Deploying the F5 BIG-IP with Privileged User Access

Welcome to the F5 configuration 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.

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 Configuration 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

- F5 PUA deployed using steps outlined in F5 Privileged User Access Deployment Guide
- Baseline configuring of BIG-IP using F5 Military Deployment Guide and DISA STIGS.
    - (F5 Military Unique Deployment Guide available upon request)
    - (DISA F5 BIP-IP STIGS located here: https://iase.disa.mil/stigs/Pages/a-z.aspx)
- Existing PKI infrastructure or MFA infrastructure (ex: RSA, Yubikey, Okta)
- Optional: Existing LDAP or AD directory

Additional Configuration Details and Examples

https://github.com/billchurch/f5-pua/issues

F5 Professional Services engagement

It is highly recommended that F5 Professional Services support your PUA deployment. F5 Professional Services provides a full range of consulting services to support you throughout the entire lifecycle of your F5 solution deployment. Our experts can help you architect, implement, maintain, and optimize your solution to support current and future needs. You'll benefit from our broad set of expertise including: application delivery; public, private, and multi-cloud; security; programmability (including iRules and iApps); and automation and orchestration.

F5 Professional Services can help you to review your inventory of applications and systems and to devise a strategy for PUA SSO enablement. While PUA is already integrated with many common applications and systems, each environment is unique and often requires a level of customization and integration.

Sample F5 PUA Professional Services Engagement Summary

This example outline of an F5 Professional Services PUA customer engagement provides an of the typical role of F5 Professional Services during a PUA deployment please review.

1. Review Customer requirements for F5 Privileged User Access and configure the in-scope BIG-IP platforms for PUA functionality.
    a. Review server-side requirements and pre-requisites to implement PUA. Please note the following:
    b. Review Customer requirements for PUA functionality. The known high-level requirements are specified below:
        i. BIG-IP APM based access control to specified resources using CAC/PIV.
        ii. BIG-IP APM Webtop providing access to multiple non-F5 server administrative console, including:
            1. Multiple HTTP/HTTPS and/or SSH web-based management consoles, known to include the following systems and administrative console access protocol/s:
                a. Storage Systems
                b. Network and Related Systems:
                c. Other Infrastructure:
                    i. Red Hat 6.0 Linux: SSH and SCP
                    ii. CentOS 6.0 Linux: SSH and SCP
                    iii. Dell R-Series iDRAC: HTTP/HTTPS
                    iv. Fidelis Command Post: HTTP/HTTPS
                    v. Fidelis Sensor: HTTP/HTTPS
                    vi. Fidelis XPS Mail Sensor: HTTP/HTTPS
                    vii. Palo Alto NGFW: HTTPS/SSH

iii. BIG-IP APM and iRules/iRulesLX based PUA & Ephemeral authentication server authentication functionality (for Server authentication)

1. RADIUS and AD/LDAP

iv. Configure APM Access policy and associated objects on each of the BIG-IP platforms.

1. AAA Authentication Servers to support AD/LDAP based authorization.

a. Authorization requirements are known to include OCSP revocation lookup and AD based authorization based on group membership,

v. Includes configuration of required Single Sign On (SSO) profiles

c. Advise Customer on changes required to non-F5 server systems.

d. Assist with the implementation of F5 PUA in Customer environment.

Configuration Tasks

Configuration per F5 Military Unique Deployment Guide and DISA STIGs

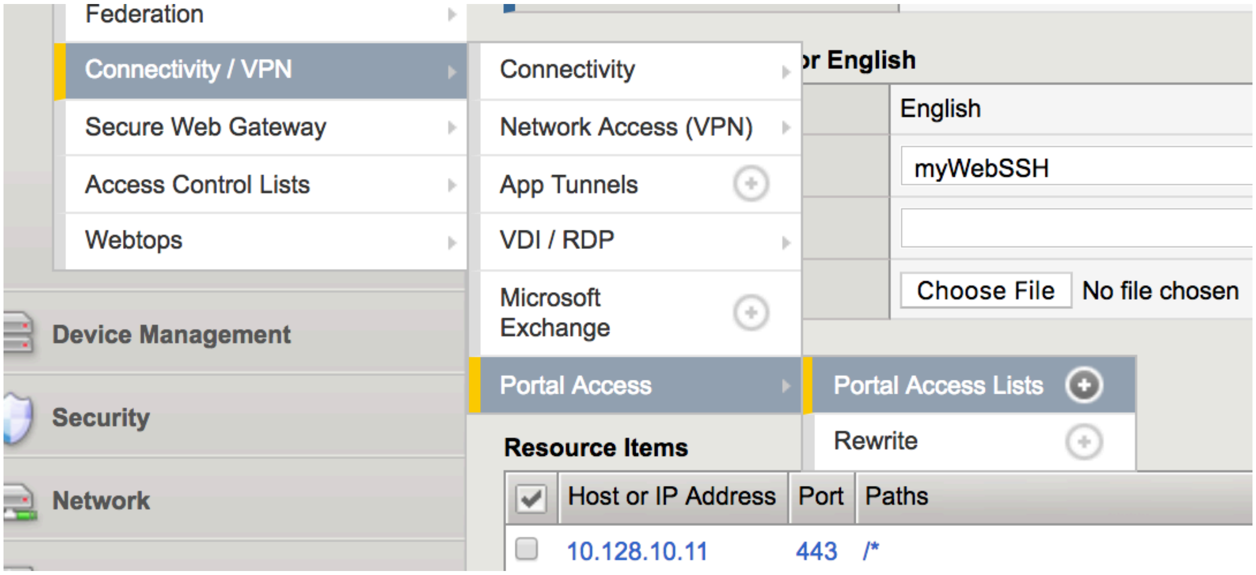
Note: F5 Military Unique Deployment Guide available upon request.

