Amway
Remote Access

Blue Book
Updated 26-JUL-2018

help.amwayconnect.com
Contents

Amway Remote Access Help Portal ................................................................. 3

General Information .................................................................................. 3

Disclaimer ................................................................................................. 3

Requirements ........................................................................................... 4

Multi Factor Authentication ....................................................................... 4

Okta MultiFactor Authentication ............................................................... 5

General Information .................................................................................. 5

Approval Requirements ............................................................................. 5

VPN Client installation and configuration ............................................... 5

Configuring the GlobalProtect Portal ...................................................... 5

Connecting to Amway ................................................................................ 7

Remote Desktop instructions ..................................................................... 8

Virtual Desktop instructions ..................................................................... 9

General Troubleshooting .......................................................................... 10

Travelers or Connection Issues ............................................................... 10

Typical application or connection issues ............................................... 11
Amway Remote Access Help Portal

Amway maintains a Remote Access Help Portal to assist with almost anything Remote Access related. There will be several references to it from within this document so it is placed here for convenience. The portal can be found at:


The following items can be found on the portal:

1. Up-to-date pertinent information on any current issues Amway may be aware of is usually posted at the top of the portal.

2. Amway Remote Access Blue Book (this document)
   
   Comprehensive guide on concepts and procedures needed to connect to various Amway resources.
   
   a. How to connect, and why Amway has certain requirements.
   b. Multi-factor Authentication.
   c. URL address global VPN Portal.
   d. ‘Common’ issues and how to possibly correct them.
   e. Remote Desktop and VMware Virtual Desktop instructions.

3. Okta Portal Password Quick Config Guide
   
   How to set up a method to change your password yourself! Anytime! Great for contractors!

4. The latest (supported) PC/MAC VPN clients for connecting to Amway.

5. Global support contact information: Amway Service Desks General Information

Disclaimer

It is possible that by following these instructions a system and/or services (VPN connections to other companies for instance) could be negatively impacted. **Amway is not responsible for non-Amway standard systems such as personal or home computers or contractor systems.** Contractors should have
their respective IT departments involved in remediating any problems with their systems.

**Requirements**

Any system that is not an Amway standard system needs to meet certain minimum supported and/or security requirements. Typically, the last (publicly released) three versions of PC’s or Mac’s are supported. Operating systems should be patched and up to date. PC’s need to have an anti-virus solution that is up to date with its virus definitions as well as running at least weekly full scans. Mac’s should have an up-to-date anti-virus installed and running weekly full scans as well. The **GlobalProtect Client** which is the VPN client application, will need to be installed. It will generate a **Host Information Profile** (HIP) which is used for validating that the workstation meets security requirements.

**Multi Factor Authentication**

Amway requires two different forms of identification when connecting to its network. The first is a User ID (Amway Native ID) and password. Amway standard systems have a certificate installed that is associated with the user and represents the second factor. Non-Amway standard systems utilize Okta to perform the 2\(^{nd}\) factor of authentication.
Okta MultiFactor Authentication

General Information
To connect to Amway using a non-Amway standard system, you need to provision Extra Verification settings in your Okta account. You have the option to use one of 4 methods: Okta Verify mobile app, Google Authenticator, Text Message Code, or YubiKey. Instructions on how to setup any one of these methods can be found here.

Approval Requirements
Amway employees can be added to the appropriate LDAP group by following the standard Access Request process in ServiceNow. They will need to be added to the group LDAP-ALT-VPN-MFA-Employees.
Non-Amway employees must have approval from an Amway upline manager and be added to the group LDAP-ALT-VPN-MFA-Contractors. The process can be initiated by contacting the appropriate Amway Service Desk (Contact Info tab on Help portal menu bar)

VPN Client installation and configuration
When using a non-Amway system, the latest supported client for both PC and MAC will always be available for download on the MFA-Portal. Users should point their browser to https://mfa-portal.amwayconnect.com and log in. Once they have logged in, they will be presented with the option to download either the Windows or MAC Global Protect Client. They should download the proper client for their workstation and proceed to install it accepting all defaults.

Configuring the GlobalProtect Portal
After successful installation of the GlobalProtect Client, the user will automatically be prompted with a field to configure the GlobalProtect Portal. The user
should enter the same URL that they pointed their browser to – **omitting the https://**.

