FortiSASE

Getting Started for End Users

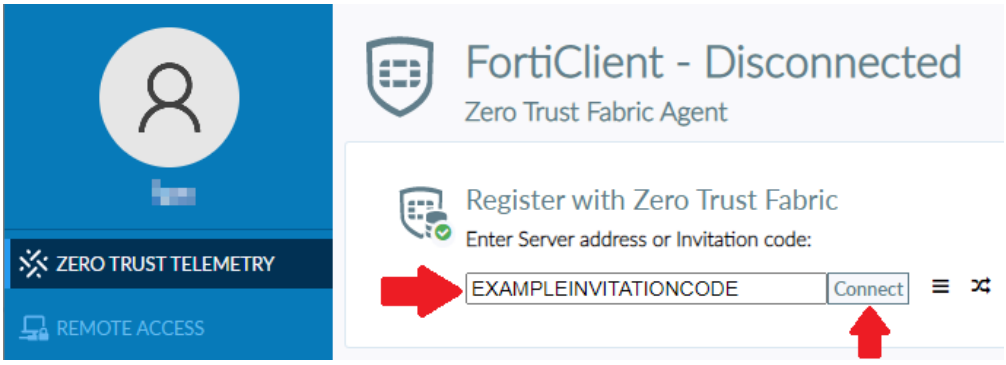
FortiSASE is a security solution that enables secure access to the web, cloud, and applications for the hybrid workforce. With FortiSASE, you enjoy a simple user experience to seamlessly access corporate applications whether working from the office, home, or anywhere, while ensuring business productivity and enhanced security.

This guide provides instructions for the following use cases:

- **Initial onboarding** - if you are using FortiClient with FortiSASE for the first time.
- **Migrating from EMS to FortiSASE** - if you previously used FortiClient with EMS.

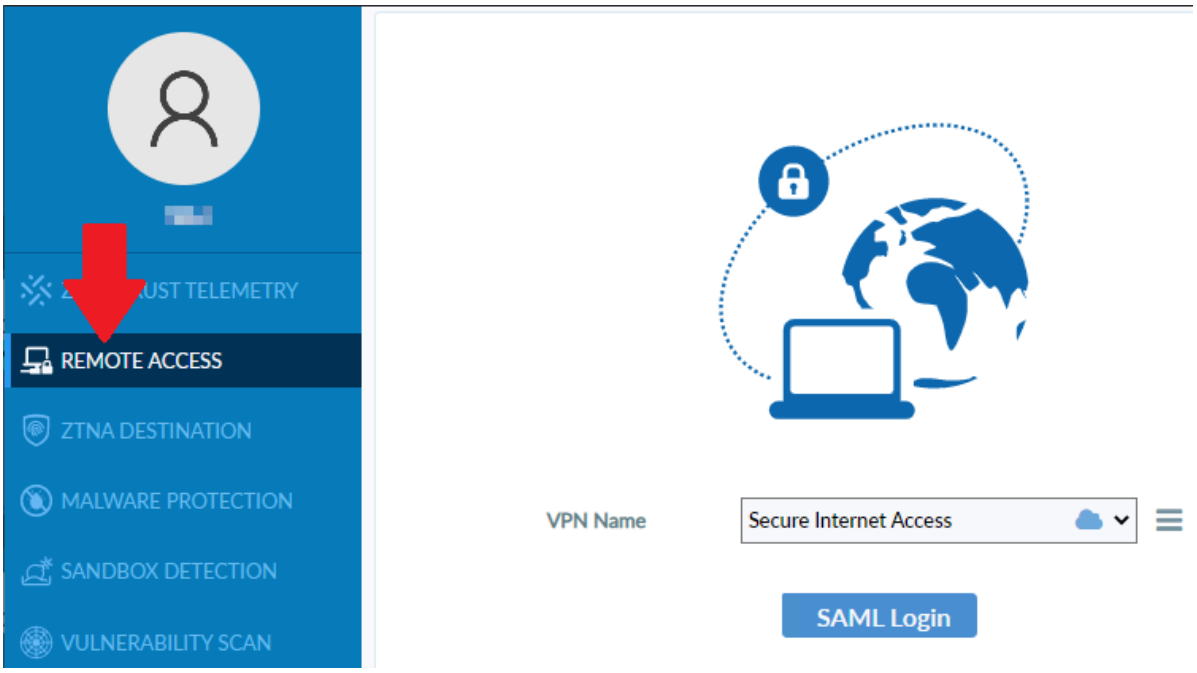
INITIAL ONBOARDING

1. Your organization's IT department will likely have already installed FortiClient on your device. If not, install FortiClient on your device. See Manually installing FortiClient on computers.
2. Once **ZERO TRUST TELEMETRY** displays **Register with Zero Trust Fabric**, in **Enter Server address or Invitation code**, enter the code that you received from your network administrator. Click **Connect**.