Configuration per DISA F5 PKE Reference Guide or per F5 MFA integration documentation

Note: F5 Networks BIG-IP Authentication Proxy: Public Key Enabling Reference Guide available here: https://powhatan.iiie.disa.mil/pki-pke/landing_pages/downloads/unclass-rg_f5_bigip_authent_proxy_v1-0.pdf

Updating the Ephemeral Auth plugin and Adding Webtop Resources

1. Create a portal access list item. Navigate to Access/Connectivity VPN/Portal Access/Portal Access Lists



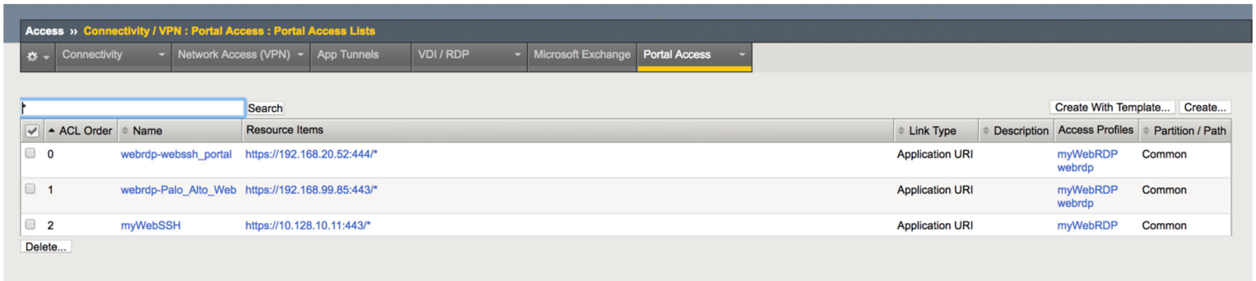
English

myWebSSH

Resource Items

☑	Host or IP Address	Port	Paths
□	10.128.10.11	443	/*

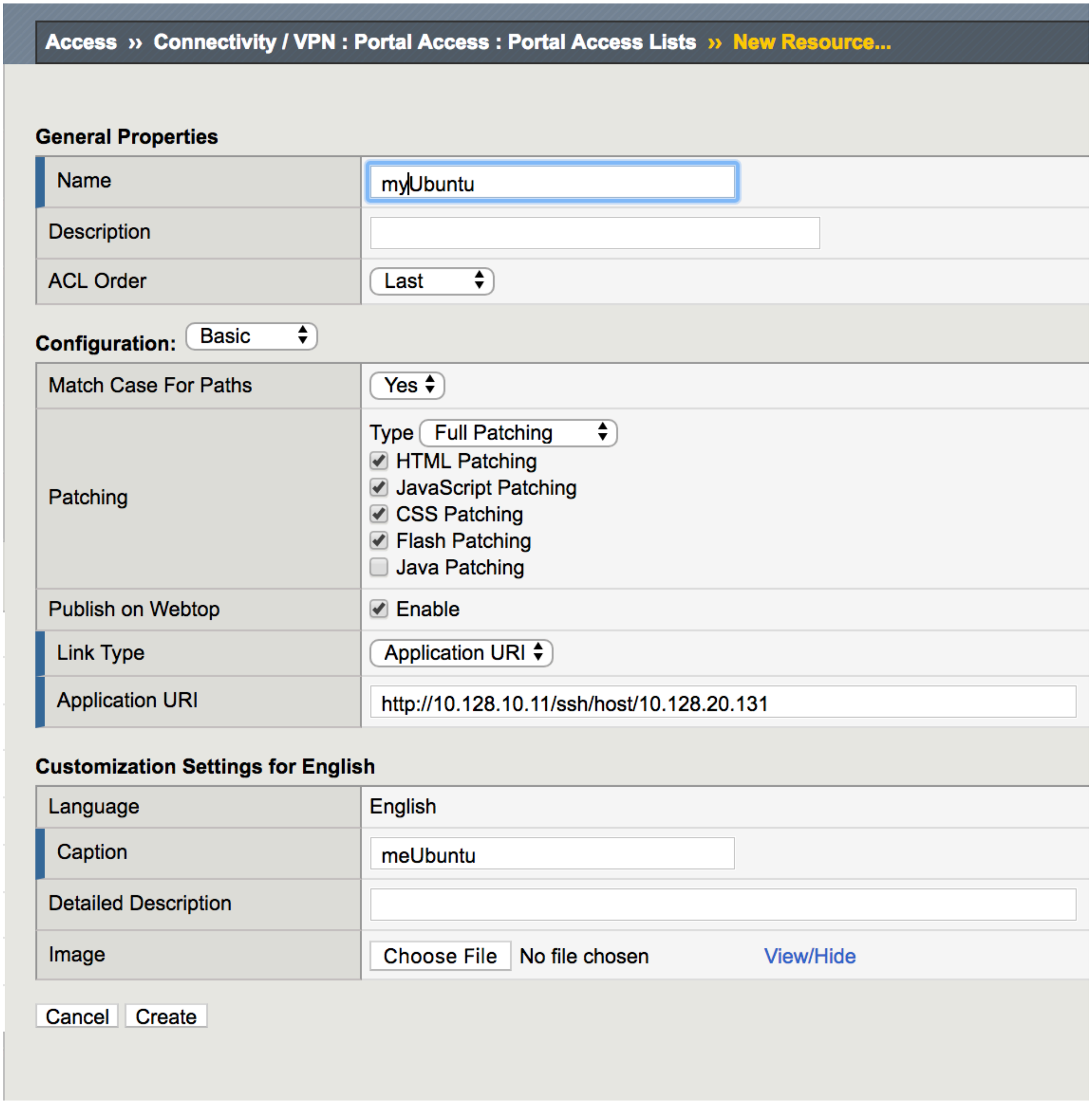
2. Click the Create button



☑	ACL Order	Name	Resource Items	Link Type	Description	Access Profiles	Partition / Path
□	0	webrdp-webssh_portal	https://192.168.20.52:444/*	Application URI		myWebRDP webrdp	Common
