VERCARA
a digicert® company

UltraDDR Agent Software for macOS (2.2.9)

User Guide

Version 2.29.0

Find more information at:

vercara.com

Call USA: +1 (844) 929 - 0808
Call EMEA: +44 808 175 1189

Introduction

UltraDDR (UltraDNS Detection and Response) is a cloud-based DNS-layer protection service that identifies and prevents attacks before they happen for devices inside and outside your network. UltraDDR detects compromises in real-time, blocking current and preventing future attacks from harming your users and network.

UltraDDR provides a Protective DNS solution that enables enterprises to get in front of threats by blocking communication before damage can occur. Protective DNS analyzes DNS queries and takes action to mitigate threats. Using years of historical domain data, UltraDDR delivers real-time observability of outbound network communication, allowing enterprises to detect and stop malware, ransomware, phishing, and supply chain attacks before they can do damage.

UltraDDR also provides comprehensive DNS firewall capabilities that allow administrators to choose categories of internet traffic—such as adult, gambling, gaming, social media and more—that are deemed risky or not acceptable under company policy, and block or flag this traffic to provide a simple, unobtrusive way of enforcing policy.

Users that are on your premises are automatically protected when UltraDDR is used as your organization's recursive DNS solution. For users that are off your premises, or for hybrid scenarios in which users can be on-premises or off-premises at-will, UltraDDR agents can be installed onto your users' devices to ensure UltraDDR policy is enforced.

Installing the UltraDDR Agent for macOS

- Download the software installer from https://macos-download.ultraddr.com/.
- Locate the PKG file on your computer (check your "Downloads" folder) and open it by double-clicking on the file to launch the UltraDDR installer.
- The UltraDDR installer is now running. Click "Continue" to proceed.
- The installer will now prompt you for an install key.

> **Administrators:** the install key can be found on the UltraDDR portal (https://ddr.ultradns.com) at Settings (⚙ icon) > UltraDDR Agent > Install > Install Key.

Silent Install

To silently install the UltraDDR Agent for macOS, a temp file named `.vercara.ultraddr.client.id` must be created on the local filesystem at `/tmp/` that contains your organization's install key. The UltraDDR Agent for macOS software installer must then be run from the macOS terminal:

- Download the software installer from https://macos-download.ultraddr.com/. These instructions

assume that the installer is downloaded to the current user's Downloads folder (`$HOME/Downloads`).

- Create a text file at `/tmp/.vercara.ultraddr.client.id`. The content of the text file must contain your organization's install key, and only the install key. the install key can be found on the UltraDDR portal (https://ddr.ultradns.com) at Settings (⚙ icon) > UltraDDR Agent > Install > Install Key.
- Run the following command from a terminal window:
  `sudo installer -store -pkg "$HOME/Downloads/UltraDDR-2.2.8.pkg" -target /`

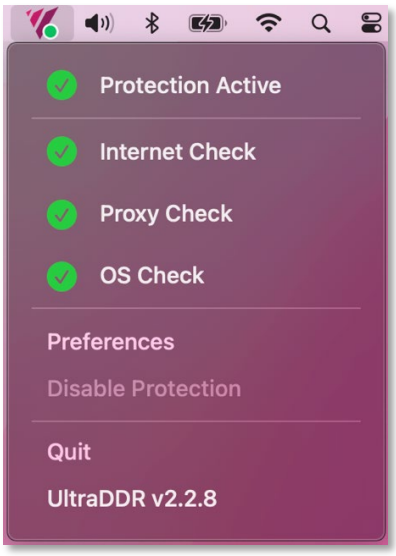
The following shell script can be used to automate this process:

```
install_key = "<install-key>"
install_dir="$HOME/Downloads"
install_file="UltraDDR-2.2.8.pkg"
echo "${install_key}" > /tmp/.vercara.ultraddr.client.id
install_path="${install_dir}/${install_file}"
sudo installer -store -pkg "${install_path}" -target /
```

(Replace "<install-key>" above with your organization's install key)

Starting the UltraDDR Status Application (Optional)

Once the UltraDDR Agent for macOS software has been installed, the UltraDDR status application can be launched by double-clicking the "UltraDDR" application icon from within the Applications folder. The UltraDDR status application provides easy access to protection status and UltraDDR application preferences. Once launched, the UltraDDR icon will now appear in the menu bar. Clicking on the UltraDDR icon in the menu bar will display protection status and provides access to UltraDDR application preferences.



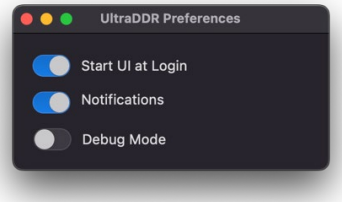
Protection status details:

- **Protection Active / Protection Inactive** – This indicates the agent's overall status, highlighting whether

protection is currently active or inactive.

