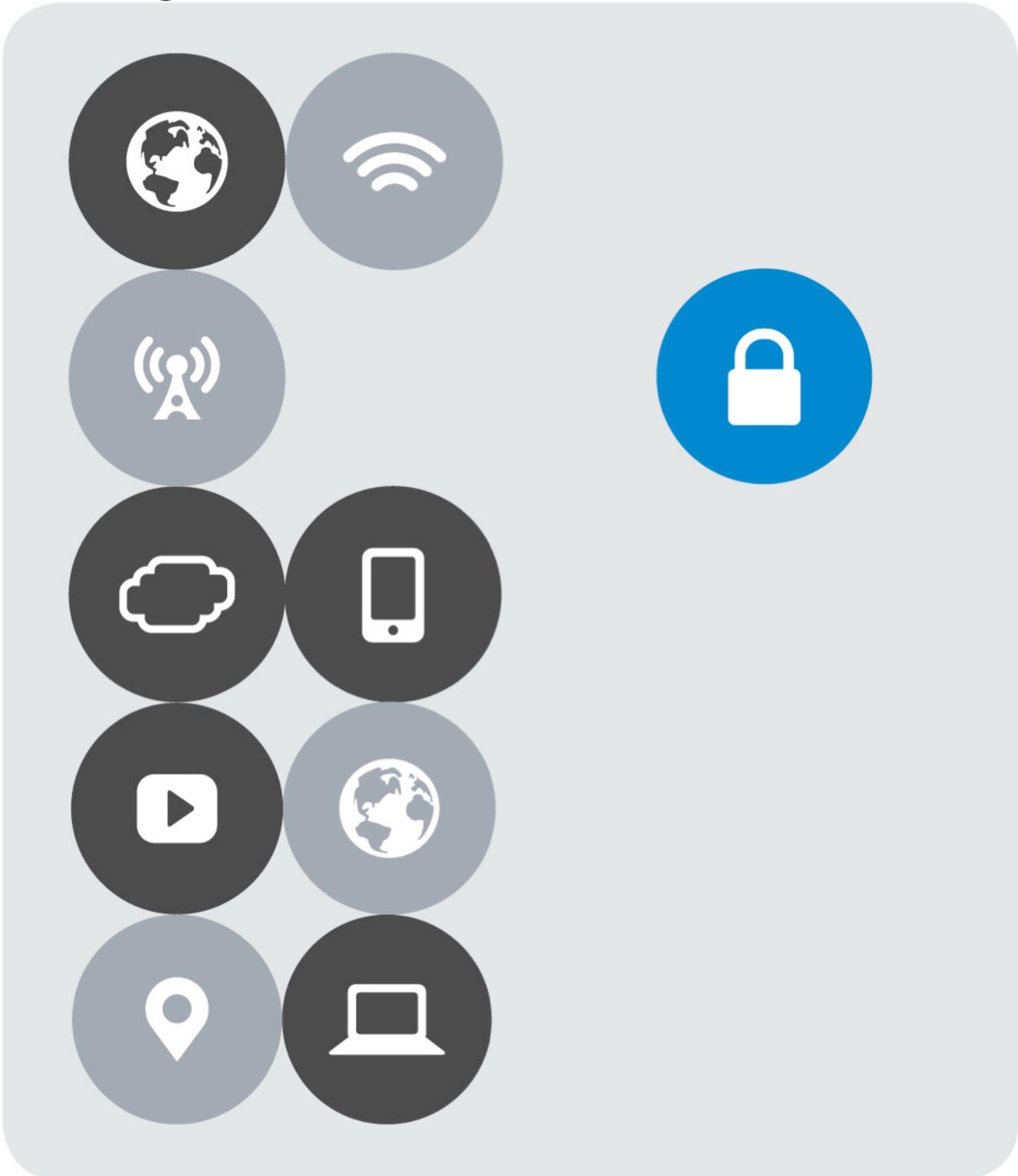




vmware®

INTEGRATION GUIDE

Load Balancing VMware Identity Manager





Version History

Date	Version	Author	Description	Compatible Versions
May 2018	3.0	Matt Mabis	Updates for MobileSSO, and Changes to some of the configurations.	VMware Identity Manager 2.x, 3.x (1)
May 2017	2.0	Matt Mabis	Update for Monitor in 2.x Editions and New VMWare Delivery Methodology	VMware Identity Manager 2.4.x, 2.6.x, 2.7.x, 2.8.x (1)
Jan 2016	1.0	Justin Venezia	Initial Document with How-To Configure F5 LTM with VMware Workspace/VIDM	VMware Workspace 1.5, 1.8, VMware Identity Manager 2.4 up to 2.7.2 (1) (2)

NOTES:

(1) The Version 1.0 Document only supports up to VMware Identity Manager 2.7.2 as there were changes in the 2.8.x Code that prevents the monitor originally suggested in the 1.0 document from working. Version 2.0 has changed the monitor to a more efficient and advanced monitor to determine if the VMware Identity Manager node is online/offline/maintenance. Because of these changes older 1.x Releases of VMware Workspace cannot use this monitor.

