Illumio®

Version 24.1

LW-VEN

Version 1.0.1

# LW-VEN Installation and Configuration Guide

# Legal Notices

**Product Version**

PCE Version: 24.1

For the complete list of Illumio components compatible with Core PCE, see the Illumio Support portal (login required).

For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal.

# LW-VEN Requirements and Limitations

This section covers the LW-VEN's setup operations, requirements, limitations, and caveats.

The LW-VEN software installs the Illumio Legacy Windows VEN Service on your supported legacy Windows machines. Once installed, the Illumio Legacy Windows VEN Service:

- Enforces policy received from the PCE.
- Consumes CPU as needed to calculate or optimize and apply the firewall while remaining idle in the background as much as possible.

You control the Illumio Legacy Windows VEN Service's operations through the PCE web console or from the command line on the Windows machine on which the LW-VEN is installed.

## Set-up Sequence

When run, the Illumio Legacy Windows VEN Service automatically does the following:

1. Checks whether this solution is supported.
2. Installs and pairs an LW-VEN on your legacy Windows Servers.
3. Creates a workload on the PCE to represent your legacy Windows Servers as a managed workload. A secured workload is known as a managed workload.
4. When running, the service:
   - Requests policy from the PCE as follows: after the LW-VEN sends a heartbeat to the PCE every five minutes, if there are any policy updates, the LW-VEN requests them from the PCE. If there are no policy updates, the LW-VEN performs a tamper check on its local policy to ensure that it hasn't been changed.
   - Applies the Illumio firewall rules obtained from the PCE to the Windows workload.

If the Illumio Legacy Windows VEN Service fails, Windows restarts it automatically.

# Requirements

- IllumioLWVENInstaller.exe

- Illumio Policy Compute Engine (PCE) release 23.2.20 or later.

- 32-bit or 64-bit Microsoft Windows Server 2003 Service Pack 1 & Service Pack 2 and Windows 2008 Service Pack 1 & Service Pack 2

- .NET Framework 4.0.0 (minimum required; versions 5.0 and later are not supported)

- A dedicated local user account with admin privileges for installing and modifying the Windows firewall, running the service, and issuing the `illumio-lwven-ctl` commands.

> IMPORTANT:
> You must disable the User Access Control (UAC) feature if it is enabled on the legacy Windows Server machines on which you plan to install the Illumio Legacy Windows VEN Service. Otherwise, you will not be able to install the LW-VEN on the machine. UAC is a Windows security feature that prevents unauthorized changes to the operating system.

- When sending requests to the PCE the LW-VEN performs peer certificate validation by validating the certificate against the generally available cert.pem file provided in the Illumio LW-VEN Service\`certs` directory. If you need to add extra certificate validations, add the appropriate .pem files to the `\certs` directory before activating the LW-VEN.

- By default, this solution doesn't collect flow information. To enable flow collection, you must configure FlowLink as described in the Flowlink Configuration and Usage Guide.

## Limitations and Caveats

Take careful note of the following limitations and caveats.

| Item | Windows 2003 Server SP1 & SP2 | Windows 2008 Server SP1 & SP2 |
|---|---|---|
| Enforcement modes | Support for:<br><br>• Idle mode | Support for:<br><br>• Idle mode |

| Item | Windows 2003 Server SP1 & SP2 | Windows 2008 Server SP1 & SP2 |
|------|-------------------------------|-------------------------------|
|  | • Full Enforcement<br><br>If you change the Enforcement Mode from **Full** to **Idle**, the Illumio Legacy Windows VEN Service removes all Illumio policy from the Windows server. If you switch back to Full enforcement, the policy is reapplied to the workload.<br><br>Although the **Visibility** and **Selective** options are not supported with Win 2003 SP1/SP2 servers, the options still appear in the PCE UI in the Enforcement drop-down menu on each Workload's details page. If you change the Enforcement mode from **Full** to **Visibility** or **Selective**, the LW-VEN ignores the policy and logs an event to the Windows Event Log and the PCE. | • Visibility mode<br><br>• Selective Enforcement<br><br>• Full Enforcement<br><br>If you change the Enforcement Mode from **Full** to **Visibility** or **Selective**, the PCE creates an Illumio ALLOW ALL rule, effectively allowing all non-blocked traffic.<br><br>NOTE: In Selective Enforcement mode, the Windows 2008 Server firewall applies all block rules before applying any allow rules. This behavior is opposite to how the standard Illumio VEN works on other Windows systems. |
| Visibility, Flow logs | By default, this solution doesn't collect flow information. To | |

