Deploying the F5 BIG-IP with Privileged User Access

Welcome to the F5 deployment guide for Privileged User Access (PUA). This document contains guidance on configuring the BIG-IP system version 13.1 and later for F5 PUA implementations, resulting in a secure, fast, and available deployment. This guide shows how to quickly and easily configure the BIG-IP system using the scripted deployment template.

Why F5 PUA?

The F5 Privileged User Access solution now provides an approved way to add CAC/PKI authentication or other strong authentication methods to network infrastructure and systems that do not natively support this functionality. It does this without requiring the addition of client software or agents anywhere in the environment and allows you to fully leverage your legacy or non-compliant systems in a safe and secure manner. It integrates directly into DoD PKI or MFA systems and may be configured to work cooperatively with existing TACACS, Active Directory, AAA servers, or a variety of third-party authentication databases. F5 PUA is DoD CIO approved as an Identify Federation Service (IFS) for facilitating both privileged and unprivileged user authentication to unclassified and secret fabric DoD Information Systems.

IFS are third-party intermediary services facilitating user-authentication to resources or relying parties. IFS may be used when a system or application does not support direct authentication with PKI or MFA credentials, or the system owner desires a single management framework for a group of heterogeneous systems.

F5 Certifications

- DoD UC APL
- FIPS 140-2 Validated - Leve 1, 2, or 3 depending on platform selection. F5 offers software (VE), F5 Full-Box FIPS platforms, integrated (HSM PCI Card), and external (Network HSM) FIPS solutions
- Common Criteria Certification
- NSA Commercial Solutions for Classified (CSfC) Components List
- DISA/JITC PKE (public key enabled)
- United States Government IPv6 Conformance Certification (USGv6)

Prerequisites and Deployment Notes

Platform Requirements

- F5 BIG-IP with TMOS v13.1.0.2 or greater
- LTM, APM, and iRules LX licensed and provisioned
- F5 PUA platform and device licenses

BIG-IP Components

The Privileged User Authentication (PUA) solution is made up of three parts on the BIG-IP. These are included in the PUA platform licensing:

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

Prerequisites

- 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
- 1-5 IP addresses for virtual servers (see Resource Table)
- **UPDATE**: It is no longer required for the WebSSH2 VIP to have a dedicated IP address as in previous versions.

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**

Resource Table

Use the following table to plan your deployment

Resource	**Description**	**Value**
WebSSH_proxy_vs_IP	Virtual server IP Address of WebSSH2 service.	
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)
    a. 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
```

3. Run **build_pua.sh**
    a. If running a fully automated script, skip to Validation
4. Answer the questions when prompted
    a. 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.cilVBvwwpN... [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)
    a. 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
```

3. Run **build_pua_offline.sh**
    a. If running a fully automated script, skip to Validation
4. Answer the questions when prompted
    a. 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:

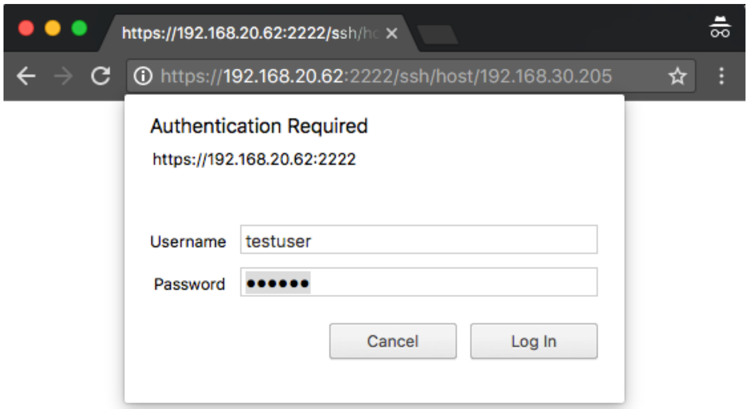
https://192.168.20.63

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


https://192.168.20.62:2222/ssh/h
https://192.168.20.62:2222/ssh/host/192.168.30.205
Cancel
Log In

