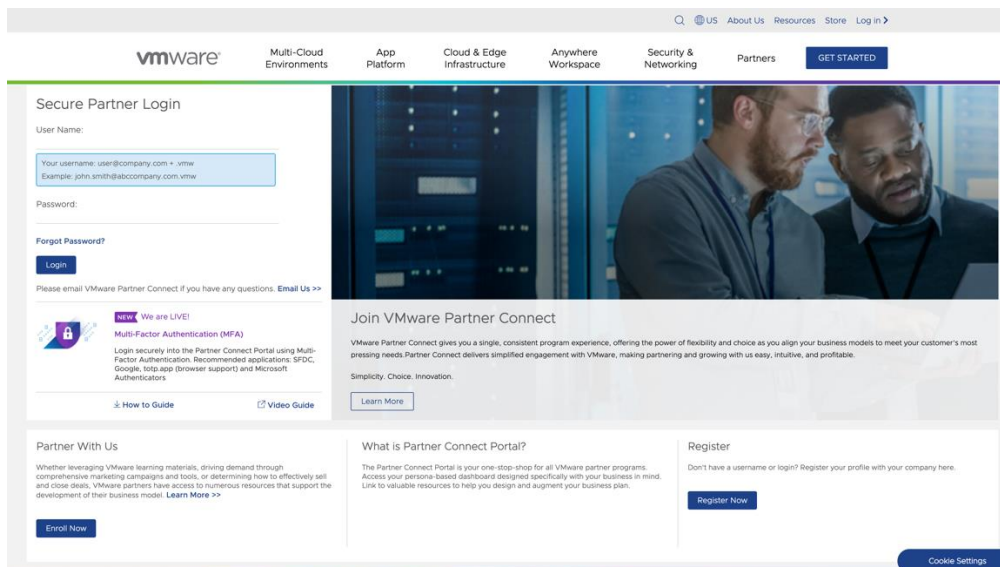


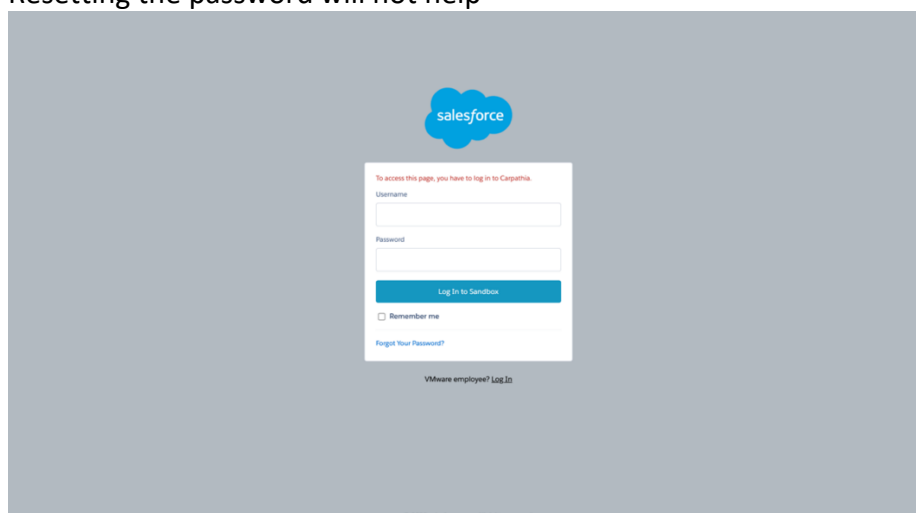
Multi-Factor Authentication User Guide

IMPORTANT DISCLAIMER

- 1) The **VMware partner login page** is the following link. Correct URL :
URL:https://vmstarcommunity.force.com/partnerconnect/PC_Login?ec=302&startURL=%2Fpartnerconnect%2Fs%2F)



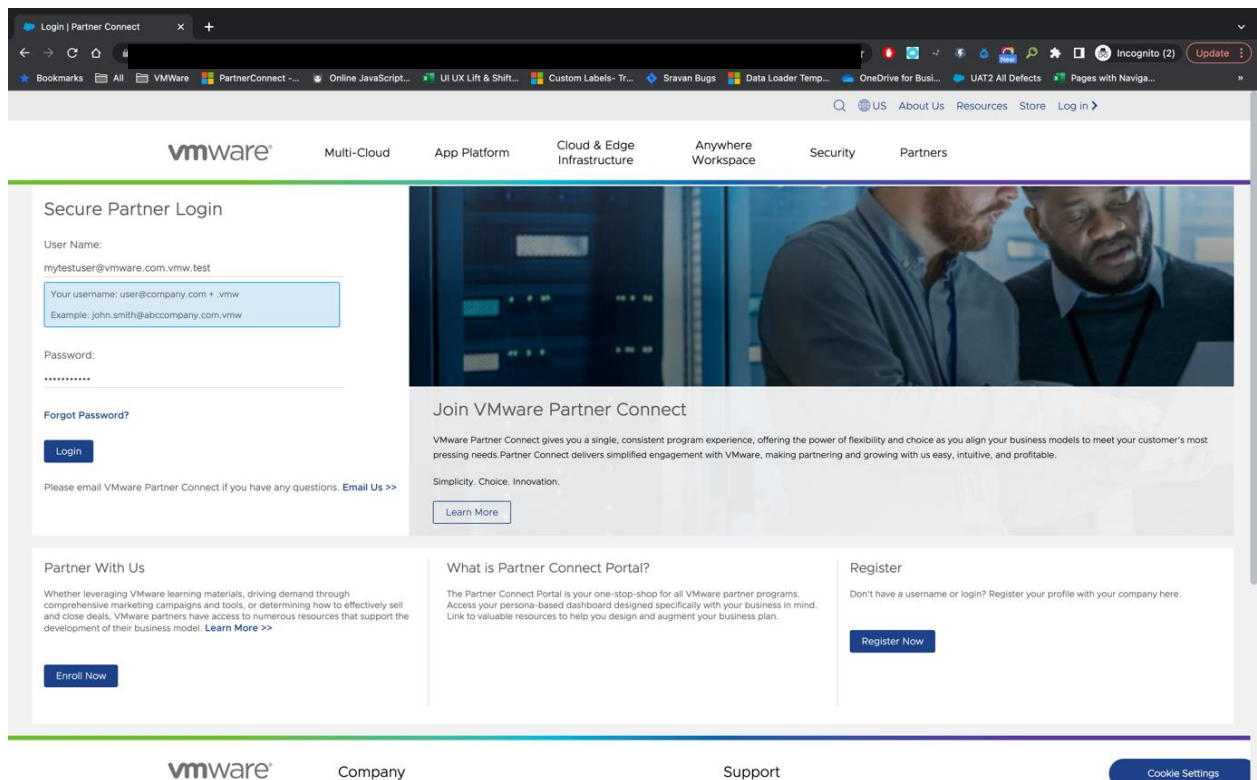
- 2) For any reason if the screen for login is showing as below (**Carpathia URL**), please try the following steps. Incorrect URL :
(<https://vmstarcommunity.force.com/Carpathia/login?ec=302&inst=2H&startURL=%2FCarpathia%2Fidentity%2Ftwofactor%2FaddTwoFactorOnly.apexp>):
- a) Clear Cache and try opening the login URL in an incognito window. i.e. STEP 1 URL
 - b) Try opening a different browser from the current used browser.
 - c) If both the above options do not work, please re-try after an hour.
 - d) Please do not request for password reset if the below screen is coming up. Resetting the password will not help



Using SFDC Authenticator

If you are currently logged into the Partner Connect Portal, please go ahead and logout prior to setting up Multi-Factor Authentication

