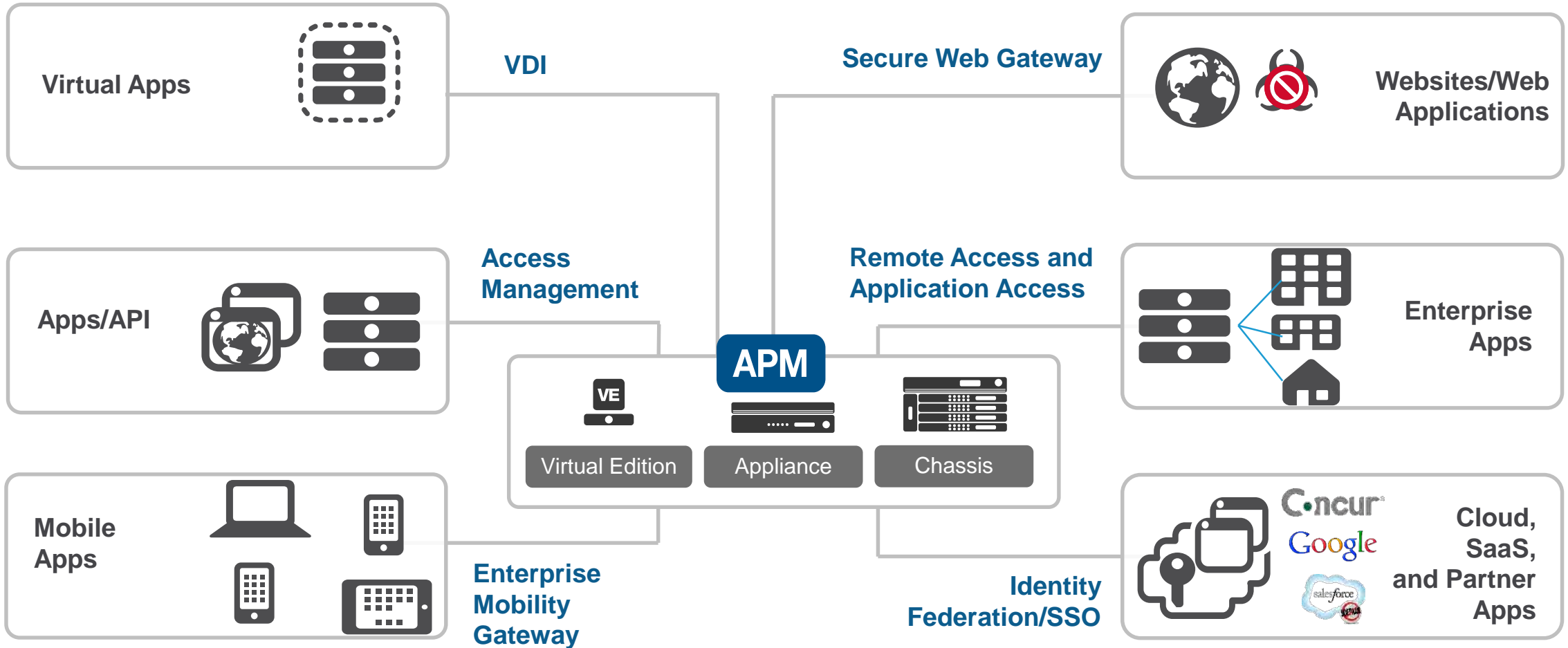


Access Policy Manager

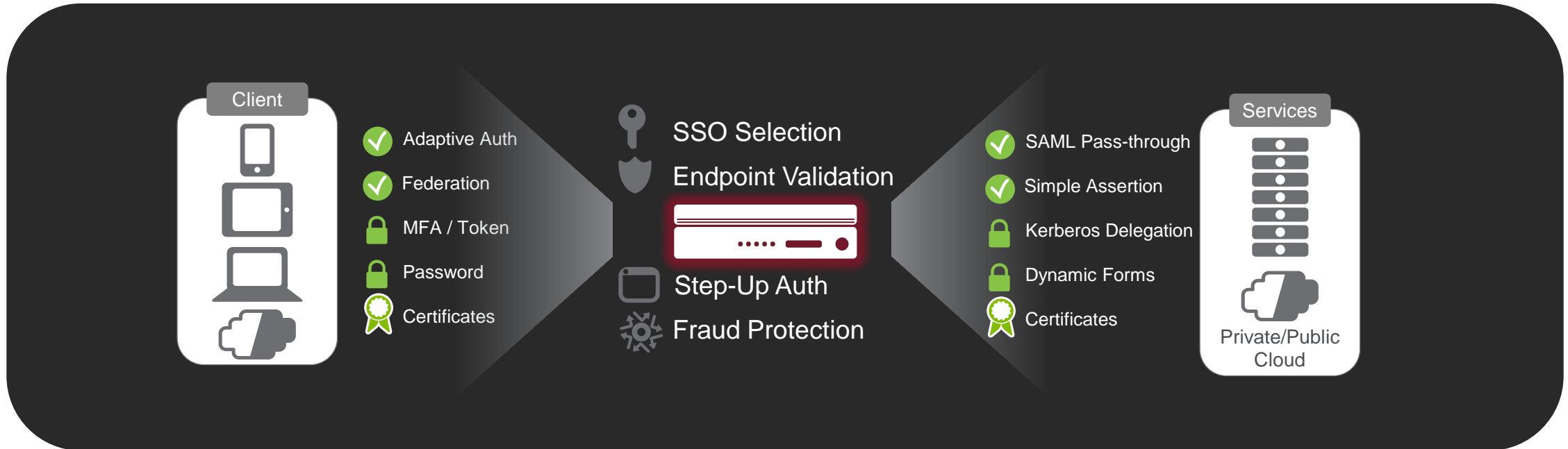
Smart Card Auth Getting Started

F5's Remote/Application Access Solutions

AUTHENTICATION, AUTHORIZATION, REMOTE ACCESS AND SSO TO ALL APPLICATIONS USING ACCESS POLICY MANAGER (APM)



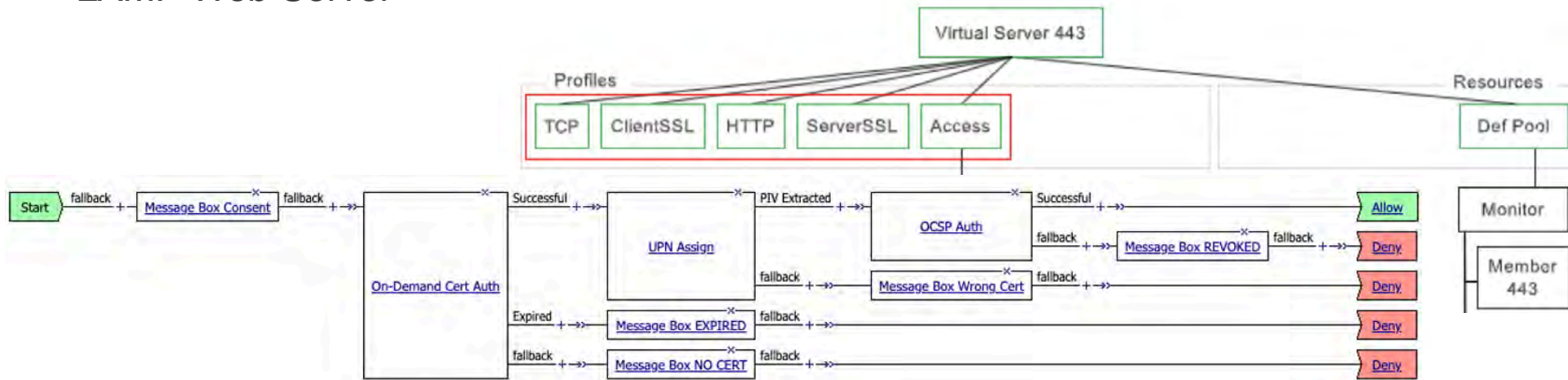
F5 Access Policy Manager (APM)



- Transform one type of authentication into another so an app may understand and use it without installing additional agents
- Allow flexible selection of SSO technique appropriate to the application
- Allow for centralized session control of all applications, even SaaS

Working Environment

- Windows 10 Workstation
- BIG-IP VE 15.1.0.2
 - Licensed and provisioned with LTM and APM
- LAMP Web Server



Enable Smart Card Authentication in BIG-IP APM

1. Generate CA Bundle(s)
2. Client SSL Profile
3. Create Pool
4. Virtual Server
5. Verify Virtual Server works
6. Access Profile
7. Verify Smart Card authentication works
8. Customize message boxes

Generate CA Bundles and Import into BIG-IP

The image shows a multi-step process:

