# Quick Start Guide for Integrating Ziften Zenith and Microsoft Windows Defender ATP

Ziften and Microsoft have agreed to a technical partnership in which Ziften's Zenith platform is able to integrate in a bidirectional fashion with the Windows Defender ATP (WDATP) platform.

## Ziften Zenith Agent Installation

Ziften agents must be installed on the desired macOS and/or Linux endpoints / servers. Telemetry from the agents is collected in the Zenith cloud backend and passed through a cloud-to-cloud integration to the WDATP platform. Telemetry collected includes process data, network connectivity, system information, user information, and alerts / detections. The WDATP console can also initiate response actions through Zenith.

## MacOS Installation

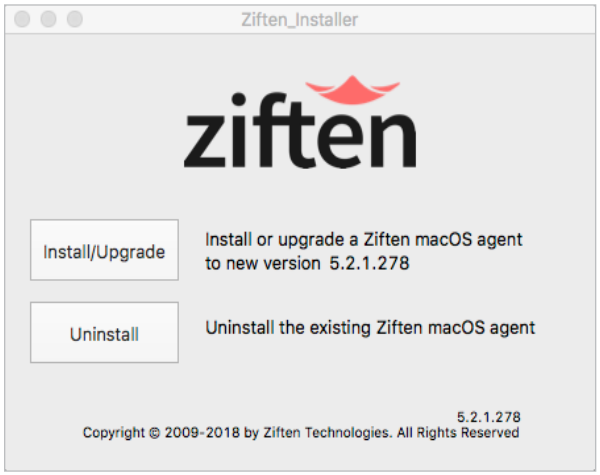
### macOS Minimum Requirements

**Hardware:**
1GHz processor / 2GB RAM

**Software:**
10.8+

### macOS GUI Installation

For small deployments and acceptance testing, administrators can install the agent by mounting the provided Ziften Installer .dmg on the target machine, and double clicking on the Installer.app inside. Installing with this method will present the following UI of install options:




### Install/Upgrade

Installs the agent if no agent is present. Upgrades an existing agent if the version is below that of the agent packaged in the Installer.app. This method preserves the existing agent GUID and onboard database.

### Uninstall

Uninstalls any existing agent and leaves behind the GUID and onboard database.

### macOS Systems Management or Commandline Installation

For normal production rollouts, push the .dmg out to systems using your company's deployment method (e.g. LANDesk, Jamf Pro, etc.). In some instances, the Ziften package must be rebuilt using a tool specific to your deployment software. The Installer.app will perform a silent install and will not display anything to the end user during install or while running.

The deployment tool must run as root and mount the .dmg and then execute the following command with the desired flag on the endpoint machine:

```
'/Volumes/<<DMG>>/<<Installer>>/Contents/MacOS/Ziften_Installer --install'
```

Where <<DMG>> is the name of your .dmg and <<Installer>> is the name of the Installer.app housed inside the .dmg.

Ziften Client Services will provide you with the exact command to pass your tool, based on the names of the files they deliver to you. The following available Installer.app flags exist and correspond to the UI install methods described above.

```
--install
--uninstall
```

### Notes

- If no flag is passed, the Installer.app will execute --install.
- The macOS agent is compatible with Gatekeeper.

## Linux Installation

### Linux Minimum Requirements

**Hardware:**
1GHz processor / 2GB RAM

**Software:**
CentOS/RHEL 5+/ Scientific Linux / Ubuntu 12+ / Fedora

### Linux Basic Install / Uninstall

To install the Ziften Linux agent, the RPM or DEB must be copied to the system. Use the following installation commands as needed:

**Redhat Package Manager Syntax:**

```
sudo rpm -i ziften_installer.rpm
```

**Debian/Ubuntu Syntax:**

```
sudo dpkg -i ziften_installer.deb
```

To uninstall the Linux agent, use the following commands as needed:

**Redhat Package Manager Syntax:**

```
sudo rpm -e ziftenagent
```

**Debian/Ubuntu Syntax:**

```
sudo dpkg -r ziftenagent
```

### Special Linux Installation Note

If auditd is not enabled, the Ziften agent may miss certain metadata, such as hashes, command lines, and user attribution data, for processes that are short lived.