□	1	webrdp-Palo_Alto_Web	https://192.168.99.85:443/*	Application URI		myWebRDP webrdp	Common
□	2	myWebSSH	https://10.128.10.11:443/*	Application URI		myWebRDP	Common

3. Create a Portal Resource Item for your SSH/Switch/Router/Device etc.
    a. Name: Your choice
    b. Type: Full Patching
    c. Link Type: Application
    d. Application URI: https://10.128.10.11/ssh/host/<yoursshserveripaddress>
    e. Caption: Your Choice
    f. Resource Items: <yourvip>
    g. Image: Nothing will produce a default image. but this can be customized to include an image icon of your choice.

For more information on portal resource configuration see https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-portal-access-13-1-0/4.html



Access » Connectivity / VPN : Portal Access : Portal Access Lists » New Resource...

General Properties

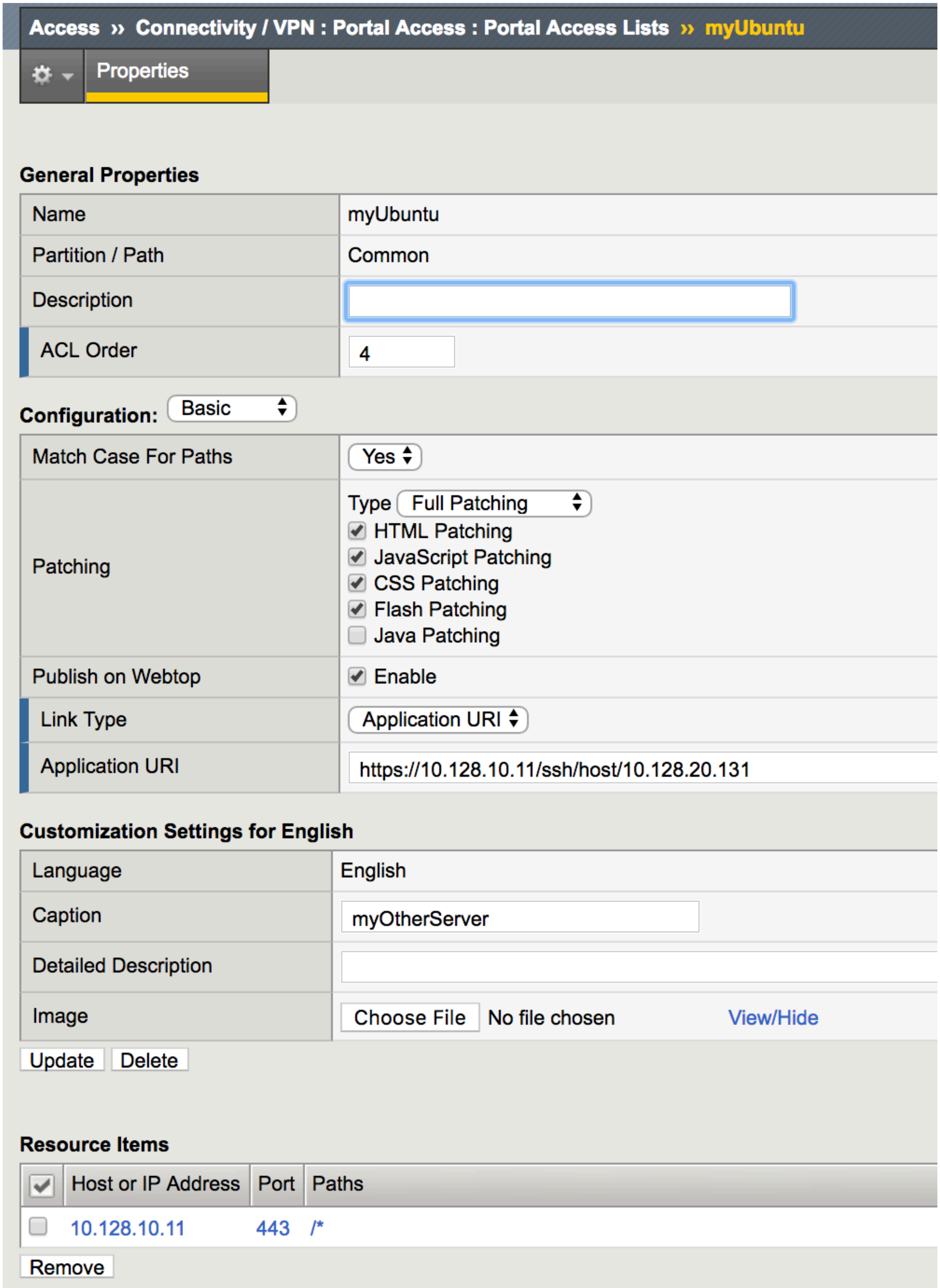
Name	myUbuntu
Description	
ACL Order	Last