- File Explorer:** A window titled 'Certificate' is open, showing a toolbar with 'Refresh', 'Uninstall', 'Certificate Clean', and 'Action' buttons. A red circle highlights the 'Copy' button.
- Command Prompt:** A terminal window shows the command `C:\Users\grabe\Desktop\CAFiles\RootCAs>type *.cer > DODRootCAs.pem` and the output `DoD_Root_CA_2_0x05_DoD_Root_CA_2.cer`.
- BIG-IP Web Interface:** The 'Import SSL Certificates and Keys' dialog is shown. The 'SSL Certificate/Key Source' section includes:
 - Import Type:** Certificate
 - Certificate Name:** DODRootCAs
 - Certificate Source:** Upload File (selected), Paste Text. The 'Choose File' button shows 'DODRootCAs.pem'.
 - Free Space on Disk:** 3990 MB

Create CA Bundle using CA Bundle Manager

System » Certificate Management : Traffic Certificate Management : Bundle Manager List » **New Bundle Manager...**

General Properties

| | |
|-------------|---------------|
| Name | DOD-CA-BUNDLE |
| Description | |

Configuration

Include Bundles

| Selected |
|------------|
| /Common |
| DODIDCAs |
| DODRootCAs |

Update Interval: 0 days

Update Now:

Trusted CA-Bundle: Select...

Proxy Server:

Proxy Server Port: 3128

Download Timeout: 8 seconds

Cancel Finished

System » Certificate Management : Traffic Certificate Management : SSL Certificate List » **DOD-CA-BUNDLE.crt**

Settings Certificate Key Certificate Signing Request Instances

General Properties

| | |
|------------------------|--|
| Name | DOD-CA-BUNDLE.crt |
| Partition / Path | Common |
| Certificate Subject(s) | DoD Root CA 3, U.S. Government DOD ID CA-49, U.S. Government DOD ID CA-50, U.S. Government DOD ID CA-51, U.S. Government DOD ID CA-52, U.S. Government |

Certificate Properties

| | |
|-----------------|-----------|
| Public Key Type | RSA |
| Public Key Size | 2048 bits |

Create ClientSSL Profile

Local Traffic » Profiles : SSL : Client » F5DODUG-ClientSSL

Properties

General Properties

| | |
|------------------|-------------------|
| Name | F5DODUG-ClientSSL |
| Partition / Path | Common |
| Parent Profile | clientssl |

Configuration: Basic Custom

Certificate Key Chain

/Common/default.crt /Common/default.key

Add Edit Delete

OCSP Stapling

Notify Certificate Status to Virtual Server

Proxy SSL

Proxy SSL Passthrough

Client Authentication Custom

| | |
|------------------------------------|---|
| Client Certificate | ignore |
| Frequency | once |
| Retain Certificate | <input checked="" type="checkbox"/> Enabled |
| Certificate Chain Traversal Depth | 1 |
| Trusted Certificate Authorities | DOD-CA-BUNDLE.crt |
| Advertised Certificate Authorities | DODIDCAs |

Create Pool

Local Traffic » Pools : Pool List » New Pool...

Configuration: Basic

Name: F5DODUG-Pool

Description:

Health Monitors:

- Active: /Common, https
- Available: http_head_f5, https_443, https_head_f5, icmp_mon, inband

Resources

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

New Members:

New Node New FQDN Node Node List

Node Name: (Optional)

Address: 192.168.10.39

Service Port: 443 HTTPS

Add

| Node Name | Address/FQDN | Service Port | Auto Populate | Priority |
|---------------|---------------|--------------|---------------|----------|
| 192.168.10.39 | 192.168.10.39 | 443 | | 0 |

Edit Delete

Cancel Repeat Finished

Create Virtual Server

Local Traffic » Virtual Servers : Virtual Server

General Properties

| | |
|--------------------------|---|
| Name | F5DODUG-V |
| Description | |
| Type | Standard |
| Source Address | <input checked="" type="radio"/> Host <input type="radio"/> Address |
| Destination Address/Mask | <input checked="" type="radio"/> Host <input type="radio"/> Address 192.168.10.7 |
| Service Port | <input checked="" type="radio"/> Port <input type="radio"/> Port 443 |