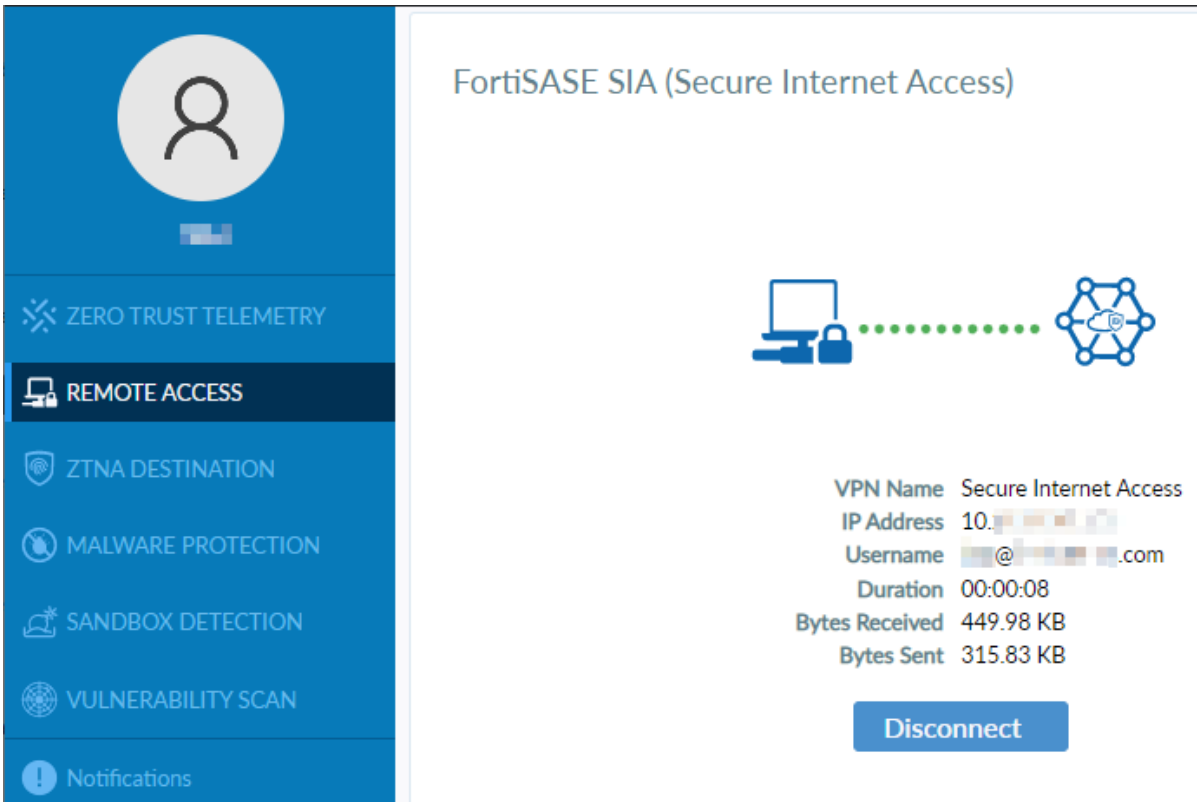


Once connected, **ZERO TRUST TELEMETRY** displays **Managed by FortiClient Cloud**.

3. Go to **REMOTE ACCESS**. **Secure Internet Access** is selected in **VPN Name** by default.



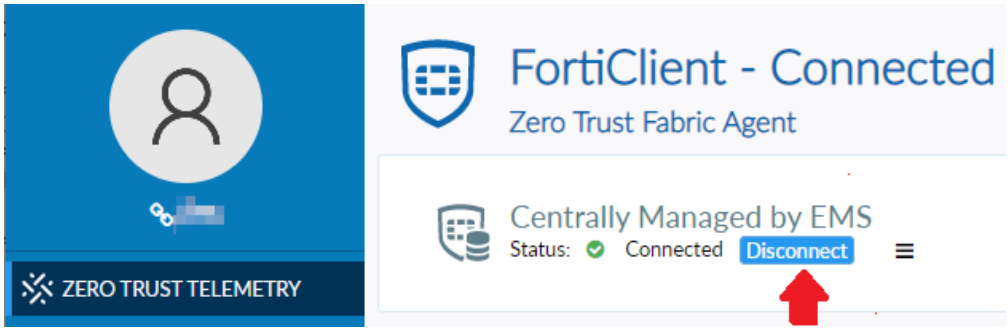
An authentication popup displays. Enter your corporate credentials. Once connected, you can securely access your corporate applications whether from the office or remote.