| Item | Windows 2003 Server SP1 & SP2 | Windows 2008 Server SP1 & SP2 |
|---|---|---|
| | enable flow collection, you can configure FlowLink. For more information, see the Flowlink Configuration and Usage Guide. | |
| Inbound/Outbound Rules | Support for:<br><br>• Inbound rules only | Support for:<br><br>• Inbound rules<br>• Outbound rules |
| Policy Rules Limitations | Support for:<br><br>• Port & protocol rules only<br>• One rule per port/protocol. For example, if you specify a rule that includes a port range, multiple single rules are created, one per port.<br>• Support for programming only a list of IP addresses and/or CIDR blocks per rule. (IP ranges are converted to CIDR blocks.) The LW-VEN always attempts to merge IP addresses into the most compact CIDR addresses possible.<br>• If the Illumio Legacy Windows VEN Service is uninstalled, all Illumio rules are removed from the firewall. | Support for:<br><br>• Port & protocol rules only<br>• Specifying a rule that includes a port range results in a single rule, but ports are shown in a comma-separated list instead of a port range.<br>• IP ranges. (CIDR blocks are converted to an IP range.) The LW-VEN always attempts to merge IP addresses into the most compact IP ranges possible.<br>• If the Illumio Legacy Windows VEN Service is uninstalled, all Illumio rules are removed from the firewall. |
| Matching rules | • **Exact Matches (port/protocol and all IPs match)**<br><br>Customer rule remains enforced; Illumio rules are not applied. | • **Exact Matches (port/protocol and all IPs match)**<br><br>Customer rule remains enforced; Illu- |

| Item | Windows 2003 Server SP1 & SP2 | Windows 2008 Server SP1 & SP2 |
|---|---|---|
| | • **Partial Matches (port/protocol match but only some or no IP addresses match)**<br><br>If a customer rule exists for the same port & protocol as an Illumio rule, the Illumio rule is applied and the customer **rule is overwritten**. | mio rules are not applied.<br><br>• **Partial Matches (port/protocol match but only some or no IP addresses match)**<br><br>If a customer rule exists for the same port & protocol as an Illumio rule, the customer **rule is disabled** and the Illumio rule applies. If the customer suspends or uninstalls the Illumio LW-VEN Service, their partially matching rules, if any, remain disabled. |
| Rule character limits | Windows limits the size of rules to approximately 8K characters. Rules that exceed 8K characters will cause the entire policy to be rejected and a message to be logged in the Window's Event Log. | Windows limits the size of rules to approximately 8K characters. Rules that exceed 8k characters are split into multiple rules. No limit on the number of rules is enforced. |
| Error handling | Log messages are written to local logs; errors and warnings are also written to the Windows Event Log and to the PCE. | |
| LW-VEN and workload names in the PCE | After you activate an LW-VEN, the LW-VEN workload appears in the PCE UI with the same name as the Server's hostname. | |
| User interface | • The **Upgrade** button that appears on the VEN page in the PCE Web Console doesn't apply to this solution. Clicking the button has no effect. | |

| Item | Windows 2003 Server SP1 & SP2 | Windows 2008 Server SP1 & SP2 |
|---|---|---|
| | • If you unpair the LW-VEN through the PCE UI by clicking **Unpair** on the LW-VEN's detail page, only the **Open All Ports** option is supported. | |

# Install and Configure the Illumio LW-VEN Service

This section details how to install and configure the Illumio LW-VEN Service.

