dev/central
AN F5 COMMUNITY
(/s/)
F5.COM (https://f5.com/) | DEVCENTRAL (/s/) | SUPPORT (https://support.f5.com/) | PARTNERS (https://partners.f5.com/) | MYF5 (https://my.f5.com/)

dev/central
AN F5 COMMUNITY
(/s/) TOPICS QUESTIONS (/s/questions) ARTICLES (/s/articles) CODE (/s/codeshare) RESOURCES (/s/resources) ABOUT (/s/getting-started)

F5.COM (https://f5.com/)DEVCENTRAL (/s/)SUPPORT (https://support.f5.com/)PARTNERS (https://partners.f5.com/)MYF5 (https://my.f5.com/)

Login (/DEVC_LoginToCommunity?startURL=//s/articles/configuring-smart-card-authentication-to-the-big-ip-traffic-management-user-interface-tmui-using-f5s-privileged-user-access-solution-31656) | Sign up (/DEVC_SignUpToCommunity) |

Back to Article List

Configuring Smart Card Authentication to the BIG-IP Traffic Management User Interface (TMUI) using F5's Privileged User Access Solution

Updated 1 year ago | Originally posted July 18, 2018 by **Steve Lyons 236154** ● F5 **(/s/profile/0051T000008t5CoQAI)**

Topics in this Article: apm (/s/articles?tag=apm), application delivery (/s/articles?tag=application delivery), iruleslx (/s/articles?tag=iruleslx), security (/s/articles?tag=security)

As promised in my last article which discussed configuring the BIG-IP as an SSH Jump Server using smart card authentication, I wanted to continue the discussion of F5's privileged user access with additional use cases. The first follow on article is really dedicated to all those customers who ask, "how do I use a smart card to authenticate to the BIG-IP TMUI?" While yes, I did provide a guide on how to do this natively, I'm here to tell you I think this is a bit easier but don't take my word for it. Try them both!

To reduce duplicating content, I am going to begin with the final configuration deployed in the previous article which has been published at https://devcentral.f5.com/s/articles/configuring-the-big-ip-as-an-ssh-jump-server-using-smart-card-authentication-and-webssh-client-31586. If you have not completed that guide, please do so prior to continuing with the Traffic Management User Interface (TMUI). With that, let's begin.

Prerequisites

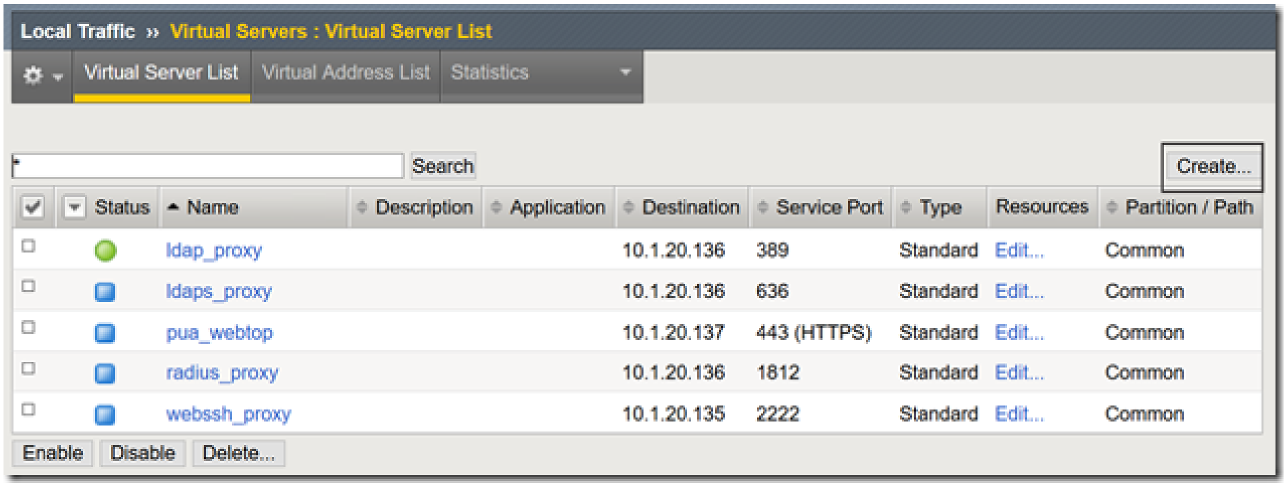
- LTM Licensed and Provisioned
- APM Licensed and Provisioned
- iRulesLX Provisioned
- 8Gb of Memory
- Completed the PUA deployment based on my previous guide.

https://devcentral.f5.com/s/articles/configuring-the-big-ip-as-an-ssh-jump-server-using-smart-card-authentication-and-webssh-client-31586

Create a Virtual Server and BIG-IP Pool

Now you may be asking yourself why would I need this? Well, if any of you have attempted this in the past you will notice you will receive an ACL error when trying to access the management IP directly from a portal access resource. Because of this, we will need to complete this step and point our portal access resource to the IP of our virtual server.

