Gemini XP1 Contingency User Guide

1. About the XP1 link

This document provides instructions of how to access the Gemini application over the 'contingency XP1' link which is an SSL VPN link based on the dual factor authentication. The 'contingency XP1' link is intended to be used by users when their Primary IX link becomes unavailable. This document provides system requirements and step by step instructions for invoking the XP1 link and for accessing the Gemini application over the XP1 link. Note that a User's Internet Explorer (IE) setting should allow the user to Install ActiveX control to successfully connect to XP1 service. Assistance may be required from your local IT support to configure the software installations on the machine to connect to theXP1 service.

2. System Requirements

2.1 Operating System requirements

Below is the system supported for XP1:

- Windows 10 with IE 11
- Windows 10 with Chrome

Note: -

1. The other browsers and operation system versions may also support XP1 however; the operating systems above have been tested and confirmed as working.
2. Windows XP no longer supported.

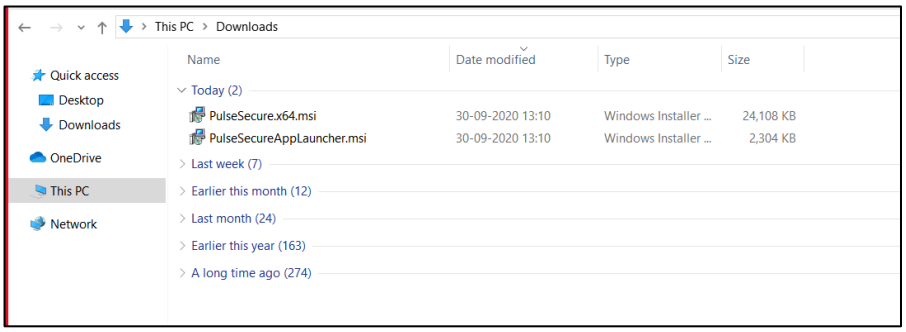
2.2 Software requirements

Prior to accessing the new XP1 link, users need to download two software using the Xoserve Website link provided, install and configure the same. This must be carried out for ensuring that the software installed are of correct version and is mandatory for the existing XP1 users as well. Below step by step procedures need to be carried out for ensuring that XP1 software are correctly installed. Admin access is mandatorily required for carrying out these activities.

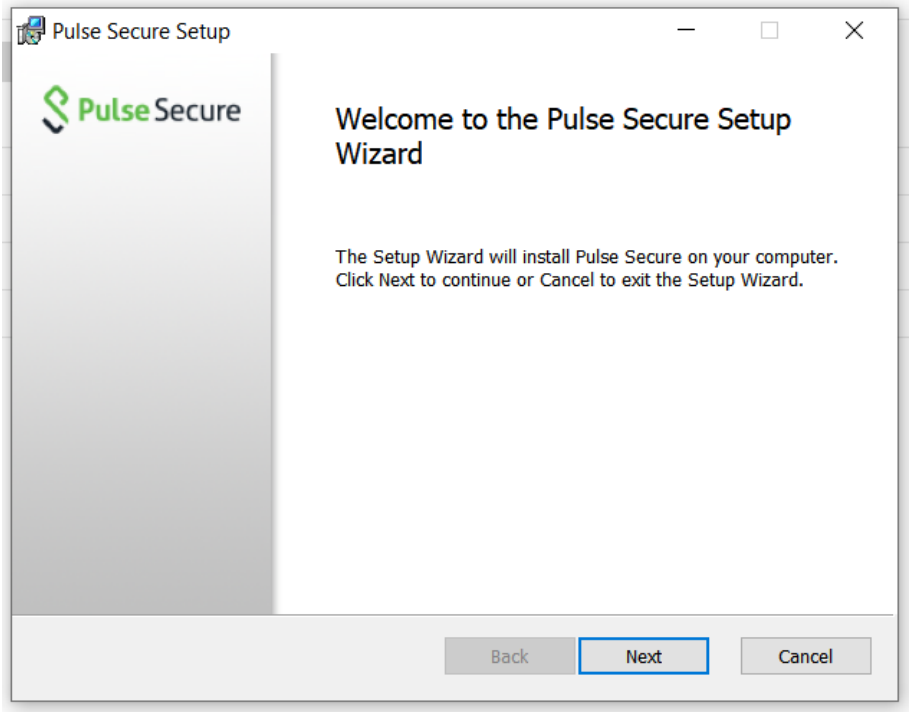
For downloading the software files, access the below two links in Xoserve Website

https://www.xoserve.com/downloads/PulseSecureAppLauncher.msi
https://www.xoserve.com/downloads/PulseSecure.x64.msi

