F5 Privileged User Access

Install Guide for TMOS v13.1

Bill Church – Principle Solutions Engineer – Defense

bill@f5.com

v1.0.12 – February 27, 2018

Contents

Introduction 3

Requirements 3

Prerequisites 3

Installation Overview 3

Script Options 3

build\_pua 3

build\_pua\_offline 3

Automation Options 3

Resource Table 4

Installation 5

Online Installation Method 5

Run Installation Script 5

Offline Installation Method 10

Run Installation Script 10

Validation 14

WebSSH2 Client 14

APM Policy and Portal Mode 14

# Introduction

The Privileged User Authentication (PUA) solution is made up of three parts.

1. WebSSH2 Client Plugin
2. Ephemeral Authentication Plugin
3. Access Policy Manager (APM) policy configuration

## Requirements

* BIG-IP with TMOS v13.1.0.2 or greater.
* 2-5 IP addresses for virtual servers (see [Resource Table](#_Resource_Table))

## Prerequisites

BIG-IP with at least APM and iRules LX licensed and provisioned

The “**build\_pua.zip**” or “**build\_pua\_offline.zip**” installation script found here:

<https://raw.githubusercontent.com/billchurch/f5-pua/master/build_pua.zip>

<https://raw.githubusercontent.com/billchurch/f5-pua/master/build_pua_offline.zip>

## Installation Overview

The installation will consist of installing and testing (in order)

1. BIG-IP Preparation
2. Script download and execution
3. Customization of APM policy

## Script Options

Two options exist for installing the PUA solution, **build\_pua** and **build\_pua\_offline**.

### build\_pua

Fetches the most recent plugins and policies from the internet ad run time.

### build\_pua\_offline

Contains all plugins and policies embedded in the script for complete off-line use

## Automation Options

See the details inside <https://github.com/billchurch/f5-pua/blob/master/pua_config.sh> for tips on how you can further automate the installation process.

## Resource Table

Use the following table to plan your deployment

|  |  |  |
| --- | --- | --- |
| **Resource** | **Description** | **Value** |
| WebSSH\_proxy\_vs\_IP | Virtual server IP Address of WebSSH2 service. **EXCLUSIVE IP** |  |
| APM\_Portal\_vs\_IP | Virtual server IP Address of APM portal for authentication |  |
| RADIUS\_proxy\_vs\_IP | Virtual server IP address of RADIUS proxy service |  |
| LDAP\_proxy\_vs\_IP | Virtual server IP address of LDAP proxy service |  |
| LDAPS\_proxy\_vs\_IP | Virtual server IP address of LDAPS proxy service |  |
| LDAP\_server\_IP | IP Address of site LDAP or AD server (required for LDAP use) |  |
| RADIUS\_server\_IP | IP Address of site RADIUS server (if RADIUS bypass is used) |  |

# Installation

## Online Installation Method

This method utilizes the **build\_pua.sh/zip** method to install the PUA solutions from online resources. This requires a BIG-IP with working Internet connectivity and DNS resolution to Internet resources.

### Run Installation Script

1. SCP **build\_pua.zip** to the BIG-IP (/config will be fine)
   1. If running an Automated or Semi-Automated setup, SCP your customized **pua\_config.sh** script to the same folder
2. Unzip **build\_pua.zip**

|  |
| --- |
| [root@pua131-build:Active:Standalone] config # **unzip build\_pua.zip**  Archive:  build\_pua.zip    inflating: build\_pua.sh |