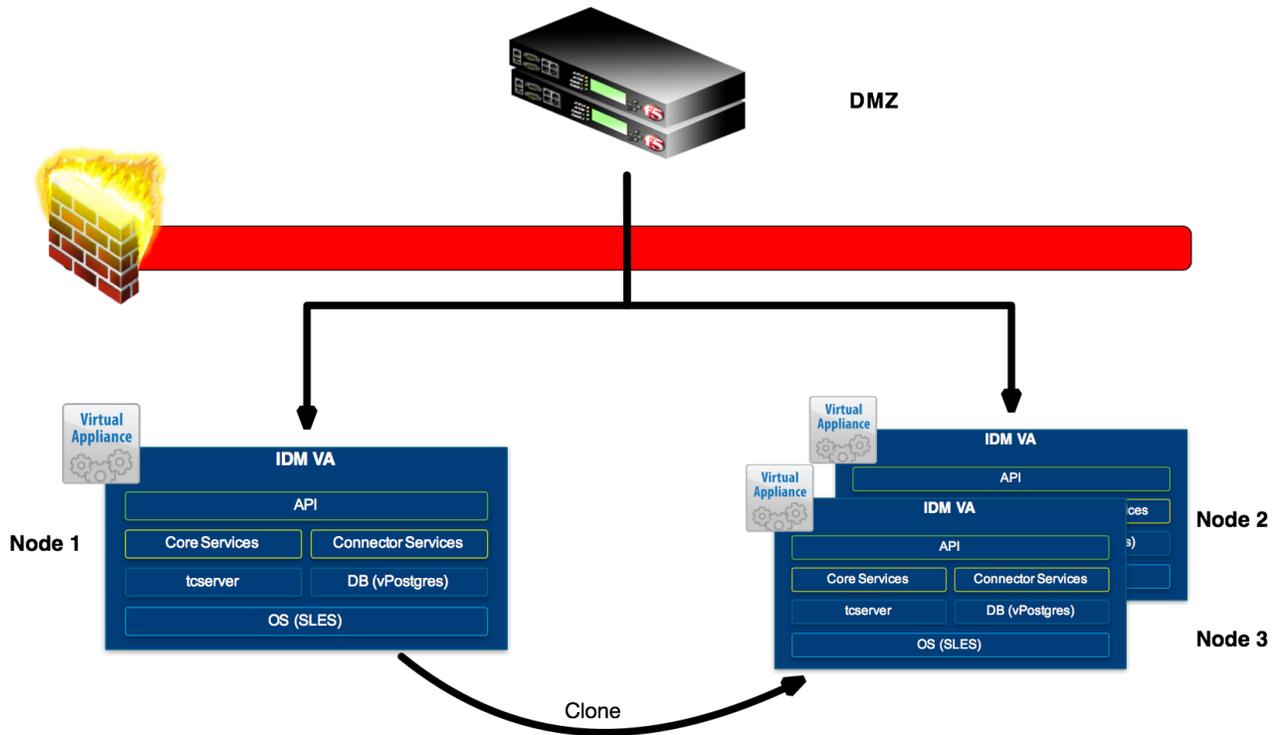
(2) The Version 1.0 Document refers to a different deployment, delivery methodology that was Changed in the 2.8.x releases of VMware Identity Manager. Version 2.0+ of the document is the current suggested path for Deployment by VMware.



Contents

Version History	2
Overview	4
Prerequisites.....	5
F5 BIG-IP Configurations	6
Create a Client SSL Profile.....	6
Create a HTTP Profile	8
Create Persistence Profile (Non-MobileSSO)	9
Create Monitor	10
Create Identity Manager Pool.....	12
Create a Port 443 Virtual Server	13
Create a Port 80 Redirect Virtual Server (Optional).....	16
MobileSSO F5 Configurations (Optional)	19
Create Persistence Profile.....	19
Create Pool	20
Create Port 88 TCP VIP.....	21
Create Port 88 UDP VIP	24
Configuring Root/Primary CA's on BIG-IP and Identity Manager	27
Configuring the FQDN for Identity Manager	33
Enable End User Portal UI for Load Balanced Configurations.....	37
Logging into Identity Manager Portal.....	41
Cloning Nodes 2 and 3	43

Overview



VMware Identity Manager combines applications and desktops in a single, aggregated workspace. Employees can then access the desktops and applications regardless of where they are based. With fewer management points and flexible access, Identity Manager reduces the complexity of IT administration.