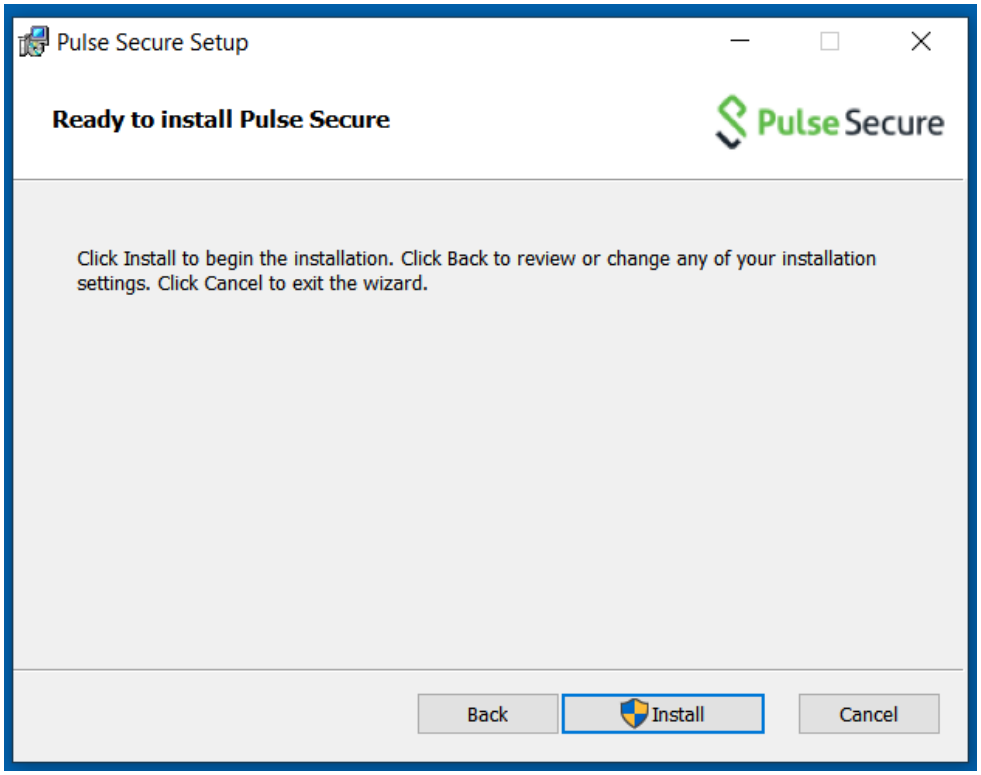
Step 1: Navigate to the location where software files are downloaded



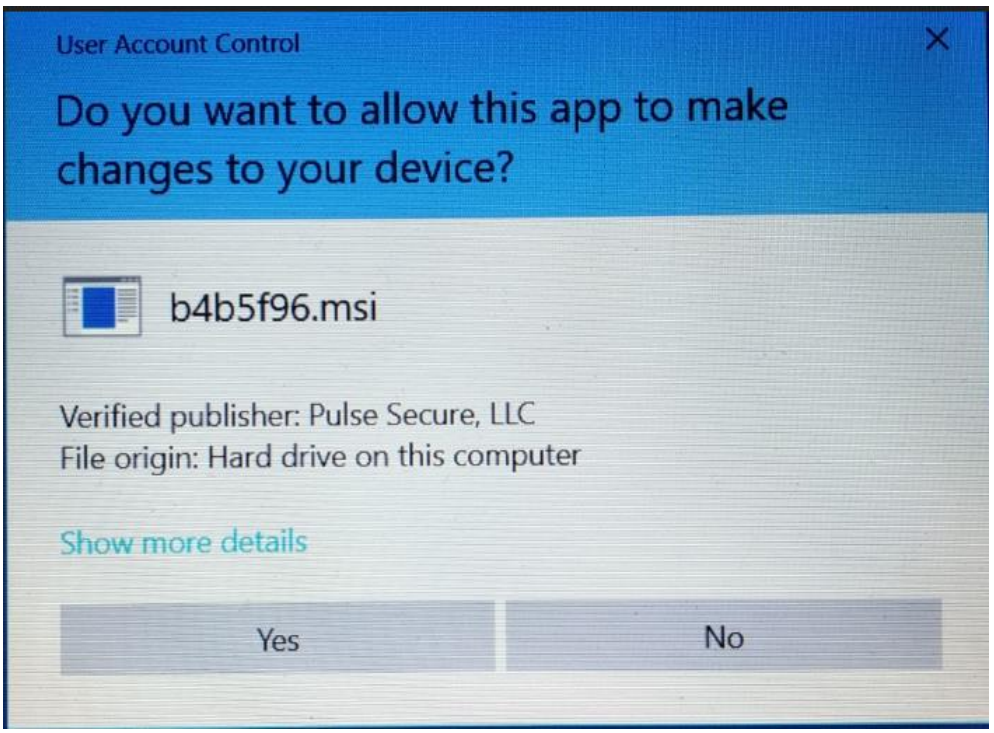
Step 2: Double Click on PulseSecure.x64.msi and click next on Home Screen