Step 1: Login to the Partner Portal using your username and password

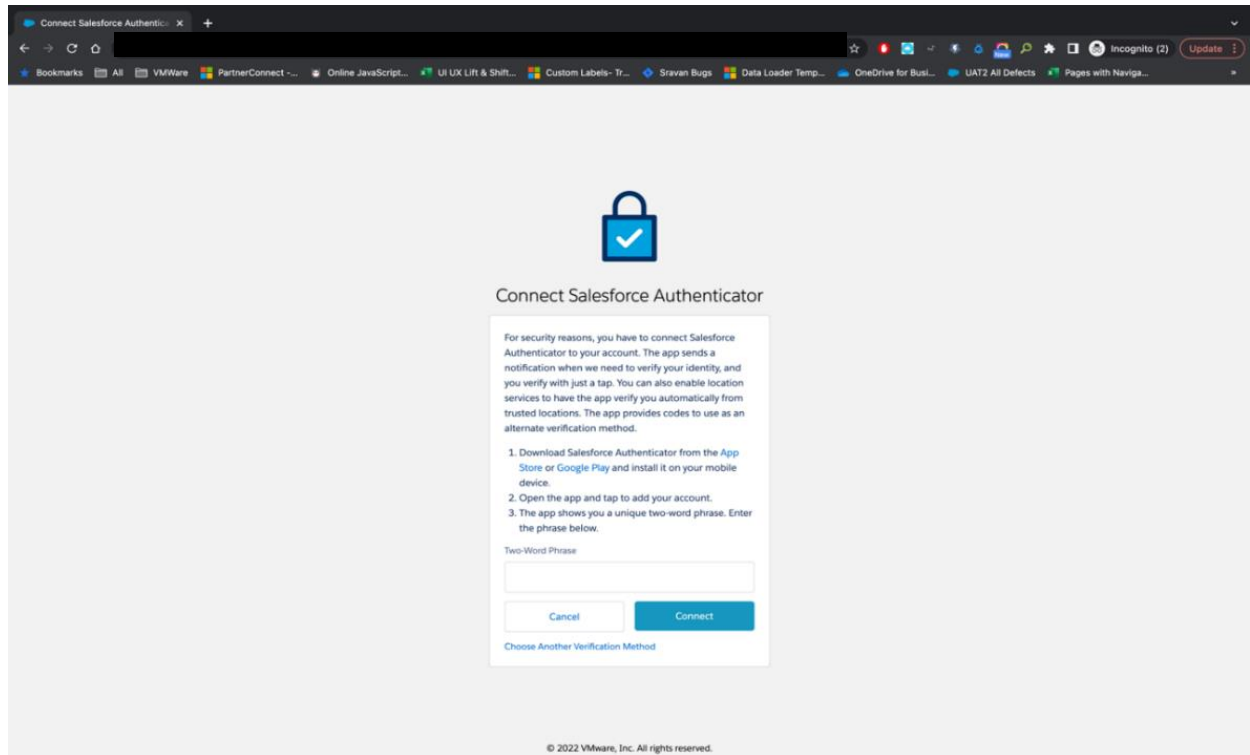
The screenshot shows the VMware Partner Connect login page in a web browser. The browser's address bar shows the URL 'Login | Partner Connect'. The page features the VMware logo at the top left, followed by navigation links: Multi-Cloud, App Platform, Cloud & Edge Infrastructure, Anywhere Workspace, Security, and Partners. The main content area is titled 'Secure Partner Login' and includes a 'User Name' field with the email 'mytestuser@vmware.com.vmw.test', a 'Password' field with masked characters, and a 'Forgot Password?' link. A 'Login' button is positioned below the password field. To the right of the login form is a large image of two men in a server room, with the text 'Join VMware Partner Connect' and a brief description of the program. Below this, there are three columns: 'Partner With Us' with an 'Enroll Now' button, 'What is Partner Connect Portal?' with a 'Learn More' button, and 'Register' with a 'Register Now' button. The footer contains the VMware logo, 'Company', 'Support', and a 'Cookie Settings' button.

After logging in, you will be shown a page with instructions on how to download the Salesforce authenticator application.

Note - If you choose to use a different third-party authenticator application click on “Choose Another Verification Method” on the bottom of the screen. More information can be found [here](#).

****If you are trying to allow multiple users to login to one Partner Portal account using the same username and password, please click [here](#) for the browser method.**

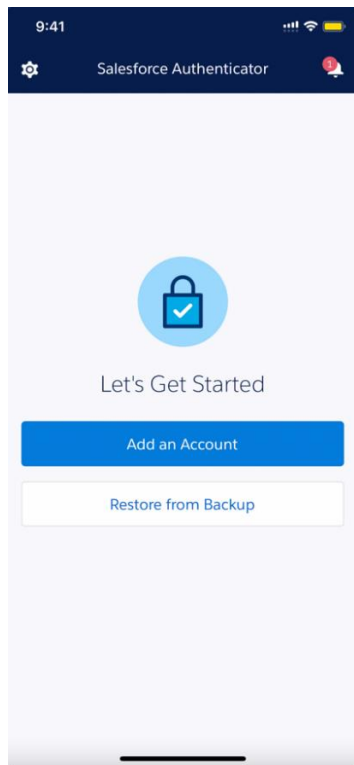
Multi-Factor Authentication



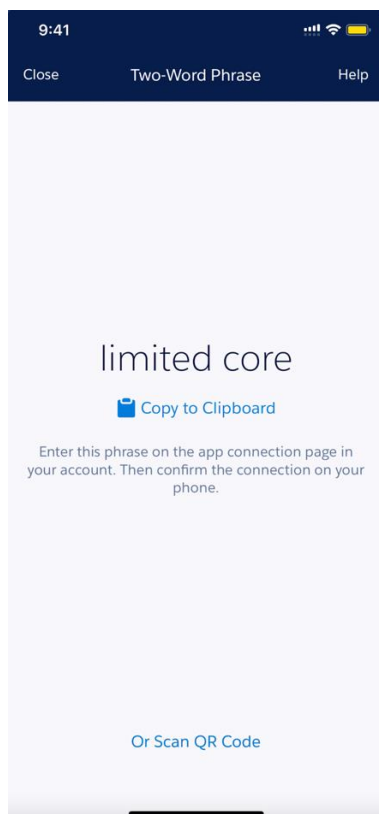
Step 2: Download the Salesforce application on the mobile device