Identity Manager is delivered as a virtual appliance (VA) that is easy to deploy onsite and integrate with existing enterprise services. Organizations can centralize assets, devices, and applications and manage users and data securely behind the firewall. Users can share and collaborate with external partners and customers securely when policy allows.

This document provides step-by-step instructions for setting up the first Identity Manager virtual appliance (Node 1), for production implementations VMware recommends the deployment of two (2) additional nodes to have a total of three (3) nodes. Nodes 2 and 3 will be cloned from the first node after it has been configured and setup with the F5 to provide a fully load balanced configuration.

Prerequisites

The following are prerequisites for this solution and must be complete before proceeding with the configuration. Step-by-step instructions for prerequisites are outside the scope of this document, see the BIG-IP documentation on support.f5.com for specific instructions.

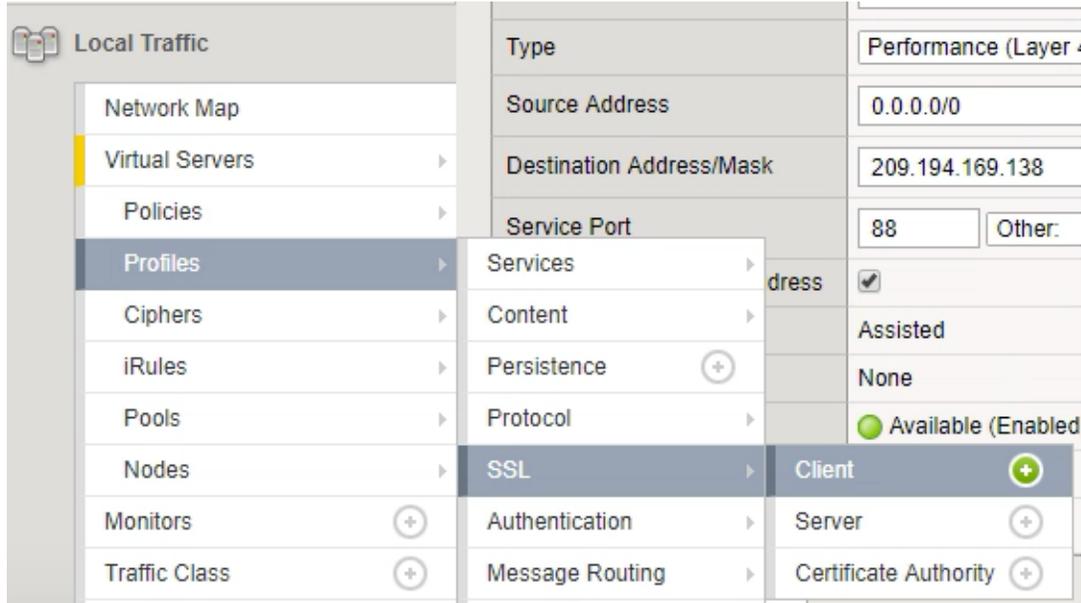
1. F5 recommends running this configuration using BIG-IP LTM version 12.x and 13.x.
2. Create/import an SSL Certificate that contains the load-balanced FQDN that will be used for Identity Manager Portal.
3. Upload the following to the BIG-IP system:
 - The SSL Certificate must be uploaded to the BIG-IP.
 - The Private Key used for the load-balanced FQDN certificate.
 - The Primary CA or Root CA for the SSL Certificate you uploaded to the BIG-IP.
NOTE: The Primary or Root CA for the FQDN Certificate will also be uploaded to the BIG- IP and are required to be loaded on each Identity Manager appliance.
4. Ensure the new FQDN for Identity Manager is in DNS with both forward and reverse records, and points to the Virtual Server IP address on the BIG-IP that will be used for load balancing the Identity Manager appliances.
5. You must have deployed a single instance of VMware Identity Manager fully configured, including the database (VMware Recommends SQL in 3-Node Configuration).

NOTE: VMware recommends the use of Certificates which support Subject Alternate Names (SANs) defining each of the node FQDNs (public or internal) within the load balanced VIP FQDN. Wildcard certificates may be used, but due to wildcard certificate formats, SAN support is typically not available with wildcards from public CAs - and public CAs may complain about supplying an internal FQDN as a SAN value even if they do support SAN values. Additionally, some VMware Identity Manager features may not be usable with wildcard certificates when SAN support is not defined.