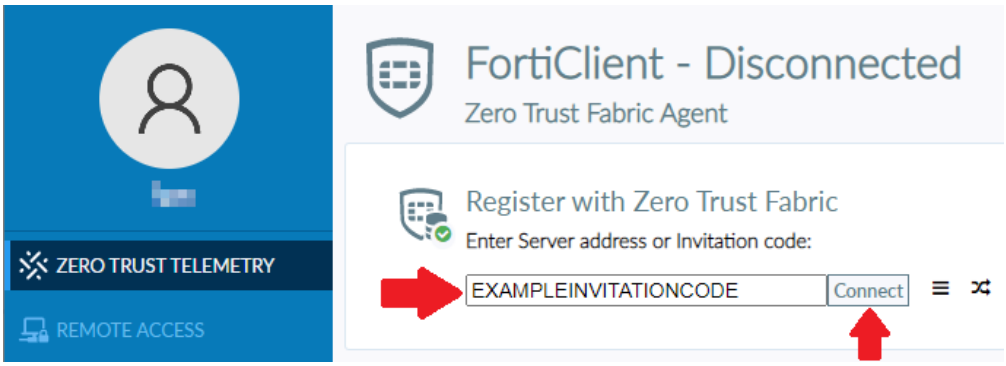
MIGRATING FROM EMS TO FORTISASE

To migrate from EMS to FortiSASE:

1. **ZERO TRUST TELEMETRY** displays that **FortiClient is Centrally Managed by EMS**. Click **Disconnect**. In the **Confirmation** dialog, click **Yes**.

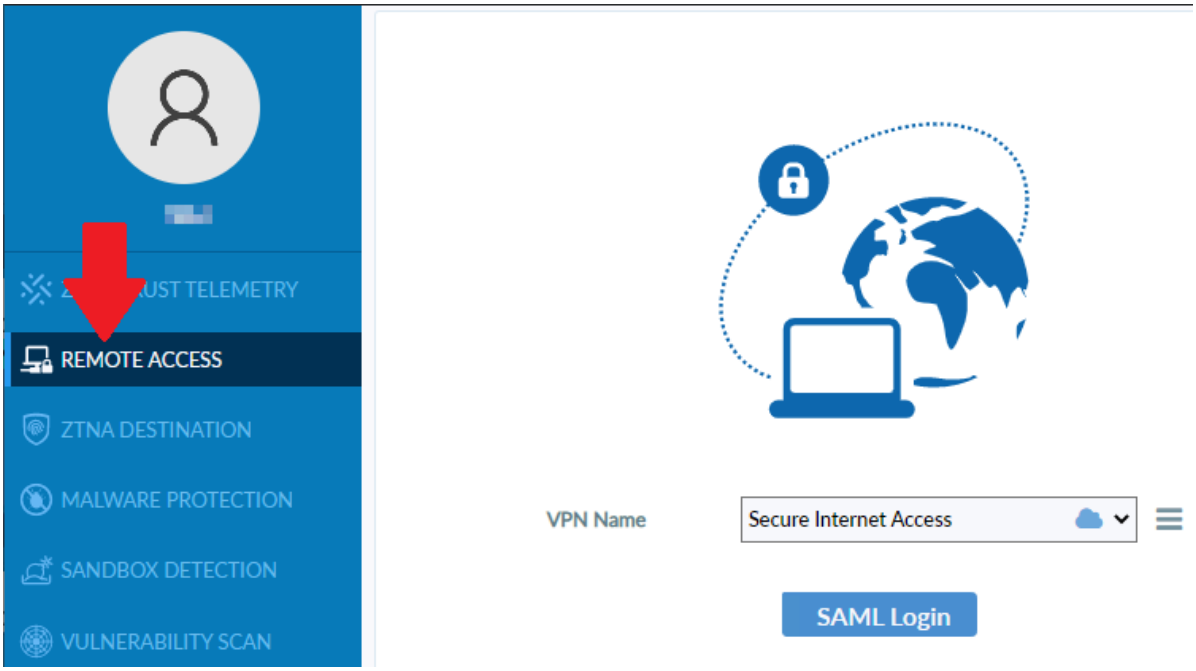


2. Once **ZERO TRUST TELEMETRY** displays **Register with Zero Trust Fabric**, in **Enter Server address or Invitation code**, enter the code that you received from your network administrator. Click **Connect**.