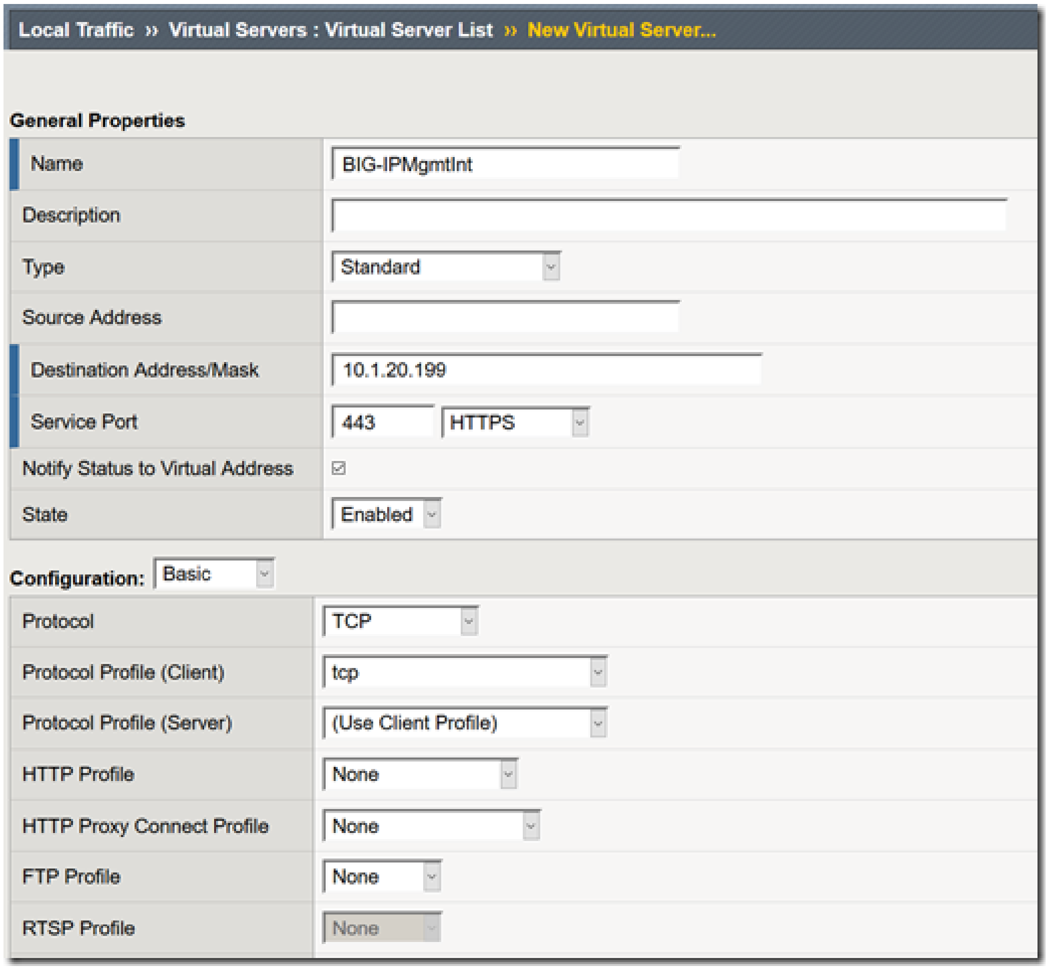
- Navigate to **Local Traffic** >> **Virtual Servers** >> Click **Create**



☑	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
□	●	ldap_proxy			10.1.20.136	389	Standard	Edit...	Common
□	🟦	ldaps_proxy			10.1.20.136	636	Standard	Edit...	Common
□	🟦	pua_webtop			10.1.20.137	443 (HTTPS)	Standard	Edit...	Common
□	🟦	radius_proxy			10.1.20.136	1812	Standard	Edit...	Common
□	🟦	webssh_proxy			10.1.20.135	2222	Standard	Edit...	Common

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/CreateVS.png?ver=2018-07-27-052803-087)

- Name: **BIG-IPMgmtInt**
- Destination Address: **This IP is arbitrary, select anything**
- Service Port: **443**



Local Traffic ›› Virtual Servers : Virtual Server List ›› New Virtual Server...

General Properties

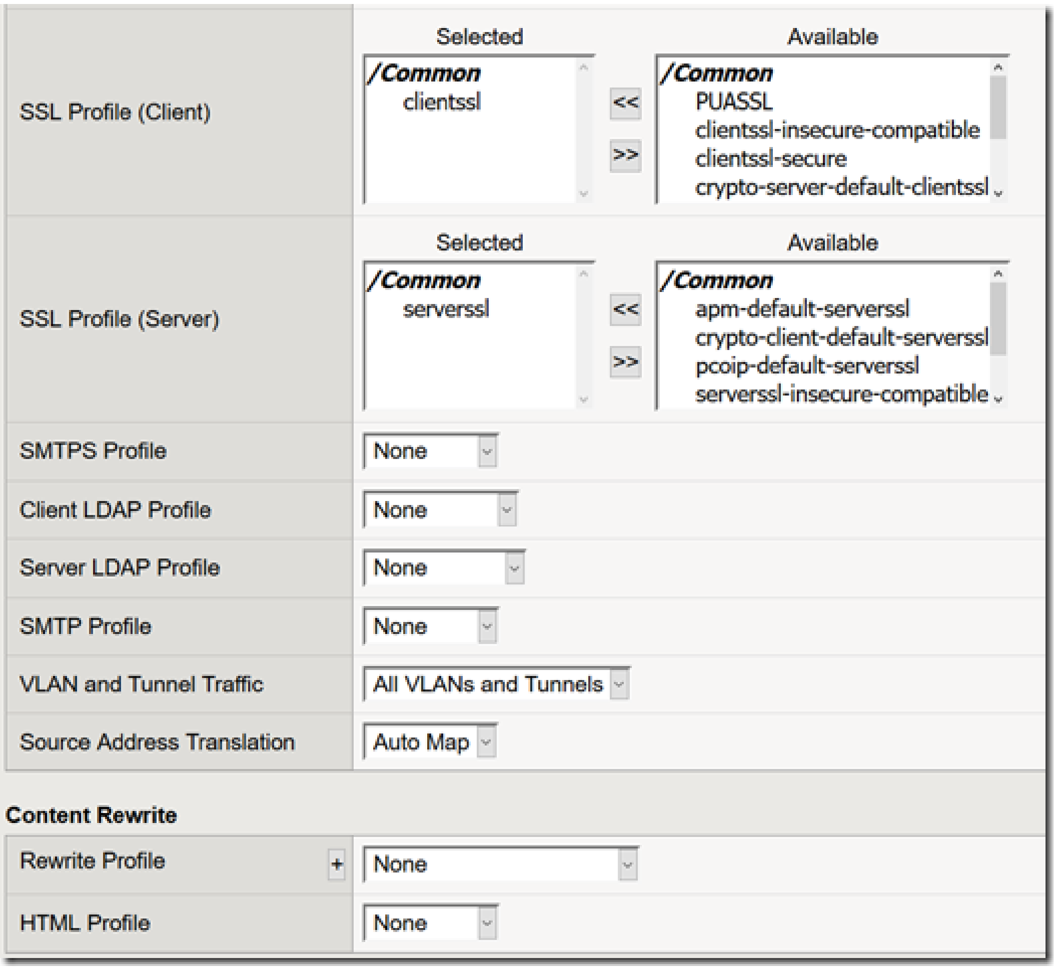
Name	BIG-IPMgmtInt
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.1.20.199
Service Port	443 HTTPS
Notify Status to Virtual Address	☑
State	Enabled

Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	None
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/VS1.png?ver=2018-07-27-052806-837)

- SSL Profile (Client): **clientssl**
- SSL Profile (Server): **serverssl**
- Source Address Translation: **Automap**



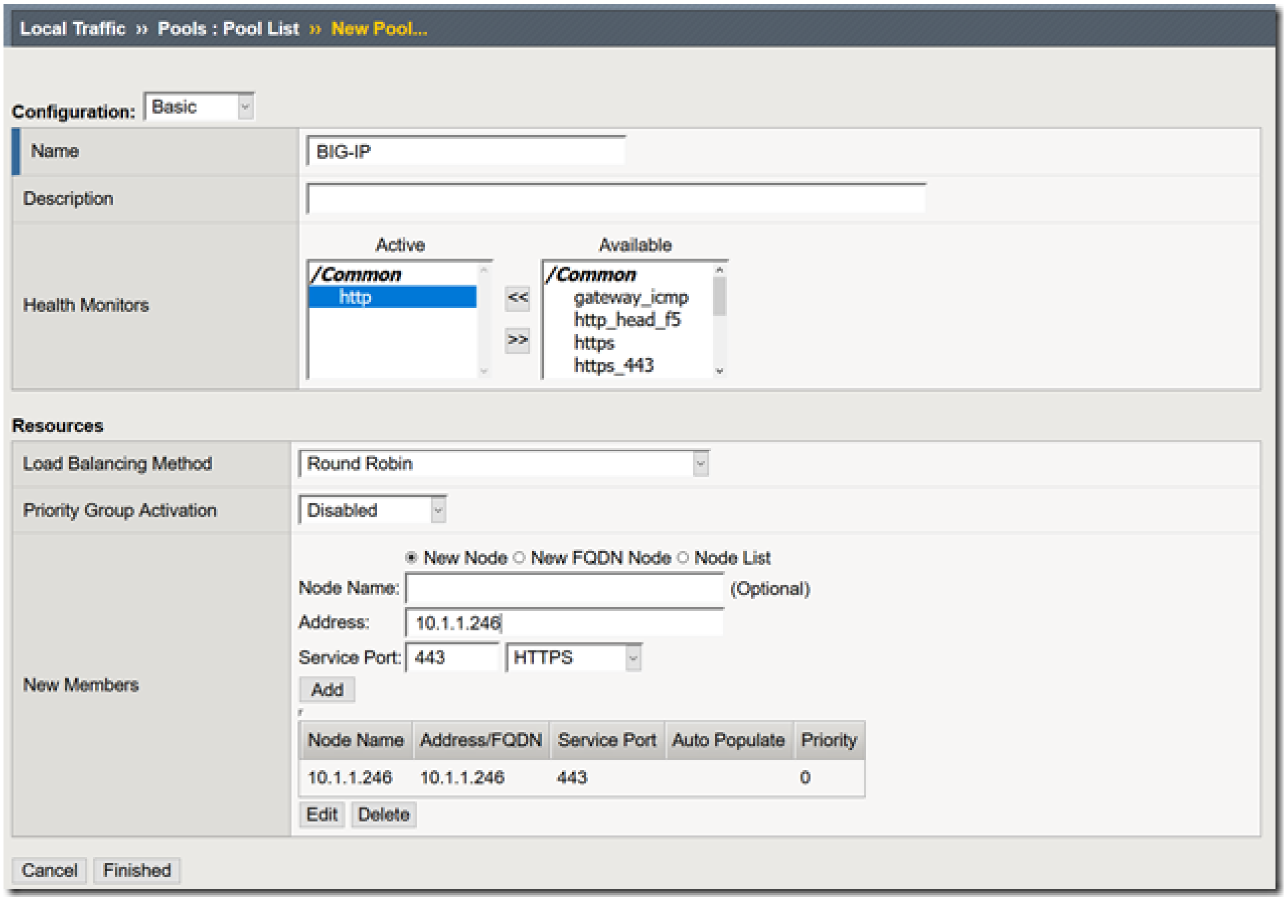
SSL Profile (Client)	Selected: /Common clientssl Available: /Common PUASSL clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl
SSL Profile (Server)	Selected: /Common serverssl Available: /Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl-insecure-compatible
SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
SMTP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

Content Rewrite

Rewrite Profile	None
HTML Profile	None

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/VS2.png?ver=2018-07-27-052810-320)

- Scroll until you reach the Default Pool option and click the + button to create a new pool.
- Name: **BIG-IP**
- Health Monitors: **HTTP**
- Address: **Management IP address**
- Service Port: **443**
- Click **Add and Finished**



Configuration: Basic

Name	BIG-IP
Description	
Health Monitors	Active: /Common http Available: /Common gateway_icmp, http_head_f5, https, https_443

