F5 Privileged User Access (PUA) BIG-IP Configuration Guide

Install Guide for TMOS v13.1.1.4 and PUA build\_pua-1.1.2

Contents

Provision and Configure Initial BIG-IP system 3

Configure Traffic Management Operating System (TMOS) STIG Compliant Settings 4

PUA Installation Introduction 7

Requirements 7

Prerequisites 7

PUA Resource Table 7

PUA Installation 8

Offline Installation Method 8

Run Installation Script 8

Production Considerations 14

Disable Test Accounts and Debug 14

Configure Local Traffic Manager, LTM 16

LTM Configuration Resource Table 16

Configure Access Policy Manager, APM 22

Operational Updates 32

Post INSTALL Updates 33

Avocent iRule 34

fidelis\_9\_2\_3\_irule iRule 35

iDRAC8 iRule 36

iDRAC9 iRule 37

USG Warning Banner 39

APM Get UPN FROM CAC 41

## Provision and Configure Initial BIG-IP system

References:

* Manual: BIG-IP System: Initial Configuration <https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-system-initial-configuration-12-0-0.html>
* K12111: Provisioning licensed BIG-IP modules <https://support.f5.com/csp/article/K12111>
* How to License F5 Systems in Closed Circuit Networks (CCNs) <https://secure.f5.com/ccn/programoverview.jsp>
* K42531434: Replacing the Configuration utility's self-signed SSL certificate with a CA-signed SSL certificate <https://support.f5.com/csp/article/K42531434>
* K13205: Configuring the BIG-IP system to resolve DNS hostnames <https://support.f5.com/csp/article/K13205>
* K3122: Using the BIG-IP Configuration utility to add an NTP server <https://support.f5.com/csp/article/K3122>
* K13833: Managing static routes in BIG-IP 11.x - 13.x and BIG-IQ 4.x - 6.x <https://support.f5.com/csp/article/K13833>
* Manual Chapter: Monitoring BIG-IP System Traffic with SNMP <https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-13-1-0/13.html>
* Manual: External Monitoring of BIG-IP Systems: Implementations <https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-13-1-0.html>
* Manual: BIG-IP Virtual Edition 13.1.0 and VMware ESXi: Setup <https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ve-setup-vmware-esxi-13-1-0.html>

Prerequisites:

* Network Firewall rules to allow SSH 22, NTP TCP 123, DNS UDP/TCP 53, AD/LDAP TCP 389/636, Kerberos TCP 88, RADIUS UDP 1645, HTTPS TCP 443
* BIG-IP VE deployed via the F5 Networks ESXi setup guide “Manual: BIG-IP Virtual Edition 13.1.0 and VMware ESXi: Setup”
* BIG-IP base and add-on registration key is available
* VLAN10, self IP address 10.1.1.70, netmask 255.255.255.0 and default gateway 10.1.1.1
* VLAN20, self IP address 10.1.3.70, netmask 255.255.255.0
* VLAN100 management IP address 10.1.10.100 on the management port and netmask 10.1.10.100 and default gateway 10.1.10.1
* DNS server IP address 10.1.1.11
* NTP server IP address 10.1.3.15
* Naming conventions
  + VLANs: uppercase only. Example: VLAN10
  + Self-IP: use the self-ip only: Example: 10.1.80.100

1. From ESXi, at the cli, run the “config” command and change the management IP, subnet and default gateway to 10.1.10.1. The default login is username:admin password:admin. The CLI default login is username:root password:default. You can only login to the cli as root initially.
   1. Reboot the BIG-IP
      1. At the command prompt type reboot and enter.
2. Run the Setup utility by logging in to the TMUI with a web browser at https://10.1.10.100 on the management interface to license and provision the BIG-IP with the applicable modules LTM, APM and iRulesLX all Nominal.
   1. If the BIG-IP does not have network connectivity to the Internet, specifically <https://license.f5.com>, then use the closed circuit network process to license the system. If an authorized removable media device is available, the dossier file can be copied off the system, uploaded to the F5 Networks licensing server and the license file can be copied the same way back to the BIG-IP.
3. Resource Provisioning: Local Traffic (LTM): Nominal; Access Policy (APM): Nominal; iRules Language Extensions (iRulesLX): Nominal. Click Next and the BIG-IP services will restart to provision the additional modules and momentary access to the TMUI will be lost.
4. Once the TMUI is available click Continue.
5. Setup Utility ›› Device Certificates >> Next
6. Host Name: BIGIP1.f5demo.com
7. Time Zone: America/Chicago
8. For the root and admin password fields use the default during setup. username:admin password:admin; username:root password:default
9. Click Next, you will be logged out, log back in with admin.
10. Click Finished to exit the setup utility. The TMUI menus will load on the left side of the TMUI page.
11. Configure VLAN10 and associate it with the interface 1.1 tag 10, Tagging: untagged, self IP address 10.1.1.70, netmask 255.255.255.0. Port Lockdown: allow default
12. Configure VLAN20 and associate it with the interface 1.2 tag 20, Tagging: untagged, self IP address 10.1.3.70, netmask 255.255.255.0. Port Lockdown: allow default
13. Configure default gateway 10.1.1.1
    1. Network ›› Routes >> add
       1. Name: default
       2. Destination: 0.0.0.0
       3. Netmask: 0.0.0.0
       4. Resource: Use Gateway
       5. Gateway Address: 10.1.1.1
14. Configure a static route for avocent
    1. Navigate to Network ›› Routes ›› Create
       1. Name: avocent
       2. Destination: 10.1.3.22 (IP address of the Avocent server)
       3. Netmask: 255.255.255.255
       4. Resource: Use Gateway
       5. Gateway Address: IP Address 10.1.3.1 (VLAN20 gateway)
15. Configure the BIG-IP to resolve DNS names, tmsh modify sys dns name-servers add { 10.1.1.11 10.1.1.12 }, tmsh save sys config. Run tmsh list sys dns name-servers to confirm the changes.
    1. From the CLI run nslookup f5demo.com. Results should be displayed.
16. Configure the BIG-IP to use an NTP server, tmsh modify sys ntp servers add { 10.1.3.15 }, tmsh save sys config. Run tmsh list sys ntp servers to confirm the changes.
    1. From the CLI run ntpq –p. Results should be displayed.

## Configure Traffic Management Operating System (TMOS) STIG Compliant Settings

To configure the BIG-IP to be compliant with applicable DISA STIG guides, run the following commands from the TMSH prompt.

1. Login to the Command Line Interface, CLI, and endure you are at the TMSH shell “admin@(BIGIP1)(cfg-sync Standalone)(Active)(/Common)(tmos)#”
   1. Type tmsh then press enter
2. For each of the following commands, run them individually at the CLI pressing enter after each one.
3. modify sys sshd banner enabled
4. modify sys sshd banner-text "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: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."
5. This command needs to be copied to a nano editor on the system to eliminate Windows hidden characters)
   1. Type q to quit TMSH
   2. Change to the directory: cd /shared
   3. Create the file: touch /shared/ssh\_include.sh
   4. Change the execution bit: Chmod +x /shared/ssh\_include.sh
   5. Run nano /shared/ssh\_include.sh
   6. Copy the below text to the file and save it.
   7. #!/bin/sh

tmsh modify sys sshd include ‘"Protocol 2

MaxAuthTries 3

Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes256-cbc

MACs hmac-sha1,hmac-ripemd160

LoginGraceTime 60

MaxStartups 5"’

* 1. Run the script: ./ssh\_include.sh
  2. Run the command:tmsh list sys sshd include (The changes should be displayed)
  3. Switch to the TMOS shell, type: tmsh then enter

1. modify sys ntp timezone America/Chicago
2. modify sys global-settings gui-security-banner enabled
3. modify sys global-settings gui-security-banner-text "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: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."
4. modify sys db ui.advisory.enabled value true
5. modify sys db ui.advisory.color value RED
6. modify sys db ui.advisory.text value "//F5DEMO SIPR//"
7. modify sys db ui.system.preferences.advancedselection value advanced
8. modify sys db ui.system.preferences.recordsperscreen value 100
9. modify sys db ui.system.preferences.startscreen value network\_map
10. modify sys db ui.users.redirectsuperuserstoauthsummary value true
11. modify sys db dns.cache value enable
12. modify sys httpd auth-pam-dashboard-timeout on
13. modify sys httpd max-clients 10
14. modify sys sshd inactivity-timeout 600
15. modify sys httpd auth-pam-idle-timeout 600
16. modify sys httpd redirect-http-to-https enabled
17. modify sys software update auto-check disabled
18. modify sys software update auto-phonehome disabled
19. modify sys snmp communities delete { comm-public }
20. modify sys daemon-log-settings tmm os-log-level informational
21. modify sys daemon-log-settings tmm ssl-log-level informational
22. modify sys daemon-log-settings mcpd audit all
23. modify sys daemon-log-settings mcpd log-level notice
24. modify auth password-policy expiration-warning 7
25. modify auth password-policy max-duration 90
26. modify auth password-policy max-login-failures 3
27. modify auth password-policy min-duration 1
28. modify auth password-policy minimum-length 8
29. modify auth password-policy password-memory 3
30. modify auth password-policy policy-enforcement enabled
31. modify auth password-policy required-lowercase 2
32. modify auth password-policy required-numeric 2
33. modify auth password-policy required-special 2
34. modify auth password-policy required-uppercase 2
35. modify sys httpd include "FileETag MTime Size"
36. save sys ucs file BIGIP1\_13\_1\_1\_4\_2-26-2020-1103
37. Create an archive System >> Archives >> New Archives
    1. File Name: BIGIP1\_13\_1\_1\_4\_2-26-2020-0649
    2. Passphrase: <known\_password>
    3. Verify Passphrase: <known\_password>
    4. Click Finished

# PUA Installation Introduction

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

* WebSSH2 Client Plugin
* Ephemeral Authentication Plugin
* Access Policy Manager (APM) policy configuration

## Requirements

* BIG-IP with TMOS v13.1.0.2 or greater.
* 1-5 IP addresses for virtual servers (see [Resource Table](#_Resource_Table))
* **UPDATE**: It is no longer required for the WebSSH2 VIP to have a dedicated IP address as in previous versions.