1. Run **build\_pua.sh**
   1. If running a fully automated script, skip to [Validation](#_Validation)
2. Answer the questions when prompted
   1. If using the **Semi-Automated** setup, the defaults will be inserted for you, to accept them just hit **<ENTER>**

|  |
| --- |
| [root@pua131-build:Active:Standalone] config # **bash build\_pua.sh**  Introduction  ============  ... Press any key to continue, or CTRL-C to cancel.  Preparing environment... [OK]  Changing to /tmp/pua.ciIVBvwwpN... [OK]  Adding ILX archive directory [OK]  Checking modules are provisioned.  Checking apm... [OK]  Checking ltm... [OK]  Checking ilx... [OK]  SUCCESS: All modules provisioned.  Type the IP address of your WebSSH2 service virtual server  and press ENTER: **192.168.20.62**  You typed **192.168.20.62**, is that correct (Y/n)? **y**  Checking IP... [OK]  Type the IP address of your RADIUS service virtual server  and press ENTER: **192.168.20.63**  You typed **192.168.20.63**, is that correct (Y/n)? **y**  Checking IP... [OK]  Type the IP address of your LDAP service virtual server  and press ENTER [**192.168.20.63**]:  You typed **192.168.20.63**, is that correct (Y/n)? **y**  Type the IP address of your LDAPS service virtual server  and press ENTER [**192.168.20.63**]:  You typed **192.168.20.63**, is that correct (Y/n)? **y**  Type the IP address of your Webtop service virtual server  and press ENTER [**192.168.20.63**]:  You typed **192.168.20.63**, is that correct (Y/n)? **y**  Checking for startup\_script\_webssh\_commands.sh... [NOT FOUND]  Downloading startup\_script\_webssh\_commands.sh... [OK]  Downloading startup\_script\_webssh\_commands.sh.sha256... [OK]  Hash check for startup\_script\_webssh\_commands.sh [OK]  Checking for BIG-IP-13.1.0.2-ILX-WebSSH2-current.tgz... [NOT FOUND]  Downloading BIG-IP-13.1.0.2-ILX-WebSSH2-current.tgz... [OK]  Downloading BIG-IP-13.1.0.2-ILX-WebSSH2-current.tgz.sha256... [OK]  Hash check for BIG-IP-13.1.0.2-ILX-WebSSH2-current.tgz [OK]  Checking for BIG-IP-ILX-ephemeral\_auth-current.tgz... [NOT FOUND]  Downloading BIG-IP-ILX-ephemeral\_auth-current.tgz... [OK]  Downloading BIG-IP-ILX-ephemeral\_auth-current.tgz.sha256... [OK]  Hash check for BIG-IP-ILX-ephemeral\_auth-current.tgz [OK]  Sample Certificate Authority  ============================  ... Would you like to download a sample CA for testing (Y/n)? **y**  Checking for ca.pua.lab.cer... [NOT FOUND]  Downloading ca.pua.lab.cer... [OK]  Downloading ca.pua.lab.cer.sha256... [OK]  Hash check for ca.pua.lab.cer [OK]  Installing CA file ca.pua.lab.cer [OK]  Creating pua\_webtop-clientssl profile with CA ca.pua.lab.cer [OK]  Placing startup\_script\_webssh\_commands.sh in /config... [OK]  Placing BIG-IP-13.1.0.2-ILX-WebSSH2-current.tgz in /var/ilx/workspaces/Common/archive... [OK]  Placing BIG-IP-ILX-ephemeral\_auth-current.tgz in /var/ilx/workspaces/Common/archive... [OK]  Creating ephemeral\_config data group... [OK]  Creating ephemeral\_LDAP\_Bypass data group... [OK]  Creating ephemeral\_RADIUS\_Bypass data group... [OK]  Creating ephemeral\_radprox\_host\_groups data group... [OK]  Creating ephemeral\_radprox\_radius\_attributes data group... [OK]  Creating ephemeral\_radprox\_radius\_client data group... [OK]  Importing WebSSH2 Workspace... [OK]  Importing Ephemeral Authentication Workspace... [OK]  Modifying Ephemeral Authentication Workspace... [OK]  Creating WEBSSH Proxy Service Virtual Server... [OK]  Creating tmm route for Plugin... [OK]  Installing webssh tmm vip startup script... [OK]  Creating WebSSH2 Plugin... [OK]  Creating Ephemeral Authentication Plugin... [OK]  Creating RADIUS Proxy Service Virtual Server... [OK]  Creating LDAP Proxy Service Virtual Server... [OK]  Creating LDAPS (ssl) Proxy Service Virtual Server... [OK]  Creating APM connectivity profile... [OK]  Checking for profile-pua\_webtop\_policy.conf.tar.gz... [NOT FOUND]  Downloading profile-pua\_webtop\_policy.conf.tar.gz... [OK]  Downloading profile-pua\_webtop\_policy.conf.tar.gz.sha256... [OK]  Hash check for profile-pua\_webtop\_policy.conf.tar.gz [OK]  Importing APM sample profile profile-pua\_webtop\_policy.conf.tar.gz [OK]  Modifying pua APM Portal Resource...[OK]  Applying pua APM Policy...[OK]  Creating Webtop Virtual Server... [OK]  RADIUS Testing Option  =====================  ... Do you want to configure this BIG-IP to authenticate against itself for testing purposes (y/N)? **y**    Are you really sure!? (y/N)? **y**  Modifying BIG-IP for RADIUS authentication against itself... [OK]  You can test WebSSH2 and Ephemeral authentication without APM configuration now  by browsing to:  **https://192.168.20.62:2222/ssh/host/192.168.30.205**    username: testuser    password: anypassword  This will allow anyone using the username testuser to log in with any password  as a guest  Saving config... [OK]  You can test your new APM webtop now by browsing to:  **https://192.168.20.63**    username: <any>    password: <any>  This will let anyone in with any policy. The next step after testing would be  to add access control through AD, MFA, or some other method.  If the RADIUS testing option was enabled, any username will log in using  Ephemeral Authentication.  Task complete.  Now go build an APM policy for pua!  Cleaning up... |