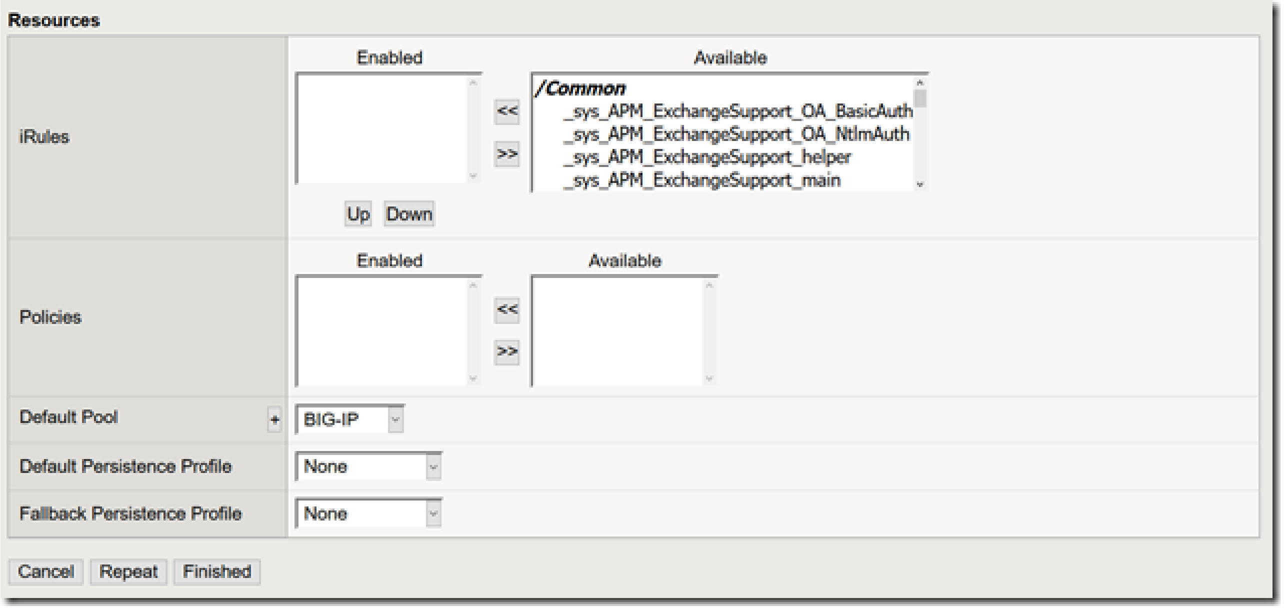
Resources

Load Balancing Method	Round Robin
Priority Group Activation	Disabled
New Members	● New Node ○ New FQDN Node ○ Node List Node Name: (Optional) Address: 10.1.1.246 Service Port: 443 HTTPS

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
10.1.1.246	10.1.1.246	443		0

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/CreatePool.png?ver=2018-07-27-052814-053)

- The pool should be selected for you after creation.
- Click **Finished**



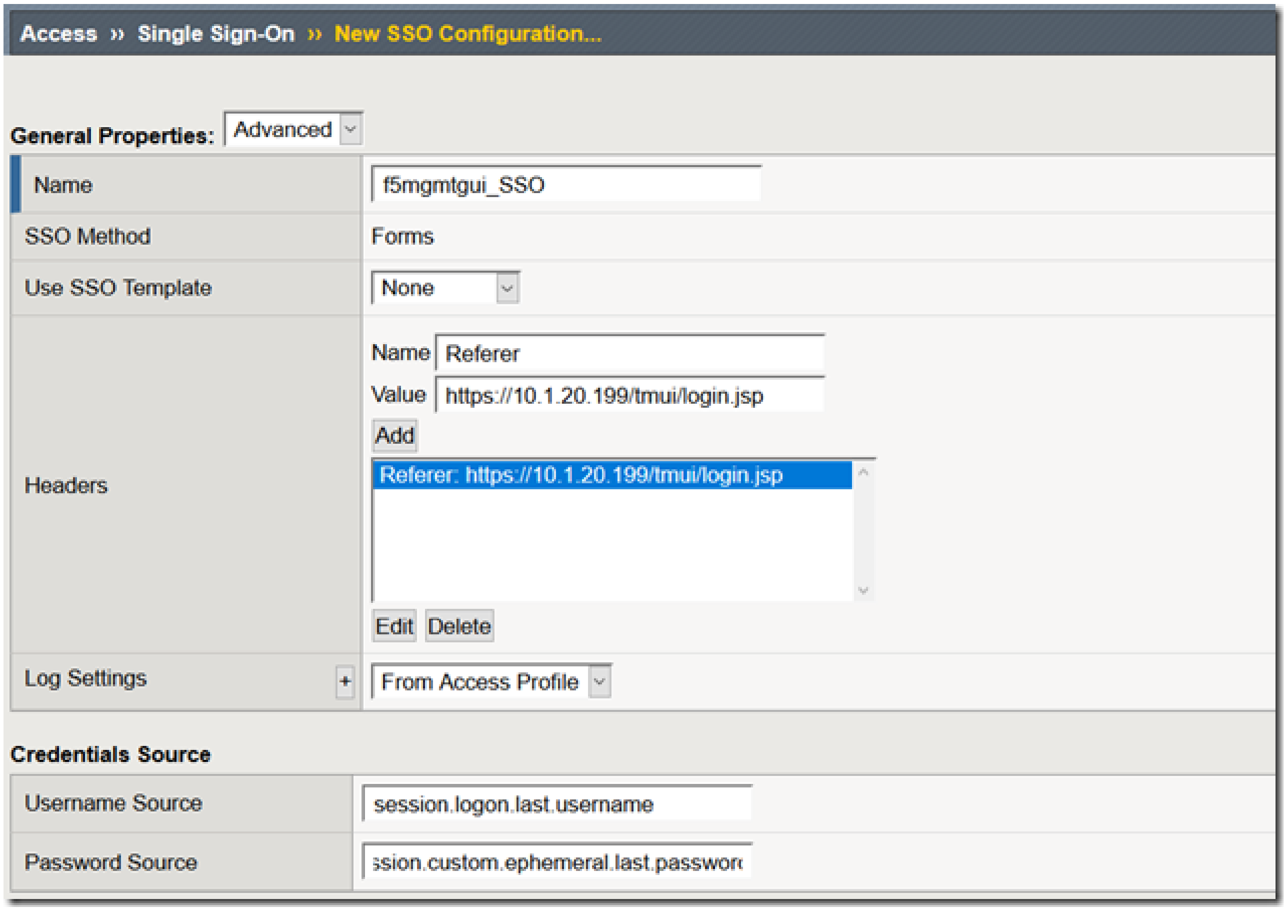
Resources

iRules	Enabled: Available: /Common _sys_APM_ExchangeSupport_OA_BasicAuth, _sys_APM_ExchangeSupport_OA_NtlmAuth, _sys_APM_ExchangeSupport_helper, _sys_APM_ExchangeSupport_main
Policies	Enabled: Available:
Default Pool	BIG-IP
Default Persistence Profile	None
Fallback Persistence Profile	None

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/SelectPool.png?ver=2018-07-27-052817-180)

Creating a Single Sign On Profile for TMUI

- Navigate to **Access** >> **Single Sign On** >> **Forms Based** >> Click **Create**
- Name: **f5mgmtgui_SSO**
- SSO Template: **None**
- Headers Name: **Referer**
- Headers Value: **https://IPofBIGIPVS/tmui/login.jsp**
- Username Source: **session.logon.last.username**
- Password Source: **session.custom.ephemeral.last.password**



Access ›› Single Sign-On ›› New SSO Configuration...