F5 BIG-IP Configurations

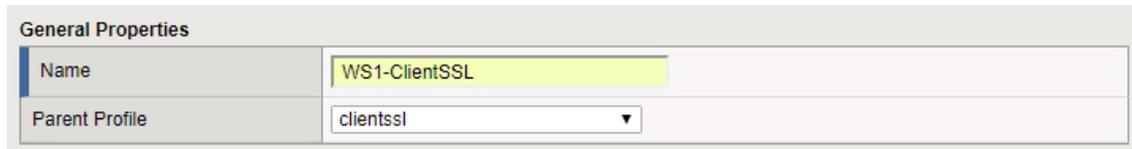
Create a Client SSL Profile

1. In the Local Traffic menus go to Profiles → SSL → Client → (+) plus icon to create a new SSL Client Profile



- a. Click **Local Traffic**.
- b. Hover over **Profiles** to open the Profiles menu.
- c. Hover over **SSL**.
- d. Hover over **Client**.
- e. Click the Add button (+) to the right of Client to create a new SSL Client Profile.

2. In the General Properties section



- a. **Name:** Enter a Unique Name
- b. **Parent Profile:** clientssl

INTEGRATION GUIDE

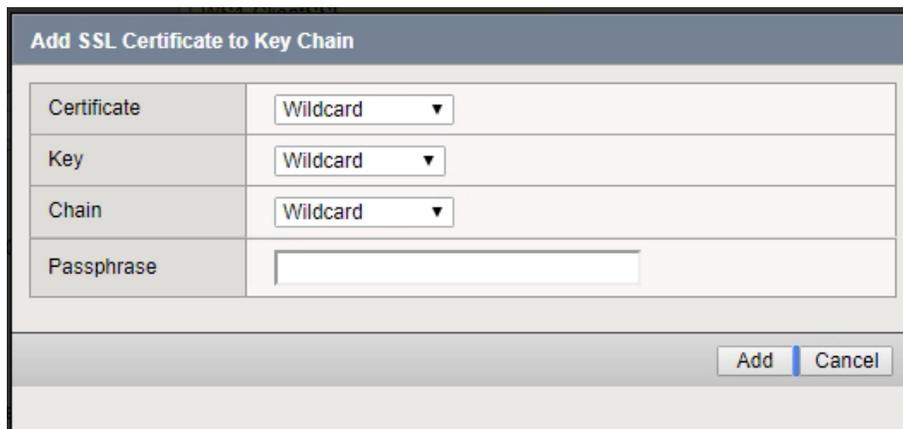
Load Balancing VMware Identity Manager

3. In the Configuration section



- a. In the Certificate Key Chain area, click the **Custom** check box.
- b. Click the **Add** button. The Add SSL Certificate to Key Chain dialog box opens.

4. In the “Add SSL Certificate to Key Chain” popup



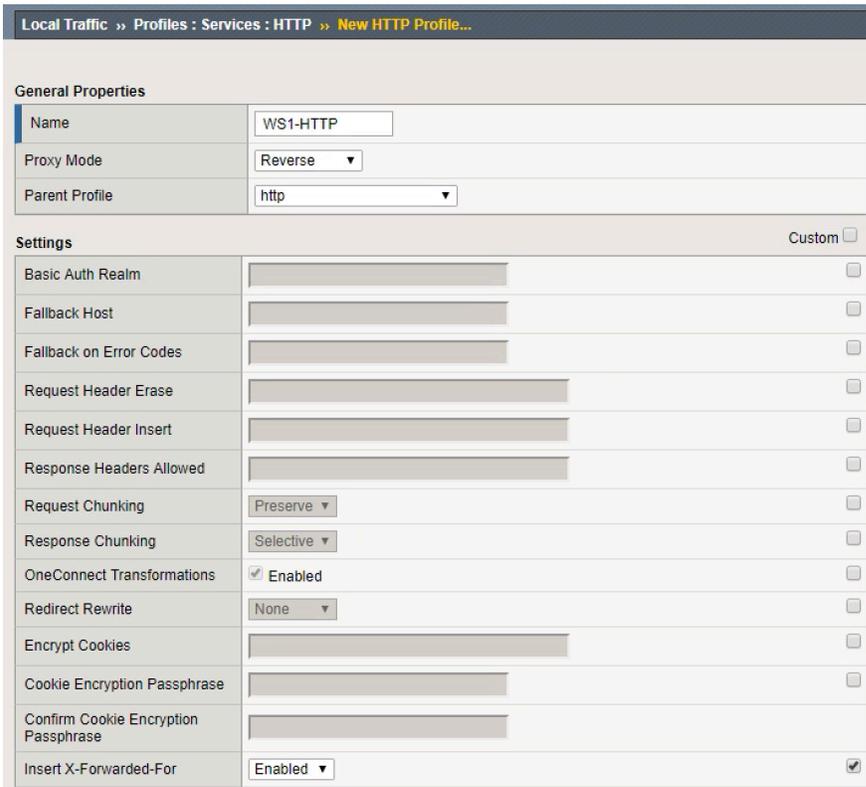
- a. **Certificate:** Select the certificate with the FQDN that you uploaded to the BIG-IP as specified in the prerequisites.
- b. **Key:** Select the certificate key that corresponds with the certificate.
- c. **Chain:** Select the primary or root CA/certificate chain that corresponds with the certificate.
- d. Click the **Add** button to add the certificate key chain to the SSL profile.
- e. Click **Finished**.