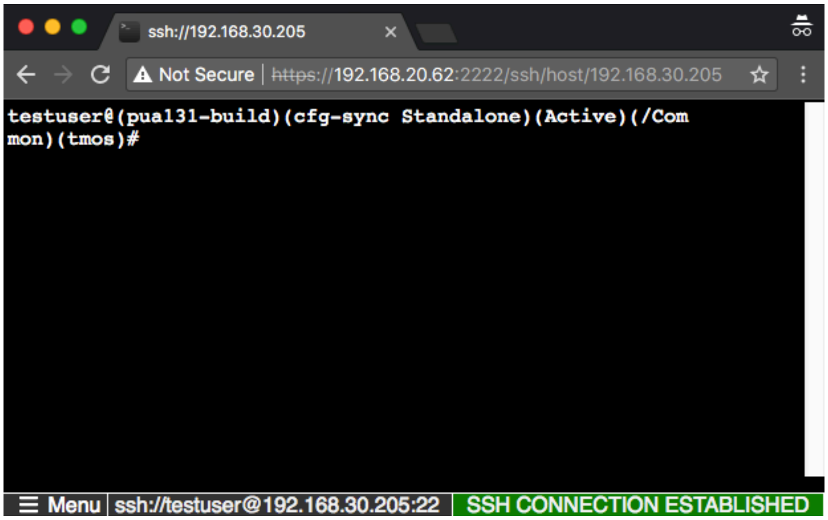
Authentication Required

https://192.168.20.62:2222

Username testuser

Password ••••••

3. You should be greeted with a tmsh prompt to the BIG-IP the script was installed on, logged in as the user ***testuser***.


ssh://192.168.30.205
Not Secure | ~~https~~://192.168.20.62:2222/ssh/host/192.168.30.205
☰ Menu

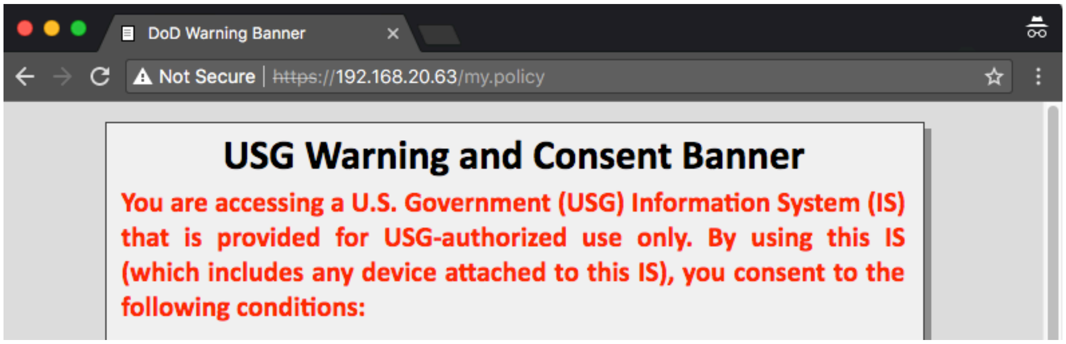
```
testuser@(pua131-build)(cfg-sync Standalone)(Active)(/Com
mon)(tmos)#
```

ssh://testuser@192.168.30.205:22 | SSH CONNECTION ESTABLISHED

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

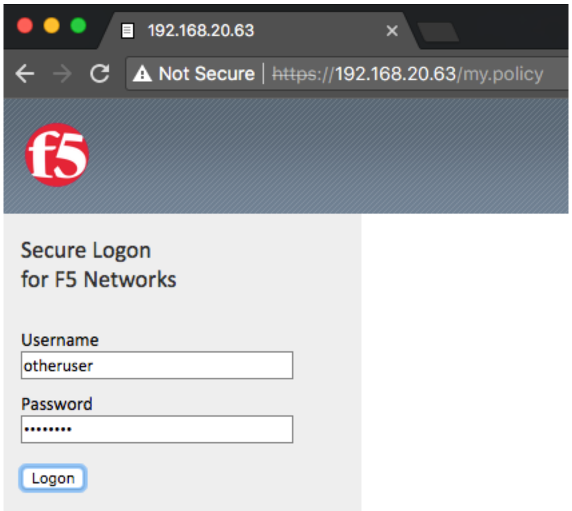
2. The sample USG Warning and Consent Banner should appear, click **OK**