General Properties: Advanced

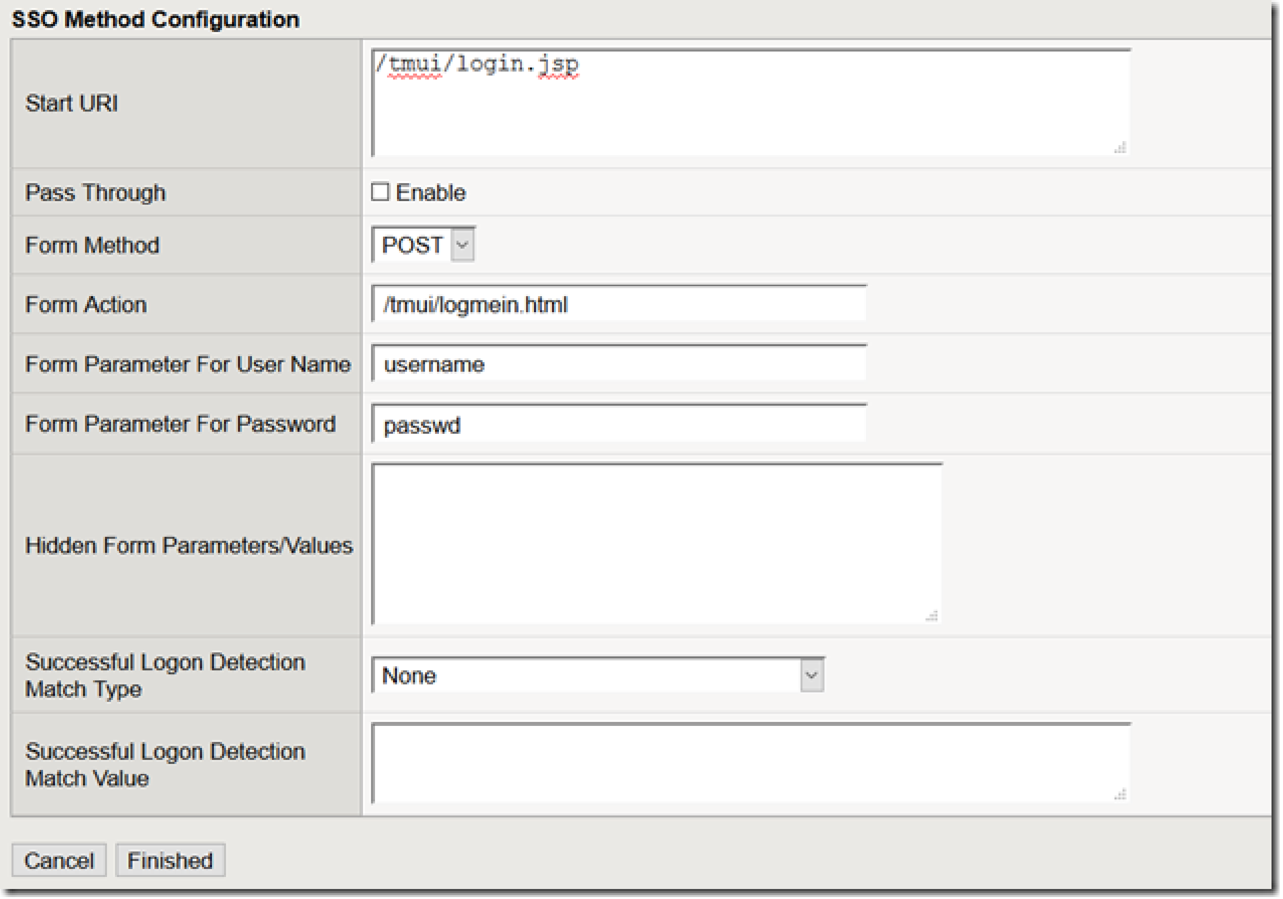
Name	f5mgmtgui_SSO
SSO Method	Forms
Use SSO Template	None
Headers	Name: Referer Value: https://10.1.20.199/tmui/login.jsp Referer: https://10.1.20.199/tmui/login.jsp
Log Settings	From Access Profile

Credentials Source

Username Source	session.logon.last.username
Password Source	ssion.custom.ephemeral.last.passwor

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/SSO1.png?ver=2018-07-27-052820-337)

- Start URI: **/tmui/login.jsp**
- Form Action: **/tmui/logmein.html**
- Form Parameter For User Name: **username**
- Form Parameter For Password: **passwd**
- Click **Finished**



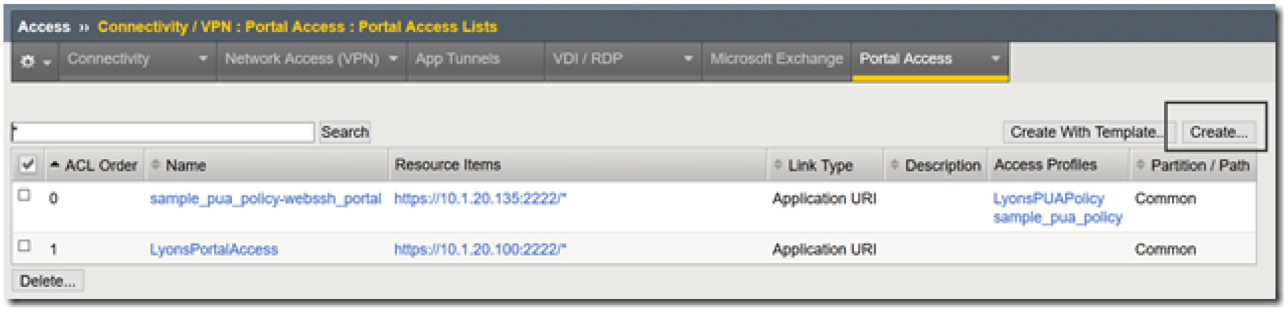
SSO Method Configuration

Start URI	/tmui/login.jsp
Pass Through	☐ Enable
Form Method	POST
Form Action	/tmui/logmein.html
Form Parameter For User Name	username
Form Parameter For Password	passwd
Hidden Form Parameters/Values	
Successful Logon Detection Match Type	None
Successful Logon Detection Match Value	

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/SSO2.png?ver=2018-07-27-052823-053)