- **Internet Check** – This confirms that the agent can successfully reach the UltraDDR resolvers directly. The verification involves performing a DNS query that only UltraDDR resolvers can respond to.
- **Proxy Check** – This confirms the successful verification of the agent's DNS proxy connectivity to UltraDDR backend services. The process validates two critical aspects: whether the service running on localhost:53 belongs to UltraDDR and if it can effectively communicate with UltraDDR's backend. This is ensured by a specific query that only UltraDDR can respond to. Note that if another DNS proxy is using port 53, this check will not succeed.
- **OS Check** – This confirms that a DNS lookup request made through the OS has successfully reached the UltraDDR resolvers. If the system is configured to use the UltraDDR agent, the lookup will be routed through the DNS proxy, ensuring that the device's DNS requests are handled by UltraDDR. This is verified by a specific query that only UltraDDR can respond to. If this check fails, it indicates that another process may have reconfigured the DNS settings and is competing with the UltraDDR agent for DNS resolution.

The following settings are available by clicking on "Preferences":



- **Start UI at Login** – enabling this setting will ensure that the UltraDDR status application is run upon user login.
- **Notifications** – enabling this will allow UltraDDR status notifications appear at the top-right corner of the user's screen. As with all macOS notifications, you can show and hide the macOS Notification Center by clicking the clock in the menu bar. Specific macOS system settings for UltraDDR notifications can be customized within the macOS System Settings at: macOS Apple Menu > System Settings… > Notifications > UltraDDR.
- **Debug Mode** – The Vercara support team may request that this setting be enabled when troubleshooting issues with UltraDDR or the UltraDDR Agent for macOS software.

Configurable Safe Search

The UltraDDR Agent includes support for enforcing Safe Search across major search engines, including Google, YouTube, Bing, and DuckDuckGo.

Safe Search is a setting that filters out explicit, adult-oriented, and inappropriate content from search results across major search engines. By enforcing Safe Search, organizations can prevent access to potentially harmful or objectionable material, reducing risks associated with accidental exposure to unsuitable content. This setting is especially beneficial in environments where browsing safety is a priority, ensuring a cleaner and more secure internet experience.

When enabled by your organization's UltraDDR administrator, this feature enforces Safe Search directly through the UltraDDR Agent, making the Agent essential for Safe Search enforcement. Details on how to enable Safe Search is documented in the *UltraDDR Agent Software for macOS Administrator's Guide*.

Installing the UltraDDR Root CA

When a site is blocked under a specific category, UltraDDR presents a block page to the user. In order for the block page to be shown to the user for sites served over HTTPS without generating browser errors, the UltraDDR Root Certificate Authority (CA) must be installed on your users' devices. Otherwise, if the UltraDDR Root CA is not installed on your users' devices, their browsers may display a "This Connection is Untrusted" (or similar) error when attempting to display block pages for sites served over HTTPS.

The UltraDDR agent software installer from version 2.2.3 and later automatically installs the UltraDDR Root Certificate Authority (CA) on the device. If you would like to install the CA on your device manually, you can download and find instructions for installing the UltraDDR Root CA files on a variety of devices at https://ca.ultraddr.com.

Uninstalling the UltraDDR Agent for macOS

Details on how to uninstall the UltraDDR Agent for macOS is documented in the *UltraDDR Agent Software for macOS Administrator's Guide*.

Microsoft Entra ID Support

The Microsoft Entra ID (formerly named Azure Active Directory) integration empowers organizations to achieve greater flexibility by allowing them to apply UltraDDR policies on a per-group basis within their organization. This empowers organizations to tailor to specific needs of each department or operational units (such as business units, teams, departments, etc.). The UltraDDR Agent Software for macOS or the UltraDDR Agent Software for Windows must be deployed for groups support.

> **Administrators:** the agent software automatically obtains the information necessary to identify the device's user from the operating system to determine group memberships. Please see the UltraDDR Microsoft Entra ID Administrator's Guide for more information.

Split-Horizon DNS

Split-Horizon DNS or Split-Brain DNS is a configuration where a DNS server provides different sets of DNS information based on the location or characteristics of the querying system. In a Split-Horizon setup, the DNS server resolves the same domain name to different IP addresses depending on whether the request originates from within the internal network (intranet) or from the external internet.

Split-horizon DNS empowers organizations to regulate access to internal resources by tailoring DNS responses depending on whether the query originates from within the organization's network or externally. This approach enhances security, boosts performance, and simplifies DNS management for improved network operations. UltraDDR administrators can define a list of domain names to "internal resources" names that should resolve locally instead of being sent externally. The UltraDDR Agent Software for Windows or the UltraDDR Agent Software for macOS must be deployed for Split-Horizon DNS support.

Administrators: the agent software can be configured to automatically determine if the device is presently on your organization's internal network (intranet) or the external internet. Please see the UltraDDR Split-Horizon DNS Administrator's Guide for more information.

Contact Support

To contact our support team for assistance, your UltraDDR administrator should have received Vercara Support portal credentials. Using these credentials, your administrator can sign into the Vercara Support portal, which contains a knowledge base for finding solutions to various questions or configuration issues. Additionally, the portal includes Vercara's ticketing dashboard, which allows for easy submission and tracking of support requests through an optimized and streamlined ticket submission process.

You can contact support directly at ultraddrsupport@vercara.com. Additional Support Team contact details can also be found on our website at https://vercara.com/support.