Configuration: Basic

| | |
|----------------------------|----------------------|
| Protocol | TCP |
| Protocol Profile (Client) | tcp |
| Protocol Profile (Server) | (Use Client Profile) |
| HTTP Profile (Client) | http |
| HTTP Profile (Server) | (Use Client Profile) |
| HTTP Proxy Connect Profile | None |
| FTP Profile | |
| RTSP Profile | |
| SSH Proxy Profile | |
| SSL Profile (Client) | |
| SSL Profile (Server) | |

Enabled

Policies

Default Pool: F5DODUG-Pool

Default Persistence Profile: None

Fallback Persistence Profile: None

Cancel **Finished**

SSL Profile (Server): serverssl

- /Common
- C3D_ClientCA_ServerSSL
- apm-default-serverssl
- crypto-client-default-serverssl
- f5aas-default-ssl
- pcoip-default-serverssl
- serverssl-insecure-compatible

Verify Virtual Server Works



The image shows a screenshot of a web browser window. The address bar displays `https://www.test.local/`. The page content includes a 'Welcome to the Web Server' message and a section for 'SSL/TLS Information'. The network details on the left side of the browser window are as follows:

Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.test.local
Connection: Keep-Alive

SSL/TLS Information

Certificate Cipher ECDHE-RSA-AES128-GCM-SHA256

Certificate Protocol TLSv1.2

Create OCSP Responder Server

Access » Authentication » New Server...

General Properties

| | |
|------|----------------|
| Name | DISA_OCSP |
| Type | OCSP Responder |

Configuration: Basic

| | |
|----------------------------|-----------------------|
| URL | http://ocsp.disa.mil/ |
| Certificate Authority File | DOD-CA-BUNDLE.crt |
| Certificate Authority Path | |

Cancel Finished

Create Access Profile

Access » Profiles / Policies : Access Profiles (Per-Session Policies) » **New Profile...**