Creating a Portal Access List and Resource

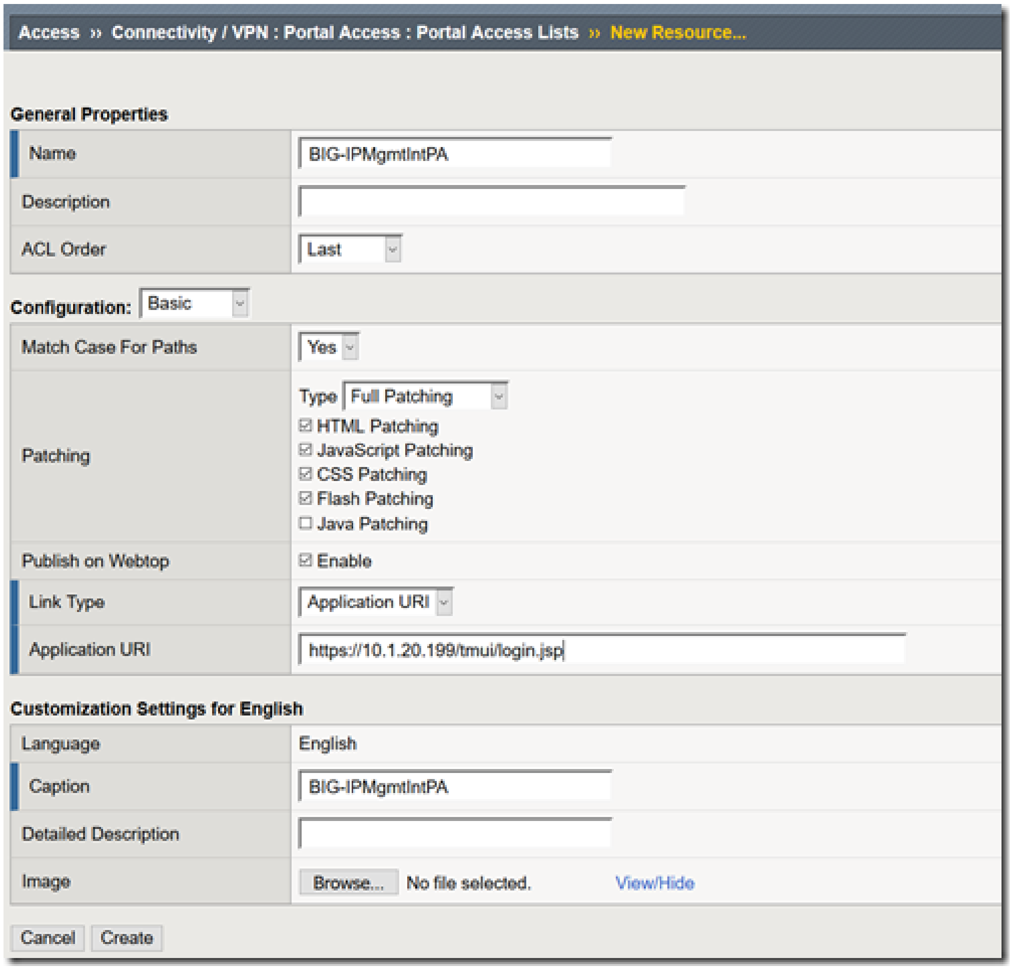
- Navigate to **Access** >> **Connectivity / VPN** >> **Portal Access** >> **Portal Access Lists** >> Click **Create**



☑	ACL Order	Name	Resource Items	Link Type	Description	Access Profiles	Partition / Path
☐	0	sample_pua_policy-webssh_portal	https://10.1.20.135:2222/*	Application URI		LyonsPUAPolicy sample_pua_policy	Common
☐	1	LyonsPortalAccess	https://10.1.20.100:2222/*	Application URI			Common

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/CreatePA.png?ver=2018-07-27-052826-227)

- Name: **BIG-IPMgmtIntPA**
- Link Type: **Application URI**
- Application URI: **https://IPofBIGIPVS/tmui/login.jsp**
- Click **Create**



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

General Properties

Name	BIG-IPMgmtIntPA
Description	
ACL Order	Last

Configuration: Basic

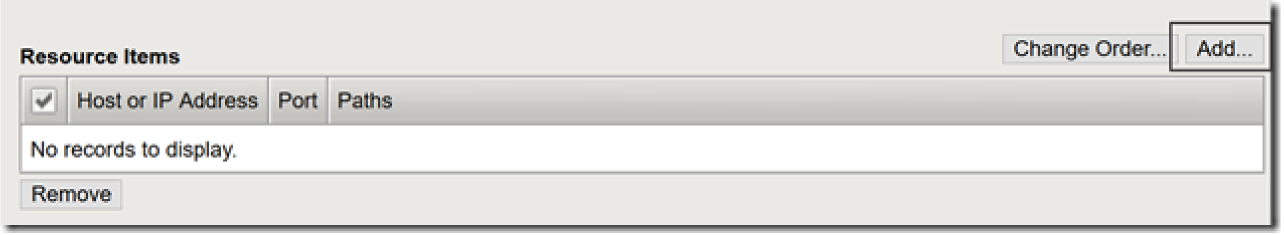
Match Case For Paths	Yes
Patching	Type Full Patching ☑ HTML Patching ☑ JavaScript Patching ☑ CSS Patching ☑ Flash Patching ☐ Java Patching
Publish on Webtop	☑ Enable
Link Type	Application URI
Application URI	https://10.1.20.199/tmui/login.jsp

Customization Settings for English

Language	English
Caption	BIG-IPMgmtIntPA
Detailed Description	
Image	Browse... No file selected. View/Hide

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/CreatePAResource.png?ver=2018-07-27-052829-243)

- After the Portal Access List is created, click the **Add** button in to add a resource.