Configuration: Basic

Match Case For Paths	Yes
Patching	Type Full Patching ☑ HTML Patching ☑ JavaScript Patching ☑ CSS Patching ☑ Flash Patching ☐ Java Patching
Publish on Webtop	☑ Enable
Link Type	Application URI
Application URI	http://10.128.10.11/ssh/host/10.128.20.131

Customization Settings for English

Language	English
Caption	meUbuntu
Detailed Description	
Image	Choose File No file chosen View/Hide



Access » Connectivity / VPN : Portal Access : Portal Access Lists » myUbuntu

General Properties

Name	myUbuntu
Partition / Path	Common
Description	
ACL Order	4

Configuration: Basic

Match Case For Paths	Yes
Patching	Type Full Patching ☑ HTML Patching ☑ JavaScript Patching ☑ CSS Patching ☑ Flash Patching □ Java Patching
Publish on Webtop	☑ Enable
Link Type	Application URI
Application URI	https://10.128.10.11/ssh/host/10.128.20.131

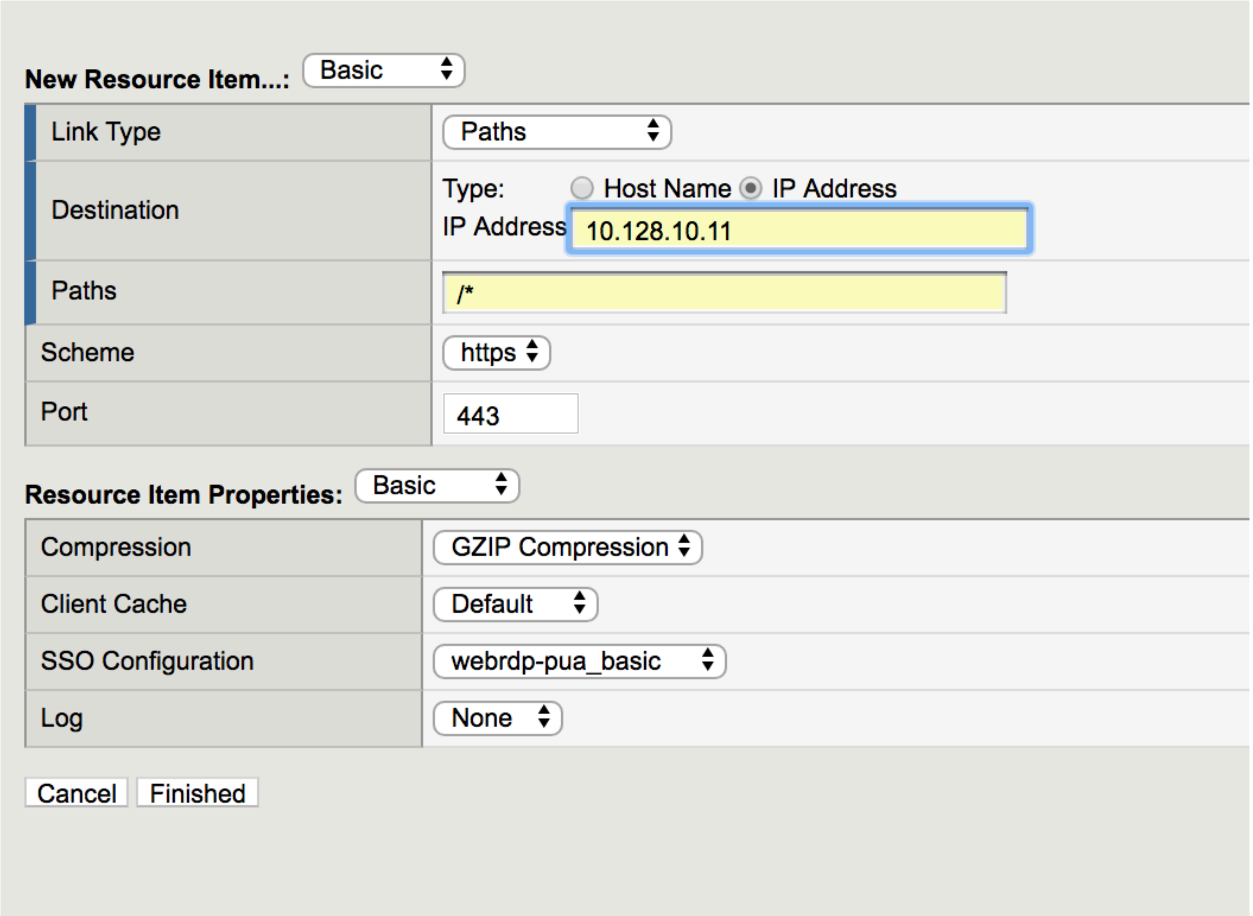