As a fix, we recommend enabling auditd. Ziften can provide an Extension to automatically enable auditd. To manually enable auditd use the following commands:

**Ubuntu:**

```
sudo apt-get -y install auditd
echo '-a always,exit -F arch=b64 -S execve' >> /etc/audit/audit.rules
service auditd restart (or systemctl restart auditd)
```

**RHEL Distributions:**

```
sudo yum install auditd
echo '-a always,exit -F arch=b64 -S execve' >> /etc/audit/audit.rules
service auditd restart (or systemctl restart auditd)
```

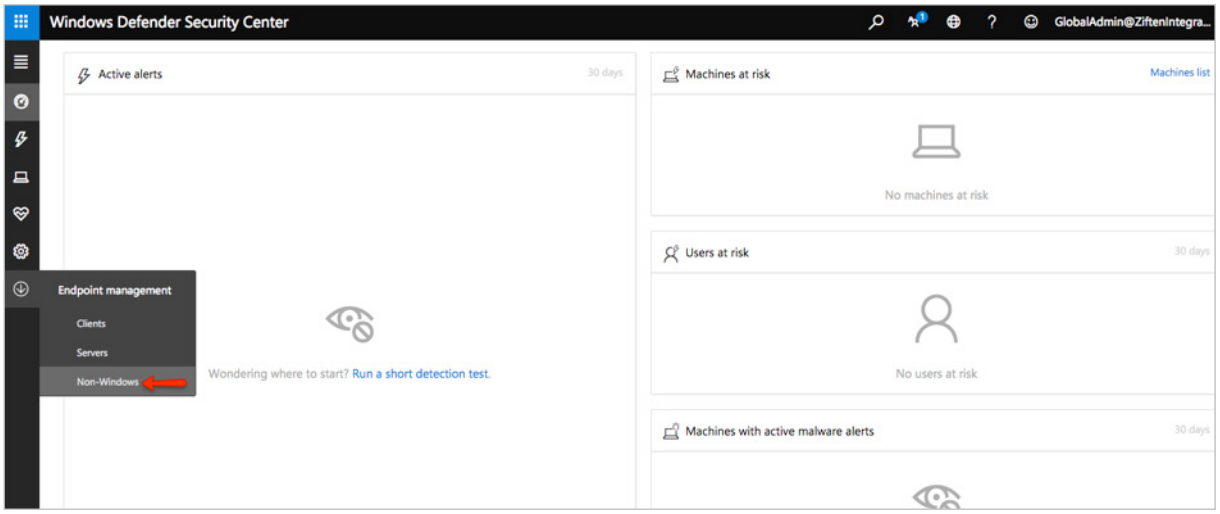
# Zenith and Security Center Backend Integration

## Prerequisites

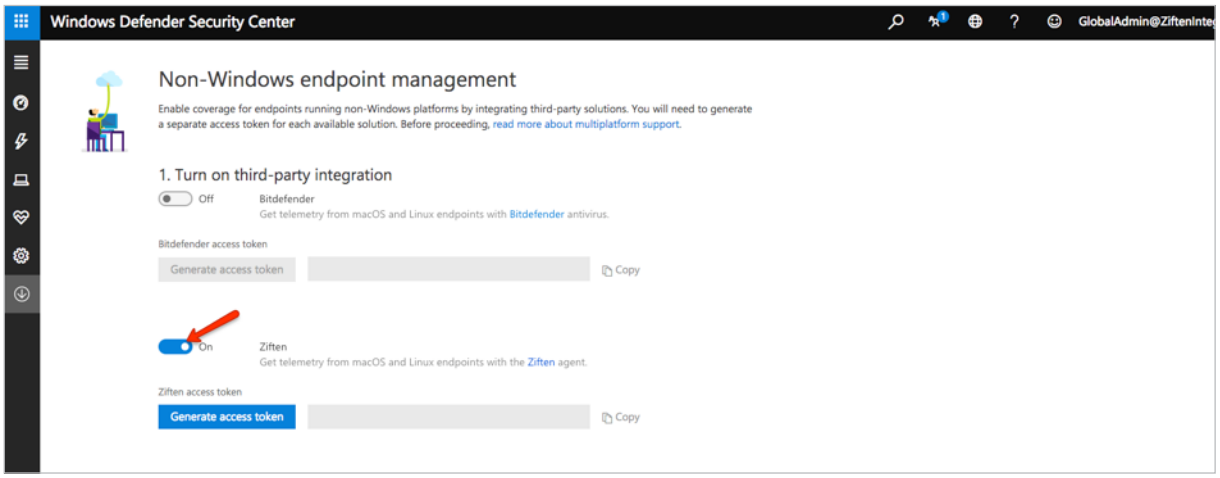
- A valid account for Microsoft Windows Defender Security Center
- Access to the rpm, deb, or dmg Ziften agents for Linux and/or macOS

## Integrate Ziften Zenith with Security Center

1. Go to Windows Defender Security Center and sign in.
2. Click the menu icon and choose Endpoint Management > Non-Windows.