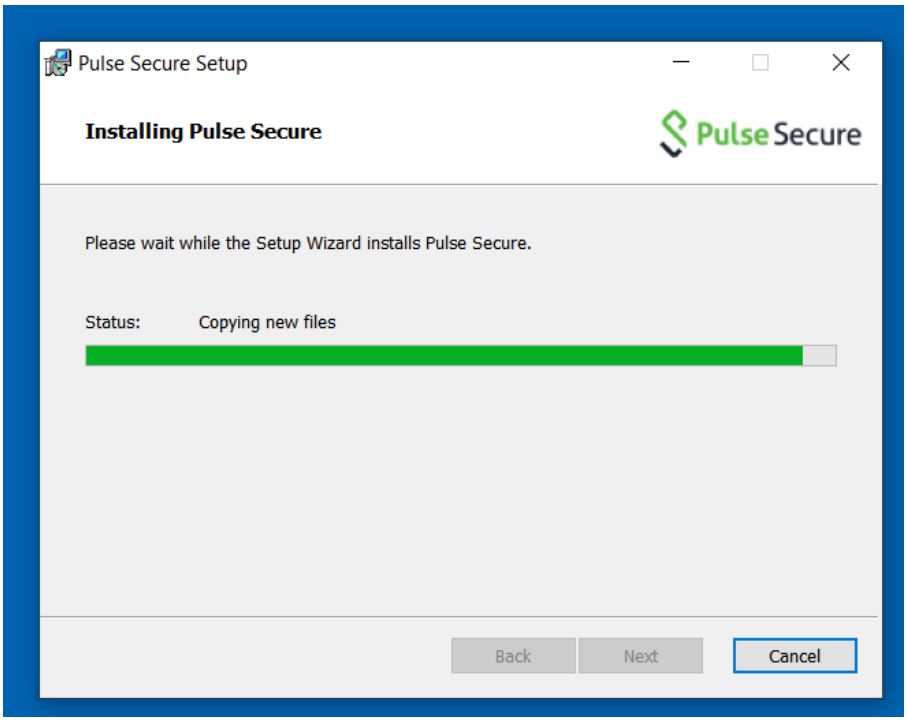
Step 3: On Ready to install Pulse Secure Screen Click Install (Admin Rights required)

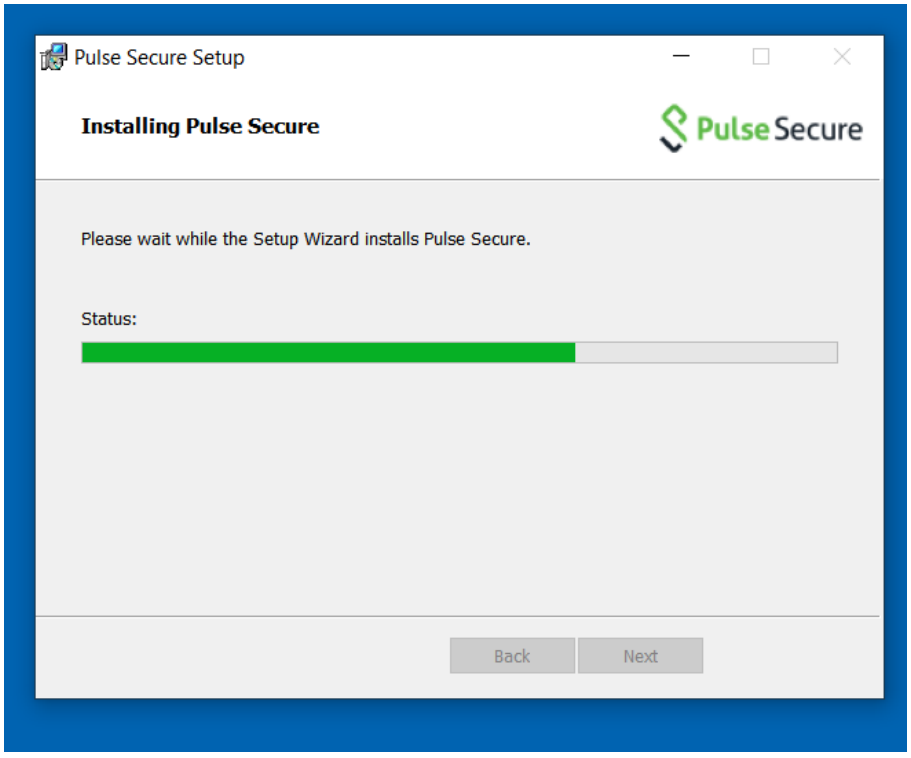


Step 4: Click on Yes for User Account Control Screen asking permission for the App to make changes to your device.