Customization Settings for English

Language	English
Caption	myOtherServer
Detailed Description	
Image	Choose File No file chosen View/Hide

Resource Items

☑	Host or IP Address	Port	Paths
□	10.128.10.11	443	/*

4. Create a portal Resource Item
   a. Link Type: Paths
   b. Destination: Host Name or IP – for host name to function correctly the BIG-IP must be able to correctly resolve the back-end device host name.
   c. Paths: /*
   d. Scheme:https
   e. SSO Configuration: The relevant SSO configuration for your PUA deployment.
   f. Click “Finished”



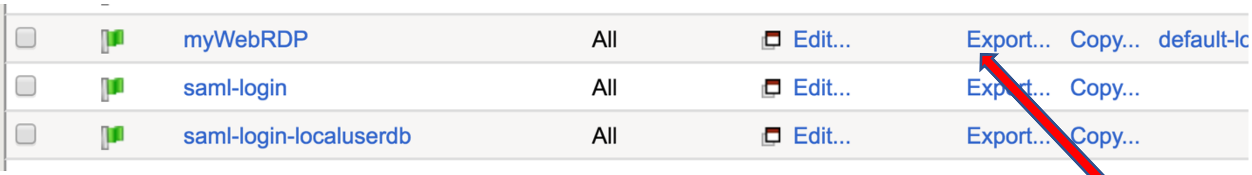
New Resource Item...: Basic

Link Type	Paths
Destination	Type: ○ Host Name ● IP Address IP Address 10.128.10.11
Paths	/*
Scheme	https
Port	443

Resource Item Properties: Basic

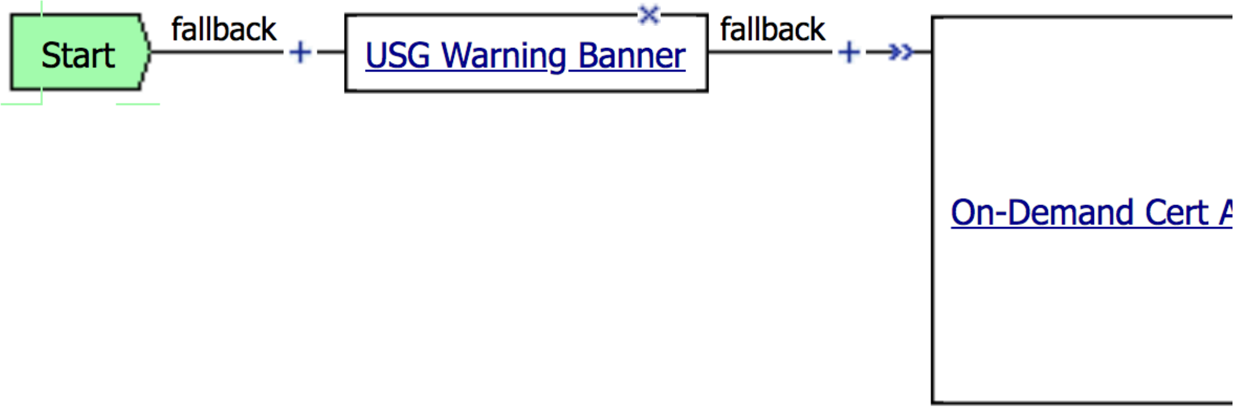
Compression	GZIP Compression
Client Cache	Default
SSO Configuration	webrdp-pua_basic
Log	None