## Prerequisites

* BIG-IP with at least APM and iRules LX licensed and provisioned. This was performed in the BIG-IP initial configuration.
* The “**build\_pua-1.1.2.zip**” installation script.

## PUA Resource Table

Use the following table to plan your deployment

|  |  |  |
| --- | --- | --- |
| **Resource** | **Description** | **Value** |
| WebSSH\_proxy\_vs\_IP | Virtual server IP Address of WebSSH2 service. | 10.1.1.71 |
| APM\_Portal\_vs\_IP | Virtual server IP Address of Webtop APM portal for authentication | 10.1.1.71 |
| RADIUS\_proxy\_vs\_IP | Virtual server IP address of RADIUS proxy service | 10.1.1.72 |
| LDAP\_proxy\_vs\_IP | Virtual server IP address of LDAP proxy service | 10.1.1.72 |
| LDAPS\_proxy\_vs\_IP | Virtual server IP address of LDAPS proxy service | 10.1.1.72 |
| LDAP\_server\_IP | IP Address of site LDAP or AD server (required for LDAP use) | 10.1.1.11:636  10.1.1.12:636 |

# PUA Installation

## Offline Installation Method

This method utilizes the **build\_pua-1.1.2.zip** method to install the PUA solutions from a closed network with limited or no Internet connectivity.

### Run Installation Script

1. SCP **build\_pua-1.1.2.zip** to the BIG-IP /shared directory
   1. Use pscp.exe “pscp.exe build\_pua-1.1.2.zip admin@10.1.10.100:/shared”
2. Unzip **build\_pua-1.1.2.zip**

|  |
| --- |
| [admin@BIGIP1:Active:Standalone] shared # **unzip**  **build\_pua-1.1.2.zip**  Archive:  build\_pua-1.1.2.zip    inflating: build\_pua.sh |

1. Run **build\_pua.sh**
   1. ./build\_pua.sh
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@BIGIP1:Active:Standalone] shared # ./build\_pua.sh  /shared/build\_pua.sh - v1.1.2 on BIG-IP v13.1.1.4  Interactive  F5 Privileged User Authentication Install Script v1.1.2  ========================================================  This script will configure a reference implementation of the F5 Privileged User Authentication solution. The only  requirements are a running and licensed system ("Active"), initial configuration complete (licensed, VLANs, self IPs),  and preferably already provisioned for APM+ILX. The script will check for and can enable it for you if you wish.  You will be prompted for IP addresses for 4 services:  1. Web top - This is the main entry point to the PUA sollution and runs the APM Web Top. This IP may be  shared with other IPs on the BIG-IP system if the protocol or port (tcp/443) do not conflict. This virtual server also  contains the WebSSH (HTTPS to SSH gateway) service  2. RADIUS Proxy - This runs the RADIUS Ephemeral Authentication Service. This IP may be shared with  other IPs on the BIG-IP system if the protocol or port (udp/1812) do not conflict. (radius\_proxy)  3. LDAP Proxy - This runs the LDAP Ephemeral Authentication Service. This IP may be shared with other  IPs on the BIG-IP system if the protocol or port (tcp/389) do not conflict. (ldap\_proxy)  4. LDAPS Proxy - This runs the LDAPS (ssl) Ephemeral Authentication Service. This IP may be shared with  other IPs on the BIG-IP system if the protocol or port (tcp/636) do not conflict. (ldaps\_proxy)  The Web Top and LDAPS services will be initially configured with a default client-ssl profile, after testing this  should be changed to use a legitimate certificate.  A sample APM policy is created and attached to the Web Top virtual server "pua\_webtop", this policy will  need to be built out and tested for the pua\_webtop service to operate correctly.  RADIUS Testing  ==============  The BIG-IP administrative interface can be configured to authenticate against itself for testing. This will allow  "admin" and anyone using the test account "testuser" with ANY password to authenticate as  a guest to the GUI or SSH. If you enable this option, instructions will be provided at the end of this script for  testing.  Press any key to continue, or CTRL-C to cancel.  Preparing environment... [OK]  Changing to /tmp/pua.GFtKmsfXRv... [OK]  Extracting archive... [OK]  Creating UCS archive before-pua-1.1.2-ObST, this will take a moment... [OK]  Adding ILX archive directory... [OK]  Checking modules are provisioned.  Checking apm... [OK]  Checking ilx... [OK]  SUCCESS: All modules provisioned.  Checking for BIG-IP-ILX-WebSSH2-current.tgz... [OK]  Hash check for BIG-IP-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]  Type the IP address of your RADIUS service virtual server  and press ENTER 10.1.1.72  You typed 10.1.1.72, is that correct (Y/n)? y  Checking valid IP... [OK]  Testing IP unused... [OK]  Type the IP address of your LDAP service virtual server  and press ENTER [10.1.1.72]:  You typed 10.1.1.72, is that correct (Y/n)? y  Type the IP address of your LDAPS service virtual server  and press ENTER [10.1.1.72]:  You typed 10.1.1.72, is that correct (Y/n)? y  Type the IP address of your Webtop service virtual server  and press ENTER [10.1.1.72]: 10.1.1.71  You typed 10.1.1.71, is that correct (Y/n)? y  Checking valid IP... [OK]  Testing IP unused... [OK]  Sample Certificate Authority  ============================  A sample CA is available for testing. This should be implemented on non-production systems only.  Would you like to install a sample CA for testing (Y/n)? **n**  **Creating pua\_webtop-clientssl profile... [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]**  **Creating WebSSH2 Workspace... [OK]**  **Extracting BIG-IP-ILX-WebSSH2-current.tgz to /var/ilx/workspaces/Common... [OK]**  **Creating WebSSH2 Plugin... [OK]**  **Importing APM sample profile ... [OK]**  **Modifying pua Web Top Link... [OK]**  **Applying pua APM Policy... [OK]**  **Creating Ephemeral Authentication Workspace... [OK]**  **Extracting BIG-IP-ILX-ephemeral\_auth-current.tgz to /var/ilx/workspaces/Common... [OK]**  **Modifying Ephemeral Authentication Workspace... [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 Webtop Virtual Server... [OK]**  **RADIUS Testing Option**  **=====================**  **You can automatcially configure the BIG-IP for RADIUS authentication against itself for testing purposes. This**  **will allow anyone who uses the userid "test user" to log in as a guest to the BIG-IP or log into any device configured**  **with Ephemeral Authentication. If this is running on a production system, this may impact access and is not**  **recommended. This option is recommended for lab and demo use only.**  **Do you want to configure this BIG-IP to authenticate against itself for testing purposes (Y/n)? n**  **Saving config... [OK]**  **You can test your new APM webtop now by browsing to:**  **https://10.1.1.71**  **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...**  **Install log file at /var/log/f5-pua-install-UGKD.log...** |

Change the RADIUS Virtual Server port

1. Local Traffic ›› Virtual Servers : Virtual Server List ›› radius\_proxy
2. Service Port: 1645

Configure the APM\_ephemeral\_auth file

1. Navigate to Local Traffic ›› iRules : LX Workspaces ›› ephemeral\_auth-0.4.5
   1. Click on APM\_ephemeral\_auth
   2. Replace line 95 with WEBSSO::select /Common/basic\_ephemeral
   3. Save the file.
   4. Click on ldap\_proxy
   5. After line 125 add SSL::disable serverside
   6. Save the file.
   7. Navigate to Local Traffic ›› iRules : LX Plugins ›› ephemeral\_auth\_plugin
   8. Click Reload from Workspace

Configure the config.json file

1. Navigate to Local Traffic ›› iRules : LX Workspaces ›› ephemeral\_auth-0.4.5
2. Click the ephemeral\_auth folder. Click Add extension file named “config.json”. Copy the contents of the config.json.sample to the new config.json file.
3. For the URL modify it to read: ldap://10.1.1.72 (BIG-IP ldap\_proxy VS IP Address)
4. For the adminDN modify it to read: CN=svc.F5DEMO.FF5BIND,OU=Service Accounts,OU=Privileged,OU=SITE\_X,DC=F5DEMO,DC=COM"
5. For the adminPassoword modify it to read the plaintext password of the adminDN account.
6. Save the file and reload the plugin from the workspace.
   1. Local Traffic ›› iRules : LX Plugins ›› WebSSH\_plugin
   2. Click Reload from Workspace.