Create a HTTP Profile

- From the **Menu** bar, click **Services** (you may need to click **Local Traffic > Profiles** first)



- Click **HTTP** from the pull-down list.
 - Click the **Create** button in the upper right-hand corner of the HTTP Profiles table.
- In the “New HTTP Profile...”



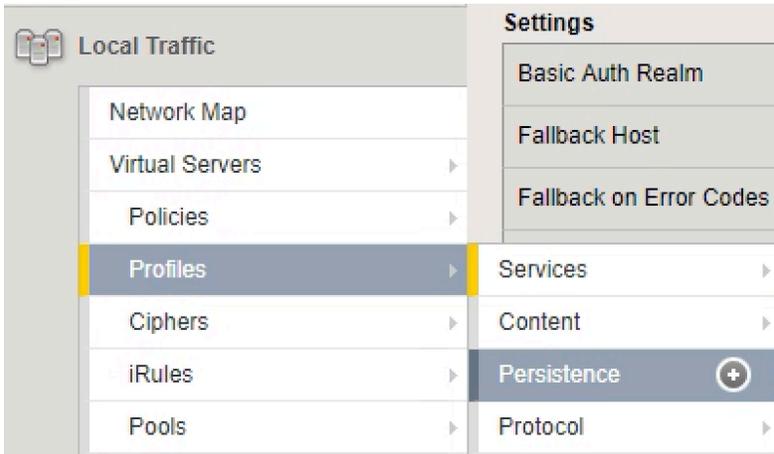
- Name:** Provide a unique name for the instance
- Insert X-Forwarded-For:** Click the **Custom** checkbox and change to **Enabled**
- Scroll to the bottom and click **Finished**

**** Important **** You must enable X-Forwarded-For headers on your BIG-IP system. Identity Manager identifies the source IP address in the X-Forwarded-For headers. Identity Manager determines which authentication method to provide based on this IP address.

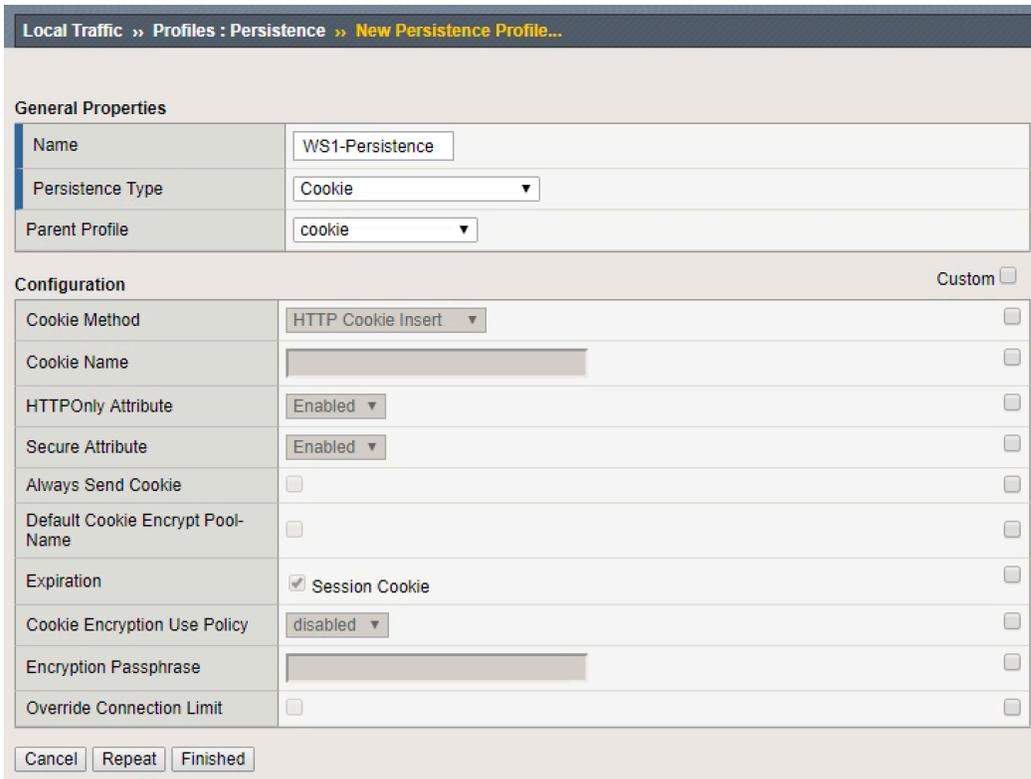
Create Persistence Profile (Non-MobileSSO)

Note: Build only 1 Persistence Profile this profile is specific for Non-MobileSSO users.