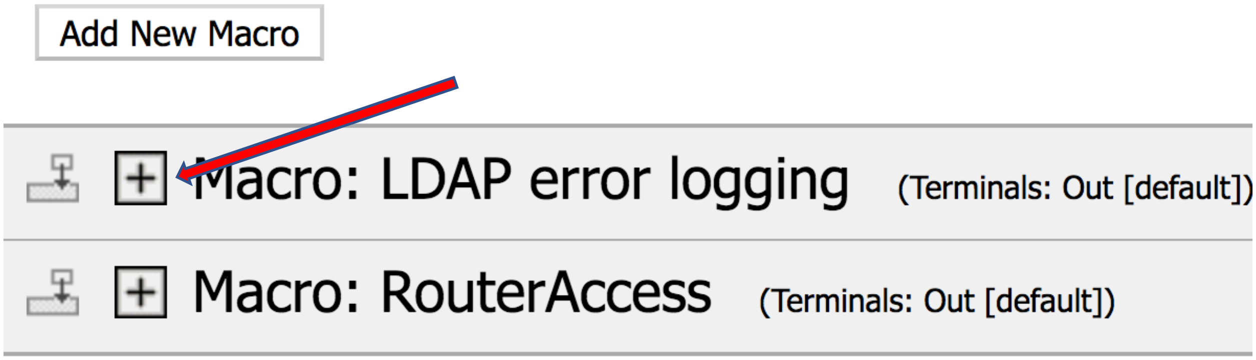
5. Add your new resource item to the webtop.
   a. Navigate to **Access** ›› **Profiles / Policies : Access Profiles (Per-Session Policies)**
   b. Click the "Edit button" under "Per Session Policy" next to your access policy



☐	myWebRDP	All	Edit...	Export...	Copy...	default-lo
☐	saml-login	All	Edit...	Export...	Copy...	
☐	saml-login-localuserdb	All	Edit...	Export...	Copy...	

   c. Your access policy will be displayed.
   d. Click the "+" button next to the Router Access macro



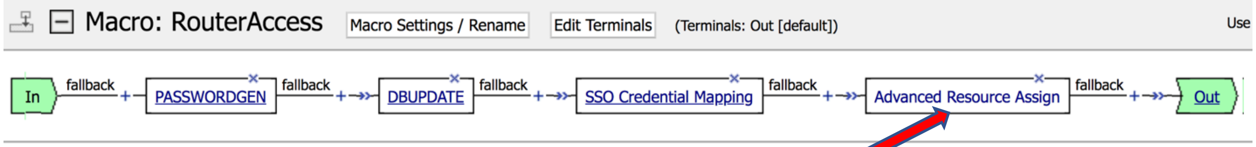


Add New Macro

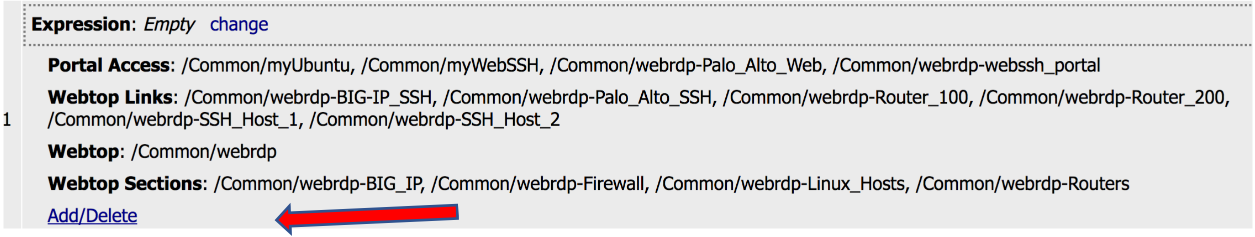
Macro: LDAP error logging (Terminals: Out [default])

Macro: RouterAccess (Terminals: Out [default])

e. Click the “Advanced resource Assign item.



f. Click the “Add/Delete” button



Expression: *Empty* change

1

Portal Access: /Common/myUbuntu, /Common/myWebSSH, /Common/webrdp-Palo_Alto_Web, /Common/webrdp-webssh_portal

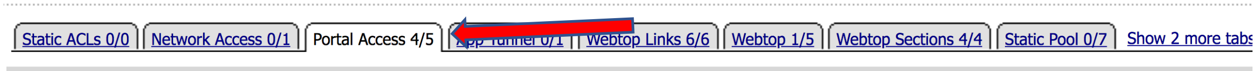
Webtop Links: /Common/webrdp-BIG-IP_SSH, /Common/webrdp-Palo_Alto_SSH, /Common/webrdp-Router_100, /Common/webrdp-Router_200, /Common/webrdp-SSH_Host_1, /Common/webrdp-SSH_Host_2