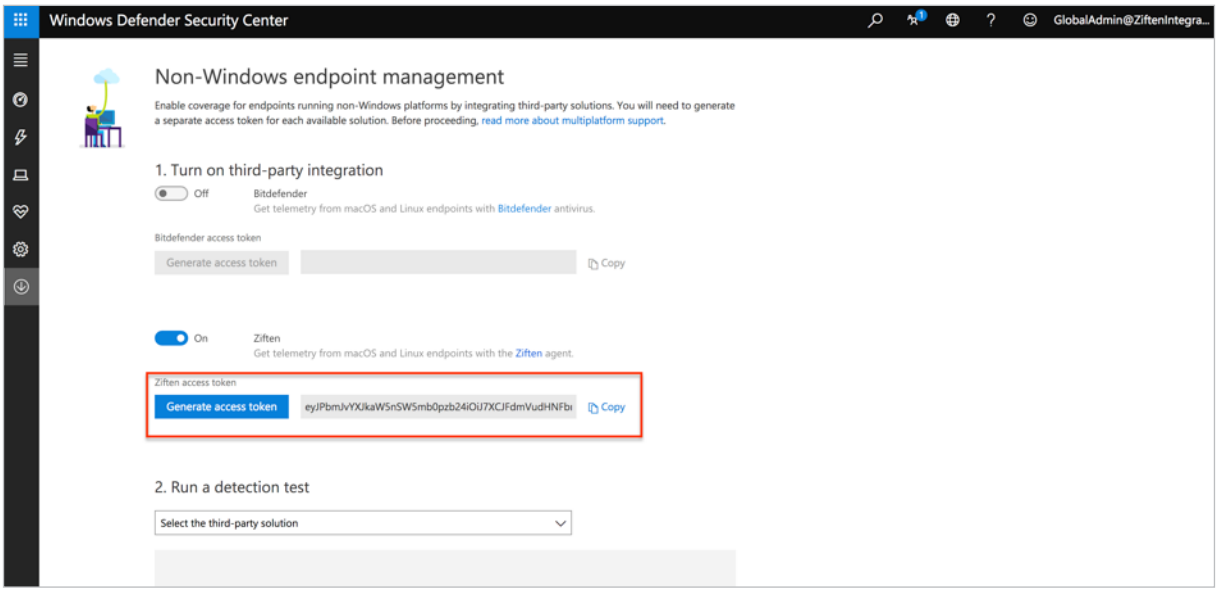

3. Under Turn on Third Party Integration, turn ON the Ziften toggle switch to get telemetry from macOS and Linux endpoints with Ziften.



4. Click Generate access token.

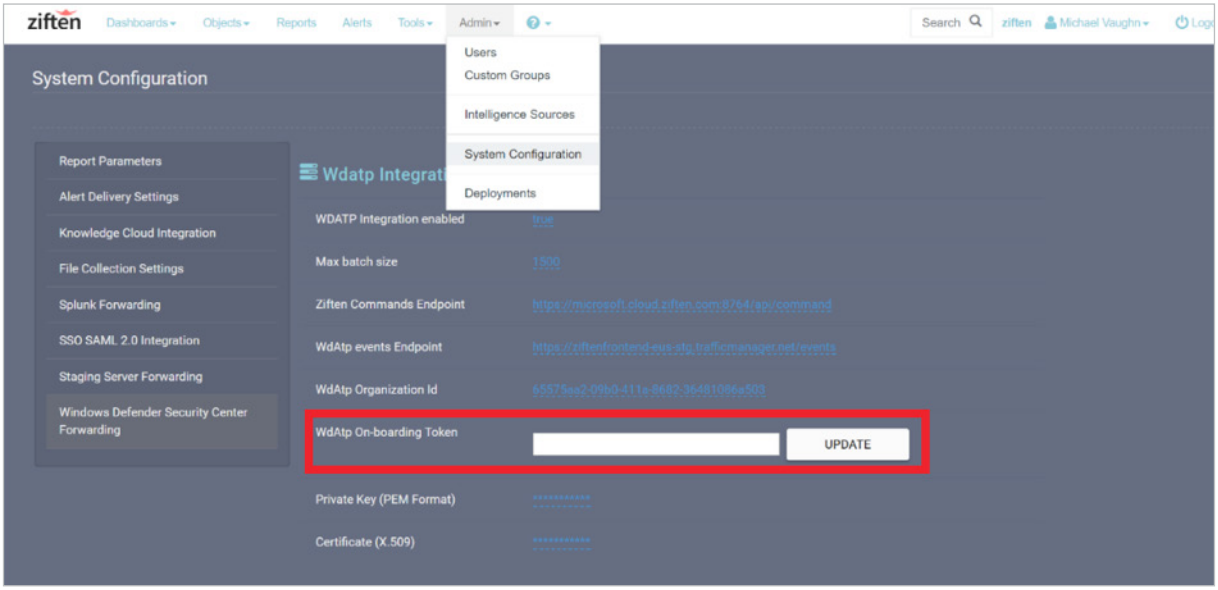
5. Click Copy.