General Properties

- Name
- Parent Profile
- Profile Type
- Profile Scope
- Customization Type

Language Settings

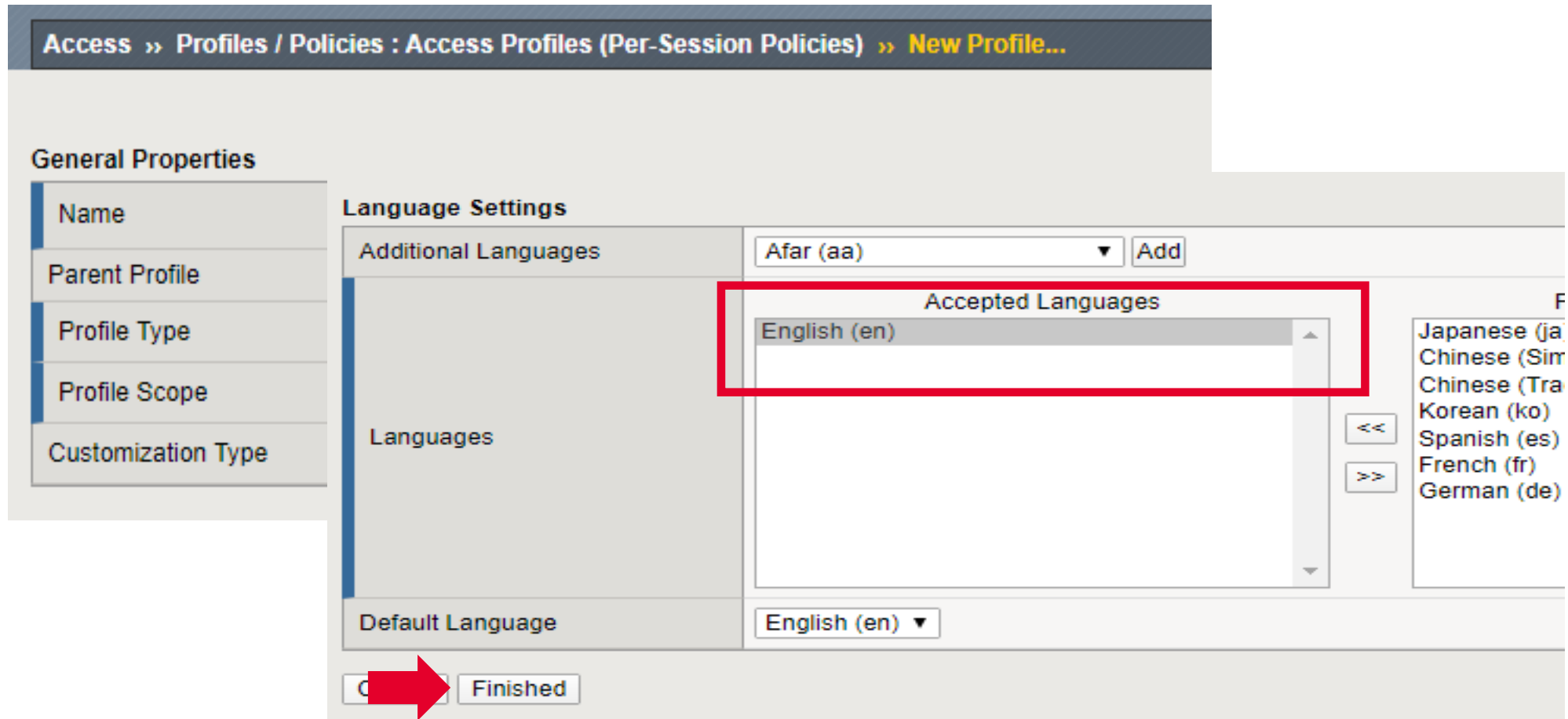
Additional Languages: Afar (aa) Add

Accepted Languages: English (en)

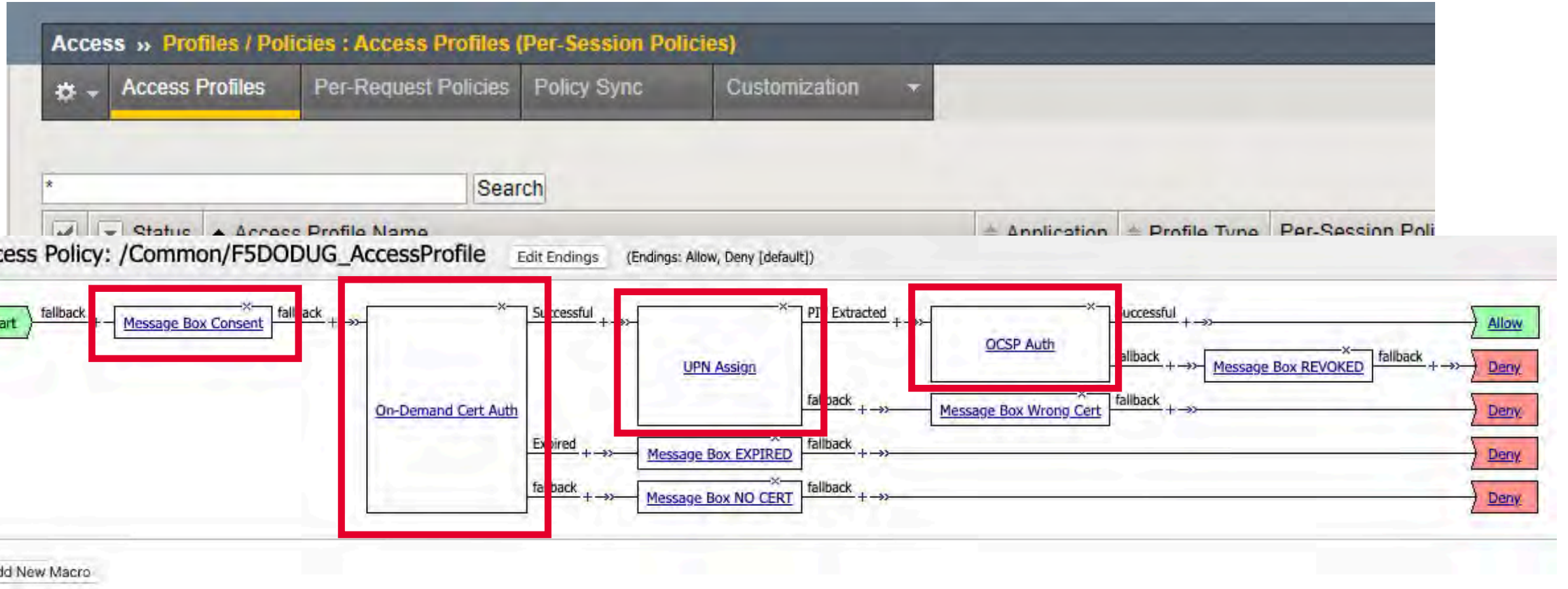
Default Language: English (en)

Japanese (ja)
Chinese (Sim)
Chinese (Tra)
Korean (ko)
Spanish (es)
French (fr)
German (de)