Configure the list of AD DNs that will bypass the LDAP proxy.

1. Local Traffic ›› iRules : Data Group List ›› ephemeral\_LDAP\_Bypass
2. Delete the existing default groups.
3. Add the following DNs:
   1. String: CN=F5DEMO System Administrators,OU=Groups,OU=Privileged,OU=F5DEMO PMO,DC=F5DEMO,DC=COM Value: <blank>
   2. String: CN=svc.F5DEMO.FF5BIND,OU=Service Accounts,OU=Privileged,OU=TEXAS,DC=F5DEMO,DC=COM Value: <blank>
   3. String: CN=svc.F5DEMO.FFIDELIS,OU=Service Accounts,OU=Privileged,OU=TEXAS,DC=F5DEMO,DC=COM Value: <blank>
   4. String: CN=svc.F5DEMO.FKVM,OU=Service Accounts,OU=Privileged,OU=TEXAS,DC=F5DEMO,DC=COM Value: <blank>
   5. String: CN=svc.F5DEMO.FSAN,OU=Service Accounts,OU=Privileged,OU=TEXAS,DC=F5DEMO,DC=COM Value: <blank>
   6. String: CN=svc.F5DEMO.FiDRAC,OU=Service Accounts,OU=Privileged,OU=TEXAS,DC=F5DEMO,DC=COM Value: <blank>
   7. String: svc.F5DEMO.FF5BIND Value: <blank>
   8. String: svc.F5DEMO.FFIDELIS Value: <blank>

Configure the RADIUS secret for WEBSSH access to the switches and routes

1. Local Traffic ›› iRules : Data Group List ›› ephemeral\_config
2. Modify the RADIUS\_SECRET attribute to the radius attribute shared with the client devices.
3. Add String: RADIUS\_ATTRIBUTE Value: 1 (This enables RADIUS attribues)

Configure the RADIUS proxy clients

1. Local Traffic ›› iRules : Data Group List ›› ephemeral\_radprox\_radius\_client
2. Add all the switches and routers, one entry per device.
   1. String: 10.1.3.xxx value: CISCO

Configure the RADIUS host groups

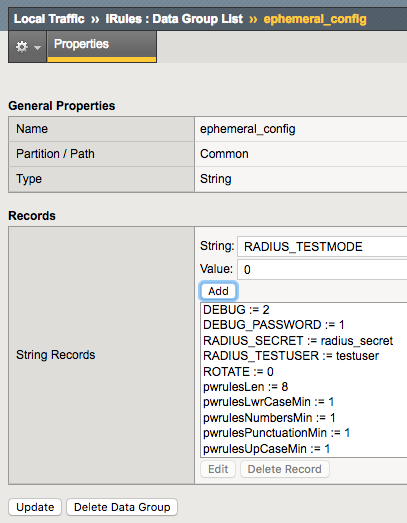
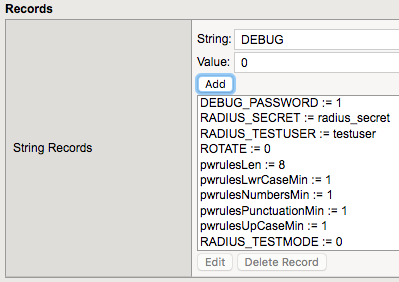
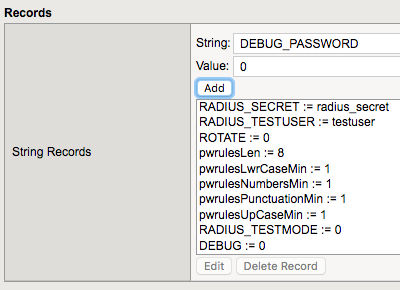
1. Local Traffic ›› iRules : Data Group List ›› ephemeral\_radprox\_host\_groups
2. For each device add the following:
   1. String: 10.1.3.xxx value: CN=F5DEMO System Administrators,OU=Groups,OU=Privileged,OU=F5DEMO PMO,DC=F5DEMO,DC=COM:15

# 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.

## Configure Local Traffic Manager, LTM

References:

* Manual: BIG-IP Local Traffic Management: Basics <https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-basics-13-0-0.html>
* Privileged User Access using 2FA <https://raw.githubusercontent.com/billchurch/f5-pua/master/build_pua_offline.zip>
* Follow the naming conventions for objects should be observed
  + Replace spaces with “\_” the underscore character
  + Virtual Servers
    - Example: pua\_webtop, ldap\_proxy, iDRAC8\_avoke, iDRAC9, iDRAC9\_21
  + Pools
    - Example: LDAP\_Pool, IDRAC9\_21\_pool, avocent\_pool
  + Nodes
    - Example: 10.1.1.xxx

## LTM Configuration Resource Table

Use the following table to plan your deployment

|  |  |  |
| --- | --- | --- |
| **Resource** | **Description** | **Value** |
| avocent | Virtual server IP Address of the avocent service. | 10.1.1.78 |
| Fidelis\_9\_2\_3\_vs | Virtual server IP Address of the Fidelis\_9\_2\_3\_vs service | 10.1.1.79 |
| iDRAC8\_avoke | Virtual server IP address of the iDRAC8\_avoke service | 10.1.1.76 |
| iDRAC8\_owl | Virtual server IP address of the iDRAC8\_owl service | 10.1.1.77 |
| iDRAC9 | Virtual server IP address of the iDRAC9 service | 10.1.1.74 |
| iDRAC9\_21 | Virtual server IP address of the iDRAC9\_21 service | 10.1.1.75 |
| avocent\_pool | Pool member IP address and TCP port of the avocent server | 10.1.3.22:443 |
| fidelis\_9\_2\_3\_pool | Pool member IP address and TCP port of the fidelis\_9\_2\_3 server | 10.1.1.82:443 |
| iDRAC8\_avoke\_pool | Pool member IP address and TCP port of iDRAC8\_avoke server | 10.1.3.23:443 |
| iDRAC8\_owl\_pool | Pool member IP address and TCP port of iDRAC8\_owl server | 10.1.3.24:443 |
| iDRAC\_pool | Pool member IP address and TCP port of iDRAC9 server | 10.1.3.20:443 |
| iDRAC9\_21\_pool | Pool member IP address and TCP port of iDRAC9\_21 server | 10.1.3.21:443 |
| LDAPS\_POOL | Pool member IP address and TCP port of AD servers for the ldaps\_proxy Virtual Server | 10.1.1.11:636  10.1.1.12:636 |
| Fidelis\_CP1 | APM Portal Resource Item IP address and TCP port of Fidelis\_CP1 server | 10.1.1.80:443 |
| Fidelis\_CP2 | APM Portal Resource Item IP address and TCP port of Fidelis\_CP2 server | 10.1.1.81:443 |
| Unity | APM Portal Resource Item IP address and TCP port of Unity server | 10.1.3.51:443 |
| APC\_DLP | APM Portal Resource Item IP address and TCP port of APC\_DLP server | 10.1.1.85:443 |
| JRSS | APM Portal Resource Item IP address and TCP port of JRSS server | 10.1.1.86:443 |
| FCSW1 | APM Webtop Link IP address of FCSW1 device | 10.1.3.101 |
| FCSW2 | APM Webtop Link IP address of FCSW2 device | 10.1.3.102 |
| SW1 | APM Webtop Link IP address of SW1 device | 10.1.3.2 |
| SW2 | APM Webtop Link IP address of SW2 device | 10.1.3.3 |
| Avoke | APM Webtop Link IP address and TCP Port of Avoke server | 10.1.1.15:8081 |