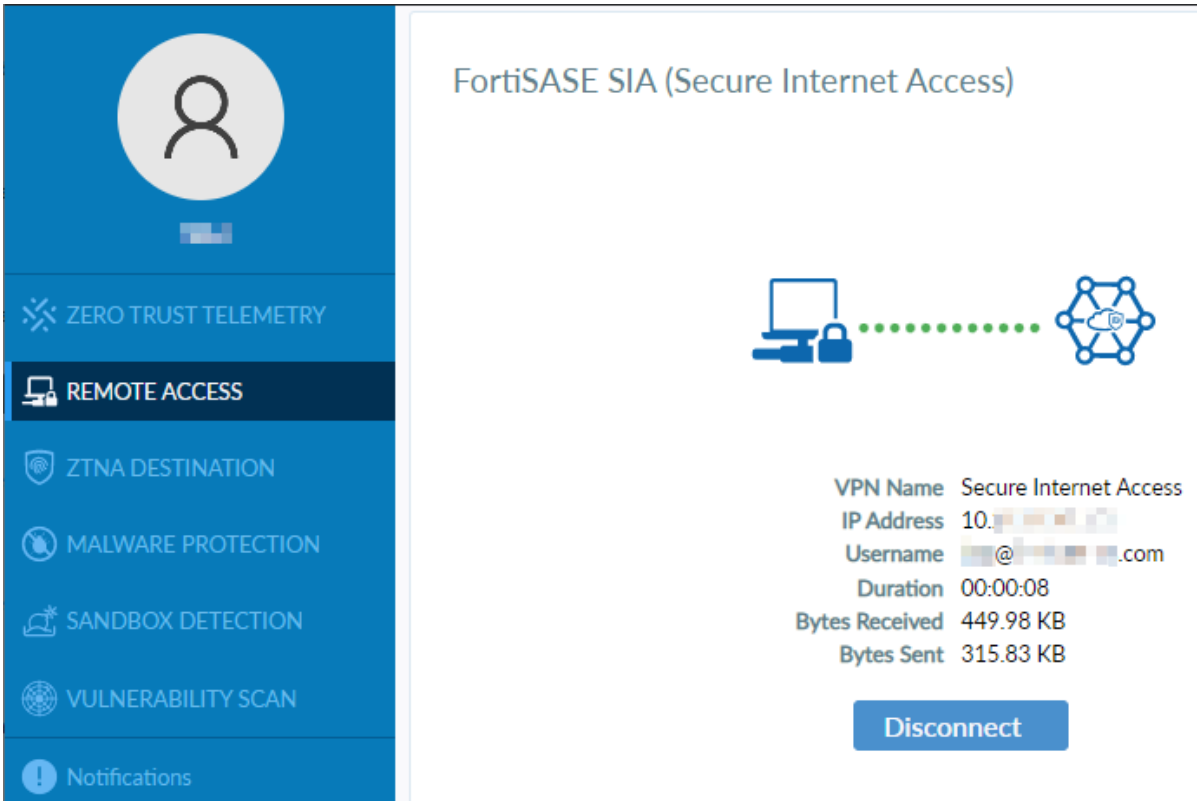


Once connected, **ZERO TRUST TELEMETRY** displays **Managed by FortiClient Cloud**.

3. Go to **REMOTE ACCESS**. **Secure Internet Access** is selected in **VPN Name** by default.



An authentication popup displays. Enter your corporate credentials. Once connected, you can securely access your corporate applications whether from the office or remote.



CONFIRMING CERTIFICATES INSTALLED CORRECTLY ON FORTICLIENT ENDPOINT

If you are seeing certificate errors in your web browser, then check the certificate store for your system for the SSL inspection and ZTNA certificates.

Windows

1. On a Windows machine with FortiClient installed and its zero trust telemetry connection to FortiSASE is established, perform one of these steps from the Windows start menu:
   - Right-click, select **Run** and enter ***certlm.msc***.
   - Right-click, select **Terminal (Admin)** to open a Windows Powershell terminal and enter ***certlm.msc***.
   - In the search bar, enter ***certlm.msc***.
2. In the **Certificate - Local Machine** view, go to **Trusted Root Certification Authorities > Certificates**.
3. Locate the SSL inspection certificate shown as **FGVMXXXXXXXXXXX**.
4. Locate the ZTNA certificate shown as **FCTEMSXXXXXXXXXX**.
5. If one or both certificates cannot be located, disconnect the FortiClient zero trust telemetry connection to FortiSASE if allowed by the endpoint profile and reconnect the zero trust telemetry connection.

MacOS

1. On MacOS with FortiClient installed and its its zero trust telemetry connection to FortiSASE is established, open the **Keychain Access** app. Ensure that you select **Open Keychain Access**.
2. In the **Keychain Access** window, go to **System Keychains > System**.
3. Locate the SSL inspection certificate shown as **FGVMXXXXXXXXXXX**.
4. Locate the ZTNA certificate shown as **FCTEMSXXXXXXXXXX**.
5. If one or both certificates cannot be located, disconnect the FortiClient zero trust telemetry connection to FortiSASE if allowed by the endpoint profile and reconnect the zero trust telemetry connection.

Visit www.fortinet.com for more details