Step 3: Open the authenticator and click on Add an Account

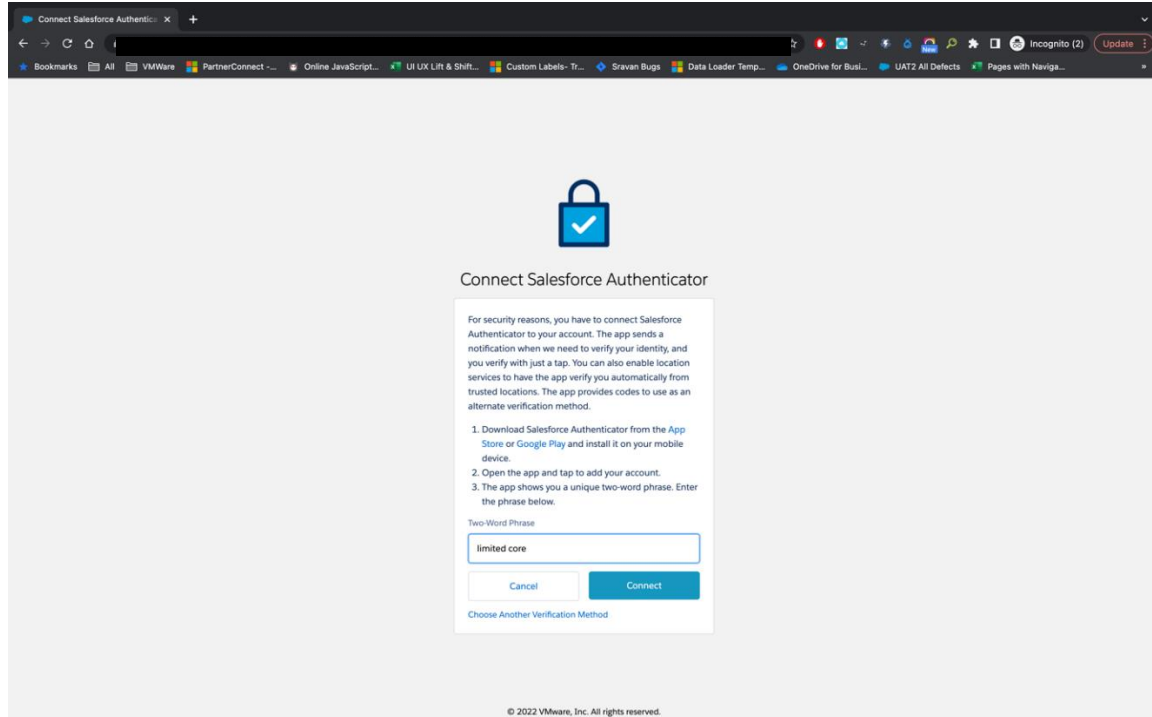


A two-phase code will be shown on the mobile app

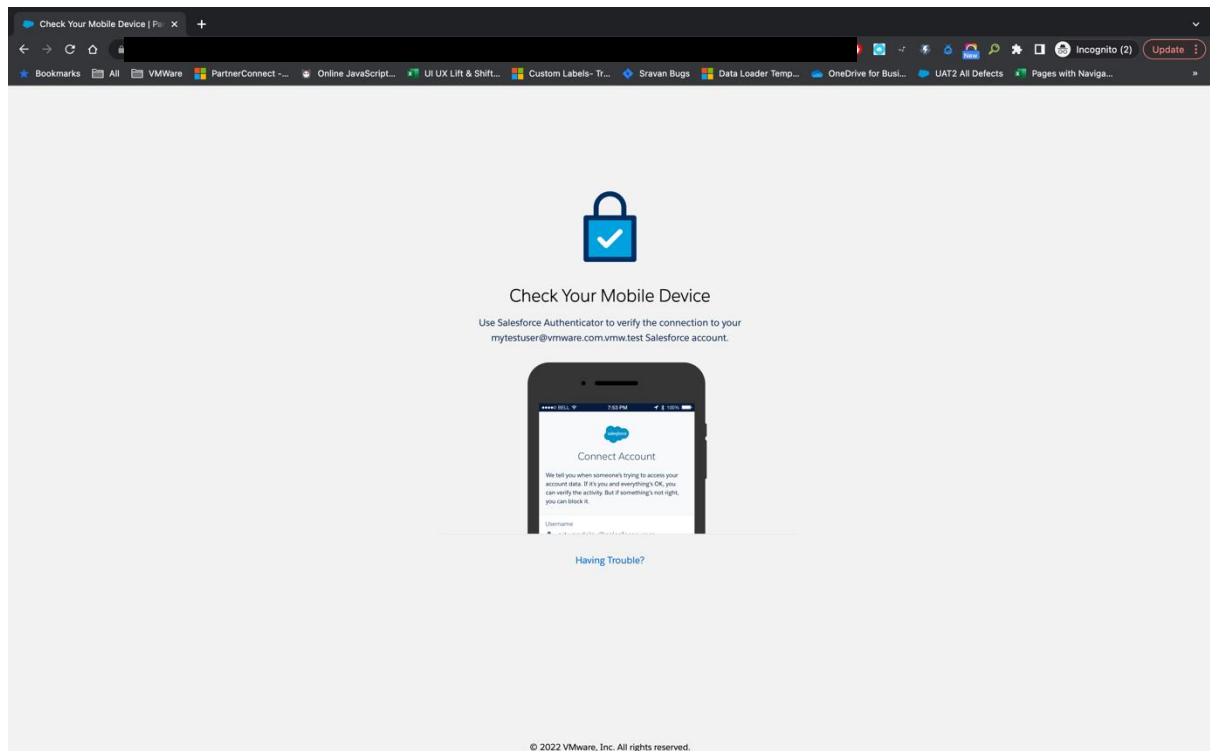


NOTE: If you are using a group username and password **and** you are the first to setup MFA, you will be the default approver for all logins using the group username and password. Please see the browser option below for group logins.

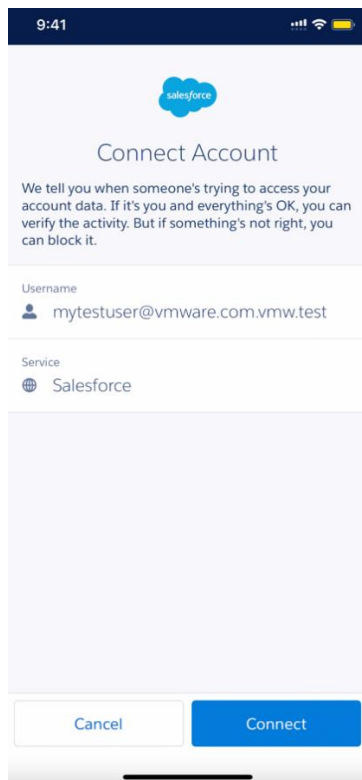
Step 4: Type the code in the browser and click on connect



There will be a push notification which will be sent to the Mobile Device. The browser will look as below

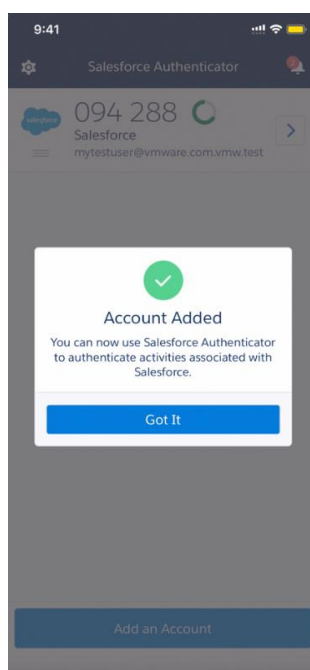


Step 5: Click on Connect to bind the device with the account.

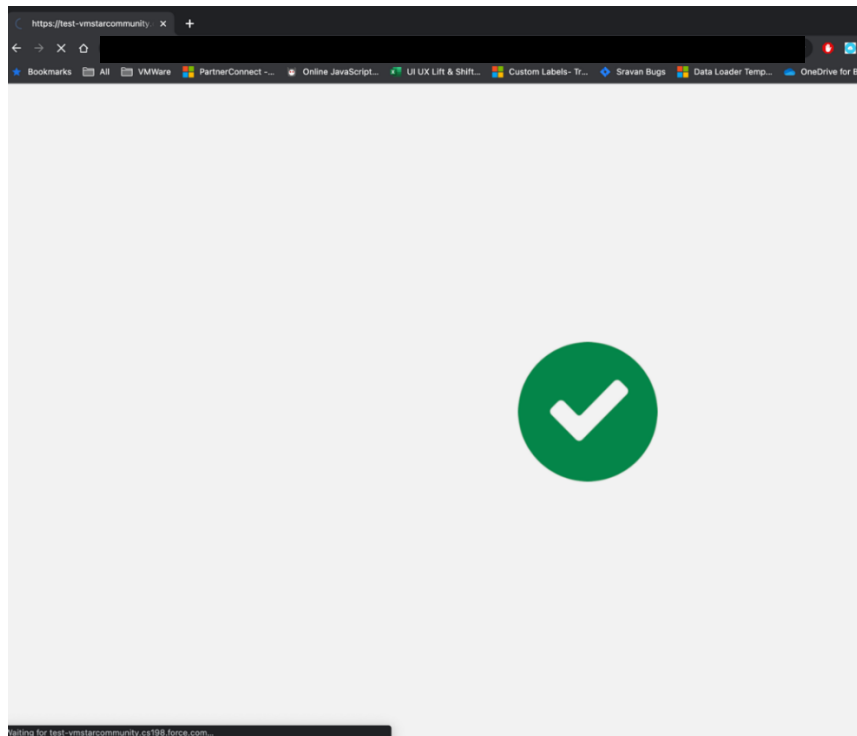


After the connection has been made, you will see a confirmation on the mobile application

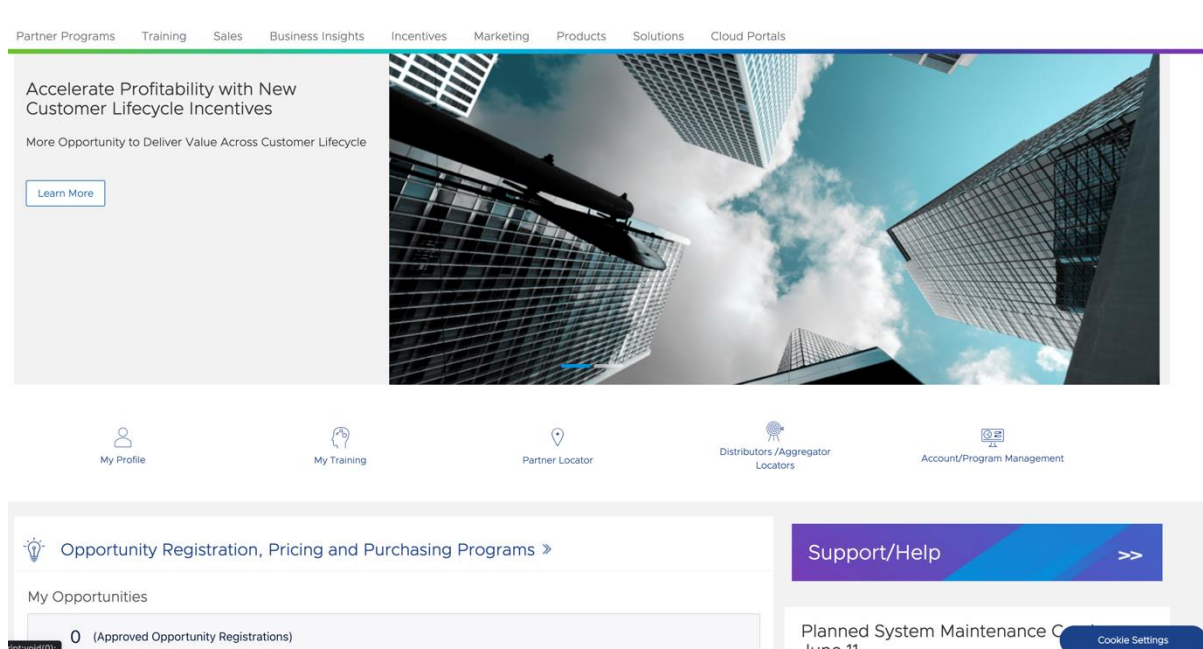
If for some reason you receive a login error message, please clear your cache and try again. If the problem persists, try using an incognito window to login instead. If problems continue to exist, please reach out to partnerconnect@vmware.com