1. In the Local Traffic menus go to Profiles → Persistence → (+) plus icon to create a new Persistence Profile



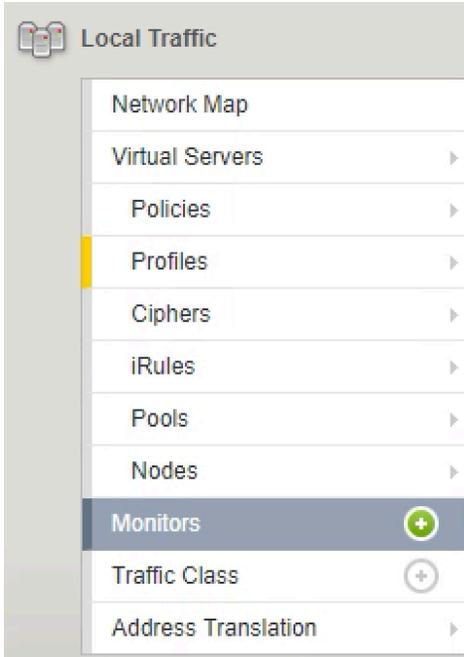
2. In the “New Persistence Profile...”



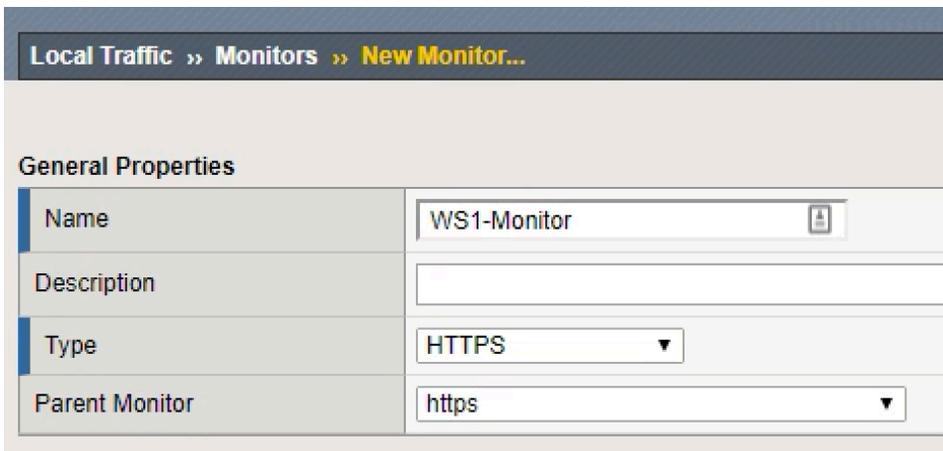
- a. **Name:** Provide a unique name.
- b. **Persistence Type:** select **Cookie**.
- c. Click **Finished**.

Create Monitor

1. In the Local Traffic menus go to Monitors → (+) plus icon to create a new Monitor



2. In the General Properties



- a. **Name:** Provide a Unique name
- b. **Type:** Select **HTTPS** from the pull-down menus

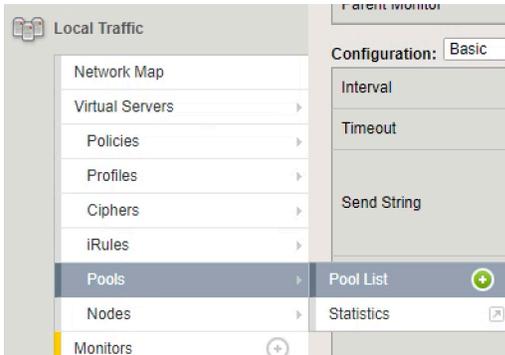
3. In the Configuration Section

Configuration: Basic ▾	
Interval	5 seconds
Timeout	16 seconds
Send String	<code>GET /SAAS/API/1.0/REST/system/health/heartbeat HTTP/1.1\r\nHost: \r\nConnection: Close\r\n\r\n</code>
Receive String	<code>ok\$</code>
Receive Disable String	404
User Name	<input type="text"/>
Password	<input type="password"/>
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alias Address	* All Addresses
Alias Service Port	* <input type="text"/> * All Ports ▾
Adaptive	<input type="checkbox"/> Enabled
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

