, along with their severity, impact, and exploitability ratings
- **Compliance**: Shows results of the compliance scan(s) you have enabled under Company Settings *(select one or more types of standards/frameworks)*
- **Reports**: Generate standard or custom reports for regulatory compliance or your company's records

Note: *Refer to the ConnectSecure documentation, accessible via the Help Link, for complete details, including troubleshooting FAQs and how-to videos.*