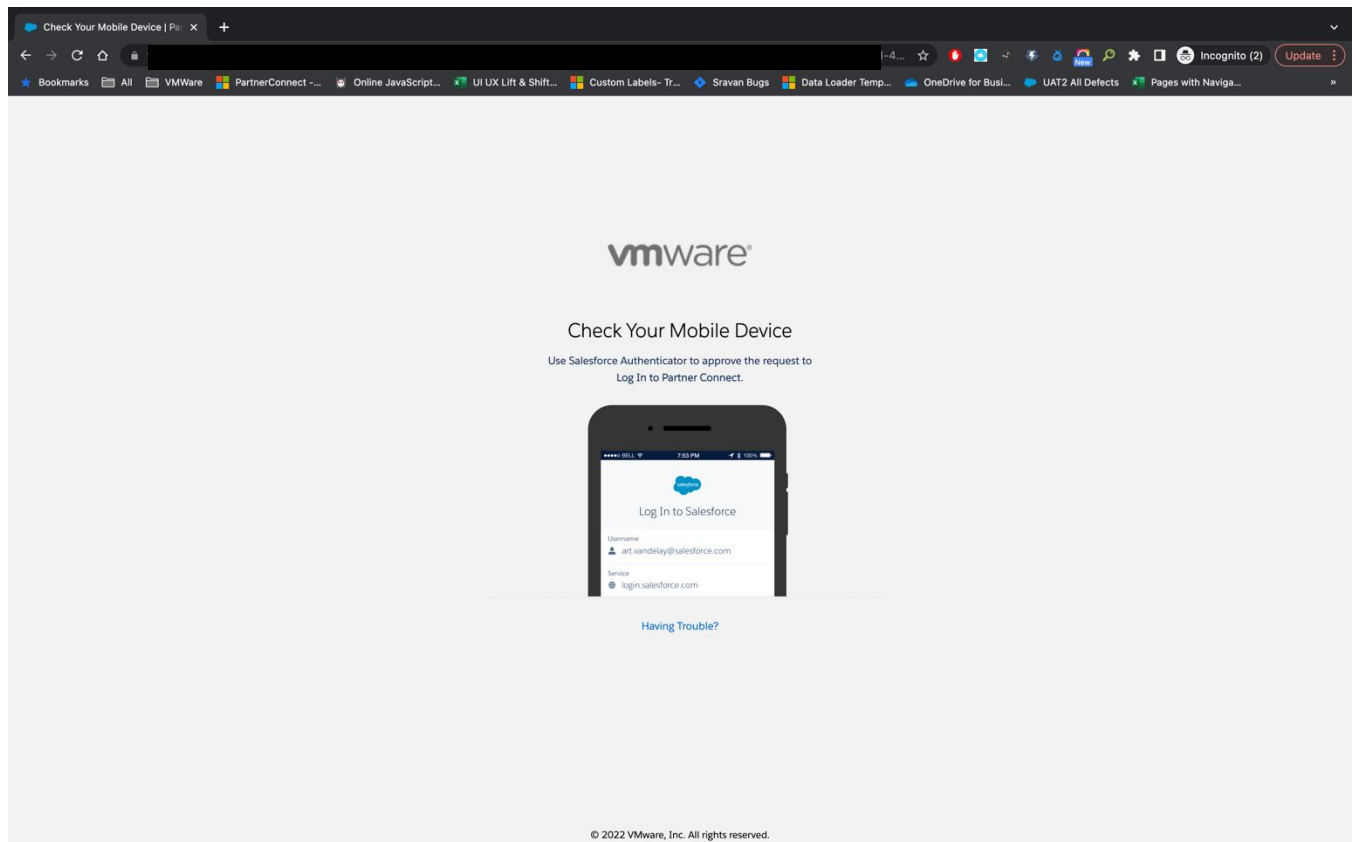
Browser will show the success message



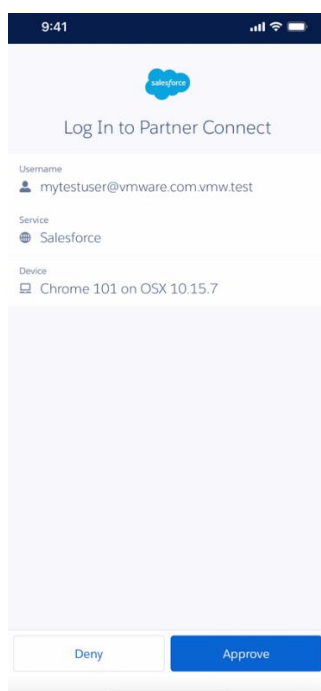
Once this is done, you will be logged into the community.



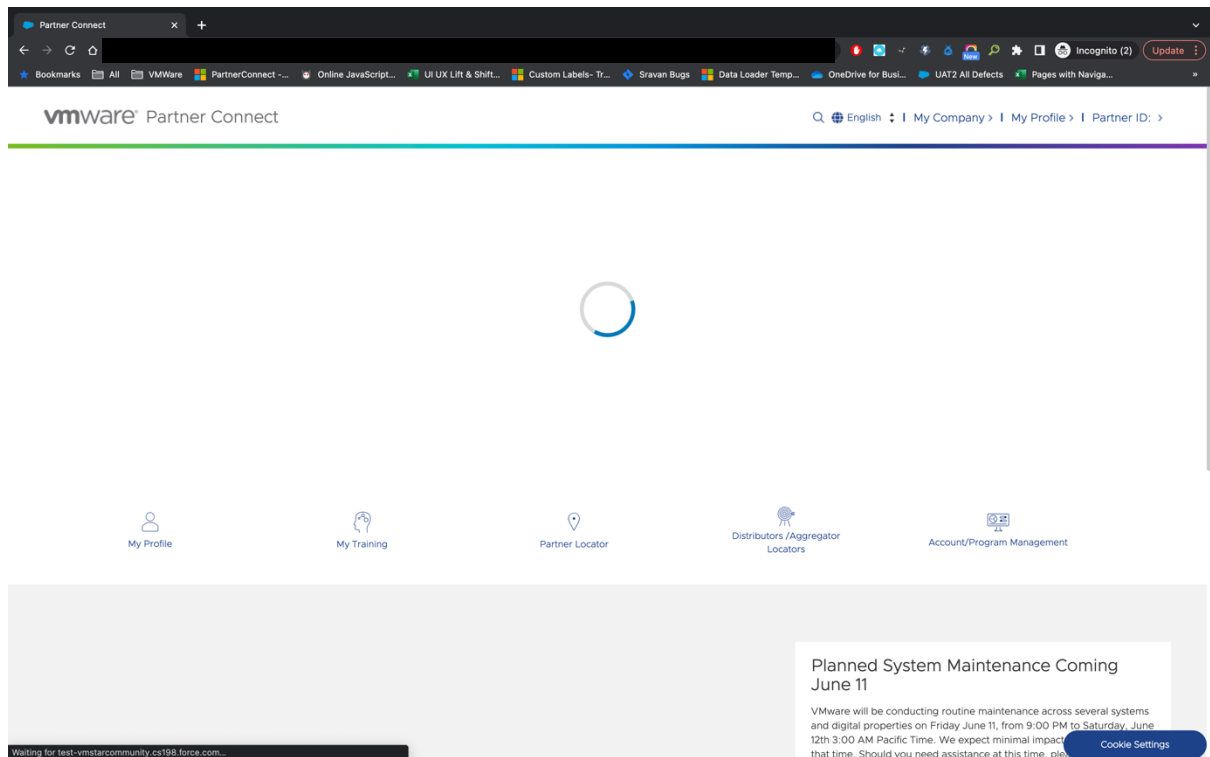
After Initial Setup: On a re-login, there will a push notification which is sent to your mobile device.