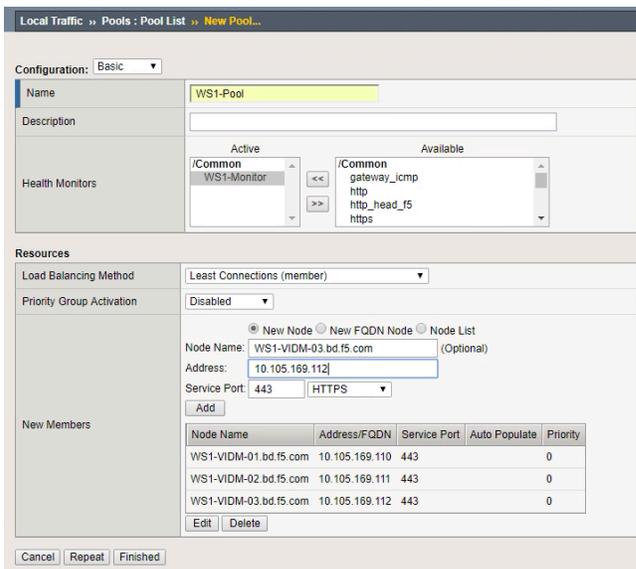
- a. In the **Send String** field, type
`GET /SAAS/API/1.0/REST/system/health/heartbeat HTTP/1.1\r\nHost: \r\nConnection:Close\r\n\r\n`
- b. In the **Receive String** field, type `ok$`
- c. In the **Receive Disable String** field, type `404`
- d. Click **Finished**.

Create Identity Manager Pool

1. In the Local Traffic menus go to Pools → Pool List → (+) plus icon to create a new Pool



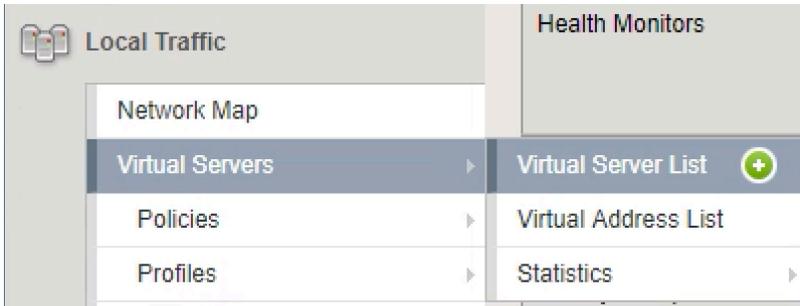
2. In the “New Pool...”



- a. **Name:** Provide a unique name.
- b. **Health Monitors:** use the Add (<<) button to move the monitor previously created to the **Active** list.
- c. **Load Balancing Method:** select **Least Connections (node)**.
- d. In the **New Members** area, complete the following for each Identity Manager node
 - i. **Node Name:** (Optional) Provide the FQDN or Identifier of the Node.
 - ii. **Address:** Provide the IP address of the First Identity Manager Node (Node 1).
 - iii. **Service Port:** type **443** or select **HTTPS** from the list.
 - iv. Click the **Add** button.
 - v. Repeat this step for each additional VMware Identity Manager node (Nodes 2 and 3 so when they are cloned they are available in the cluster).
- e. Click the **Finished** button.

Create a Port 443 Virtual Server

1. In the Local Traffic menus go to Virtual Servers → Virtual Servers List → (+) plus icon to create a new Virtual Server



2. In the General Properties section.

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

General Properties	
Name	WS1-VS-443
Description	
Type	Standard ▼
Source Address	
Destination Address/Mask	10.105.169.11
Service Port	443 HTTPS ▼
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled ▼

- a. **Name:** Provide a unique name.
- b. **Destination Address/Mask:** type the IP Address associated to the FQDN for the virtual server.
- c. **Service Port:** type 443 or select **HTTPS** from the list.