6. Then, in a separate window, login to your Ziften console:
`https://<YourServerName>.cloud.ziften.com/admin/systemconfig/WDATP_INTEGRATION`

7. From the top menu, select Admin > System Configuration.

8. Past the Ziften Access Token in the WdATP On-boarding Token field.

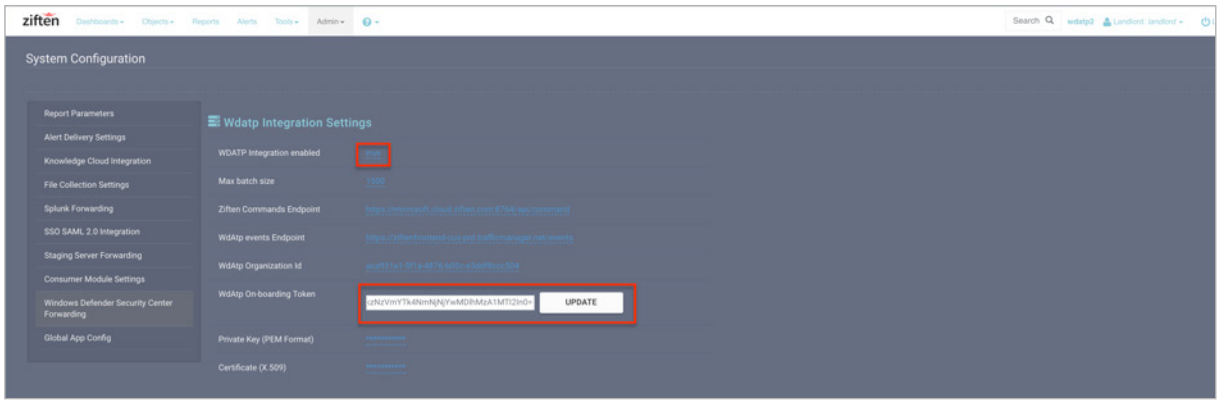


9. Click UPDATE.

10. A ‘Success’ message in green should appear to the right of the UPDATE button.

11. Ensure that the WDATP Integration Enabled field reads ‘true’.

12. Ziften Zenith is now integrated with Microsoft Windows Defender Security Center. Ziften events can now be viewed in Windows Defender Security Center.




## Test the Integration

To check the success of the Zenith to Windows Defender Security Center integration:

1. Confirm Ziften agents are installed on target endpoints. For details regarding the installation, refer to the initial part of this document.

2. On macOS or Linux, start a new terminal session.

3. Paste the following text into the terminal window and press enter:

```
echo
dGVzdD0vYmluL3NsZWVwO2NwIC9iaW4vc2xlZXAgL3RtcC9tYWxpY2lvdXNhdHRhY2tlcjsvdG1wL-
21hbGljaW91c2F0dGFja2VyIDU7cm0gL3RtcC9tYWxpY2lvdXNhdHRhY2tlciAK | base64 --de-
code | bash
```

4. Navigate to the Machine List.

5. Locate your test machine.

6. View details and confirm positive test results. Note, it may take up to 15 minutes for the results to populate.

Read more about protecting non-Windows operating systems with Windows Defender Advanced Threat Protection by clicking here: https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-atp/configure-endpoints-non-windows-windows-defender-advanced-threat-protection