You can either approve or deny the request from the device



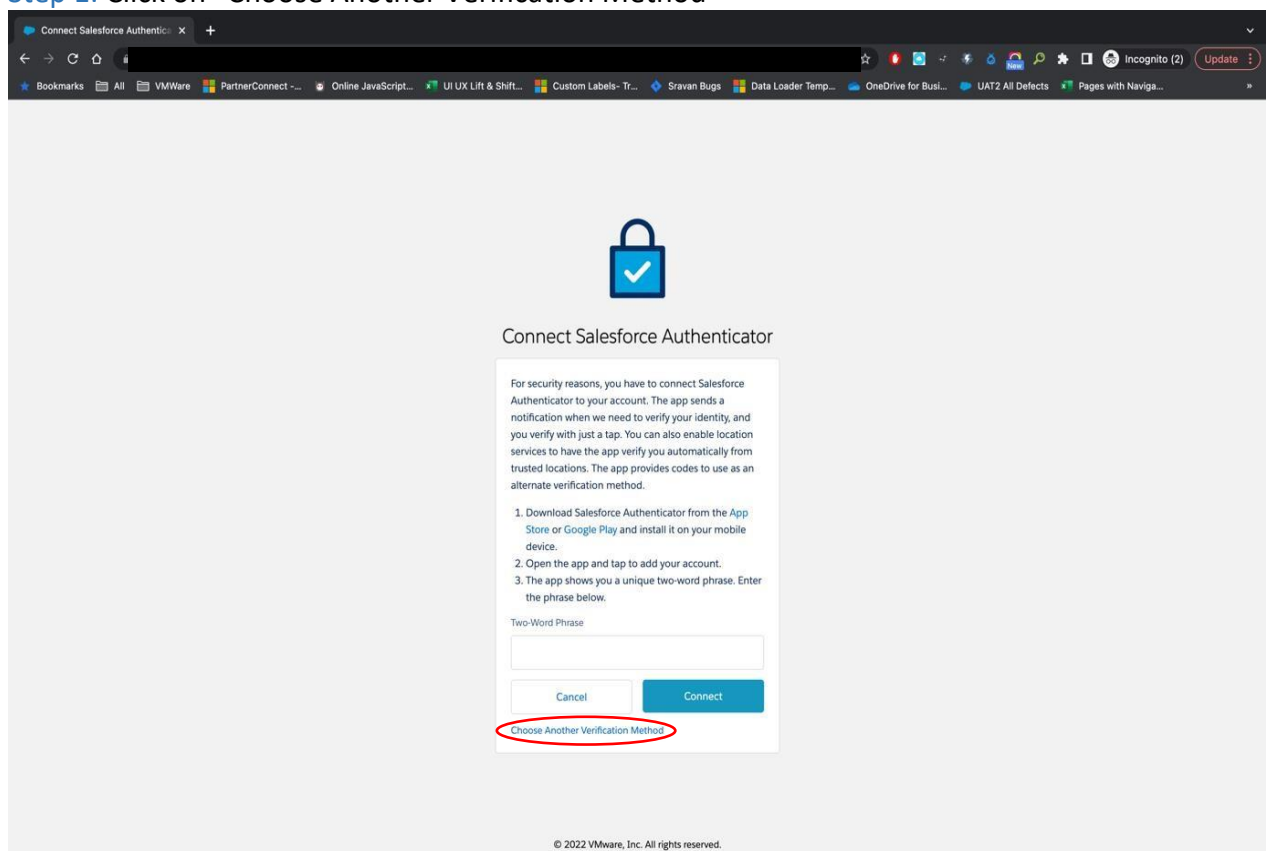
On approval, you are logged into the community



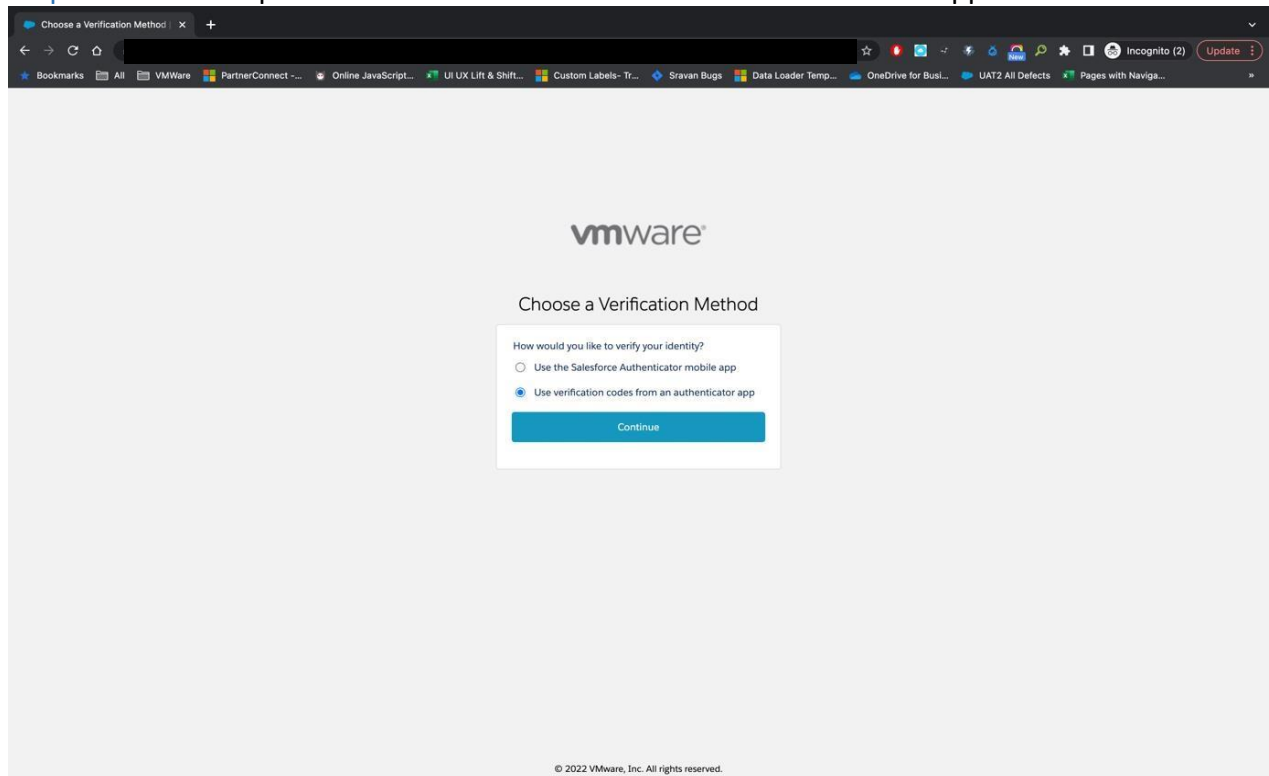
Using a Different Mobile Authenticator Application

If you choose to use a different third-party mobile authenticator application other than Salesforce – please see below.

Step 1: Click on “Choose Another Verification Method”

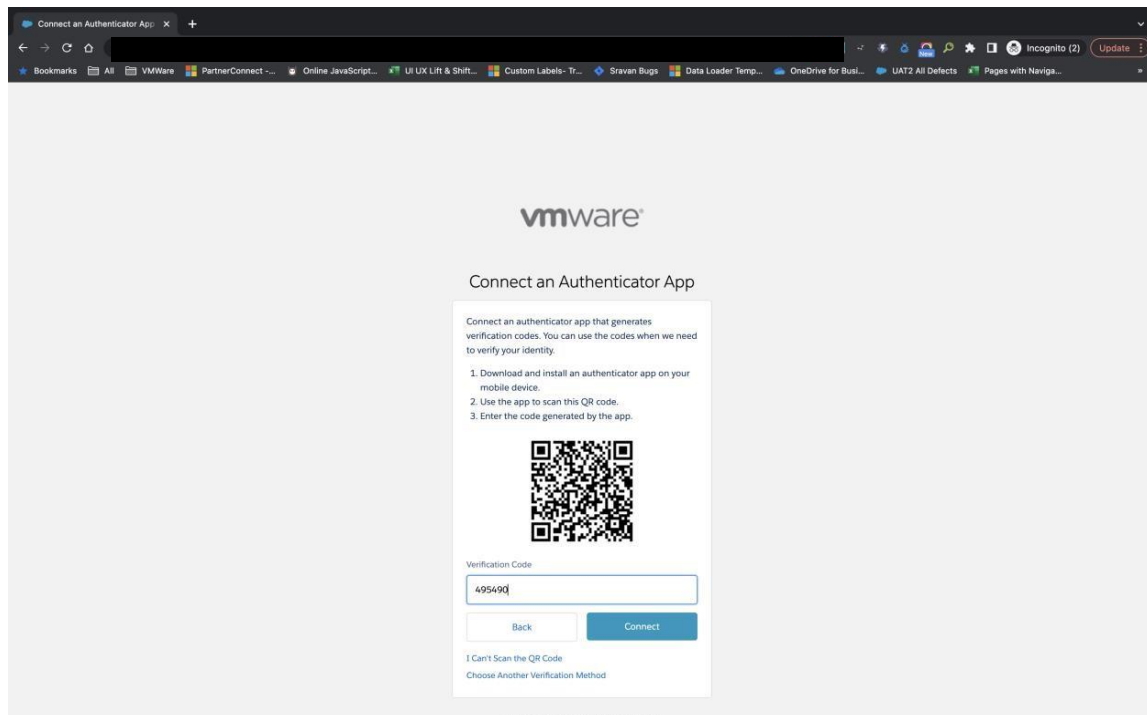


Step 2: Select the option “Use verification codes from an authenticator app”