## Procedure

Perform the following steps.

### STEP 1: (Recommended) Back Up the Existing Firewall Configuration

Before you install the Illumio LW-VEN Service, Illumio recommends that you back up your legacy Window's existing firewall configuration in case it becomes necessary to revert back to it. For example, reversion would be necessary if you uninstall the Illumio LW-VEN Service.

### STEP 2: Create or Find a Pairing Profile with the Appropriate Settings

> IMPORTANT:
> Note that this solution differs from the standard VEN pairing process in that it doesn't use the pairing script available in the pairing profile. Only a properly-encoded pairing key is required to pair the LW-VEN installed on your legacy Windows server with the PCE.

All pairing keys are generated from a Pairing Profile and are encoded with settings from that profile. The pairing key you obtain or generate for this solution must have been generated from a pairing profile with the appropriate settings for your type of Windows server.

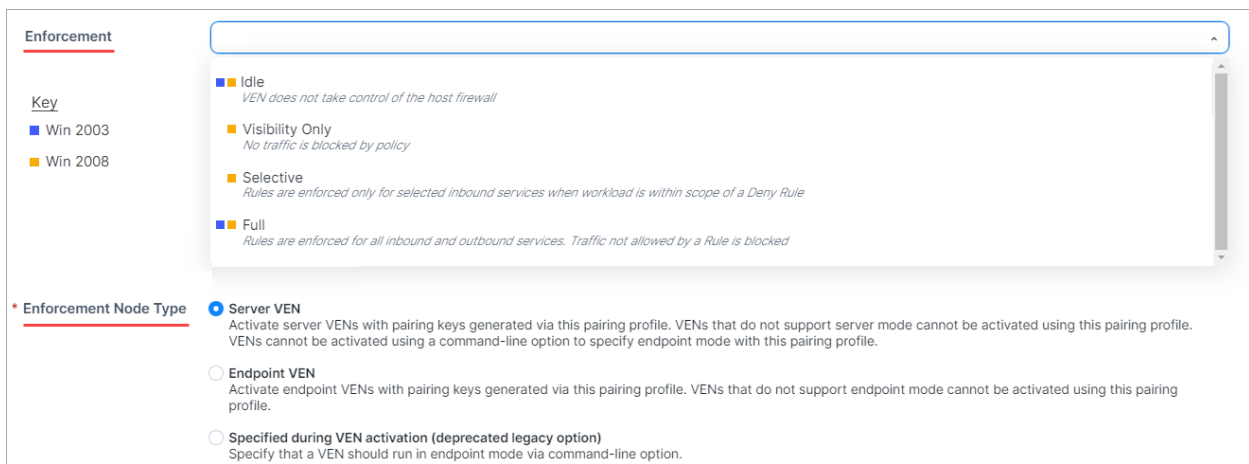**Minimum required pairing profile settings**

| Operating System | Supported Enforcement Modes | Supported Enforcement Node Type |
|---|---|---|
| Win 2003 Server SP1 & SP2 | • Idle (recommended)<br>• Full | Server VEN |
| Win 2008 Server SP1 & SP2 | • Idle | Server VEN |

| Operating System | Supported Enforcement Modes | Supported Enforcement Node Type |
|---|---|---|
| | • Visibility<br><br>• Selective<br><br>• Full | |

## Option 2.1 - Create a new Pairing Profile

To create a new pairing profile, go to **Servers & Endpoints > Pairing Profiles** and con-figure settings using this image and the table above as a guide.

For more information about creating a pairing profie, see Configure a Pairing Profile.



## Option 2.2 - Find an existing Pairing Profile with the proper settings

To identify an existing pairing profile with the appropriate settings for your server type, go **Servers & Endpoints > Pairing Profiles** and find a profile with **Enforcement Node Type: Server VEN** and the Enforcement mode(s) appropriate for your Windows Server.