1. Create DoD Certificate Bundle
   1. System ›› Certificate Management : Traffic Certificate Management : SSL Certificate List >> import
   2. Import type: Certificate
   3. Certificate name: DoDBundle
   4. Browse to the DoDBundle file. Click Import.
2. Associate the DoD Certificate Bundle with the pua\_webtop-clientssl profile
   1. Local Traffic ›› Profiles : SSL : Client ›› pua\_webtop-clientssl
   2. Trusted Certificate Authorities: DoDBundle
   3. Advertised Certificate Authorities: DoDBundle
   4. Click Update
3. Create pools
   1. Local Traffic ›› Pools : Pool List >> Create
      1. LDAPS\_POOL
         1. Gateway\_icmp monitor
         2. Load Balancing Method: Round Robin
         3. New Members: 10.1.1.11 and 10.1.1.12 port 636 clicking add after the first node is added then click Finished.
         4. After about 5 seconds the LDAPS\_POOL status should turn green.
         5. Go to Local Traffic ›› Virtual Servers : Virtual Server List ›› ldaps\_proxy >> Resources and set the Default Pool to LDAPS\_POOL
         6. Go to Local Traffic ›› Virtual Servers : Virtual Server List ›› ldap\_proxy >> Resources and set the Default Pool to LDAPS\_POOL. The non-secure LDAP VS proxies traffic to LDAPS on port 636.
         7. SSL Profile (Server): serverssl
         8. Both Virtual Server statuses should turn green.
      2. IDRAC9\_21\_pool
         1. https monitor
         2. Load Balancing Method: Round Robin
         3. Members: 10.1.3.21 port 443, click Add then Finished.
      3. IDRAC\_pool (ESXi1)
         1. https monitor
         2. Load Balancing Method: Round Robin
         3. Members: 10.1.3.20 port 443, click Add then Finished.
      4. Avocent\_pool
         1. https monitor
         2. Load Balancing Method: Round Robin
         3. Members: 10.1.3.22 port 443, click Add then Finished.
      5. fidelis\_9\_2\_3\_pool
         1. https monitor
         2. Load Balancing Method: Round Robin
         3. Members: 10.1.1.82 port 443, click Add then Finished.
      6. iDRAC8\_avoke\_pool
         1. inband monitor
         2. Load Balancing Method: Round Robin
         3. Members: 10.1.3.23 port 443, click Add then Finished.
      7. iDRAC8\_owl\_pool
         1. inband monitor
         2. Load Balancing Method: Round Robin
         3. Members: 10.1.3.24 port 443, click Add then Finished.
      8. All pool statuses should be green.
4. Create HTML Rules
   1. Local Traffic ›› Profiles : Content : HTML : Rules
   2. Create new Raise Event on Tag: Rule name: Body
      1. Match Settings:Match Tag Name: body
   3. Create new Raise Event on Tag: Rule name: fidelis923
      1. Match Settings:Match Tag Name:input, Match Attribute Name:name, Match Attribute Value:submit
   4. Create new Raise Event on Tag: Rule name: Script
      1. Match Settings:Match Tag Name:span, Match Attribute Name:id, Match Attribute Value:span\_dellTech
5. Create HTTP content profiles
   1. Local Traffic ›› Profiles : Content : HTML
   2. Create new profile:avocent
      1. Parent Profile: html
      2. Content-Type Selection: text/html, text/xhtml
      3. HTML Rules: body
   3. Create new profile: fidelis923
      1. Parent Profile: html
      2. Content-Type Selection: text/html, text/xhtml
      3. HTML Rules:fidelis923
   4. Create new profile: idrac
      1. Parent Profile: html
      2. Content-Type Selection: text/html, text/xhtml
      3. HTML Rules:Script
   5. Create new profile: idrac9
      1. Parent Profile: html
      2. Content-Type Selection: text/html, text/xhtml
      3. HTML Rules:body
6. Import custom iRules. The iRules are at the end of this document.
   1. Local Traffic ›› iRules : iRule List
      1. Create new: avocent and copy the avocent iRule code into the definition box and click Finished. Repeat for fidelis\_9\_2\_3\_irule, iDRAC8 and iDRAC9.
7. Create custom Virtual Servers
   1. Local Traffic ›› Virtual Servers : Virtual Server List >> Create
      1. Name: avocent
      2. Destination Address/Mask: 10.1.1.78
      3. Service Port: 443
      4. HTTP Profile: http
      5. SSL Profile (Client): pua\_webtop-clientssl
      6. SSL Profile (Server): serverssl
      7. Source Address Translation: AutoMap
      8. Connection Limit: 10000
      9. Connection Rate Limit: 1000
      10. HTML Profile: avocent
      11. iRules: avocent
      12. Default Pool: avocent\_pool
      13. Click Finished
   2. Local Traffic ›› Virtual Servers : Virtual Server List >> Create
      1. Name: fidelis\_9\_2\_3\_vs
      2. Destination Address/Mask: 10.1.1.79
      3. Service Port: 443
      4. HTTP Profile: http
      5. SSL Profile (Client): pua\_webtop-clientssl
      6. SSL Profile (Server): serverssl
      7. Source Address Translation: AutoMap
      8. Connection Limit: 10000
      9. Connection Rate Limit: 1000
      10. HTML Profile: fidelis923
      11. iRules: fidelis\_9\_2\_3\_irule
      12. Default Pool: fidelis\_9\_2\_3\_pool
      13. Click Finished
   3. Local Traffic ›› Virtual Servers : Virtual Server List >> Create
      1. Name: iDRAC8\_avoke
      2. Destination Address/Mask: 10.1.1.76
      3. Service Port: 443
      4. HTTP Profile: http
      5. SSL Profile (Client): pua\_webtop-clientssl
      6. SSL Profile (Server): serverssl
      7. Source Address Translation: AutoMap
      8. Connection Limit: 10000
      9. Connection Rate Limit: 1000
      10. HTML Profile: idrac
      11. iRules: iDRAC8
      12. Default Pool: iDRAC8\_avoke\_pool
      13. Click Finished
   4. Local Traffic ›› Virtual Servers : Virtual Server List >> Create
      1. Name: iDRAC8\_owl
      2. Destination Address/Mask: 10.1.1.77
      3. Service Port: 443
      4. HTTP Profile: http
      5. SSL Profile (Client): pua\_webtop-clientssl
      6. SSL Profile (Server): serverssl
      7. Source Address Translation: AutoMap
      8. Connection Limit: 10000
      9. Connection Rate Limit: 1000
      10. HTML Profile: idrac
      11. iRules: iDRAC8
      12. Default Pool: iDRAC8\_owl\_pool
      13. Click Finished
   5. Local Traffic ›› Virtual Servers : Virtual Server List >> Create
      1. Name: iDRAC9
      2. Destination Address/Mask: 10.1.1.74
      3. Service Port: 443
      4. HTTP Profile: http
      5. SSL Profile (Client): pua\_webtop-clientssl
      6. SSL Profile (Server): serverssl
      7. Source Address Translation: AutoMap
      8. Connection Limit: 10000
      9. Connection Rate Limit: 1000
      10. HTML Profile: idrac9
      11. iRules: iDRAC9
      12. Default Pool: iDRAC\_pool
      13. Click Finished
   6. Local Traffic ›› Virtual Servers : Virtual Server List >> Create
      1. Name: iDRAC9\_21
      2. Destination Address/Mask: 10.1.1.75
      3. Service Port: 443
      4. HTTP Profile: http
      5. SSL Profile (Client): pua\_webtop-clientssl
      6. SSL Profile (Server): serverssl
      7. Source Address Translation: AutoMap
      8. Connection Limit: 10000
      9. Connection Rate Limit: 1000
      10. HTML Profile: idrac9
      11. iRules: iDRAC9
      12. Default Pool: iDRAC9\_21\_pool
      13. Click Finished
8. Enable PUA Authentication to the Management Interface After the PUA installation
   1. Ensure that there are users in the Active Directory Group CN=F5DEMO System Administrators,OU=Groups,OU=Privileged,OU=F5DEMO PMO,DC=F5DEMO,DC=COM before proceeding.
   2. Enable admin to login to the CLI
   3. Navigate to System ›› Users : User List
      1. Click on admin
      2. Terminal Access: Advanced Shell
      3. Click Update
   4. System ›› Users : Remote Role Groups
      1. Click create
      2. Group Name: Admins
      3. Line Order: 1001
      4. Attribute String: memberOf=CN=F5DEMO System Administrators,OU=Groups,OU=Privileged,OU=F5DEMO PMO,DC=F5DEMO,DC=COM
      5. Remote Access: Enabled
      6. Assigned Role: Administrator
      7. Terminal Access: tmsh
      8. Click Finished
   5. Navigate to System ›› Users : Authentication
      1. Click Change
      2. User Directory: Remote – Active Directory
      3. Host: 10.1.1.72 (This is the ldaps\_proxy Virtual Server IP Address)
      4. Port: 636
      5. Remote Directory Tree: DC=F5DEMO,DC=COM
      6. Scope: Sub
      7. Bind: DN: svc.F5DEMO.FF5BIND
      8. Bind: Password: <new\_ svc.F5DEMO.FF5BIND\_password>
      9. Bind: Confirm: <new\_ svc.F5DEMO.FF5BIND\_password>
      10. SSL: Enabled
      11. SSL CA Certificate: None
      12. SSL Client Key: None
      13. SSL Client Certificate: None
      14. SSL Check Peer: Not Checked
      15. Login Attribute Name: sAMAccountName
      16. Fallback to Local: Check Enabled
      17. Click Finished
      18. Log out and login with an Active Directory user account in the CN=F5DEMO System Administrators,OU=Groups,OU=Privileged,OU=F5DEMO PMO,DC=F5DEMO,DC=COM group.
      19. If the login is unsuccessful, login with admin and look at the /var/log/secure log for the failure.