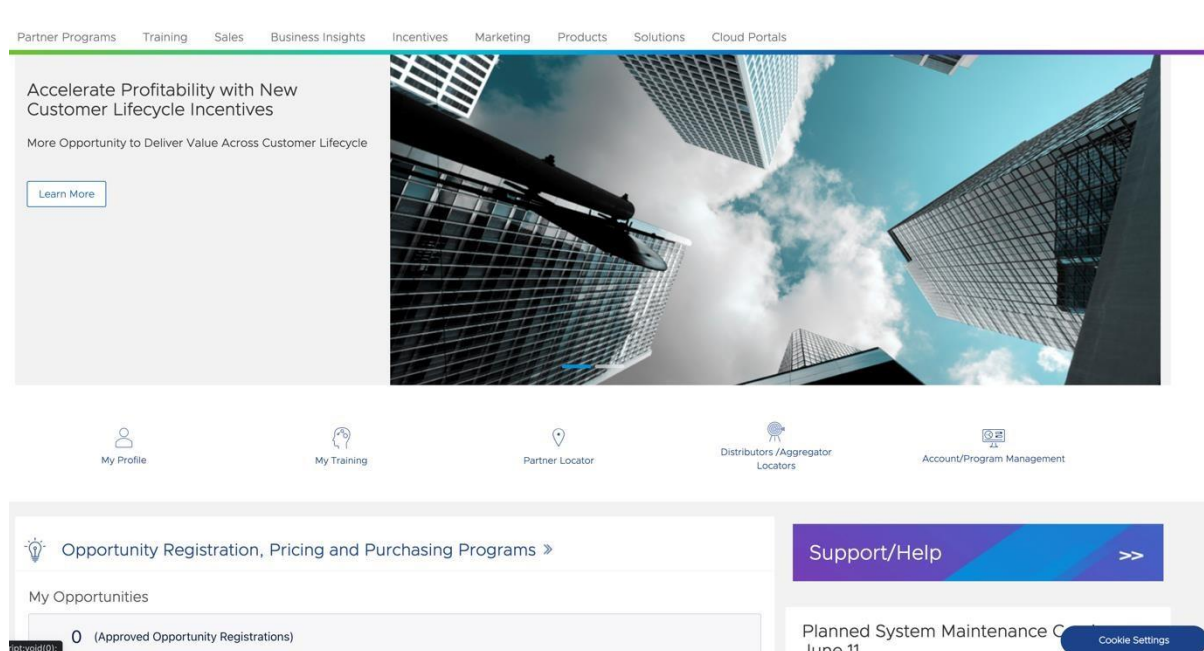
NOTE: If you are using a group username and password **and** you are the first to setup MFA, you will be the default approver for all logins using the same group username and password. Please see the browser option below.

Step 3: Scan the generated QR code within the authenticator application and type in the one-time password that is generated. Click connect.

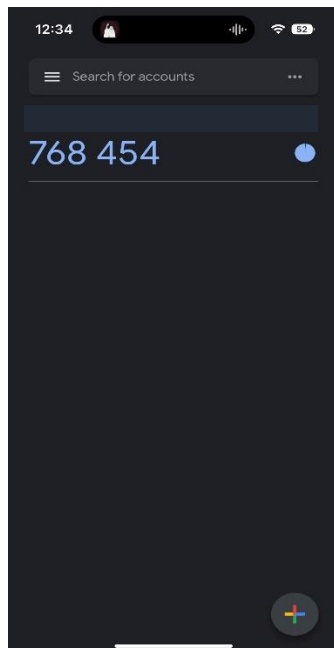


If for some reason you receive a login error message, please clear your cache and try again. If the problem persists, try using an incognito window to login instead. If problems continue to exist, please reach out to partnerconnect@vmware.com

You will then be logged into the Partner Portal.



After Initial Setup: On a re-login, all you will need to do is open the third-party application that you chose to setup Multi-Factor Authentication with and enter in the 6-digit totp code that is shown.



Verify Your Identity

You're trying to **Log In to Partner Connect**. To make sure your Salesforce account is secure, we have to verify your identity.

Use the authenticator app on your mobile device to generate a verification code.

Username:

Verification Code

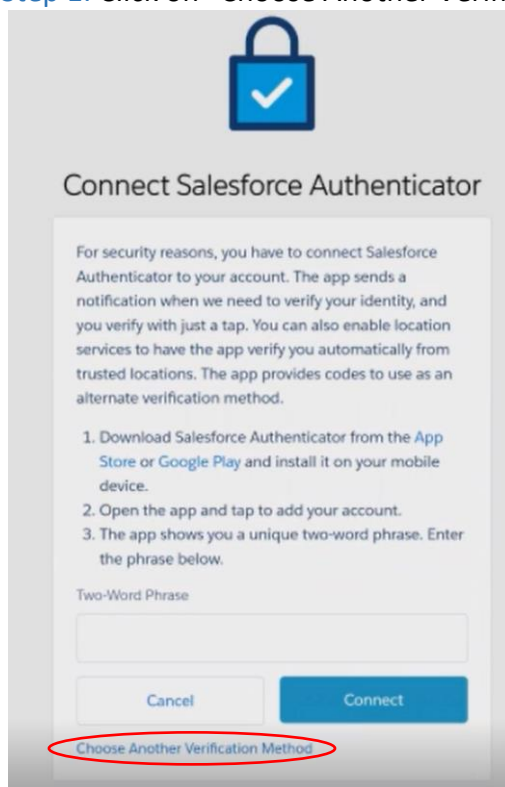
Verify


After clicking “Verify”, you will then be logged into the Partner Portal.

Using A Web Browser Application (totp.app)

If multiple users are sharing one Partner Connect Portal account (not recommended), you do not have a corporate issued mobile device to download an application to, or you are not allowed to bring a corporate device onsite with a customer – please use this method

Step 1: Click on “Choose Another Verification Method”





Connect Salesforce Authenticator

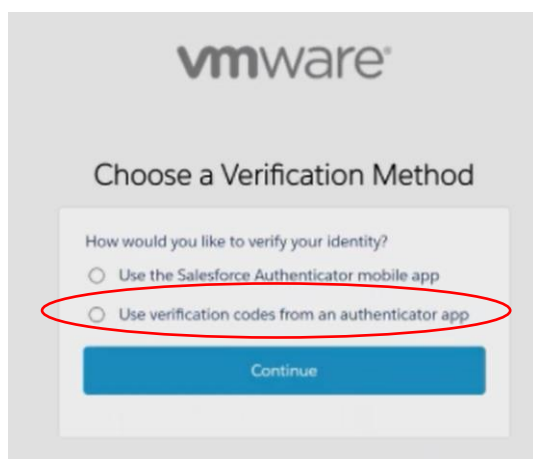
For security reasons, you have to connect Salesforce Authenticator to your account. The app sends a notification when we need to verify your identity, and you verify with just a tap. You can also enable location services to have the app verify you automatically from trusted locations. The app provides codes to use as an alternate verification method.


1. Download Salesforce Authenticator from the [App Store](#) or [Google Play](#) and install it on your mobile device.
2. Open the app and tap to add your account.
3. The app shows you a unique two-word phrase. Enter the phrase below.

Two-Word Phrase

[Choose Another Verification Method](#)

Step 2: Click on “Use verification codes from an authenticator app”





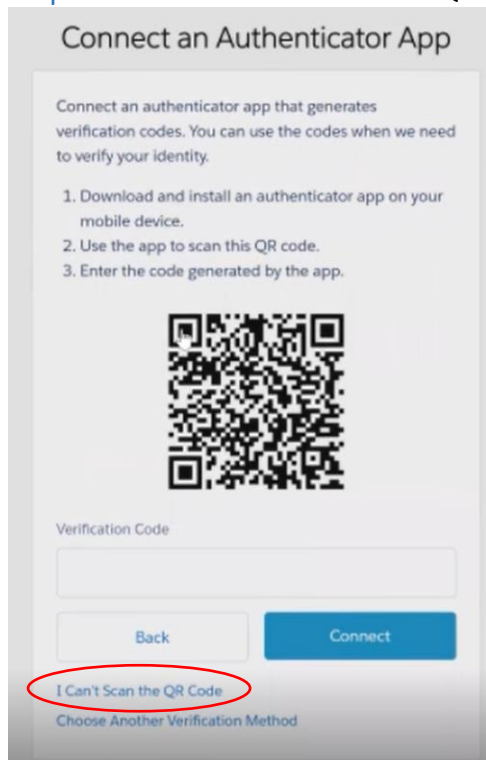
Choose a Verification Method

How would you like to verify your identity?

☐ Use the Salesforce Authenticator mobile app

☐ Use verification codes from an authenticator app


Step 3: Click on “I Can’t Scan the QR Code”



Connect an Authenticator App

Connect an authenticator app that generates verification codes. You can use the codes when we need to verify your identity.

1. Download and install an authenticator app on your mobile device.
2. Use the app to scan this QR code.
3. Enter the code generated by the app.