Finished



Modify Access Policy



Apply Access Profile to Virtual Server

| Access Policy | |
|--|---|
| Access Profile |  F5DODUG_AccessProfile ▼ |
| Connectivity Profile | + None ▼ |
| Per-Request Policy | None ▼ |
| VDI Profile | None ▼ |
| Application Tunnels (Java & Per-App VPN) | <input type="checkbox"/> Enabled |
| OAM Support | <input type="checkbox"/> Enabled |
| ADFS Proxy | <input type="checkbox"/> Enabled |
| PingAccess Profile | None ▼ |

Verify Virtual Server Works with Access Profile

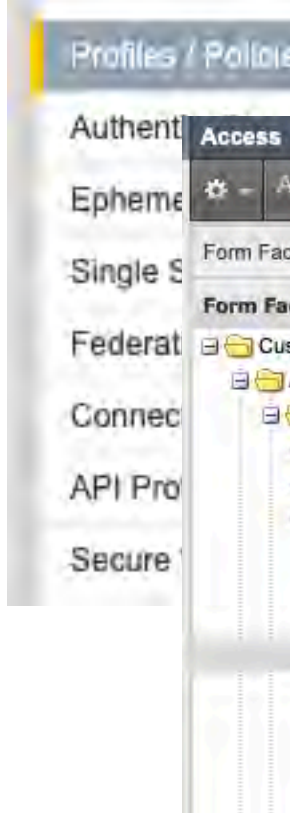
The image shows a browser window with the URL `https://www.test.local/my.policy_nonce?nonce=FwrxoRXkdLkBG7Fq`. The page displays the F5 logo and a message: "You've selected the wrong certificate. Please select the certificate that contains PIV@mil." Below this message is a link: [Click here to continue](#). In the foreground, a "DOD CONSENT" dialog box is visible, also featuring the F5 logo and a link: [Click here to continue](#). At the bottom of the dialog, there is an "OK" button.

Welcome to the V

v:11.0) like Gecko

800; TIN=296000

SSL/TLS Infor



Department of Defense Consent Banner

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

- 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.

OK, Proceed To Application

More Resources

APM Training videos

- <https://devcentral.f5.com/s/articles/Free-F5-Training-Getting-Started-with-BIG-IP-APM>

YouTube

- <https://www.youtube.com/user/f5networksinc>
- <https://www.youtube.com/user/devcentral>
- <https://www.youtube.com/channel/UCMiRji4gfmK-PKB6CN5HmGA> - F5 Government Solutions