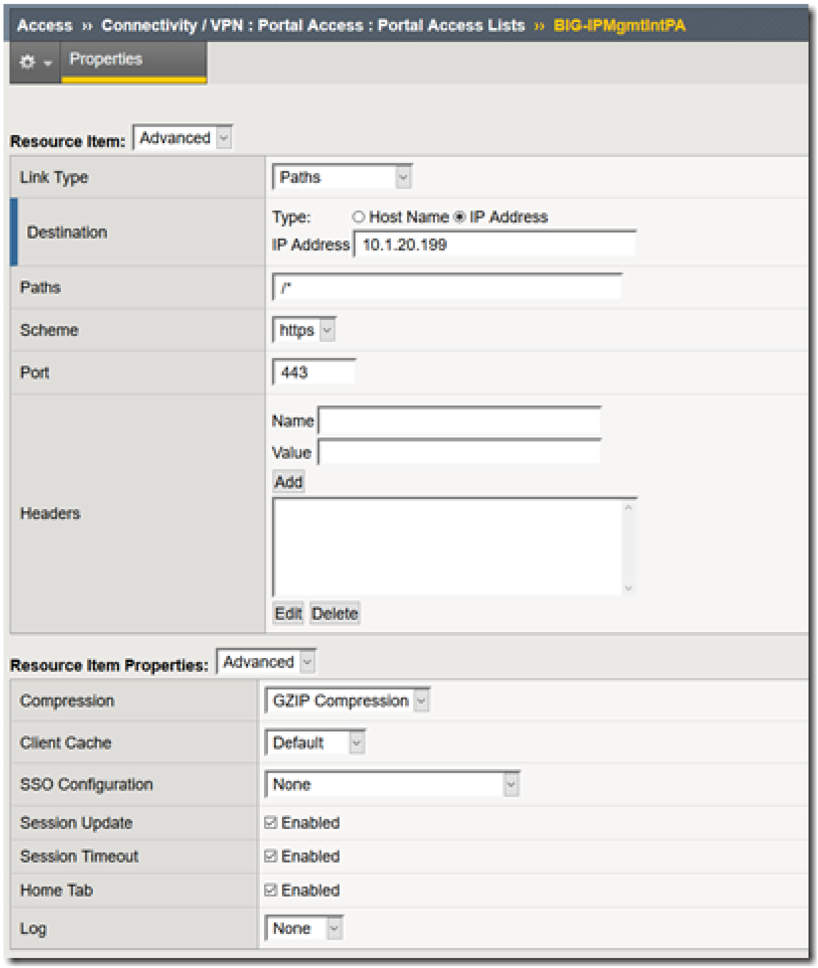


Resource Items

✓	Host or IP Address	Port	Paths
No records to display.			

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/AddResource.png?ver=2018-07-27-052832-633)

- Link Type: **Paths**
- Destination Type: **IP**
- Destination IP Address: **IP of the BIGIP virtual server**
- Paths: /*
- Scheme: **https**
- Port: **443**
- SSO Configuration: **Select the SSO profile created previously in this article**
- Click **Finished**



Access » Connectivity / VPN : Portal Access : Portal Access Lists » BIG-IPMgmtIntPA

Resource Item: Advanced

Link Type	Paths
Destination	Type: ○ Host Name ● IP Address IP Address 10.1.20.199
Paths	/*
Scheme	https
Port	443
Headers	Name Value Add Edit Delete

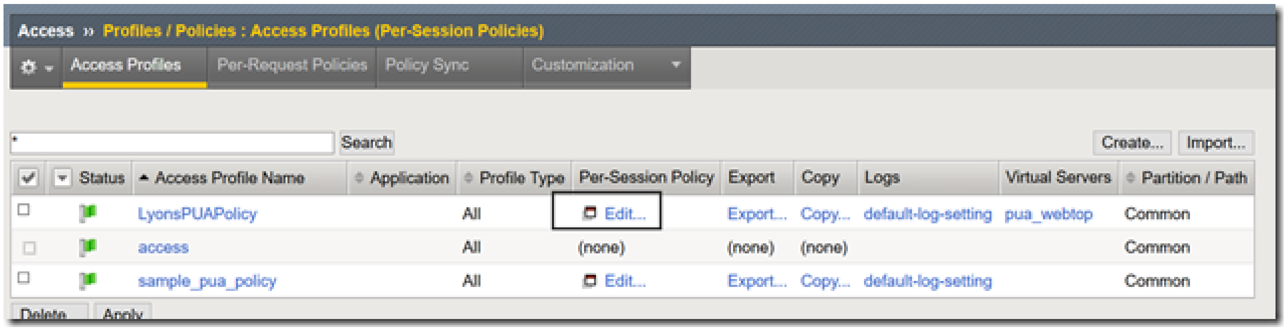
Resource Item Properties: Advanced

Compression	GZIP Compression
Client Cache	Default
SSO Configuration	None
Session Update	☑ Enabled
Session Timeout	☑ Enabled
Home Tab	☑ Enabled
Log	None

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/AddRes1.png?ver=2018-07-27-052836-257)

Assign the new Portal Access Resource

- Navigate to **Access** >> **Profiles / Policies** >> Click the **Edit** button in the row of the PUA Policy created using the previous guide.

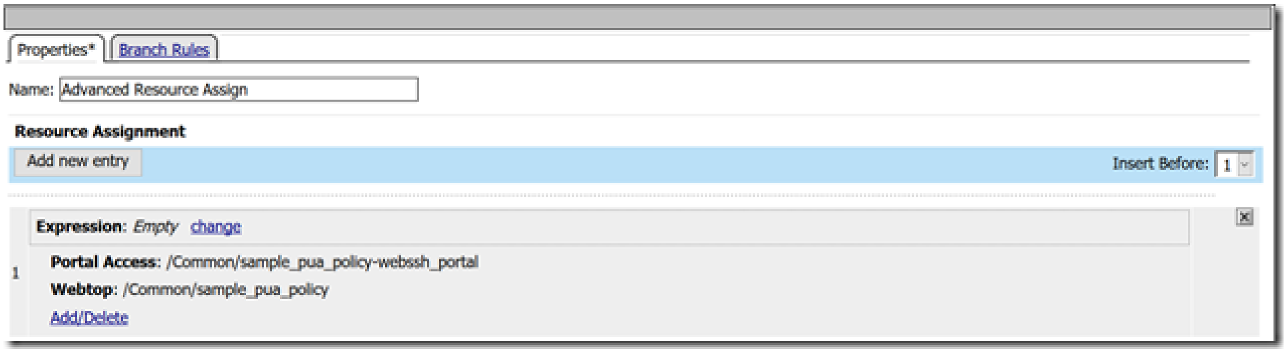


Access » Profiles / Policies : Access Profiles (Per-Session Policies)

☑	Status	Access Profile Name	Application	Profile Type	Per-Session Policy	Export	Copy	Logs	Virtual Servers	Partition / Path
□		LyonsPUAPolicy		All	Edit...	Export...	Copy...	default-log-setting	pua_webtop	Common
□		access		All	(none)	(none)	(none)			Common
□		sample_pua_policy		All	Edit...	Export...	Copy...	default-log-setting		Common

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/EditPUAPolicy.png?ver=2018-07-27-052839-460)

- From the Admin Access Macro click **Advanced Resource Assign**
- Click the **Add / Delete** Button from the Resource Assignment page.