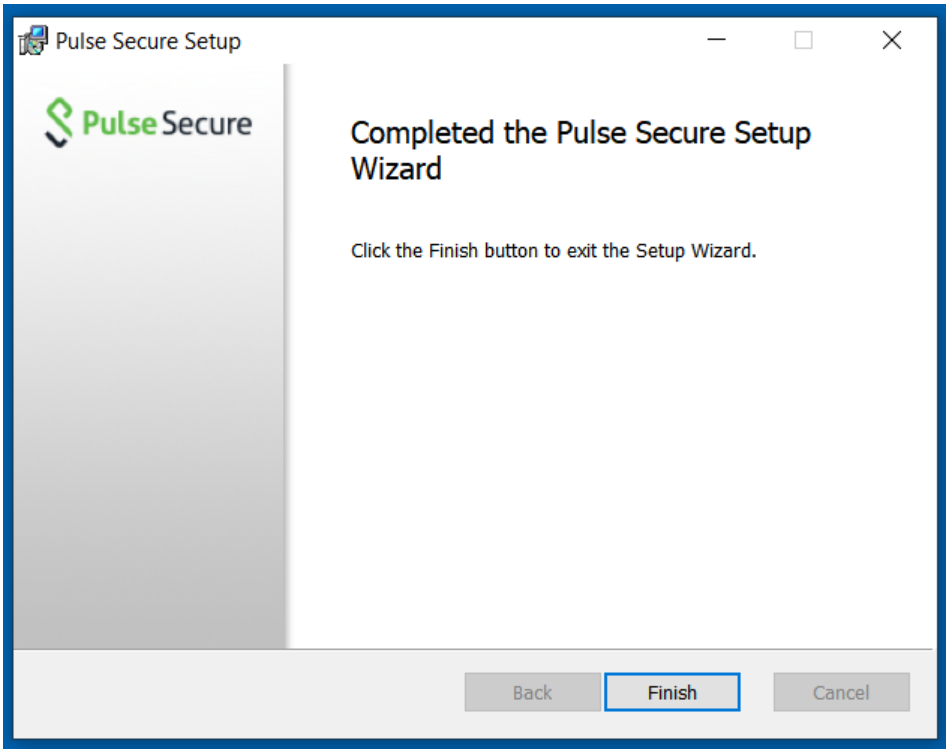
Step 4: Pulse Secure will start copying files and start Installation



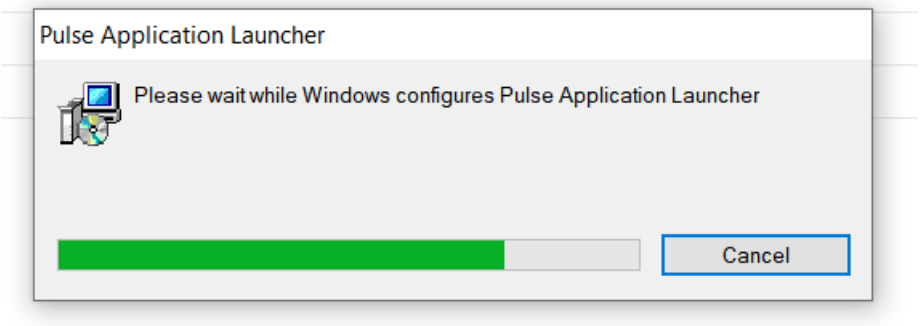


Step 5: Click on Cancel Button when asked for username and password.

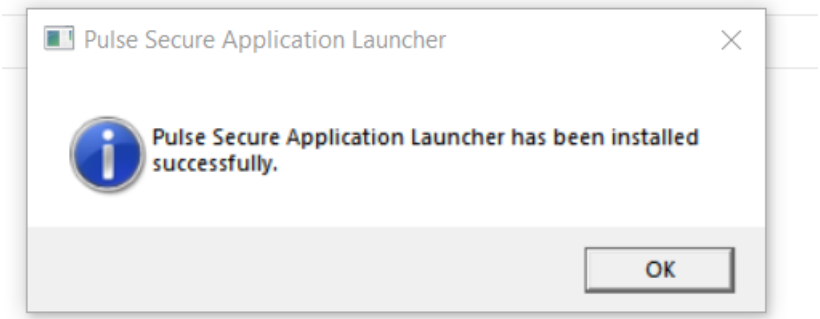
Step 5: Pulse Secure Installation Completion Screen. Click on Finish.