## Offline Installation Method

This method utilizes the **build\_pua\_offline.sh/zip** method to install the PUA solutions from a closed network or a BIG-IP with limited or no Internet connectivity.

### Run Installation Script

1. SCP **build\_pua\_offline.zip** to the BIG-IP (/config will be fine)
   1. If running an Automated or Semi-Automated setup, SCP your customized **pua\_config.sh** script to the same folder
2. Unzip **build\_pua\_offline.zip**

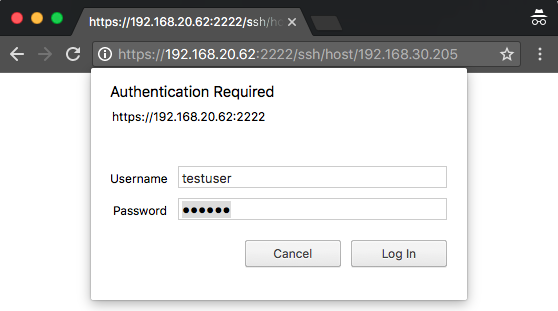
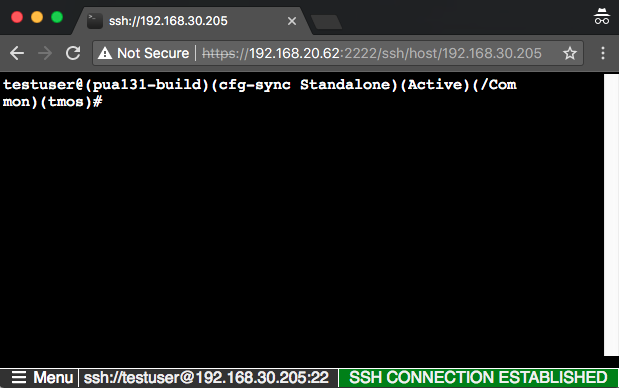
|  |
| --- |
| [root@pua131-build:Active:Standalone] config # **unzip build\_pua\_offline.zip**  Archive:  build\_pua\_offline.zip    inflating: build\_pua\_offline.sh |

1. Run **build\_pua\_offline.sh**
   1. If running a fully automated script, skip to [Validation](#_Validation)
2. Answer the questions when prompted
   1. If using the **Semi-Automated** setup, the defaults will be inserted for you, to accept them just hit **<ENTER>**