## Configure Access Policy Manager, APM

References:

* BIG-IP APM 13.1.1 Knowledge Center <https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20APM&version=13.1.1>

1. Create ldap objects
   1. Access ›› Authentication ›› LDAP >> Create
   2. ldap\_aaa
   3. Server Connection: direct
   4. Server Address: 10.1.1.11
   5. Base Search DN: DC=F5DEMO,DC=COM
   6. Admin DN: CN=svc.F5DEMO.FF5BIND,OU=Service Accounts,OU=Privileged,OU=TEXAS,DC=F5DEMO,DC=COM
   7. Admin Password: <svc.F5DEMO.FF5BIND \_password>
   8. Click Finished
   9. Access ›› Authentication ›› LDAP >> Create
   10. ldap\_noncac
   11. Server Connection: direct
   12. Server Address: 10.1.1.11
   13. Base Search DN: DC=F5DEMO,DC=COM
   14. Admin DN: CN=svc.F5DEMO.FF5BIND,OU=Service Accounts,OU=Privileged,OU=TEXAS,DC=F5DEMO,DC=COM
   15. Admin Password: <svc.F5DEMO.FF5BIND \_password>
   16. Click Finished.
2. Create Single Sign-On Objects
   1. Navigate to Access ›› Single Sign-On : Form Based >> Create
      1. Name Fidelis\_SSO
      2. Use SSO Template: None
      3. Start URI: /j/login.html
      4. Form Method: POST
      5. Form Action: /j/login.html
      6. Form Parameter For User Name: j\_username
      7. Form Parameter For Password: j\_password
      8. Click Finished
   2. Navigate to Access ›› Single Sign-On : Form Based >> Create
      1. Name fidelis\_9\_2\_3
      2. Use SSO Template: None
      3. Click the name fidelis\_9\_2\_3
      4. Headers: Accept-Encoding:deflate,gzip ; Referer:https://10.1.1.82 (IP of the fidelis server)
      5. Start URI: /j/login.html
      6. Form Method: POST
      7. Form Action: login
      8. Form Parameter For User Name: username
      9. Form Parameter For Password: password
      10. Click Finished
   3. Navigate to Access ›› Single Sign-On : Forms - Client Initiated >> Create
      1. SSO Configuration Name: unity-ci1
      2. Form Settings: Create
      3. Form Name: frm1
      4. Request Detection: /cas/login
      5. Request Method: Get
      6. Form Identification: Form Parameters
      7. Form Parameters:
         1. password %{session.custom.ephemeral.last.unencryptedpassword} Secure: no
         2. username: %{session.sso.token.last.username} Secure: no
      8. Advanced Settings: Injection method: Custom Javascript Injection

<script>

function \_\_f5submit() {

document.getElementById("password").value = '%{session.custom.ephemeral.last.unencryptedpassword}';

document.getElementById("username").value = '%{session.sso.token.last.username}@f5demo.com';

document.getElementById("submit").click();

}

if (window.addEventListener) {

window.addEventListener('load',\_\_f5submit,false);

} else if (window.attachEvent) {

window.attachEvent('onload',\_\_f5submit);

} else {

window.onload=\_\_f5submit;