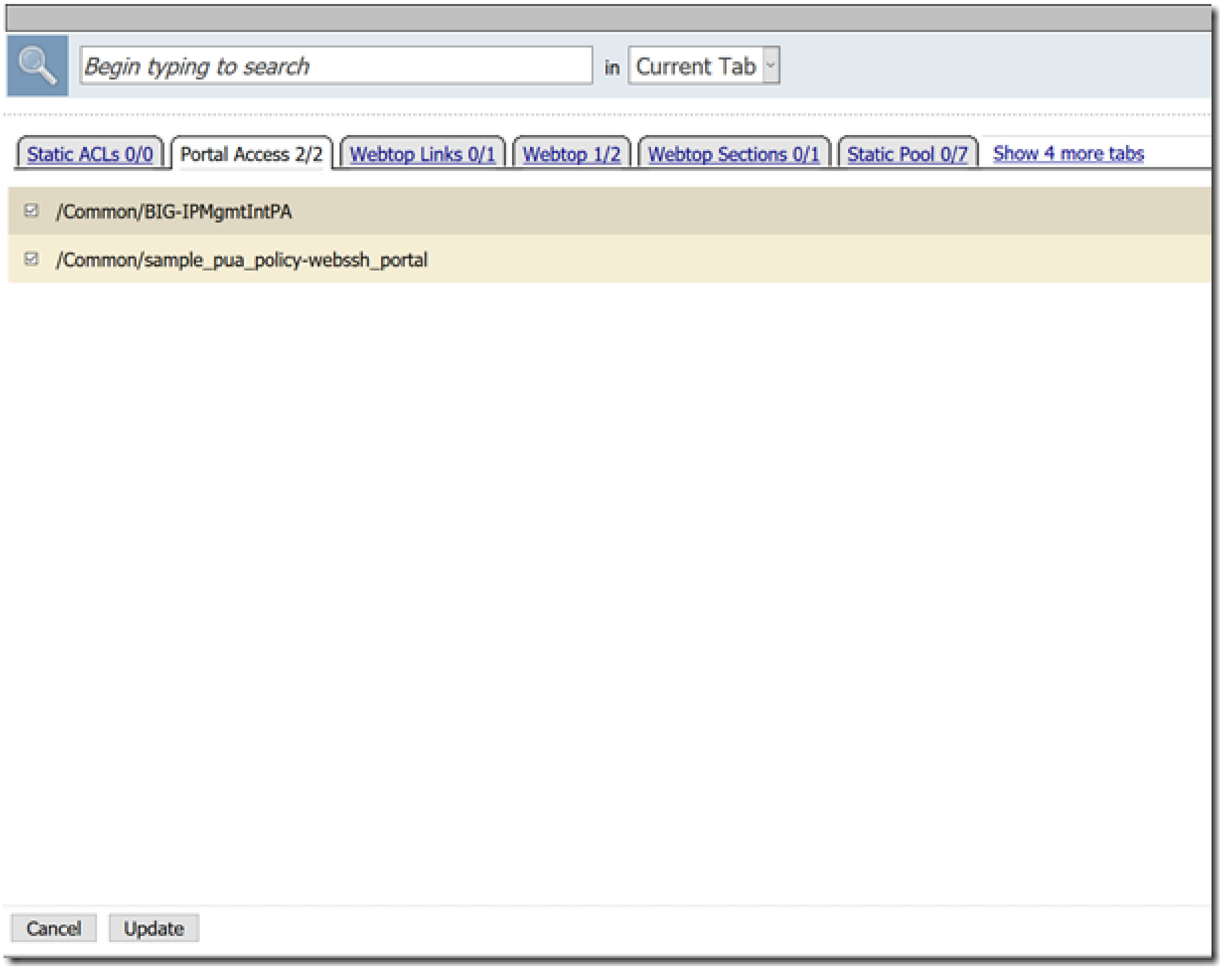
Name: Advanced Resource Assign

Resource Assignment

1 **Expression:** *Empty*
Portal Access: /Common/sample_pua_policy-webssh_portal
Webtop: /Common/sample_pua_policy

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/AddPAtoPolicy.png?ver=2018-07-27-052842-837)

- Select the **Portal Access** tab and place a check mark next to the portal access resource created in the previous steps.
- Click **Update**
- Click **Apply Access Policy**



☑ /Common/BIG-IPMgmtIntPA
☑ /Common/sample_pua_policy-webssh_portal

(https://devcentral.f5.com/s/Portals/0/Users/122/54/236154/CheckBox.png?ver=2018-07-27-052846-070)

Validation Testing

- From a web browser navigate to webtop.demo.lab.

- Click **OK, Proceed to Application**
- Select your user certificate when prompted and click OK

- From the Webtop, select the portal access resource you created in previous steps.

- If successful, you will be redirected to the BIG-IP TMUI as shown below.

Now you have successfully configured SSO to the BIG-IP TMUI using forms based authentication. I'm sure many of you are wondering how it is possible to perform forms based authentication when I provided no password in this entire article. This is possible because of the ability for the F5 PUA solution to generate a one-time password on behalf of the user and present it to the application. Thanks for following and I will continue with additional use cases and capabilities of the F5 BIG-IP.

Appendix

If for any reason you attempt to logout of TMUI and are logged back in immediately, it is likely because of middle ware you have in place on your workstation though no need to worry, there's an iRule for that! Simply add the following iRule to the Webtop virtual server and you will be good to go.

```
when HTTP_REQUEST {     #log local0. "[HTTP::uri]"     switch -glob [HTTP::uri] {
```

```
}
```

Topics in this Article:

apm (/s/articles?tag=apm) application delivery (/s/articles?tag=application delivery) iruleslx (/s/articles?tag=iruleslx) security (/s/articles?tag=security)

The DevCentral Team (/s/profile/0051T000008OdrBQAS) **(F5 Networks)** **published this new Knowledge.**