LearnF5

- <https://account.f5.com/learnf5/signin>

Webinars

- <https://www.f5.com/company/events/webinars>

Support

- <https://support.f5.com/csp/home>

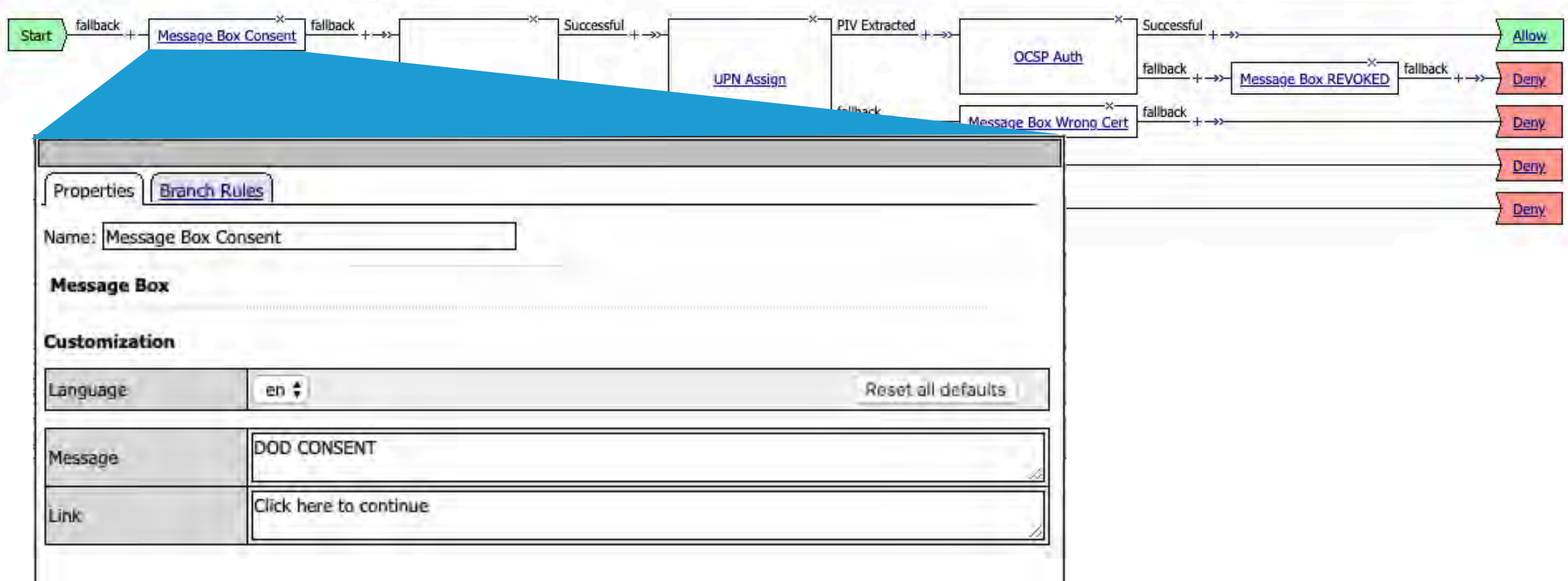
Q&A



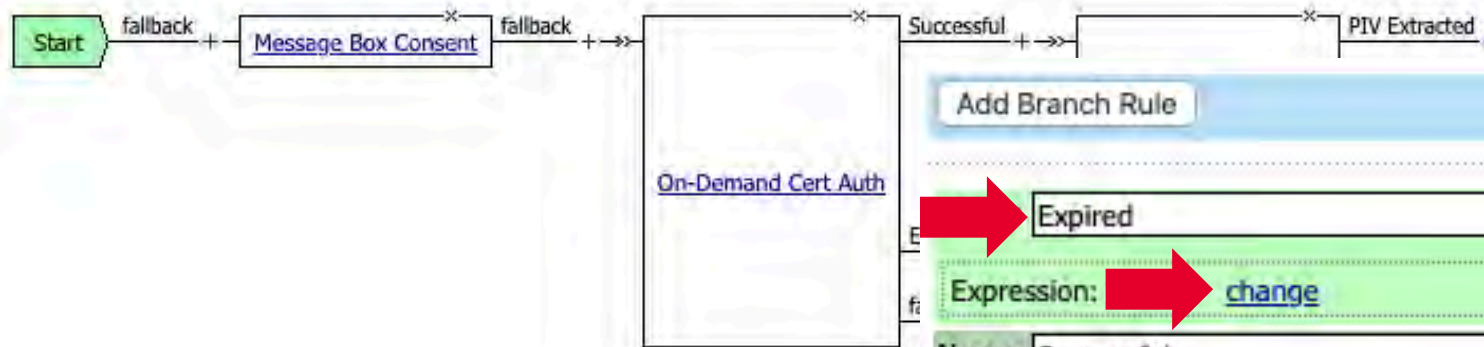
Appendix/Backup APM

Access Profile Policy Continued

Access Policy: /Common/F5DODUG_AccessProfile [Edit Endings](#) (Endings: Allow, Deny [default])



Add Branch Rule



Add Branch Rule

Insert Before: 1: Expired

Expired

Expression: change

Name: Successful

Expression: Client Certificate

Name: fallback

Advanced*

```

expr {[mcget {session.ssl.cert.valid}] == "0"}
  
```

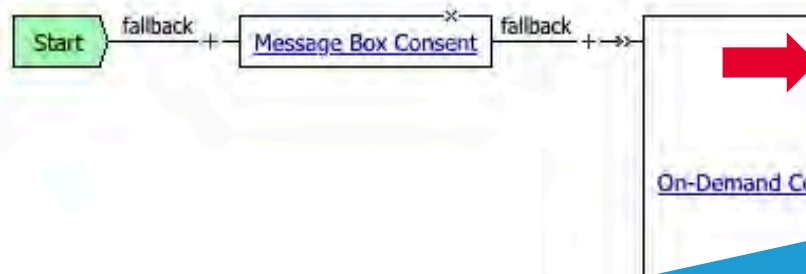
Properties Branch Rules

Name: On-Demand Cert Auth

On-Demand Cert Auth

Auth Mode

Request



Properties Branch Rules

Add Branch Rule Insert Before: 1: PIV Extracted

Name: PIV Extracted

Expression: `expr {[mcget {session.logon.last.username}] != "UPN-NOT-FOUND"}` [change](#)