After entering this information, click on Connect. They will then be prompted to log in again and complete the multifactor authentication request. This very first log in is very important as it will download all additional client settings required for remote connectivity – most importantly – retrieving the list of gateways available to connect to (this replaces the individual profiles required for setup on Pulse Secure).
Connecting to Amway

1. Access the Application by clicking on the icon in your System Tray.
   
     ![System Tray Icon](image)

   a.

2. Click on Connect

   ![Connect Button](image)

   a.

3. Enter your Amway credentials and follow on-screen prompts to complete Multifactor Authentication

4. Once successfully connected, the app will automatically minimize to the system tray.
Remote Desktop instructions

A common need is to be able to remote into a computer system that you may use regularly. The computer being connected to is called a ‘host’. The computer contacting a host is called a ‘client’. You will need to know the name of the host system to be able to connect to it. In addition, to use a MAC system as a host, ‘File Sharing’ and ‘Screen Sharing’ will need to be enabled on that MAC system.

You will need a Remote Desktop application on the client you are using. Windows based clients usually have Remote Desktop Connection built in (usually found in Accessories). Mac clients will need to download and install the Microsoft Remote Desktop Connection app from the Apple store to access Windows hosts; and/or download and install the ‘Remote Desktop – VNC’ app from the Apple store to access MAC hosts.

Start the Remote Desktop application and when prompted for the computer to connect to, enter the name of the Amway host. Try the short name first, if that doesn’t work try using the longer name.

USWSA#####
USWSA#####.na.intranet.msd   Most Windows systems
USWSA#####.local           Most MAC systems

Your client system should now have control over the Amway host system. Remember to LogOff from the Amway host system when finished using it. How varies depending on system) and then end the VPN connection by selecting ‘Disconnect’ in the Pulse Secure application.
Virtual Desktop instructions

For those individuals needing to access virtual desktop systems, you will need to download and install the appropriate client for your system from:

https://www.VMware.Com/Go/ViewClients

You will need to configure various options when the client is installed:

- Network Protocol Configuration = IPV4
- At the Custom Setup screen remove (deselect) USB Redirection
- Log in as current user
- Server name = mydesktop.intranet.local

After finishing the install, you can then run the client application. You should see an icon for mydesktop.intranet.local.

On the right side of the menu bar there should be an icon with 3 bars. Select the following items in order: “Configure SSL...”. “Do not verify server identity certificates”, [OK].

After establishing a VPN connection, you can then start the Horizon View client. To authenticate, use your User ID (Amway Native ID), your Amway network password, and select “NA” for the domain.
General Troubleshooting

The Amway Remote Access Help Portal will usually contain information on any known current issues at the beginning of the portal.

Travelers or Connection Issues

GlobalProtect will attempt to automatically connect users to the proper gateway based on their Geo-Location. In the event that they experience slowness, or they think they are connected to the wrong location, they can choose a different location from the Gateway dropdown list.

1. After connecting, re-open the app via the System Tray icon.

   a. 2. Choose your desired location to connect to via the Gateway list
a.

3. The application will automatically initiate a connection to the chosen Gateway location.

**Typical application or connection issues**

**Mac-Specific Issue**

Some versions of MacOS may experience an issue where, after installing the Globalprotect app, it just continually says “Connecting” and never actually establishes a connection. Newer versions of MacOS have an extra layer of security that causes this problem. Fortunately, there is a fix:

1. Boot Mac OS into recovery mode: Reboot, hold Command + R
2. Launch the Terminal
3. Enter the command "**spctl kext-consent add PXPZ95SK77**" in the terminal window and press Enter (PXPZ95SK77 is the unique identifier for Palo Alto Networks software)
a. There will be no output indicating whether this was successful or not – just type carefully and check for typo’s

4. Reboot

5. Attempt connecting with Globalprotect again, this time it should work.

**Gathering General Connection-specific information**

If you do experience issues with the app or connectivity, important information can be gathered from the Settings tab.

1. Launch the application from the System Tray

   a. 2. Click on the Gear icon in the upper right
3. Select Settings
4. Click on the Connection tab
5. Information from this screen will help the support groups do some basic troubleshooting before gathering detailed logs from the end user.