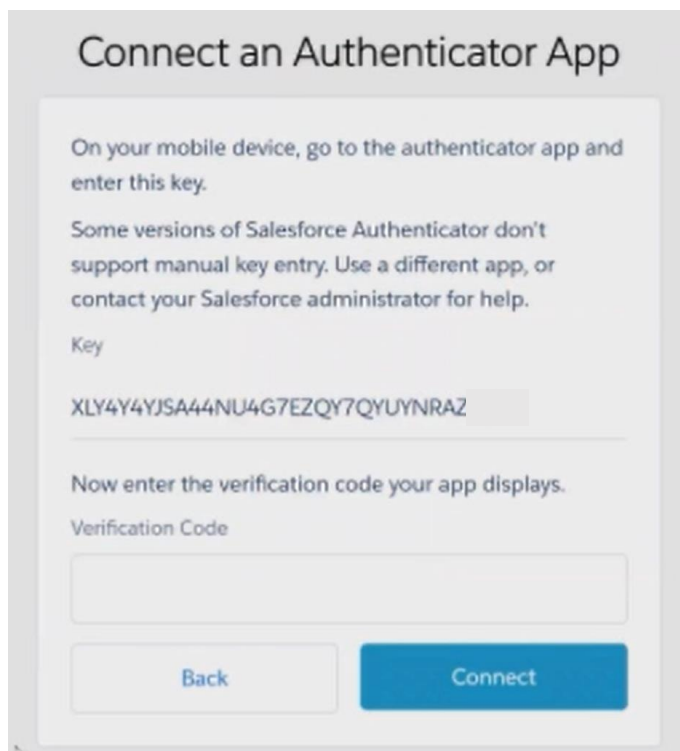
Verification Code

[Back](#) [Connect](#)

[I Can't Scan the QR Code](#)

[Choose Another Verification Method](#)

A Unique Key will then be displayed on your screen (**NOTE: you do not need to use a mobile device for this method**):



Connect an Authenticator App

On your mobile device, go to the authenticator app and enter this key.

Some versions of Salesforce Authenticator don't support manual key entry. Use a different app, or contact your Salesforce administrator for help.

Key

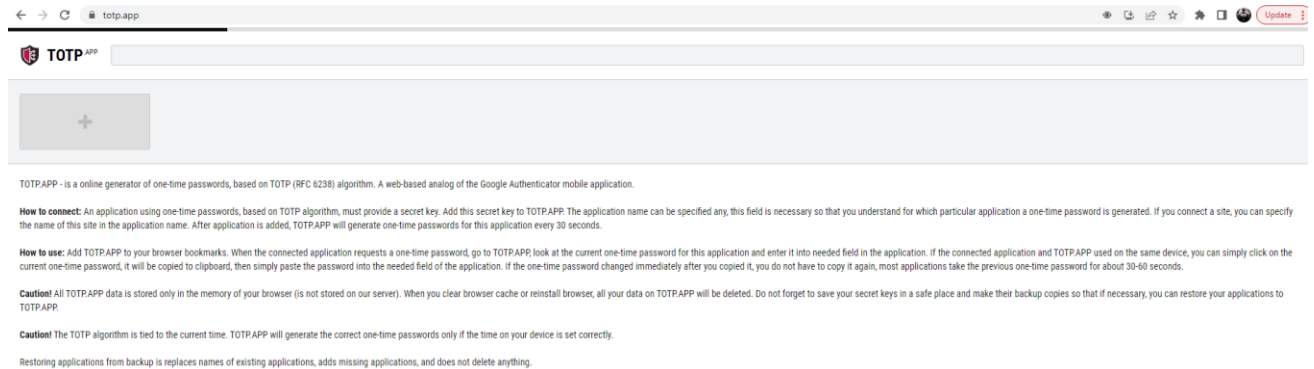
XLY4Y4YJSA44NU4G7EZQY7QYUYNRAZ

Now enter the verification code your app displays.

Verification Code

[Back](#) [Connect](#)

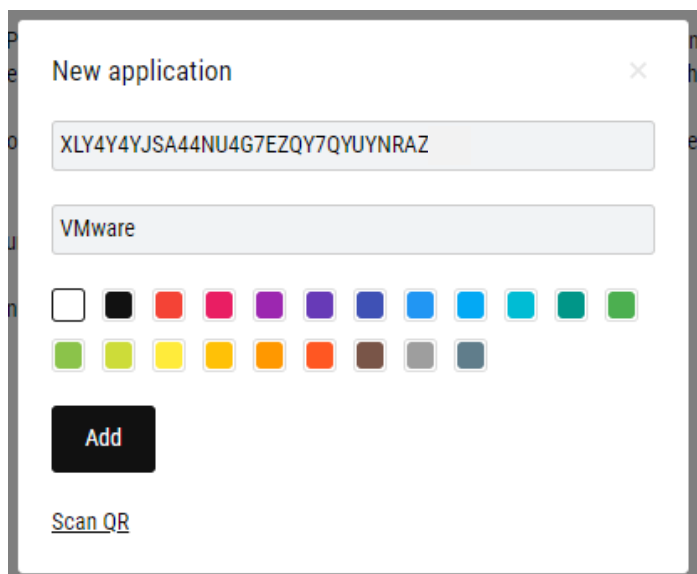
Step 4: On a separate browser window, head over to “totp.app”



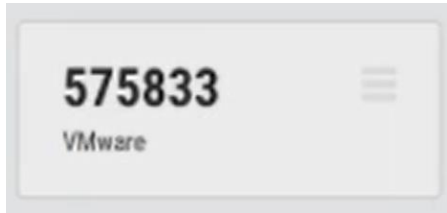
Step 5: Click on the “Add” button on the top left of your screen



Step 6: Enter in the Unique Key that was displayed on your Partner Portal page, then click “Add”



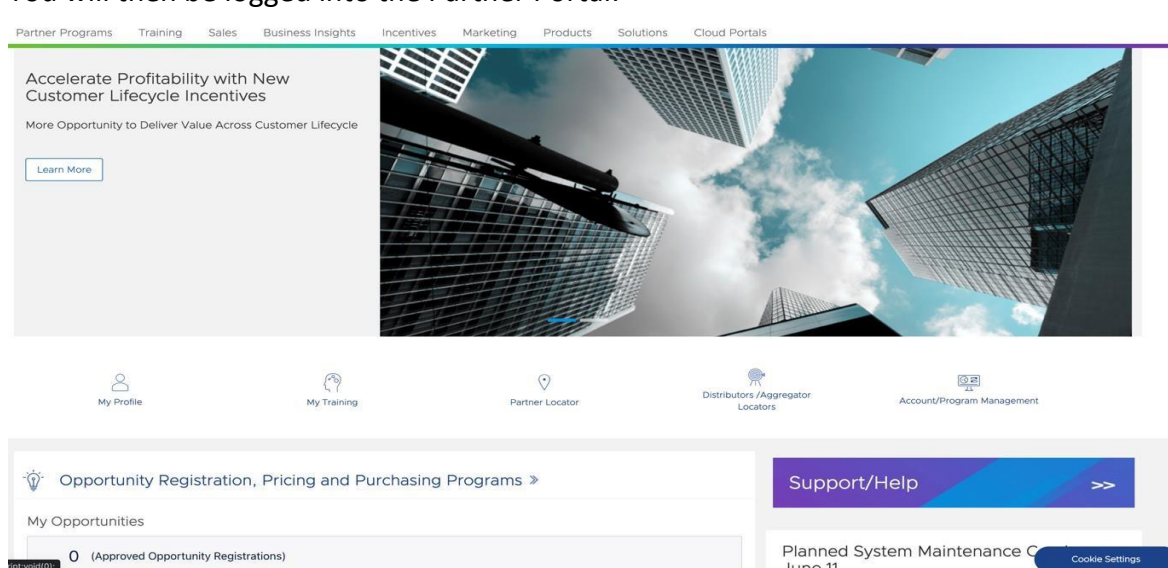
Your Partner Portal account will now be connected to the totp.app website.
A temporary one-time password (totp) will be displayed on the top left of your screen.



Step 7: Please enter in this passcode on your Partner Portal window and click connect.

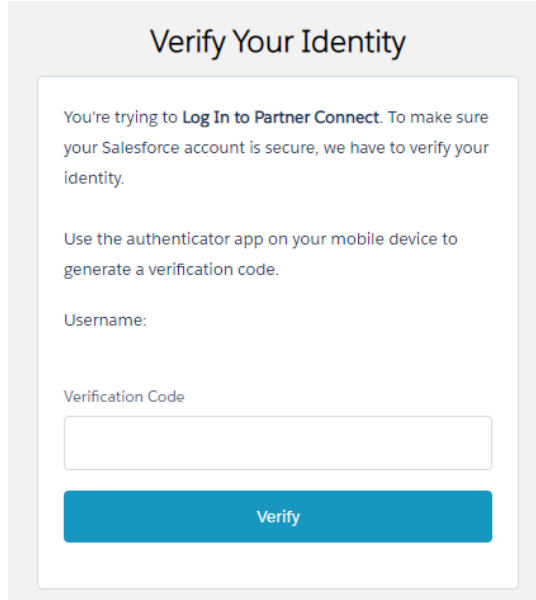
A screenshot of a web page titled "Connect an Authenticator App". The page contains instructions for connecting an authenticator app. It shows a "Key" field with the value "XLY4Y4YJSA44NU4G7EZQY7QYUYNRAZ" and a "Verification Code" field with the value "575833". There are "Back" and "Connect" buttons at the bottom.