Name: fallback

Properties Branch Rules

Name: UPN Assign

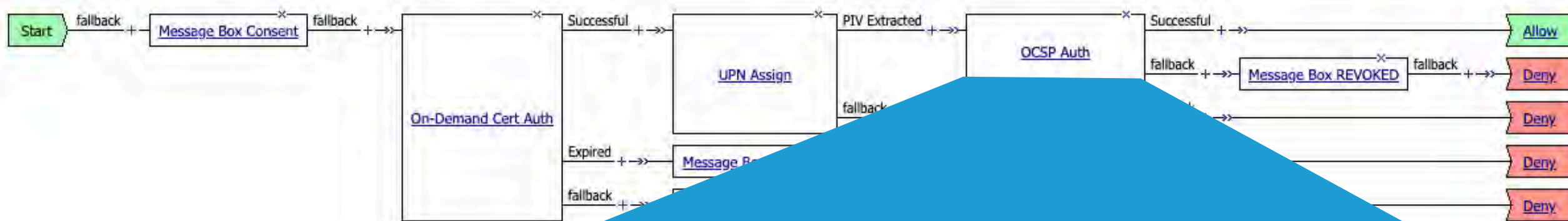
Variable Assign

Add new entry Insert Before: 1

Assignment

```
1 session.logon.last.upn = set x509e_fields [split [mcget {session.ssl.cert.x509extension}] "\n"]; # For each element in the list: foreach field $x509e_fields { # If the element contains UPN: if { $field contains "othername:UPN" } { ## set start of UPN variable set start [expr {[string first "othername:UPN<" $field +14]} # UPN format is <user@domain> # Return the UPN, by finding the index of opening and closing brackets, then use string range to get everything between. return [string range $field $start [expr {[string first ">" $field $start] - 1 } ] ]; } } # Otherwise return UPN Not Found: return "UPN-NOT-FOUND"; change
```


```
2 session.logon.last.username = set upn [mcget {session.logon.last.upn}]; if {[string first "@" $upn] >= 0} { return [string range $upn 0 [expr {[string first "@" $upn] - 1 } ] ]; } else { return $upn; } change
```

Properties **Branch Rules**

Name:

OCSP Auth Agent

| | |
|------------------|---|
| OCSP Responder |  /Common/DISA_OCSP |
| Certificate Type | User |

Consent Banner Appendix

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head><title>Department of Defense</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"><!--/
if(self != top) { top.location = self.location; }
window.onerror=function(){ return function(){ return; } }
<? include_customized_page("logout", "session_expired.js"); ?>
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)", globalTimeoutInterval);
}
function dropdown(){
var allDIVs = document.getElementsByTagName('div');
for(i=0; i < allDIVs.length; i++) {
if(allTDs[i].innerHTML.indexOf('region') > 0 ) {
var replacetext = '<select name="region" value="" autocomplete="off">{%session.custom.cas_pool}</select>';
allTDs[i].innerHTML = replacetext;
}
}
}
function SubmitResult(choice) {
var f = document.getElementById("hidden_form");
f.my_result.value = 1;
f.submit();
}
-->
</script>
<style type="text/css">
BODY {
text-align:center;
background-color: rgb(162, 208, 255);margin: 0 0 0 0;
}
#shadow-container {
margin:20px auto 0 auto;width:612px
```

UPN Assign Appendix

session.logon.last.upn

```
set x509e_fields [split [mcget
{session.ssl.cert.x509extension}] "\n"];
# For each element in the list:
foreach field $x509e_fields {
# If the element contains UPN:
if { $field contains "othername:UPN" } {
## set start of UPN variable
set start [expr {[string first "othername:UPN<"
$field] +14}]
# UPN format is <user@domain>
# Return the UPN, by finding the index of
opening and closing brackets, then use
string range to get everything between.
return [string range $field $start [expr { [string
first ">" $field $start] - 1 } ] ]; } }
# Otherwise return UPN Not Found:
return "UPN NOT-FOUND";
```

session.logon.last.username

```
set upn [mcget {session.logon.last.upn}]; if {[string first
"@ " $upn] >= 0} {
return [string range $upn 0 [expr { [string first "@ " $upn]
- 1 } ] ]; } else { return $upn; }
```