USG Warning and Consent Banner

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

3. Enter a random username other than *testuser* and any password. Click **Logon**.

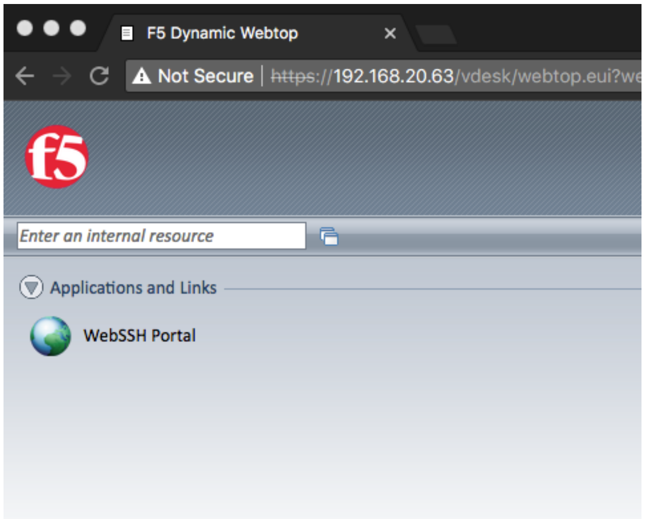


Secure Logon
for F5 Networks

Username: otheruser

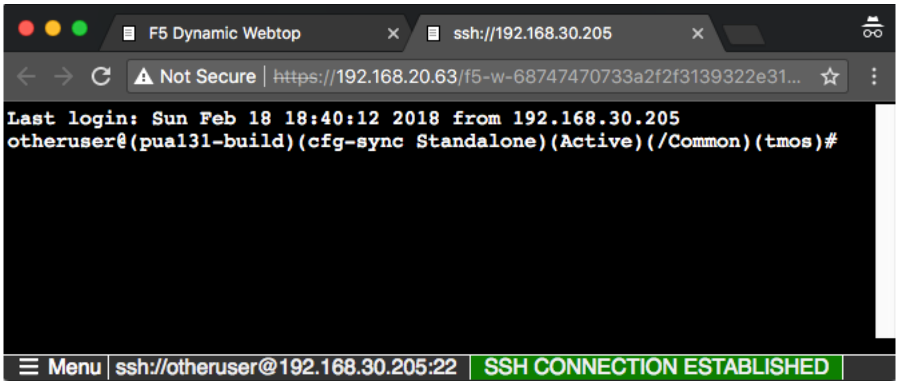
Password: ••••••••

4. You should be directed to the webtop, click the **WebSSH Portal** icon.



F5 Dynamic Webtop
Not Secure | https://192.168.20.63/vdesk/webtop.eui?we
Enter an internal resource
Applications and Links
WebSSH Portal

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.


F5 Dynamic Webtop
ssh://192.168.30.205
Not Secure | https://192.168.20.63/f5-w-68747470733a2f2f3139322e31...
☰ Menu | ssh://otheruser@192.168.30.205:22
SSH CONNECTION ESTABLISHED

```
Last login: Sun Feb 18 18:40:12 2018 from 192.168.30.205
otheruser@(pua131-build)(cfg-sync Standalone)(Active)(/Common)(tmos)#
```