Webtop: /Common/webrdp

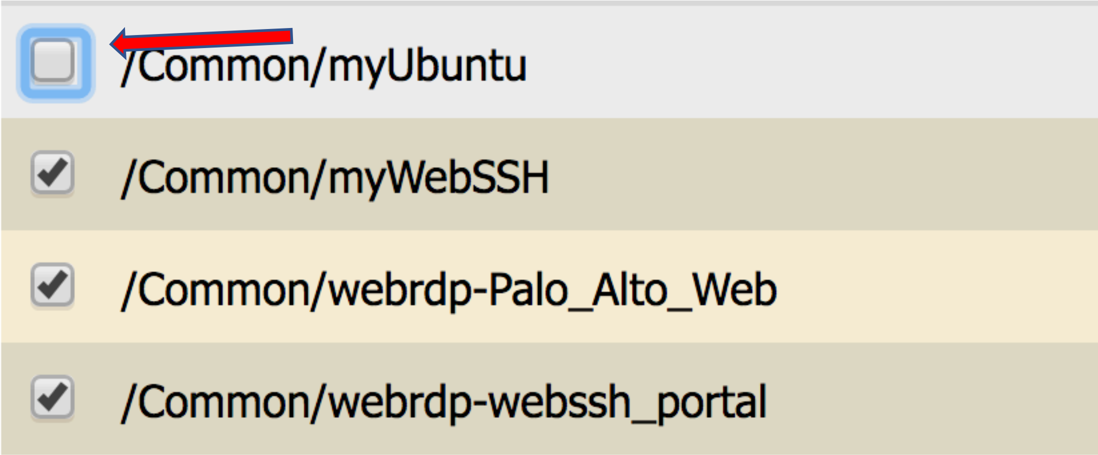
Webtop Sections: /Common/webrdp-BIG_IP, /Common/webrdp-Firewall, /Common/webrdp-Linux_Hosts, /Common/webrdp-Routers

Add/Delete

g. Click the Portal Access Tab



h. Check the radio button for you new item



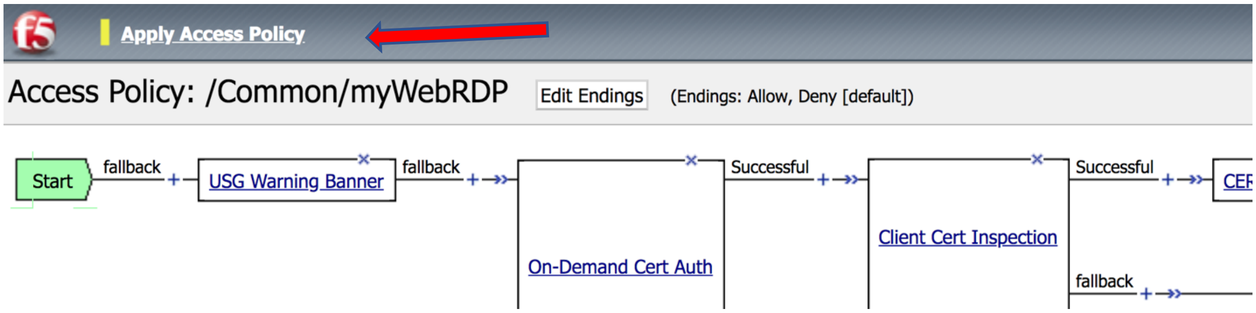
☐ /Common/myUbuntu

☑ /Common/myWebSSH

☑ /Common/webrdp-Palo_Alto_Web

☑ /Common/webrdp-webssh_portal

6. Apply the access Policy



7. Make the requisite changes on your device to point your device at the BIG-IP radius VIP for PUA. Note that each device will be different.

In this example I used an ubuntu server. the instructions for setting up PAM radius can easily be found on the internet. The following set of instructions were used and worked for Ubuntu in my case

Enabling Linux PAM RADIUS Auth
sudo apt-get install libpam-radius-auth
sudo vim /etc/pam_radius_auth.conf
Comment out other Radius server pointing to localhost
Add our own Radius server (tab separated) and give us 30 seconds to return a response
10.1.1.1:1812   this_password_should_be_30_plus_chars_long   30
sudo vim /etc/pam.d/sshd
add the following line:
auth sufficient pam_radius_auth.so
above already existing line
@include common-auth
sudo vim /etc/ssh/sshd_config
uncomment or add:
ChallengeResponseAuthentication yes
restart ssh
sudo service ssh restart or pkill -HUP ssh

Note: The Radius password in radius_auth.conf must match the shared secret that has been configured in PUA.