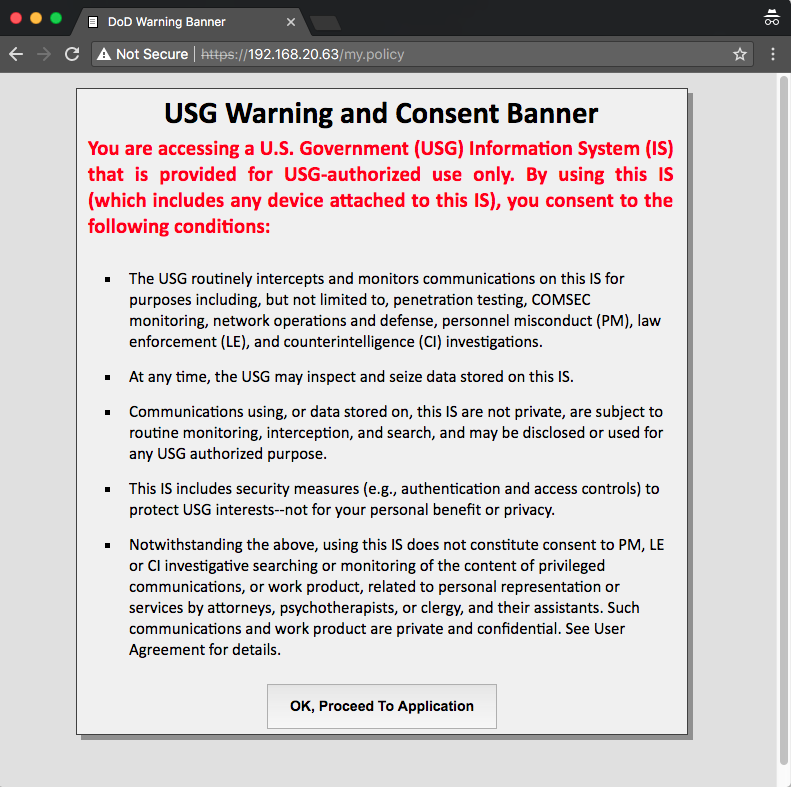
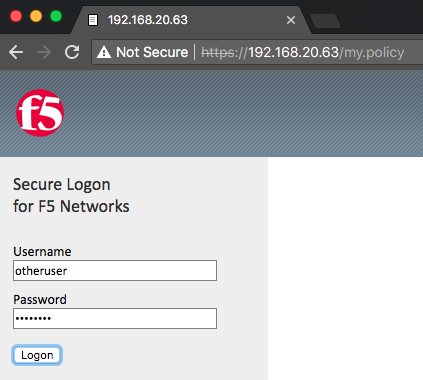
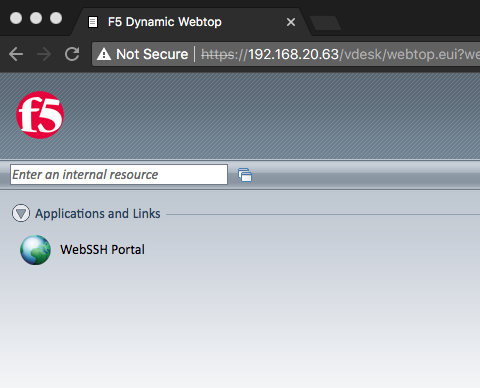
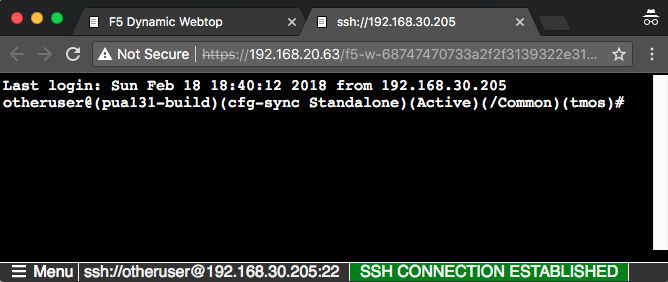
|  |
| --- |
| [root@pua131-build:Active:Standalone] config # **bash build\_pua\_offline.sh**  Introduction  ============  ... Press any key to continue, or CTRL-C to cancel.  Preparing environment... [OK]  Changing to /tmp/pua.cN9WbyIUdO... [OK]  **Offline mode detected. Skipping downloads.**  Extracting archive [OK]  Adding ILX archive directory [OK]  Checking modules are provisioned.  Checking apm... [OK]  Checking ltm... [OK]  Checking ilx... [OK]  SUCCESS: All modules provisioned.  Type the IP address of your WebSSH2 service virtual server  and press ENTER: **192.168.20.62**  You typed **192.168.20.62**, is that correct (Y/n)? **y**  Checking IP... [OK]  Type the IP address of your RADIUS service virtual server  and press ENTER: **192.168.20.63**  You typed **192.168.20.63**, is that correct (Y/n)? **y**  Checking IP... [OK]  Type the IP address of your LDAP service virtual server  and press ENTER [**192.168.20.63**]:  You typed **192.168.20.63**, is that correct (Y/n)? **y**  Type the IP address of your LDAPS service virtual server  and press ENTER [**192.168.20.63**]:  You typed **192.168.20.63**, is that correct (Y/n)? **y**  Type the IP address of your Webtop service virtual server  and press ENTER [**192.168.20.63**]:  You typed **192.168.20.63**, is that correct (Y/n)? **y**  Checking for startup\_script\_webssh\_commands.sh... [OK]  Hash check for startup\_script\_webssh\_commands.sh [OK]  Checking for BIG-IP-13.1.0.2-ILX-WebSSH2-current.tgz... [OK]  Hash check for BIG-IP-13.1.0.2-ILX-WebSSH2-current.tgz [OK]  Checking for BIG-IP-ILX-ephemeral\_auth-current.tgz... [OK]  Hash check for BIG-IP-ILX-ephemeral\_auth-current.tgz [OK]  Sample Certificate Authority  ============================  ... Would you like to install a sample CA for testing (Y/n)? **y**  Checking for ca.pua.lab.cer... [OK]  Hash check for ca.pua.lab.cer [OK]  Installing CA file ca.pua.lab.cer [OK]  Creating pua\_webtop-clientssl profile with CA ca.pua.lab.cer [OK]  Placing