Step 6: Launch second Installer PulseApplicationLauncher.msi



Step 7: Pulse Secure Application Launcher will be installed successfully. Click on OK



2.3 Network requirements

Users should have Internet connectivity from the desktop/laptop to access XP1. A Wi-Fi based internet connectivity is preferred even though corporate web proxy server-based internet access is also supported. If the users are using a corporate web proxy server for Internet access, then please add '127.0.0.1;*.geminints.com' to the proxy exception list on the Internet Explorer.

2.4 Citrix client and SSL certificate root certificate

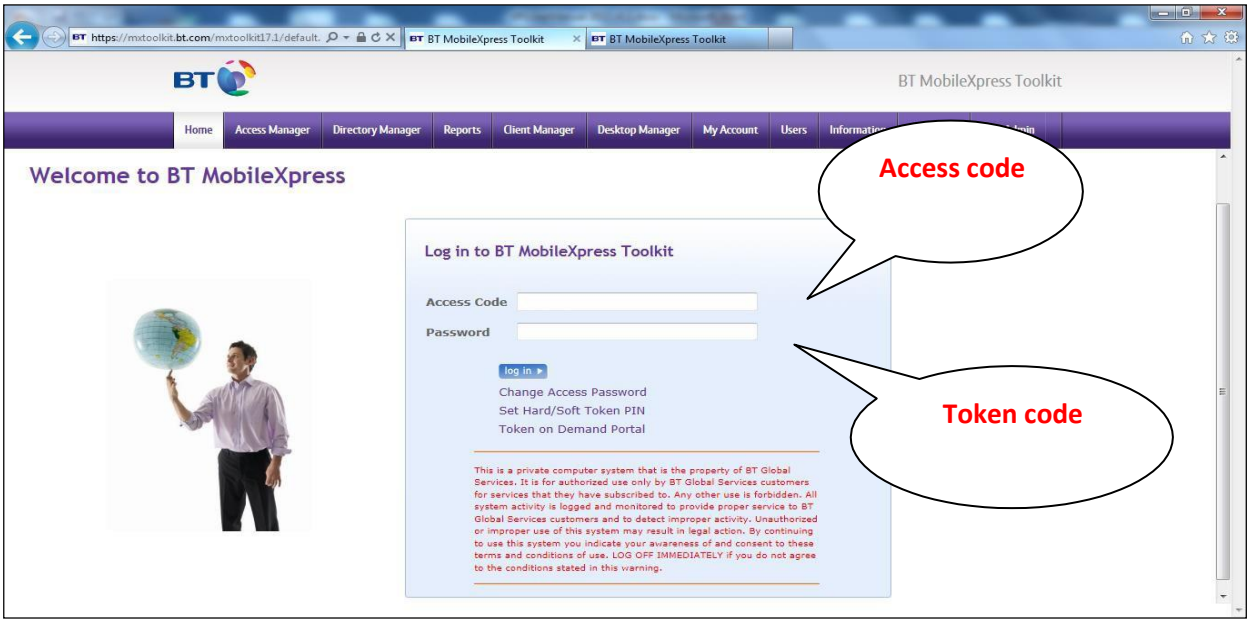
If the desktop / laptop used for XP1 access is different than that of primary IX access, then please ensure that Citrix client is installed on the desktop / laptop. The User should ensure that the attached root certificate is imported in the browser under the 'Trusted Root Certification Authorities'.

Note: - SSL V2 & V3 are obsolete and no longer supported which has known vulnerabilities.