The following creates a user
Create user for linux (No Password) that matches a valid user
useradd -m <youruser>

You can see if authentication is working on the server by tailing the auth log.
tail -f /var/log/auth.log

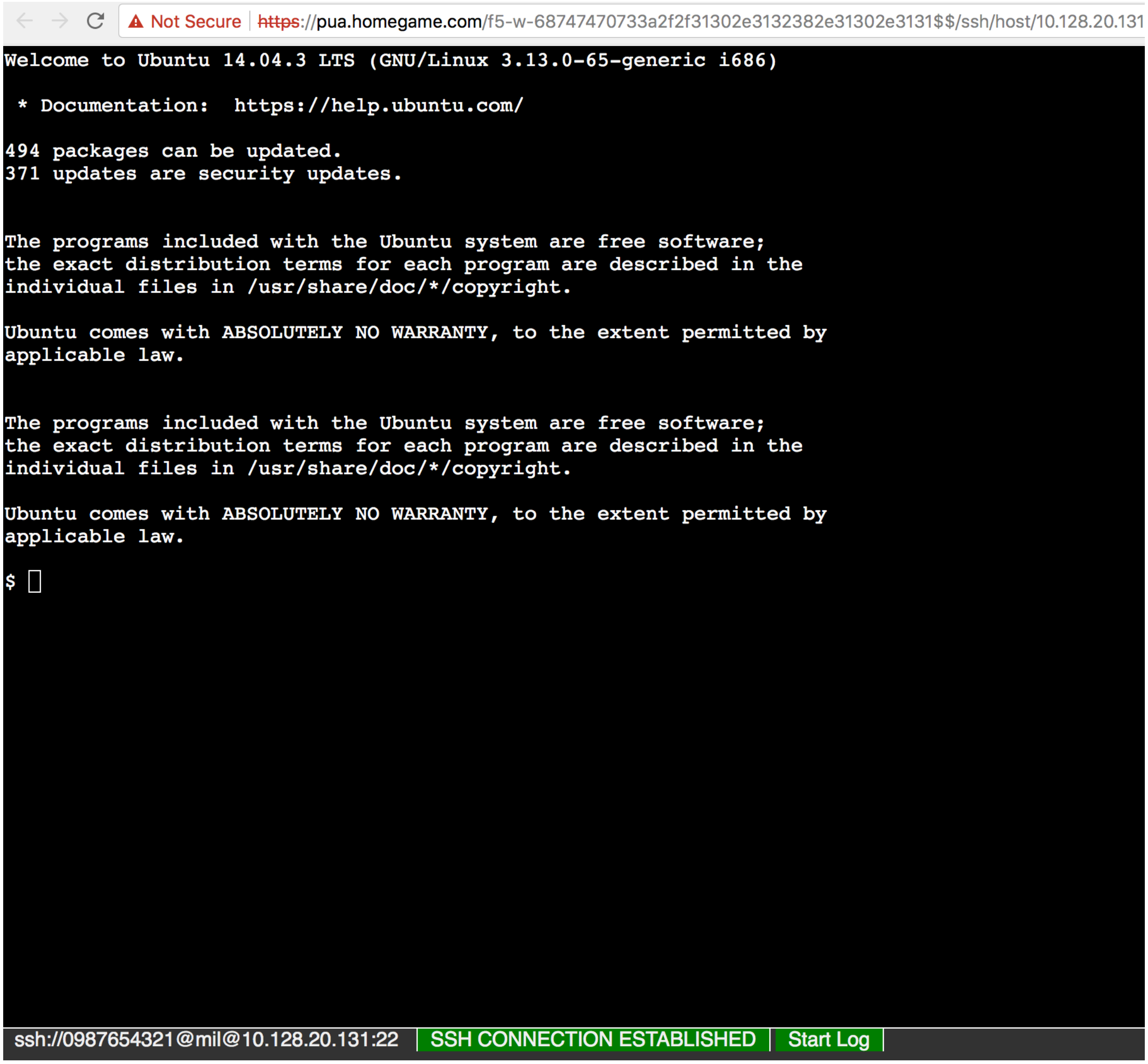
Also, when you are running a test and you want to see that radius packets are being sent from the server to the Radius VIP on the BIG-IP you can

>tail -f /var/log/apm (to see what is happening on the BIG-IP)

Or a simple tcpdump … note you can leave off the port number. radius auth sometimes happens from different port numbers depending upon the device that you are configuring to use PUA>

- Tcpdump -nni 0.0 host <ipofradiusviponBIG-IP> port 1812

8. Test.
   a. Navigate to your PUA URL
   b. Authenticate
   c. You should see your new portal access resource
   d. Click on it… and you should be signed in.



Not Secure | https://pua.homegame.com/f5-w-68747470733a2f2f31302e3132382e31302e3131$$/ssh/host/10.128.20.131

```
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.13.0-65-generic i686)

 * Documentation:  https://help.ubuntu.com/

494 packages can be updated.
371 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ 
```

```
ssh://0987654321@mil@10.128.20.131:22 | SSH CONNECTION ESTABLISHED | Start Log
```

Note: If you are adding hundreds of items this can be scripted.