}

</script>

* + 1. Click OK, Click OK

1. Create the Portal Access objects.
   1. Access ›› Connectivity / VPN : Portal Access : Portal Access Lists >> create
      1. Name: Fidelis\_CP1
      2. Link Type: Application URI
      3. Application URI: [https://10.1.1.80/](https://172.26.1.80/)
      4. Click Create
      5. Click on Add under Resource Items
      6. Link Type: Paths
      7. Destination: Type: IP Address 10.1.1.80 (IP address of the Fidelis CP1 server)
      8. Paths: /\*
      9. Scheme: https
      10. Port: 443
      11. Compression: No Compression
      12. Client Cache: No Cache
      13. SSO Configuration: Fidelis\_SSO
      14. Session Update: unchecked
      15. Session Timeout: unchecked
      16. Home Tab: unchecked
      17. Log: none.
      18. Click Finished.
   2. Access ›› Connectivity / VPN : Portal Access : Portal Access Lists >> create
      1. Name: Fidelis\_CP2
      2. Link Type: Application URI
      3. Application URI: https://10.1.1.81/
      4. Click Create
      5. Click on Add under Resource Items
      6. Link Type: Paths
      7. Destination: Type: IP Address 10.1.1.81 (IP address of the Fidelis CP2 server)
      8. Paths: /\*
      9. Scheme: https
      10. Port: 443
      11. Compression: No Compression
      12. Client Cache: No Cache
      13. SSO Configuration: Fidelis\_SSO
      14. Session Update: unchecked
      15. Session Timeout: unchecked
      16. Home Tab: unchecked
      17. Log: none.
      18. Click Finished.
   3. Access ›› Connectivity / VPN : Portal Access : Portal Access Lists >> create
      1. Name: Unity
      2. Link Type: Application URI
      3. Application URI: [https://10.1.3.51/](https://172.26.3.51/)
      4. Click Create
      5. Click on Add under Resource Items
      6. Link Type: Paths
      7. Destination: Type: IP Address 10.1.3.51 (IP address of the unity server)
      8. Paths: /\*
      9. Scheme: https
      10. Port: 443
      11. Compression: No Compression
      12. Client Cache: No Cache
      13. SSO Configuration: unity-ci1
      14. Session Update: unchecked
      15. Session Timeout: unchecked
      16. Home Tab: unchecked
      17. Log: none.
      18. Click Finished.
   4. Access ›› Connectivity / VPN : Portal Access : Portal Access Lists >> create
      1. Name: APC\_DLP
      2. Link Type: Application URI
      3. Application URI: [https://10.1.1.85/](https://172.26.1.85/)
      4. Caption: Fidelis APC (DLP)
      5. Click Create
      6. Click on Add under Resource Items
      7. Link Type: Paths
      8. Destination: Type: IP Address 10.1.1.85 (IP address of the Fidelis APC (DLP) server)
      9. Paths: /\*
      10. Scheme: https
      11. Port: 443
      12. Compression: No Compression
      13. Client Cache: No Cache
      14. SSO Configuration: Fidelis\_SSO
      15. Session Update: unchecked
      16. Session Timeout: unchecked
      17. Home Tab: unchecked
      18. Log: none.
      19. Click Finished.
   5. Access ›› Connectivity / VPN : Portal Access : Portal Access Lists >> create
      1. Name: JRSS
      2. Link Type: Application URI
      3. Application URI: [https://10.1.1.86/](https://172.26.1.86/)
      4. Caption: Fidelis JRSS
      5. Click Create
      6. Click on Add under Resource Items
      7. Link Type: Paths
      8. Destination: Type: IP Address 10.1.1.86 (IP address of the JRSS server)
      9. Paths: /\*
      10. Scheme: https
      11. Port: 443
      12. Compression: No Compression
      13. Client Cache: No Cache
      14. SSO Configuration: Fidelis\_SSO
      15. Session Update: unchecked
      16. Session Timeout: unchecked
      17. Home Tab: unchecked
      18. Log: none.
      19. Click Finished.
2. Create Webtop Links
   1. Navigate to Access ›› Webtops : Webtop Links >> Create
      1. Name: Avoke
      2. Link Type: Application URI
      3. Application URI: [http://10.1.1.15:8081/browser](http://172.26.1.15:8081/browser) (IP Address of the BIG-IP Virtual Server for Avoke)
      4. Caption: Avoke
      5. Click Finished
   2. Navigate to Access ›› Webtops : Webtop Links >> Create
      1. Name: FCSW1
      2. Link Type: Application URI
      3. Application URI: https://%{session.server.network.name}/ssh/host/10.1.3.101 (IP Address of the BIG-IP pua webtop IP for WebSSH to FCSW1 IP)
      4. Caption: FCSW1
      5. Click Finished
   3. Navigate to Access ›› Webtops : Webtop Links >> Create
      1. Name: FCSW2
      2. Link Type: Application URI
      3. Application URI: https://%{session.server.network.name}/ssh/host/10.1.3.102 (IP Address of the BIG-IP pua webtop IP for WebSSH to FCSW2 IP)
      4. Caption: FCSW2
      5. Click Finished
   4. Navigate to Access ›› Webtops : Webtop Links >> Create
      1. Name: SW1
      2. Link Type: Application URI
      3. Application URI: https://%{session.server.network.name}/ssh/host/10.1.3.2 (IP Address of the BIG-IP pua webtop IP for WebSSH to SW1 IP)
      4. Caption: SW1
      5. Click Finished
   5. Navigate to Access ›› Webtops : Webtop Links >> Create
      1. Name: SW2
      2. Link Type: Application URI
      3. Application URI: https://%{session.server.network.name}/ssh/host/10.1.3.3 (IP Address of the BIG-IP pua webtop IP for WebSSH to SW2 IP)
      4. Caption: SW2
      5. Click Finished
   6. Navigate to Access ›› Webtops : Webtop Links >> Create
      1. Name: avocent\_wl
      2. Link Type: Application URI
      3. Application URI: https://10.1.1.78 (IP Address of the BIG-IP Virtual Server for Avocent)
      4. Caption: avocent
      5. Click Finished
   7. Navigate to Access ›› Webtops : Webtop Links >> Create
      1. Name: fidelis\_9\_2\_3\_wl
      2. Link Type: Application URI
      3. Application URI: https://10.1.1.79 (IP Address of the BIG-IP Virtual Server for Fidelis GW JRSS)
      4. Caption: Fidelis GW JRSS
      5. Click Finished
   8. Navigate to Access ›› Webtops : Webtop Links >> Create
      1. Name: iDRAC8\_avoke\_wl
      2. Link Type: Application URI
      3. Application URI: https://10.1.1.76/start.html (IP Address of the BIG-IP Virtual Server for iDRAC8 avoke)
      4. Caption: iDRAC8 avoke
      5. Click Finished
   9. Navigate to Access ›› Webtops : Webtop Links >> Create
      1. Name: iDRAC8\_owl\_wl
      2. Link Type: Application URI
      3. Application URI: https://10.1.1.77/start.html (IP Address of the BIG-IP Virtual Server for iDRAC8 owl)
      4. Caption: iDRAC8 owl
      5. Click Finished
   10. Navigate to Access ›› Webtops : Webtop Links >> Create
       1. Name: iDRAC9
       2. Link Type: Application URI
       3. Application URI: https://10.1.1.74 (IP Address of the BIG-IP Virtual Server for ESX1\_iDRAC)
       4. Caption: ESX1\_iDRAC
       5. Click Finished
   11. Navigate to Access ›› Webtops : Webtop Links >> Create
       1. Name: iDRAC9\_21\_wl
       2. Link Type: Application URI
       3. Application URI: https://10.1.1.75 (IP Address of the BIG-IP Virtual Server for ESX2\_iDRAC)
       4. Caption: ESXi2\_iDRAC
       5. Click Finished
3. Configure Webtop Sections
   1. Navigate to Access ›› Webtops : Webtop Sections >> Create
      1. Name: Administration
      2. Display Order: 1
      3. Caption: Administration
      4. Click Finished
      5. Click on the Webtop section name
      6. Click Add
      7. Select the following: BIG-IP, FCSW1, FCSW2, SW1, SW2, Unity, avocent\_wl, credgen, iDRAC8\_avoke\_wl, iDRAC8\_owl\_wl, iDRAC9, iDRAC9\_21\_wl.
      8. Click Update.
   2. Navigate to Access ›› Webtops : Webtop Sections >> Create
      1. Name: Operation
      2. Display Order: 2
      3. Caption: Operation
      4. Click Finished
      5. Click on the Webtop section name
      6. Click Add
      7. Select the following: Fidelis\_CP1, Fidelis\_CP2, APC\_DLP, JRSS, fidelis\_9\_2\_3\_wl, Avoke.
      8. Click Update.
4. Copy the pua policy Access ›› Profiles / Policies : Access Profiles (Per-Session Policies)
   1. Click the Copy link for the pua policy
   2. Rename it to puawithldap.
5. Change the USG Warning Banner
   1. Navigate to Access ›› Profiles / Policies : Customization : Advanced : Access Profiles : /Common/puawithldap: Access Policy: Message Pages: USG Warning Banner: Message\_box.inc paste the USG Warning Banner HTML code into the Advanced customization editor. You can find the html at the end of this document.
   2. To save, click off the message\_box.inc file and click the save icon at the top. Apply the access policy.
6. Edit the puawithldap Access Policy
7. Navigate to Access ›› Profiles / Policies : Access Profiles (Per-Session Policies) >> puawithldap
   1. Click on the puawithldap policy name. Change the Profile Scope: Global
   2. Click Update
   3. Navigate to the Access Policy tab.
   4. Visual Policy Editor: Edit Access Policy for Profile "puawithldap"
   5. Delete the Logon page, Variable Assign and Admin Access VPE object, NOT the macros.
   6. Expand the GET UPN from CAC Macro. The expression code has a syntax error in it.
      1. Delete the failure VPE object on the NO UPN branch of Check UPN.
      2. Edit Check UPN, click the Check UPN Name
      3. Click change for the Expression and remove the text NO-UPN-FOUND. Click Save.
      4. Click on the name GET UPN from CAC, Click change.
      5. Paste the contents of the APM Get UPN From CAC Custom Expression listed at the end of this document in the Custom Expression field.
      6. Click Finished. Click Save
   7. Add on-demand certificate auth to the fallback branch of the USG Warning Banner.
   8. Add the Macro Get UPN from CAC to the successful branch of the on-demand certificate auth VPE object. Change the terminal endings on Not Found to Deny and Found to Allow. Apply the access policy. The TMUI will timeout even if you are editing the APM policy as it doesn’t update the idle session timeout value.
   9. Add an LDAP query object on the Found branch of the Get UPN from CAC VPE object.
   10. Server: /Common/ldap\_aaa
   11. SearchDN: DC=F5DEMO,DC=COM
   12. SearchFilter: userPrincipalName=%{session.custom.ephemeral.upn}
   13. Fetch groups to which the user or group belong: all
   14. Fetch users that belong to the group: all
   15. Required Attributes (optional): sAMAccountName
   16. Click on Branch rules and change the branch Name to Success: Expression: LDAP Query has Passed. Click save.
   17. On the Success branch of the LDAP Query add Variable Assign. Each of the new entries are a separate entry. NOTE: Type the values, do not copy and paste. If you copy and paste, hidden windows characters will prevent saving the VPE object.
       1. Add new entry: Custom Variable: session.logon.last.username AAA Attribute: LDAP attribute name sAMAccountName
       2. Click Finished.
       3. Add new entry: Custom Variable: session.custom.ephemeral.last.username Session Variable: session.logon.last.username
       4. Click Finished.
       5. Add new entry: Custom Variable: session.custom.ephemeral.last.dn AAA Attribute: LDAP attribute name dn
       6. Click Finished.
       7. Click Save.
   18. On the fallback branch of the Variable Assign add a Macro Admin Access
   19. On the Out branch of the Admin Access add a Variable Assignment NOTE: Type the values, do not copy and paste. If you copy and paste, hidden windows characters will prevent saving the VPE object.
       1. Name var assign
       2. Add new entry: Custom Variable: session.custom.ephemeral.last.unencryptedpassword Custom Expression: mcget -secure {session.custom.ephemeral.last.password}
       3. Click Finished.
       4. Click Save.
   20. On the fallback branch of On-Demand Cert Auth add a logon page
       1. In the Form Header Text change the value to Secure Logon <br> for F5DEMO. Click save.
   21. On the fallback branch of the logon page, add an LDAP Auth object.
       1. Name: LDAP Auth
       2. Server /Common/ldap\_noncac
       3. SearchDN: DC=F5DEMO,DC=COM
       4. SearchFilter: sAMAccountName=%{session.logon.last.username}
       5. Click Save.
   22. On the Successful branch of LDAP Auth object add LDAP Query object
       1. Name: LDAP Query non-cac
       2. Server: /Common/ldap\_aaa
       3. SearchDN: DC=F5DEMO,DC=COM
       4. SearchFilter: sAMAccountName=%{session.logon.last.username}
       5. Fetch groups to which the user or group belong: all
       6. Fetch users that belong to the group: all
       7. Required Attributes (optional): sAMAccountName, dn, userPrincipalName
       8. Click on Branch rules and change the branch to Success: Expression: LDAP Query has Passed. Click save.
   23. On the Success branch of LDAP Query non-cac add a Variable Assignment
       1. Name: var assign non-cac
       2. Add new entry session.custom.ephemeral.upn = LDAP attribute name userPrincipalName
       3. Add new entry session.custom.ephemeral.last.username = Session Variable session.logon.last.username
       4. Add new entry session.custom.ephemeral.last.dn = Session Variable dn
   24. On the fallback branch of the Variable Assign add a Macro Admin Access
   25. On the Out branch of the Admin Access add a Variable Assignment.NOTE: Type the values, do not copy and paste. If you copy and paste, hidden windows characters will prevent saving the VPE object.
       1. Name Variable assign non-cac
       2. Add new entry Custom Variable: session.custom.ephemeral.last.unencryptedpassword Custom Expression: mcget -secure {session.custom.ephemeral.last.password}
   26. Click on the ending after the var assign non-cac and change the Deny to Allow.
   27. Apply Access Policy.
   28. Edit the Advanced Resource Assignment for the Admin Access Macro
       1. Resource Assignment
          1. Change Expression: Agent Sel: LDAP Query: User is a member of: CN=F5 Test Users,OU=Groups,OU=TEXAS,DC=F5DEMO,DC=COM
          2. Click Add Expression.Click Finished
          3. Add/Delete:
             1. Portal Access: /Common/APC\_DLP, /Common/Fidelis\_CP1, /Common/Fidelis\_CP2, /Common/JRSS
             2. Webtop Links: /Common/Avoke, /Common/fidelis\_9\_2\_3\_wl
             3. Webtop: /Common/webtop
             4. Click Update.
       2. Resource Assignment Add new entry
          1. Change Expression: Agent Sel: LDAP Query: User is a member of: User is a member of CN=F5DEMO System Administrators,OU=Groups,OU=Privileged,OU=F5DEMO PMO,DC=F5DEMO,DC=COM
          2. Add/Delete:
             1. Portal Access: /Common/APC\_DLP, /Common/Fidelis\_CP1, /Common/Fidelis\_CP2, /Common/JRSS, /Common/Unity
             2. Webtop Links: /Common/avocent\_wl, /Common/Avoke, /Common/BIG-IP, /Common/credgen, /Common/FCSW1, /Common/FCSW2, /Common/fidelis\_9\_2\_3\_wl, /Common/iDRAC8\_avoke\_wl, /Common/iDRAC8\_owl\_wl, /Common/iDRAC9, /Common/iDRAC9\_21\_wl, /Common/SW1, /Common/SW2
             3. Webtop: /Common/webtop
             4. Webtop Sections: /Common/Administration, /Common/Operation
       3. Click Save.
   29. Apply the access policy.
8. Modify the puawithldap Policy for Multi-Domain SSO
   1. Navigate to Access ›› Profiles / Policies : Access Profiles (Per-Session Policies) >> puawithldap
   2. Click on the SSO / Auth Domains tab
   3. Domain Mode: Multiple Domains
   4. Primary Authentication URI: https://10.1.1.71 (This is the pua\_webtop Virtual Server IP Address)
   5. Primary Cookie Options: Secure checked
   6. SSO Configuration: basic\_ephemeral
   7. Authentication Domain Configuration
      1. Cookie: Host
      2. Address 10.1.1.78 (Avocent)
      3. SSO Configuration: None
      4. C
      5. Repeat for fidelis and iDRAC Virtual Server IP Addresses
      6. Apply Access Policy
9. Create the iDRAC, Avocent and Fidelis Access Policies
10. Navigate to Access ›› Profiles / Policies : Access Profiles (Per-Session Policies) >> Create
    1. Name: IDRAC
    2. Profile Type: LTM-APM
    3. Profile Scope: Global
    4. Languages: English (en)
    5. Click Finished.
    6. Edit the IDRAC policy
    7. Click on the SSO / Auth Domains tab
    8. Domain Mode: Multiple Domains
    9. Primary Authentication URI: https://10.1.1.71 (This is the pua\_webtop Virtual Server IP Address)
    10. Primary Cookie Options: Secure checked
    11. SSO Configuration: None
    12. Authentication Domain Configuration
        1. Cookie: Host
        2. Address 10.1.1.76
        3. Click update
        4. Authentication Domains: Add
        5. Repeat iDRAC Virtual Server IP Addresses
    13. Click on the Access Policy tab
    14. Visual Policy Editor: Edit Access Policy for Profile "IDRAC"
        1. Change the fallback ending from Deny to Allow by clicking Deny and selecting the Allow Ending.
    15. Apply Access Policy
11. Navigate to Access ›› Profiles / Policies : Access Profiles (Per-Session Policies) >> Create
    1. Name: avocent\_ap
    2. Profile Type: LTM-APM
    3. Profile Scope: Global
    4. Languages: English (en)
    5. Click Finished.
    6. Edit the avocent\_ap policy
    7. Click on the SSO / Auth Domains tab
    8. Domain Mode: Multiple Domains
    9. Primary Authentication URI: https://10.1.1.71 (This is the pua\_webtop Virtual Server IP Address)
    10. Primary Cookie Options: Secure checked
    11. SSO Configuration: None
    12. Authentication Domain Configuration
        1. Cookie: Host
        2. Address 10.1.1.xxx (This is the avocent Virtual Server IP Address)
        3. Click update
    13. Click on the Access Policy tab
    14. Visual Policy Editor: Edit Access Policy for Profile "avocent\_ap"
        1. Change the fallback ending from Deny to Allow by clicking Deny and selecting the Allow Ending.
    15. Apply Access Policy
12. Navigate to Access ›› Profiles / Policies : Access Profiles (Per-Session Policies) >> Create
    1. Name: fidelis9\_2\_3\_ap
    2. Profile Type: LTM-APM
    3. Profile Scope: Global
    4. Languages: English (en)
    5. Click Finished.
    6. Edit the fidelis9\_2\_3\_ap policy
    7. Click on the SSO / Auth Domains tab
    8. Domain Mode: Multiple Domains
    9. Primary Authentication URI: https://10.1.1.71 (This is the pua\_webtop Virtual Server IP Address)
    10. Primary Cookie Options: Secure checked
    11. SSO Configuration: None
    12. Authentication Domain Configuration
        1. Cookie: Host
        2. Address 10.1.1.79 (This is the fidelis9\_2\_3\_ap Virtual Server IP Address)
        3. Click update
    13. Click on the Access Policy tab
    14. Visual Policy Editor: Edit Access Policy for Profile "fidelis9\_2\_3\_ap "
        1. Change the fallback ending from Deny to Allow by clicking Deny and selecting the Allow Ending.
    15. Apply Access Policy
13. Modify the pua\_webtop Virtual Server
14. Navigate to Local Traffic ›› Virtual Servers : Virtual Server List ›› pua\_webtop
    1. SSL Profile (Server): serverssl
    2. Source Address Translation: Auto Map
    3. Connection Limit: 10000
    4. Connection Rate Limit: 1000
    5. Access Policy: Access Profile: puawithldap
    6. HTTP Compression Profile: None
    7. Click Update
15. Apply the Access Profiles to the Virtual Servers
16. Navigate to Local Traffic ›› Virtual Servers : Virtual Server List >> avocent
    1. Access Policy: Access Profile: avocent\_ap
    2. Click update
17. Navigate to Local Traffic ›› Virtual Servers : Virtual Server List >> fidelis\_9\_2\_3\_vs
    1. Access Policy: Access Profile: fidelis9\_2\_3\_ap
    2. Click update
18. Navigate to Local Traffic ›› Virtual Servers : Virtual Server List >> iDRAC8\_avoke
    1. Access Policy: Access Profile: IDRAC
    2. Click update
19. Navigate to Local Traffic ›› Virtual Servers : Virtual Server List >> iDRAC8\_owl
    1. Access Policy: Access Profile: IDRAC
    2. Click update
20. Navigate to Local Traffic ›› Virtual Servers : Virtual Server List >> iDRAC9
    1. Access Policy: Access Profile: IDRAC
    2. Click update
21. Navigate to Local Traffic ›› Virtual Servers : Virtual Server List >> iDRAC9\_21
    1. Access Policy: Access Profile: IDRAC
    2. Click update