You can filter the list by Enforcement Node Type.

## STEP 3: Obtain or Generate a Pairing Key in the PCE Web Console

Choose one of the following options to obtain a pairing key.

> IMPORTANT:
> As detailed in STEP 2: Create or Find a Pairing Profile with the Appropriate Settings, make sure that the pairing key you obtain or generate for this solution was generated from a pairing profile with the appropriate settings for your type of Windows server.

### Option 3.1 - Copy a Pairing Key from an existing Pairing Profile

1. Expand the **Servers & Endpoints** section in the left navigation.

2. Click **Workloads**.

3. Click **Add**, and then choose **Pair Workload with Pairing Profile**.
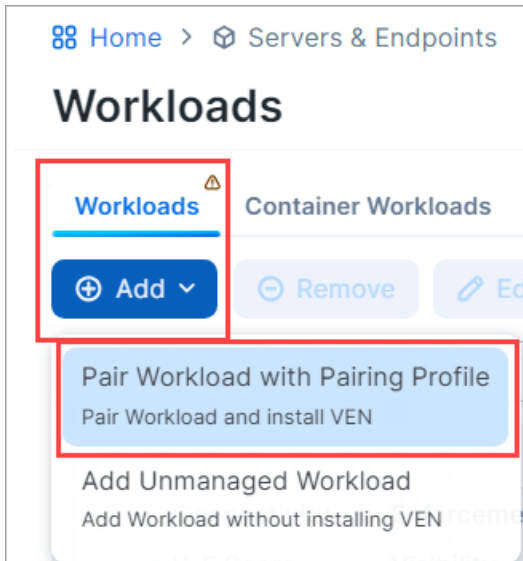
4. In the **Pick a Pairing Profile** drop-down list, select the pairing profile you iden-
   tified previously that has the appropriate settings for your legacy Windows
   server (see STEP 2: Create or Find a Pairing Profile with the Appropriate
   Settings.).
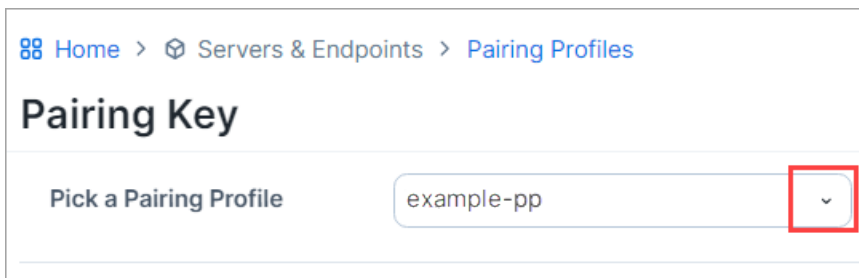


5. Scroll down to **Pairing Scripts** and copy and preserve the Key for use in STEP 4.
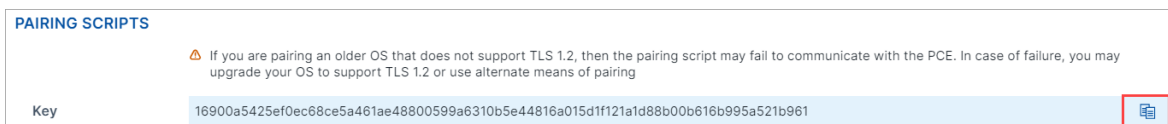


> IMPORTANT:
> Don't copy the pairing script available in the pairing profile. Pairing
> scripts are not used with this solution.

## Option 3.2 - Generate a new Pairing Key from an existing Pairing Profile

1. Expand the **Servers & Endpoints** section in the left navigation.

2. Click **Pairing Profiles**.

3. Click an existing pairing profile that has the appropriate settings for your legacy Windows server (see STEP 2: Create or Find a Pairing Profile with the Appropriate Settings.)