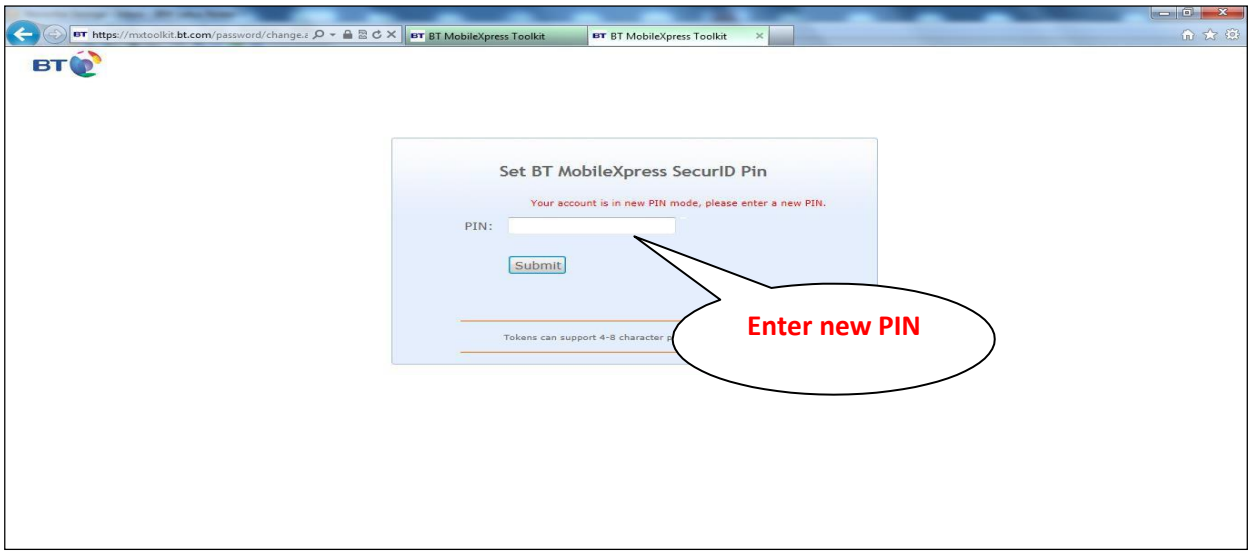
3. Setting the RSA token PIN

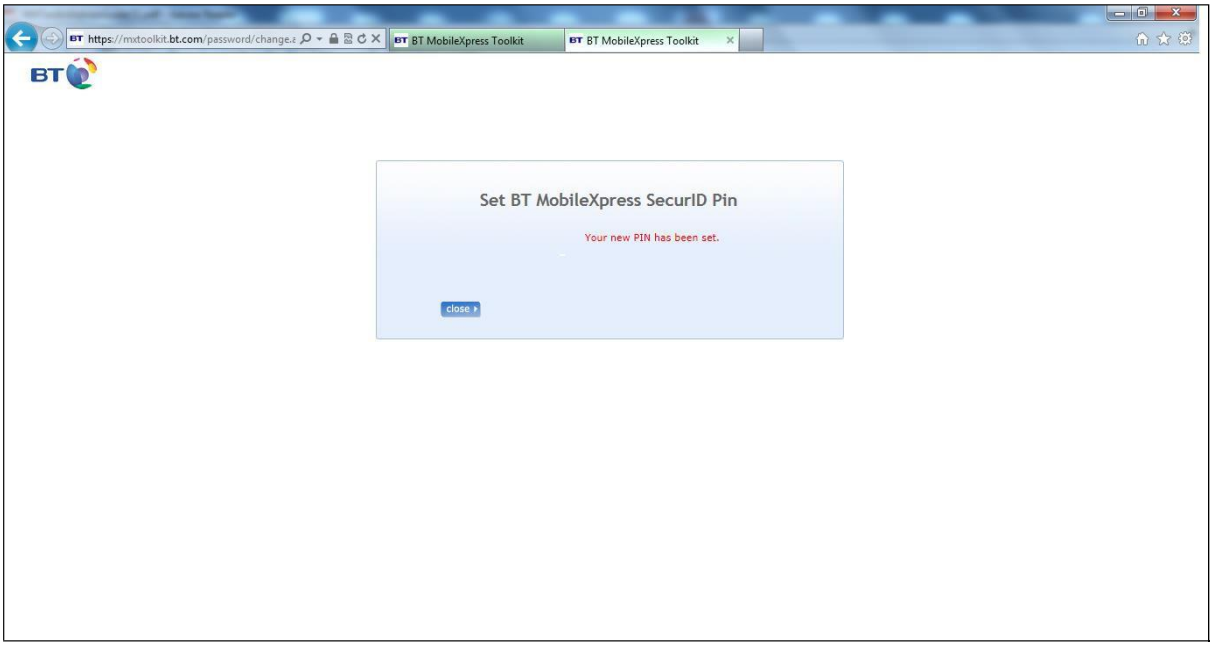
The XP1 authentication involves dual factor authentication using the RSA hardware token. Dual factor authentication involves two factors namely a PIN and a token code. The PIN is set by the user. The token code is a six-digit number which is displayed on the RSA token which changes every 60 seconds. The PIN must be set before XP1 service can be accessed. Use the instructions below to set the PIN.

1) Open the browser and type the URL https://mxtoolkit.bt.com/password/change.aspx. Below screen should appear.



2) Type the Access code and the password. The password is the token code which is displayed on the RSA token. For example, if the token code displayed on the RSA token is 278 308 then type the password as 278308 (no spaces in between). Click on 'log-in'.