## Operational Updates

If the Service Account password for CN=svc.F5DEMO.FF5BIND,OU=Service Accounts,OU=Privileged,OU=TEXAS,DC=F5DEMO,DC=COM is changed in Active Directory, it needs to be updated on the BIG-IP in multiple places.

1. Navigate to System ›› Users : Authentication
   1. Click Change
   2. Bind: Password: <new\_ svc.F5DEMO.FF5BIND\_password>
   3. Bind: Confirm: <new\_ svc.F5DEMO.FF5BIND\_password>
   4. Click Finished
2. Navigate to Access ›› Authentication ›› ldap\_aaa
   1. Admin Password: <new\_ svc.F5DEMO.FF5BIND\_password>
   2. Verify Admin Password: <new\_ svc.F5DEMO.FF5BIND\_password>
   3. Click Update
3. Navigate to Access ›› Authentication ›› ldap\_noncac
   1. Admin Password: <new\_ svc.F5DEMO.FF5BIND\_password>
   2. Verify Admin Password: <new\_ svc.F5DEMO.FF5BIND\_password>
   3. Click Update
4. Navigate to Local Traffic ›› iRules : LX Workspaces ›› ephemeral\_auth-0.4.5
   1. Click on config.json
   2. adminPassword: <new\_ svc.F5DEMO.FF5BIND\_password>
   3. Click Save File
   4. Navigate to Local Traffic ›› iRules : LX Plugins ›› ephemeral\_auth\_plugin
   5. Click Reload from Workspace

## Post INSTALL Updates

1. Create a PKI Token exception to allow username and password authentication.
   1. Create the datagroup “cac\_exception\_dg” Type “string”.
      1. To allow specific users to authentication with username/password, enter their Active Directory sAMAccountName in the name field and click “Add” then update. Example “rob.eastman.ctr.sa”. It must be entered in all lowercase.
      2. To remove a user from the exception list, click the user and select delete then update.
   2. Create the iRule “cac\_exception\_irule”

when ACCESS\_POLICY\_AGENT\_EVENT {

switch [string tolower [ACCESS::policy agent\_id]] {

"cacexception" {

ACCESS::session data set "session.custom.iscacexempt" 0

set username [string tolower [ACCESS::session data get session.logon.last.username]]

if {[class match $username equals cac\_exception\_dg]}{

ACCESS::session data set "session.custom.iscacexempt" 1

}

}

}

}

* 1. Apply the “cac\_exception\_irule” to the “pua\_webtop” Virtual Server.
  2. Modify the pua webtop Access Policy.
     1. After the Logon Page on the fallback branch, add an irule event object. Name: CAC Exception, ID: cacexception. Add a bracnch rule, Name: Yes CAC Exempt, Advanced: expr {[mcget {session.custom.iscacexempt}] == “1”}
     2. Move the LDAP Auth Branch to the “Yes CAC Exempt” branch.
     3. Edit Endings Name: CAC Req Color: light blue Customization “Your session could not be established. You must use your token to login.”
     4. Edit the CAC Exemption fallback branch from Deny to CAC Req.
  3. Apply the Access policy

# Avocent iRule

# Needs an HTML profile and an HTML rule looking for tag "body"

#

when HTTP\_REQUEST {

HTML::disable

if { [HTTP::uri] ends\_with "/login.php" } {

HTML::enable

log local0. "HIT LOGIN"

set workaround 1

} elseif { [info exists workaround] } {

unset workaround

}

}

when HTML\_TAG\_MATCHED {

log local0. "at HTML\_TAG\_MATCHED: [HTML::tag name]"

if { [info exists workaround] } {

switch [HTML::tag name] {

"body" {

log local0. "at body..."

set username [ACCESS::session data get session.sso.token.last.username]

set password [ACCESS::session data get -secure session.sso.token.last.password]

set newstring "<script>

var checkExist = setInterval(function() {

if (document.getElementsByName(\"loginUsername\")\[0\]) {

clearInterval(checkExist);

var un = document.getElementsByName(\"loginUsername\")\[0\];

un.focus();

un.value = \"$username\";

var ev = document.createEvent('Event');

ev.initEvent('input', true, false);

un.dispatchEvent(ev);

var pw = document.getElementsByName(\"loginPassword\")\[0\];

pw.focus();

pw.value = \"$password\";

var ev = document.createEvent('Event');

ev.initEvent('input', true, false);

pw.dispatchEvent(ev);

var la = document.getElementsByName(\"language\")\[0\];

la.focus();

la.value = \"en\";

var ev = document.createEvent('Event');

ev.initEvent('input', true, false);

la.dispatchEvent(ev);

doAction('login');

}

}, 2000); // check every 2 seconds. Can be adjusted if timing is an issue.