4. Click **Generate Key**.

5. Scroll down to **Pairing Scripts** and copy and preserve the Key for use in STEP 4.

### Option 3.3 - Create a new Pairing Profile

1. Expand the **Servers & Endpoints** section in the left navigation.

2. Click **Pairing Profiles**.

3. Click **Add** and configure the settings appropriate for your legacy Windows server as described in Option 2.1 - Create a new Pairing Profile.

4. Click **Save**.

5. Open the Pairing Profile you just created.

6. Scroll down to **Pairing Scripts** and copy and preserve the Key for use in STEP 4.

> IMPORTANT:
> Don't copy the Pairing Script. The script is not used in this solution.

## STEP 4: Install, configure, and pair the Illumio Legacy Windows VEN Service on a legacy Windows server

> IMPORTANT:
> - You must disable the User Access Control (UAC) feature if it is enabled on the legacy Windows Server machines on which you plan to install the Illumio Legacy Windows VEN Service. Otherwise, you will not be able to install the LW-VEN on the machine. UAC is a Windows security feature that prevents unauthorized changes to the operating system.
> - You must install and activate the Illumio Legacy Windows VEN Service from a dedicated local admin account.
> - Only the Illumio LW-VEN Service account user can run the LW-VEN service and issue `illumio-lwven-ctl` commands.

1. Obtain the `IllumioLWVENInstaller.exe` file and place it on the Windows server. (Recommended location: `C:\Users\Administrator`). The installer is available on the Illumio Support portal.

2. Perform one of the following installation + activation options:

| Option 4.1 - Respond to prompts | Option 4.2 - No prompts (useful for automated processes) |
|---|---|
| Launch the file from a command line or by double-clicking the file. <br><br>(a) Install<br><br>• **Select Destination Location**<br><br>The default installation location depends on whether the legacy Windows server is a 32-bit or 64-bit machine.<br><br>○ 32-bit machines: (`C:\Program Files\Illumio LW-VEN Service`)<br><br>○ 64-bit machines: (`C:\Program Files(x86)\Illumio LW-VEN Service`)<br><br>• **Select Additional Tasks**<br><br>○ Make sure the path option is selected, and then click Next.<br><br>• **Ready to Install**<br><br>○ Click **Install**.<br><br>• **Complete the Setup Wizard**<br><br>○ Select "Launch illumio-lwven-ctl activate"<br><br>○ Click **Finish**. The `certs.pem` file is added immediately after you click **Finish**.<br><br>(b) Activate and configure<br><br>• **Complete the Setup Wizard** | Enter the following command at a command prompt:<br><br>`C:\Users\Administrator>illumio-lwven-ctl activate --management-server <pcehost:port> --activation-code <pairing-key> [--passsword <account-password>]`<br><br>IMPORTANT: For a fully automated activation process, make sure to include the --password option and specify the user account password. Otherwise, you are prompted to enter a password to complete the activation.<br><br>Messages appear:<br><br>• Resolving: `<pcehost>`<br><br>• Pairing to PCE `<pcehost:port>`<br><br>• `POST /org/0/agents/activate`<br><br>• Activation Complete |

| Option 4.1 - Respond to prompts | Option 4.2 - No prompts (useful for automated processes) |
|---|---|
| <ul><li>Select "Launch illumio-lwven-ctl activate"</li><li>Click Finish. The certs.pem file is added immediately after you click Finish.</li></ul><ul><li>**Enter hostname: port for PCE address**: Enter the subdomain (s) and domain of your PCE's web address and port (for example, `example.illum.io:8443`).</li></ul><ul><li>**Enter pairing key for LW-VEN**: Paste the pairing key that you obtained in STEP 3 and then press **Enter**.</li></ul>Messages appear:<ul><li>Pairing to `<pcehost:port>`</li><li>Activation Complete</li><li>You are prompted to enter the user account password, which is necessary to run the Illumio LWVEN Service.</li></ul> |  |

3. Go to **Servers & Endpoints > Workloads > VENs**.

4. Click the name of the LW-VEN you added.

5. Confirm the following on the LW-VEN's details page:

   - **NODE** section:

     - Hostname: `<your-Windows-Server-Computer-Name>`

     - Enforcement Node Type: See STEP 2: Create or Find a Pairing Profile with the Appropriate Settings.