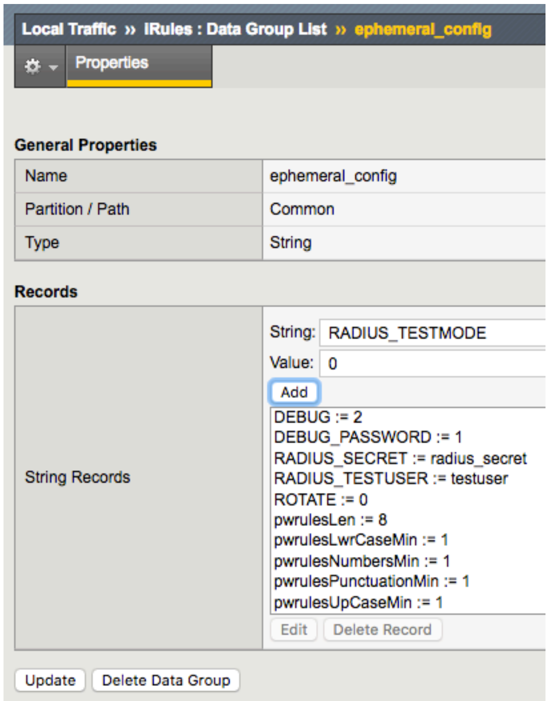
Production Considerations

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 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**



Local Traffic » iRules : Data Group List » ephemeral_config

General Properties

Name	ephemeral_config
Partition / Path	Common
Type	String

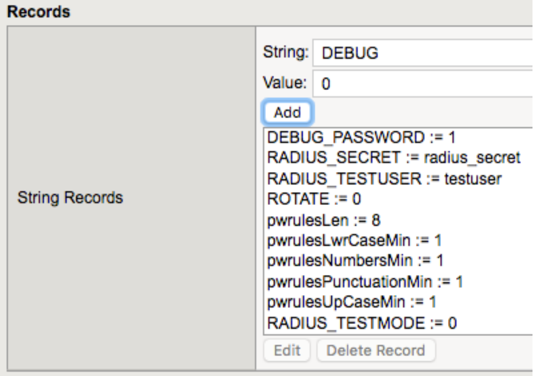
Records

String Records

String: RADIUS_TESTMODE
Value: 0

```
DEBUG := 2
DEBUG_PASSWORD := 1
RADIUS_SECRET := radius_secret
RADIUS_TESTUSER := testuser
ROTATE := 0
pwrulesLen := 8
pwrulesLwrCaseMin := 1
pwrulesNumbersMin := 1
pwrulesPunctuationMin := 1
pwrulesUpCaseMin := 1
```

5. Find and select **DEBUG** and click **Edit**
6. Under **Value**, enter **0** and click **Add**



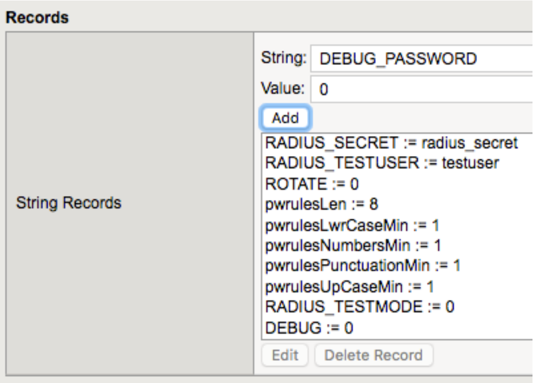
Records

String Records

String: DEBUG
Value: 0

```
DEBUG_PASSWORD := 1
RADIUS_SECRET := radius_secret
RADIUS_TESTUSER := testuser
ROTATE := 0
pwrulesLen := 8
pwrulesLwrCaseMin := 1
pwrulesNumbersMin := 1
pwrulesPunctuationMin := 1
pwrulesUpCaseMin := 1
RADIUS_TESTMODE := 0
```

7. Find and select **DEBUG_PASSWORD** and click **Edit**
8. Under **Value**, enter **0** and click **Add**



Records

String Records

String: DEBUG_PASSWORD
Value: 0

```
RADIUS_SECRET := radius_secret
RADIUS_TESTUSER := testuser
ROTATE := 0
pwrulesLen := 8
pwrulesLwrCaseMin := 1
pwrulesNumbersMin := 1
pwrulesPunctuationMin := 1
pwrulesUpCaseMin := 1
RADIUS_TESTMODE := 0
DEBUG := 0
```

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.