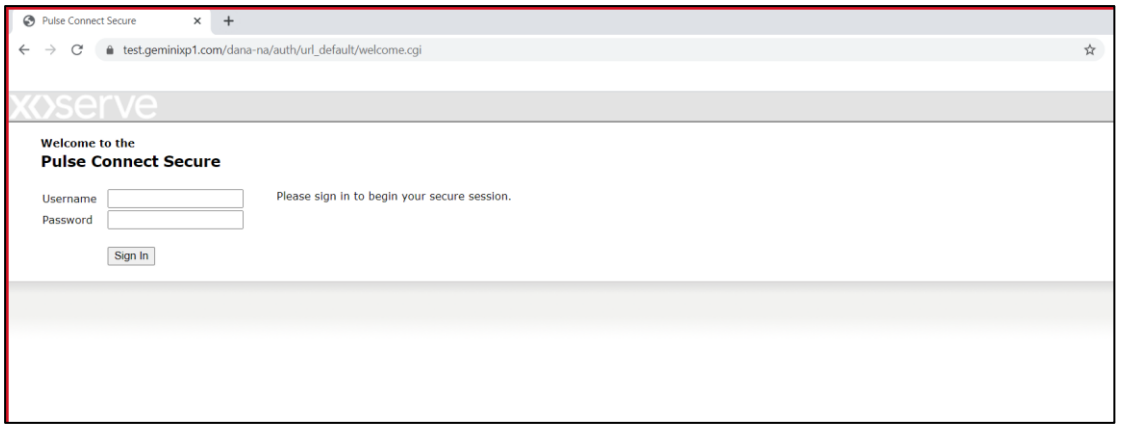


3) The PIN is now set. Click 'Close'. Please secure the PIN as it is required to access XP1 service.

Note: If you want to reset the PIN at a later point of time then get in touch with the Xoserve Service desk on **08456000506**. The Service Desk will configure the token in new PIN mode. Once this is done then you need to follow the steps above (step 1 to step 3) to set a new PIN.

4. Connecting to XP1

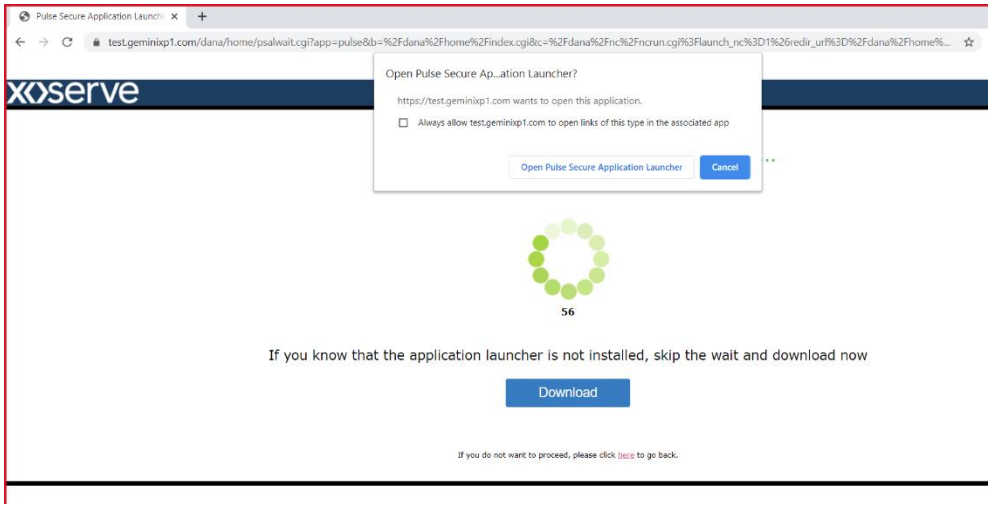
Step 1: Launch test URL https://xp1.geminixp1.com. Enter Credentials using RSA token. Below screen should appear. Type the Access code and password (PIN + token code) and click Sign In.