     - Version: 1.0.0

- ○ **HOST** section:
    - OS: LW-VEN 1.0.0

6. You can perform the following operations on the LW-VEN (For details, see the VEN Administration Guide):

    - ○ Edit the LW-VEN

    - ○ Generate a support bundle (see Support report).

    - ○ Mark the LW-VEN Suspended

        > NOTE:
        > This should be necessary only if you issue the `illumio-lwven-ctl` suspend command and receive a message indicating that the LW-VEN failed to inform the PCE of its suspension.

    - ○ Unpair the LW-VEN

        > NOTE:
        > If you unpair the LW-VEN through the PCE UI by clicking **Unpair** on the LW-VEN's detail page, only the **Open All Ports** option is supported.

## STEP 5: Create Security Policy

In the PCE web console, create label-based policies for your Windows Server 2003 SP1 & SP2 and Windows Server 2008 SP1 & SP2 workloads. For information on how to create policies, see the Security Policy Guide.

# Manage and Troubleshoot the Illumio LW-VEN

This section covers Illumio LW-VEN pairing and activation concepts, Illumio firewall rules, tamper detection, support bundle generation, common commands, and troubleshooting.

## About Paring and Activation

The terms "activation" and "pairing" indicate the same function from different perspectives; namely, putting the workload under managed control by the PCE:

- The LW-VEN sees itself as activated or deactivated.
- The PCE sees an LW-VEN as paired or unpaired.

| Pairing and Activating the LW-VEN | |
|---|---|
| 1 | The LW-VEN is installed. | The PCE remains unaware the LW-VEN is present. |
| 2 | The LW-VEN and the PCE are paired. | The PCE uses a pairing key (activation code) to pair with the LW-VEN. After pairing, the PCE becomes aware of the LW-VEN. |
| 3 | The LW-VEN is activated. | The LW-VEN uses an activation code generated by the PCE. After activation, the LW-VEN is ready to function. |

## Unpairing, deactivating, and uninstalling the LW-VEN

Here's how these operations work in this solution:

- **Unpairing** the LW-VEN through the PCE UI or by issuing `illumio-lwven-ctl unpair` unpairs the LW-VEN from the PCE and uninstalls the LW-VEN software.
- **Deactivating** the LW-VEN by issuing `illumio-lwven-ctl deactivate` unpairs the LW-VEN from the PCE but doesn't remove the LW-VEN software.
- **Uninstalling** the Illumio Legacy Windows VEN Service through the *Windows Control Panel > Programs and Features*:
    - Unpairs the LW-VEN from the PCE
    - Removes the Workload object from the PCE

◦ Removes Illumio firewall rules and any working files

◦ Uninstalls the LW-VEN software from the Windows server

## View the Illumio rules applied to the native firewall

Illumio rules applied to the Windows Server's native firewall begin with `Illumio`. For example: `IllumioInTcp14000Permit`

There are two ways to view Illumio firewall rules:

- Generate a Support Report and look in the **Firewall.txt** file.

- Issue a command on the Windows Server:

> NOTE:
> Using the `findstr` filter shows only the first line of the rule, not the entire rule.

- **Win 2003 SP1/SP2**: `C:\Users\Administrator> netsh firewall show portopening enable | findstr /R "Illumio.*"`

- **Win 2008 SP1/SP2**: `C:\Users\Administrator> netsh advfirewall firewall show rule name=all | findstr /R "Illumio.*"`

## Tamper detection

The Illumio Legacy Windows VEN Service performs tamper checking whenever it heartbeats to the PCE (every 5 minutes) and discovers that there is no new policy to apply. Whenever the policy update check occurs, the Illumio Legacy Windows VEN Service checks whether the last-applied Illumio policy on the legacy server differs from the last applied policy from the PCE. If a difference is detected, the Legacy Windows VEN Service reverts the policy to the intended state so that the correct PCE security policy is enforced.