startup\_script\_webssh\_commands.sh in /config... [OK]  Placing BIG-IP-13.1.0.2-ILX-WebSSH2-current.tgz in /var/ilx/workspaces/Common/archive... [OK]  Placing BIG-IP-ILX-ephemeral\_auth-current.tgz in /var/ilx/workspaces/Common/archive... [OK]  Creating ephemeral\_config data group... [OK]  Creating ephemeral\_LDAP\_Bypass data group... [OK]  Creating ephemeral\_RADIUS\_Bypass data group... [OK]  Creating ephemeral\_radprox\_host\_groups data group... [OK]  Creating ephemeral\_radprox\_radius\_attributes data group... [OK]  Creating ephemeral\_radprox\_radius\_client data group... [OK]  Importing WebSSH2 Workspace... [OK]  Importing Ephemeral Authentication Workspace... [OK]  Modifying Ephemeral Authentication Workspace... [OK]  Creating WEBSSH Proxy Service Virtual Server... [OK]  Creating tmm route for Plugin... [OK]  Installing webssh tmm vip startup script... [OK]  Creating WebSSH2 Plugin... [OK]  Creating Ephemeral Authentication Plugin... [OK]  Creating RADIUS Proxy Service Virtual Server... [OK]  Creating LDAP Proxy Service Virtual Server... [OK]  Creating LDAPS (ssl) Proxy Service Virtual Server... [OK]  Creating APM connectivity profile... [OK]  Checking for profile-pua\_webtop\_policy.conf.tar.gz... [OK]  Hash check for profile-pua\_webtop\_policy.conf.tar.gz [OK]  Importing APM sample profile profile-pua\_webtop\_policy.conf.tar.gz [OK]  Modifying pua APM Portal Resource...[OK]  Applying pua APM Policy...[OK]  Creating Webtop Virtual Server... [OK]  RADIUS Testing Option  =====================  ... Do you want to configure this BIG-IP to authenticate against itself for testing purposes (y/N)? **y**    Are you really sure!? (y/N)? **y**  Modifying BIG-IP for RADIUS authentication against itself... [OK]  You can test WebSSH2 and Ephemeral authentication without APM configuration now  by browsing to:  **https://192.168.20.62:2222/ssh/host/192.168.30.205**    username: testuser    password: anypassword  This will allow anyone using the username testuser to log in with any password  as a guest  Saving config... [OK]  You can test your new APM webtop now by browsing to:  **https://192.168.20.63**    username: <any>    password: <any> |