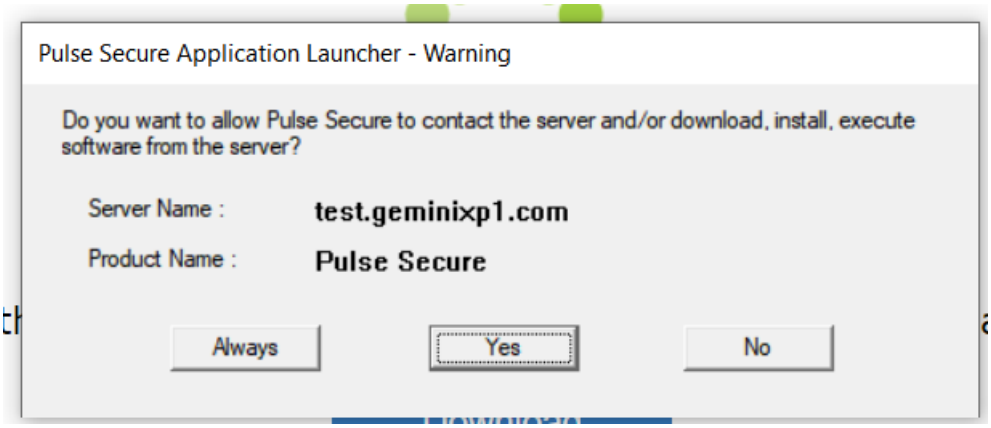
The password is the PIN + token code. For example, if the PIN is 1465 and token code that is displayed on the RSA token is 236 071 then please type the password as 1465236071.

If the password is typed incorrectly 5 consecutive times, then the system will prompt the user to re sync the token following unsuccessful credentials being entered. For this the system will ask the user to wait until the token code is changed in the display of the RSA token. The User should then type only the token code when prompted.

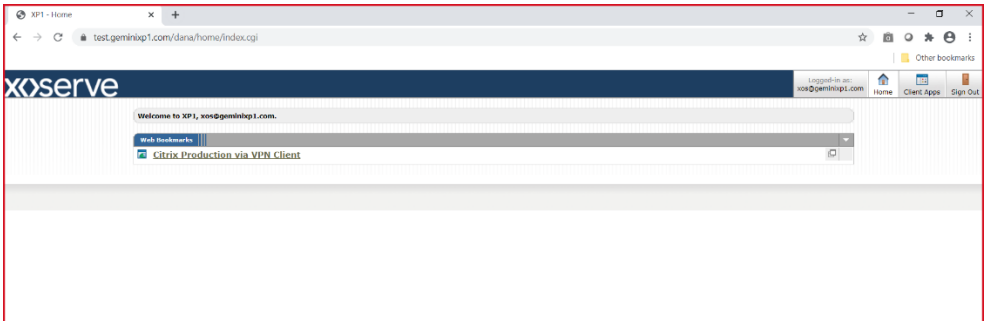
Step 2: Select Always allow and Click on Open Pulse Secure Application Launcher.



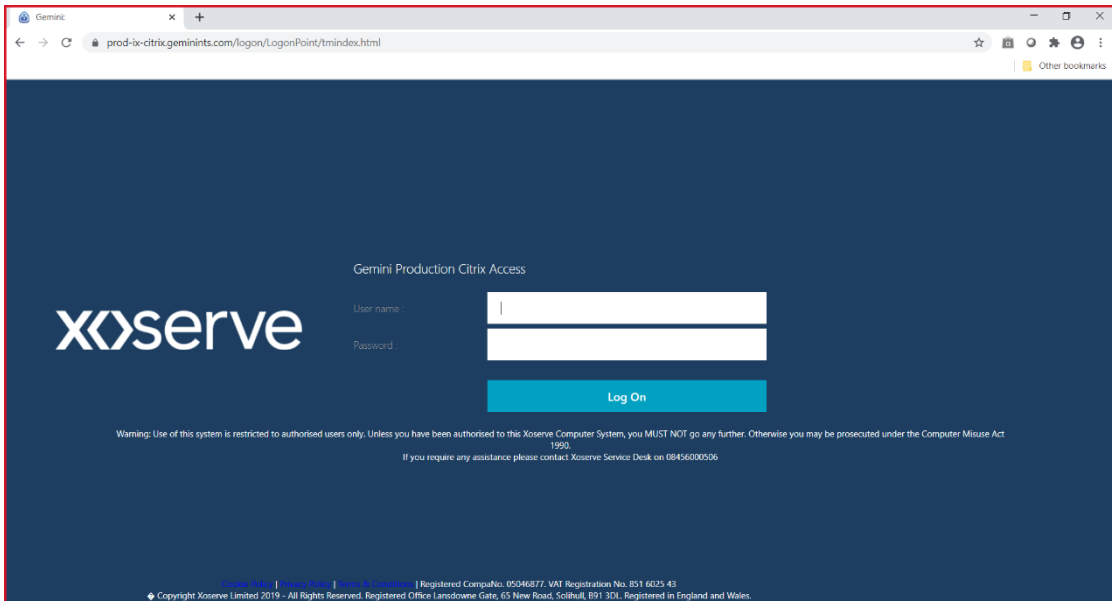
Step 10: Click on Yes in Application Launcher Pop-up



Step 11: Click on Citrix Production via VPN Client



Step 12: Gemini Production Citrix Page will be received.



<< End of Document>>