You will then be logged into the Partner Portal:



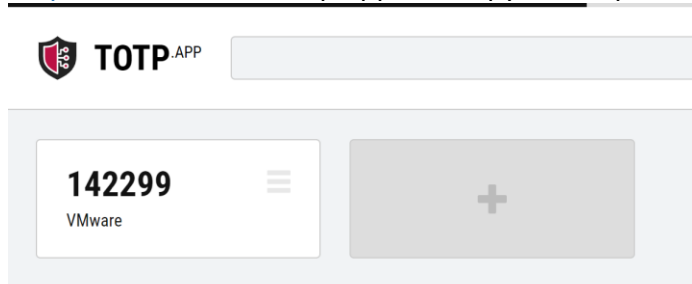
After Initial Setup: On a re-login, all you will need to do is enter in the totp that is generated on totp.app.

Step 1: Login to your Partner Portal account

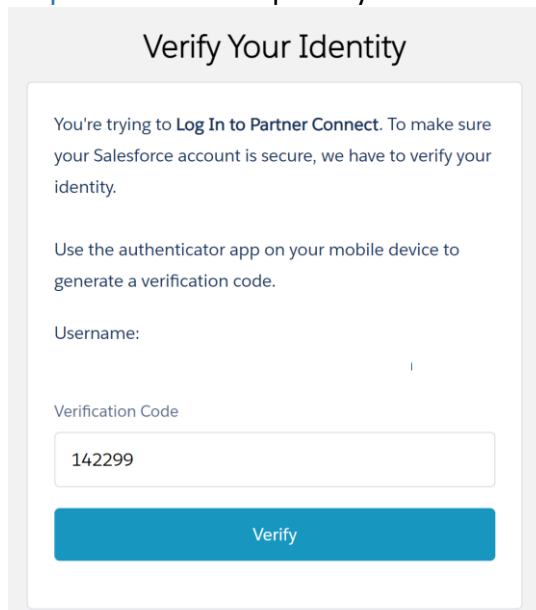


The screenshot shows a web form titled "Verify Your Identity". The text inside the form reads: "You're trying to **Log In to Partner Connect**. To make sure your Salesforce account is secure, we have to verify your identity." Below this, it says: "Use the authenticator app on your mobile device to generate a verification code." There are two input fields: "Username:" and "Verification Code". The "Verification Code" field is empty. At the bottom of the form is a blue button labeled "Verify".

Step 2: Head over to [totp.app](#) and copy the totp that is displayed

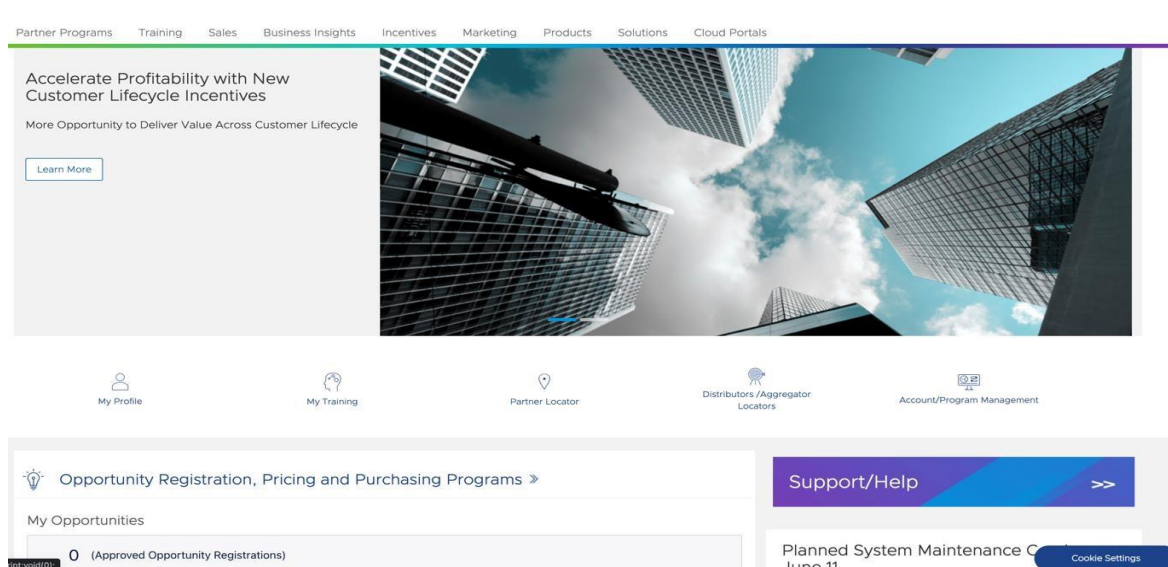


Step 3: Enter the totp into your Partner Portal and click "Verify"



This screenshot is identical to the one in Step 1, but the "Verification Code" field now contains the value "142299". The "Verify" button remains at the bottom.

You will then be logged into the Partner Portal:



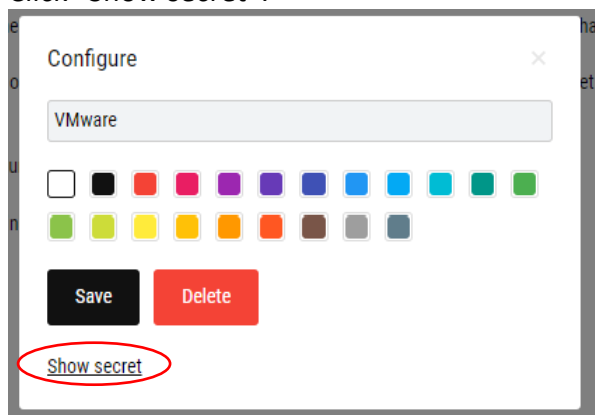
If you are sharing a Partner Portal account, please share the Unique Key with other users and they will be able to enter in the same key on their browser on the totp.app website. They will be able to login to the Partner Portal using their browser once they have the unique key. NOTE: This is not a recommended method. Be careful who you share the key with as your account contains sensitive data.

To find the Unique Key once again, please go back to the totp.app website.

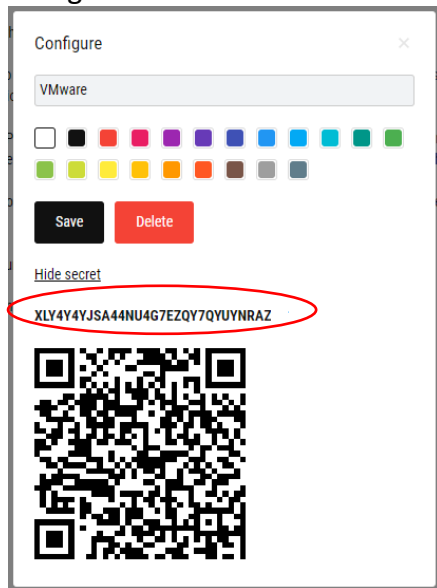
Click on the 3 lines displayed with your current totp:



Click "Show secret":



Your Unique Key will then be displayed. Please share this key with any users who also need to login to the Partner Portal account:



FAQ

Q. Who should I contact if I am having problems logging into the Partner Portal using Multi-Factor Authentication (MFA)?

A: Please reach out to partnerconnect@vmware.com if there are any issues logging in.

Q. Will all users need to use MFA when logging in?

A: Yes. If you are currently a partner that has an account in the Partner Portal, you will need to use MFA when logging in.

Q. Do I need to enter a phrase every time I login using SFDC Authenticator?

A: You will only need to enter in a phrase on your first login using the SFDC Authenticator. After your initial setup, you will only need to approve or deny the login request on your mobile device.

Q. What is the purpose of MFA?

A: Using MFA adds a second layer of protection for your sensitive data. The first being your username and password when logging into the Partner Portal, the second being a third-party authenticator app. We want to be sure sensitive data stays secure and is only visible to those who have access to view it.

Q. Does the mobile device I have matter when using the authenticator?

A: Authenticators will work on both iPhone and Android devices. If you do not have a device that fits these parameters, please use our browser option.

Q. Do I need to use a specific authenticator when logging into the Partner Portal?

A: Salesforce Multi-Factor Authentication (MFA), Google MFA, and Microsoft MFA are our recommended mobile authenticators to use when using a mobile application. If you are using the browser option, please use [totp.app](#).

Q: If I am using a group username and password to access the partner portal, how does this impact me?

A: If you have multiple users leveraging the same username and password to access the portal, you will need to either designate one user to approve all attempted logins through their mobile device **OR** use the browser option ([totp.app](#)) to allow group logins. If for some reason that user leaves the company, changes their mobile device, loses their device, or you lose the unique key to your account when using the browser option - reach out to partnerconnect@vmware.com for a MFA reset.

Q: What should I do if I receive a login error message when trying to connect my authentication application with my partner account?

A: If for some reason you receive a login error message, please clear your cache, and try again. If the problem persists, try using an incognito window to login instead. If problems continue to exist, please reach out to partnerconnect@vmware.com