# Validation

## WebSSH2 Client

1. Open a web browser and navigate to the first URL given by the script.   
   example: **https://192.168.20.62:2222/ssh/host/192.168.30.205**
2. Enter the username **testuser** with any password and click login  
   
3. You should be greeted with a tmsh prompt to the BIG-IP the script was installed on, logged in as the user ***testuser***.  
   

## APM Policy and Portal Mode

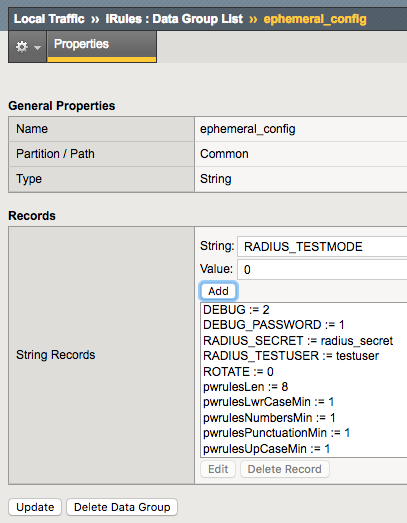
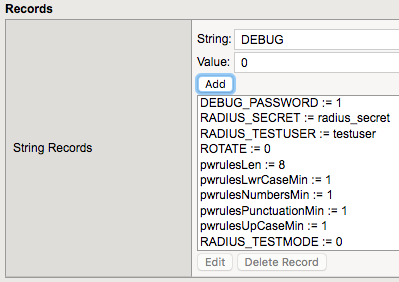
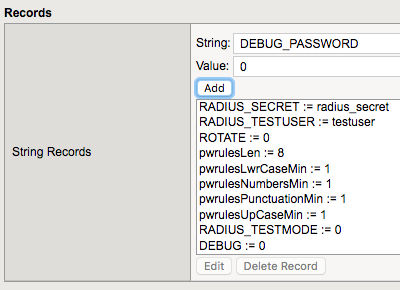
1. Open a web browser and navigate to the second URL given by the script.   
   example: [**https://192.168.20.63**](https://192.168.20.63)
2. The sample USG Warning and Consent Banner should appear, click **OK**
3. Enter a random username other than *testuser* and any password. Click **Logon**.  
   
4. You should be directed to the webtop, click the **WebSSH Portal** icon.  
   
5. You should be presented with another WebSSH2 screen, logged into the BIG-IP the script was installed on as the user you provided in step 3. 

# Production Considerations

The solution enables test accounts to ensure all components are configured correctly as well as additional debug messages, these should be disabled on production systems.

You may prevent the creation of these test accounts as well as additional debug messages from the start by utilizing the ***pua\_config.sh*** script and setting ***disabletest=”y”***. Otherwise follow the instructions outlined in [Disable Test Accounts and Debug](#_Disable_Test_Accounts).

## Disable Test Accounts and Debug

1. Navigate to **Local Traffic > iRules > Data Group List**
2. Click **ephemeral\_config**
3. Find and select **RADIUS\_TESTMODE** and click **Edit**
4. Under **Value**, enter **0** and click **Add**
5. Find and select **DEBUG** and click **Edit**
6. Under **Value**, enter **0** and click **Add**
7. Find and select **DEBUG\_PASSWORD** and click **Edit**
8. Under **Value**, enter **0** and click **Add**  
   
9. Click **Update**

Test accounts and additional debug messages are now disabled on the system. You will need to cause the pua\_webtop virtual server to trigger RULE\_INIT in order to reload this configuration.