</script>"

HTML::tag append $newstring

unset workaround

HTML::disable

}

}

}

}

# fidelis\_9\_2\_3\_irule iRule

# Needs an HTML profile and an HTML rule looking for tag "body"

when HTTP\_REQUEST {

HTML::disable

if { [HTTP::uri] ends\_with "/cas/login?service=https%3A%2F%2F10.1.1.79%2Fj%2Flogin.html" } {

HTML::enable

log local0. "HIT LOGIN"

set workaround 1

} elseif { [info exists workaround] } {

unset workaround

}

}

when HTML\_TAG\_MATCHED {

log local0. "at HTML\_TAG\_MATCHED: [HTML::tag name]"

if { [info exists workaround] } {

switch [HTML::tag name] {

"input" {

log local0. "at html tag..."

set username [ACCESS::session data get session.sso.token.last.username]

set password [ACCESS::session data get -secure session.sso.token.last.password]

set newstring "<script>

var checkExist = setInterval(function() {

if (document.getElementById(\"username\")) {

clearInterval(checkExist);

var un = document.getElementById(\"username\");

un.focus();

un.value = \"$username\";

var ev = document.createEvent('Event');

ev.initEvent('input', true, false);

un.dispatchEvent(ev);

var pw = document.getElementById(\"password\");

pw.focus();

pw.value = \"$password\";

var ev2 = document.createEvent('Event');

ev2.initEvent('input', true, false);

pw.dispatchEvent(ev2);

document.getElementsByTagName(\"input\")\[5\].click();

}

}, 2000); // check every 2 seconds. Can be adjusted if timing is an issue.

</script>"

HTML::tag append $newstring

unset workaround

HTML::disable

}

}

}

}

# iDRAC8 iRule

# Needs an HTML profile and an HTML rule looking for tag "body"

when HTTP\_REQUEST {

HTML::disable

if { [HTTP::uri] ends\_with "/login.html" } {

HTML::enable

log local0. "HIT LOGIN"

set workaround 1

} elseif { [info exists workaround] } {

unset workaround

}

}

when HTML\_TAG\_MATCHED {

log local0. "at HTML\_TAG\_MATCHED: [HTML::tag name]"

if { [info exists workaround] } {

switch [HTML::tag name] {

"span" {

log local0. "at body..."

set username [ACCESS::session data get session.sso.token.last.username]

set password [ACCESS::session data get -secure session.sso.token.last.password]

set newstring "<script>

var checkExist = setInterval(function() {

if (document.getElementsByName(\"password\")\[0\]) {

clearInterval(checkExist);

var un = document.getElementsByName(\"user\")\[0\];

un.focus();

un.value = \"$username\";

var ev = document.createEvent('Event');

ev.initEvent('input', true, false);

un.dispatchEvent(ev);

var pw = document.getElementsByName(\"password\")\[0\];

pw.focus();

pw.value = \"$password\";

var ev = document.createEvent('Event');

ev.initEvent('input', true, false);

pw.dispatchEvent(ev);

var lb = document.getElementById(\"submit\_lbl\");

lb.click();

}

}, 2000); // check every 2 seconds. Can be adjusted if timing is an issue.

</script>"

HTML::tag append $newstring

unset workaround

HTML::disable

}

}

}

}

# iDRAC9 iRule

# Needs an HTML profile and an HTML rule looking for tag "body"

when HTTP\_REQUEST {

HTML::disable

if { [HTTP::uri] ends\_with "/restgui/start.html" } {

HTML::enable

log local0. "HIT LOGIN"

set workaround 1

} elseif { [info exists workaround] } {

unset workaround

}

}

when HTML\_TAG\_MATCHED {

log local0. "at HTML\_TAG\_MATCHED: [HTML::tag name]"

if { [info exists workaround] } {

switch [HTML::tag name] {

"body" {

log local0. "at body..."

set username [ACCESS::session data get session.sso.token.last.username]

set password [ACCESS::session data get -secure session.sso.token.last.password]

set newstring "<script>

var checkExist = setInterval(function() {

if (document.getElementsByName(\"username\")\[0\]) {

clearInterval(checkExist);

var un = document.getElementsByName(\"username\")\[0\];

un.focus();

un.value = \"$username\";

var ev = document.createEvent('Event');

ev.initEvent('input', true, false);

un.dispatchEvent(ev);

var pw = document.getElementsByName(\"password\")\[0\];

pw.focus();

pw.value = \"$password\";

var ev = document.createEvent('Event');

ev.initEvent('input', true, false);

pw.dispatchEvent(ev);

var lb = document.getElementsByTagName(\"button\")\[0\];

lb.focus();

lb.click();

}

}, 2000); // check every 2 seconds. Can be adjusted if timing is an issue.

</script>"

HTML::tag append $newstring

unset workaround

HTML::disable

}

}

}

}

# USG Warning Banner

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">

<html>

<head>

<title>DOD Warning Banner</title>

<link rel="stylesheet" type="text/css" href="/public/include/css/apm.css">

<script language="JavaScript" src="/public/include/js/session\_check.js"></script>

<script language="javascript"><!--//

window.onerror=function(){ return function(){ return; } }

/////////////////////////////////////////////////////////////////////////

// function to return the customized screen when session expiration

// is detected on the client-side

/////////////////////////////////////////////////////////////////////////

function SessionExpired\_CustomizedScreenGet()

{

return '<br><h3>Session Expired/Timeout</h3><br>Due to user inactivity, your session expired. Click the following link to start a new session.<br><br><table id="IHoptions"><tr><td><a href="[SESSION\_RESTART\_URL]" class="option"><img src="/public/images/sq-positive.gif" ></a><a href="[SESSION\_RESTART\_URL]">Start a new session</a></td></tr></table>';

}

function sessionTimedOut() {

showSplashLayer("MessageDIV", SessionExpired\_CustomizedScreenGet());

}

function OnLoad() {

try{

if ( "undefined" != typeof(window.external) && "unknown" != typeof(window.external)

&& "undefined" != typeof(window.external.WebLogonNotifyUser) && "unknown" != typeof(window.external.WebLogonNotifyUser) ){

window.external.WebLogonNotifyUser();

}

}catch(e){};

window.setTimeout("sessionTimeoutCheck(sessionTimedOut)", globalTimoutInterval);

}

function SubmitResult(choice) {

var f = document.getElementById("hidden\_form");

f.my\_result.value = 1;

f.submit();

}

-->

</script>

<style type="text/css">

BODY {

background-color: #E0E0E0;margin: 0 0 0 0;

text-align:center;

font-size:62.5%;

font-facomy:verdana,helvetica,arial,sans-serif;

}

#shadow-container {

background-color:#909090;

margin:20px auto 0 auto;width:612px

}

#container {

position:relative;

background-color:#F0F0F0;

border:1px solid #404040;

padding:5px 5px 5px 5px;

width:600px;

text-align:left;

left:-5px;

top: -5px;

}

#titlebox {

width:598px;

height:35px;

text-align:center;

font-size:2.2em;

font-weight:bold;

}

#faultbox {

padding:6px 6px 0 6px;

width:586px;

text-align:justify;

font-size:1.5em;

color: #FF0000;

font-weight:bold;

}

#gotobox {

padding-top:5px;

width:598px;

text-align:left;

font-size:1.2em;

}

#gotobox ul {

list-style-type:square;

}

#gotobox li {

padding:7px;

}

#btn{

width:230px;

height:45px;

font-facomy:arial,helvetica,courier;

font-size:14px;

font-weight:bold;

}

#buttonbox {

text-align:center

}

</style>

</head>

<body onload="OnLoad()">

<div id="shadow-container">

<div id="container">

<div id="titlebox">DoD Warning and Consent Banner</div>

<div id="faultbox">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:</div>

<div id="gotobox">

<ul>

<li>The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.</li>

<li>At any time, the USG may inspect and seize data stored on this IS.</li>

<li>Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.</li>

<li>This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.</li>

<li>Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.</li>

</ul>

</div>

<div id="buttonbox">

<button id="btn" onclick="javascript:SubmitResult(1);return 1;">OK</button>

</div>

</div>

</div>

<form method="post" id="hidden\_form" name="hidden\_form" action="/my.policy">

<input type='hidden' id="my\_result" value='0' name='choice'>

</form>

</body>

</html>

# APM Get UPN FROM CAC

Custom Variable: session.custom.ephemeral.upn

Custom Expression: set e\_fields [split [mcget {session.ssl.cert.x509extension}] "\n"]; foreach qq $e\_fields { if {[string first "othername:UPN" $qq] >= 0} { return [string range $qq [expr { [string first "<" $qq] + 1 } ] [expr { [string first ">" $qq] - 1 } ] ]; } }