## Support report

You can generate the Illumio Legacy Windows VEN Service support report. It includes the following information:

Firewall.txt: Lists all the rules currently programmed in the native Windows Firewall.

- Logs specifying:
    - When policy was last received
    - When policy was last applied and what was applied
    - System information (output of the `systeminfo` command)

## Generate a Support Report

### Option 1:

This is the simplest way to generate a report.

> NOTE:
> This option assumes that the LW-VEN is in a running state on the Windows
> Server.

1. Go to Servers & Endpoints > Workloads > VENs
2. Click the name of the LW-VEN you added to go to its details page.
3. Click Generate Support Bundle.

The bundle is uploaded to the PCE (may take up to 10 minutes).

### Option 2:

This option is useful if the LW-VEN is stopped due to a major problem.

- Issue `illumio-lwven-ctl support-report`

The location of the report on the Windows server is returned after you issue the command. This report is not sent to the PCE.

### Logs

The Illumio LW-VEN Service logs its operations locally on the Windows Server. Logs are rotated from primary to backup when their size reaches 10MB or once every 24 hours at midnight.

#### Location

- 32-bit: `C:\Program Files\Illumio LW-VEN Service\logs`
- 64-bit: `C:\Program Files (x86)\Illumio LW-VEN Service\logs`

#### Archive

By default, seven log archives are preserved on the workload.

# Commands

You can issue the following commands to interact with the Illumio LW-VEN Service.

> NOTE:
> - Only the Illumio LW-VEN Service account user can issue `illumio-lwven-ctl` commands.
> - All commands include the prefix `illumio-lwven-ctl`

- `activate`

- `status`

- `restart`

- `stop`

- `start`

- `unpair`

  Removes the Illumio policy from the firewall, removes the LW-VEN from the PCE, and uninstalls the LW-VEN software from the Window's server. You can also uninstall the LW-VEN from the PCE by clicking Unpair for the appropriate LW-VEN on the PCE VEN page. With this unpairing method, it may take up to five minutes for the LW-VEN to be unpaired and uninstalled.

- `deactivate`

  Removes the Illumio policy from the firewall; removes the PCE objects from the PCE and from the Illumio LW-VEN Service; does not remove the LW-VEN software from the installation directory (in case you want to later re-activate the LW-VEN without having to install the LW-VEN package).

- `support-report`

- `suspend`

  Suspends the Illumio LW-VEN Service and uninstalls Illumio policy from the firewall.

- `unsuspend`

  Enables and starts the Illumio LW-VEN Service; retrieves and applies the latest PCE policy.

# Troubleshooting

This section describes how to troubleshoot common issues.

| Issue | Remediation |
|---|---|
| The Illumio Legacy Windows VEN Service stops. | Check logs: Windows Event Viewer Log Local Illumio logs |
| Problem receiving policy from the PCE. | |
| Problem applying policy to the workload created by the Illumio Legacy Windows VEN Service. | |
| Problem with the connection between the Illumio Legacy Windows VEN Service and the PCE. | The Illumio Legacy Windows VEN Service tries every five minutes to reconnect to the PCE. |
| Unable to install, stop, suspend, or unpair the Illumio Legacy Windows VEN Service. | These issues may be caused by the User Access Control (UAC) feature if it is enabled on your legacy Windows Server machines. UAC is a Windows security feature that prevents unauthorized changes to the operating system. Disable the User Access Control (UAC) feature if it is enabled. |
| Pairing the LW-VEN with the PCE fails; a message indicates that the pairing key was generated from a pairing profile with unsupported settings for this solution, such as the wrong Enforcement mode or Enforcement Node Type. | Obtain a properly-encoded pairing key (see STEP 2) and repeat STEP 3 and STEP 4. |