3. In the Configuration section.

Configuration: Basic					
Protocol	TCP				
Protocol Profile (Client)	tcp-wan-optimized				
Protocol Profile (Server)	tcp-lan-optimized				
HTTP Profile	WS1-HTTP				
HTTP Proxy Connect Profile	None				
FTP Profile	None				
RTSP Profile	None				
SSL Profile (Client)	<table border="1"> <thead> <tr> <th>Selected</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td>/Common WS1-ClientSSL</td> <td>/Common WorkspaceOne-SSL clientsssl clientsssl-insecure-compatible clientsssl-secure</td> </tr> </tbody> </table>	Selected	Available	/Common WS1-ClientSSL	/Common WorkspaceOne-SSL clientsssl clientsssl-insecure-compatible clientsssl-secure
Selected	Available				
/Common WS1-ClientSSL	/Common WorkspaceOne-SSL clientsssl clientsssl-insecure-compatible clientsssl-secure				
SSL Profile (Server)	<table border="1"> <thead> <tr> <th>Selected</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td>/Common serverssl-insecure-compatible</td> <td>serverssl splitssession-default-serverssl wom-default-serverssl /Common/Demo-HZN-CPA.app Demo-HZN-CPA_server_ssl</td> </tr> </tbody> </table>	Selected	Available	/Common serverssl-insecure-compatible	serverssl splitssession-default-serverssl wom-default-serverssl /Common/Demo-HZN-CPA.app Demo-HZN-CPA_server_ssl
Selected	Available				
/Common serverssl-insecure-compatible	serverssl splitssession-default-serverssl wom-default-serverssl /Common/Demo-HZN-CPA.app Demo-HZN-CPA_server_ssl				
SMTSP 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				

- a. **Protocol Profile (Client):** select **tcp-wan-optimized** from the pull-down menus.
- b. **Protocol Profile (Server):** select **tcp-lan-optimized** from the pull-down menus.
- c. **HTTP Profile:** select the HTTP previously created.
- d. **SSL Profile Client:** select the Client SSL profile previously created and click the “<<” button to move to selected.
- e. **SSL Profile (Server):** select **serverssl-insecure-compatible** and click the “<<” button to move to selected.
- f. **Source Address Translation:** select **Auto Map**.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

4. Scroll down to the Resources section.

Resources									
iRules	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td><div style="border: 1px solid gray; height: 40px;"></div></td><td><div style="border: 1px solid gray; padding: 2px;"><i>/Common</i> HTML5-HZN74-Fix-2 Origin-Header-LTM _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth</div></td></tr><tr><td colspan="2" style="text-align: center;"><< >></td></tr><tr><td colspan="2" style="text-align: center;">Up Down</td></tr></tbody></table>	Enabled	Available	<div style="border: 1px solid gray; height: 40px;"></div>	<div style="border: 1px solid gray; padding: 2px;"><i>/Common</i> HTML5-HZN74-Fix-2 Origin-Header-LTM _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth</div>	<< >>		Up Down	
Enabled	Available								
<div style="border: 1px solid gray; height: 40px;"></div>	<div style="border: 1px solid gray; padding: 2px;"><i>/Common</i> HTML5-HZN74-Fix-2 Origin-Header-LTM _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth</div>								
<< >>									
Up Down									
Policies	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td><div style="border: 1px solid gray; height: 40px;"></div></td><td><div style="border: 1px solid gray; height: 40px;"></div></td></tr><tr><td colspan="2" style="text-align: center;"><< >></td></tr></tbody></table>	Enabled	Available	<div style="border: 1px solid gray; height: 40px;"></div>	<div style="border: 1px solid gray; height: 40px;"></div>	<< >>			
Enabled	Available								
<div style="border: 1px solid gray; height: 40px;"></div>	<div style="border: 1px solid gray; height: 40px;"></div>								
<< >>									
Default Pool	+ <div style="border: 1px solid gray; padding: 2px; display: inline-block;">WS1-Pool ▼</div>								
Default Persistence Profile	<div style="border: 1px solid gray; padding: 2px; display: inline-block;">WS1-Persistence ▼</div>								
Fallback Persistence Profile	<div style="border: 1px solid gray; padding: 2px; display: inline-block;">None ▼</div>								

Cancel Repeat Finished

- a. **Default Pool:** select the pool previously created from the pull-down menus.
- b. **Default Persistence Profile:** select the persistence profile previously created from the pull-down menus.
- c. Click the **Finished** button.

Create a Port 80 Redirect Virtual Server (Optional)

1. In the Local Traffic menus go to Virtual Servers → Virtual Servers List → (+) plus icon to create a new Virtual Server



- 2.

Local Traffic » Virtual Servers : Virtual Server List » **New Virtual Server...**

General Properties

Name	WS1-VS-Redirect
Description	
Type	Standard ▼
Source Address	
Destination Address/Mask	10.105.169.11
Service Port	80 HTTP ▼
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled ▼

- a) **Name:** Provide a unique name.
- b) **Destination Address/Mask:** type the IP Address associated to the FQDN for the virtual server.
- c) **Service Port:** type 80 or select HTTP from the list.

3. In the Configuration section.

Configuration: Basic					
Protocol	TCP				
Protocol Profile (Client)	tcp-wan-optimized				
Protocol Profile (Server)	tcp-lan-optimized				
HTTP Profile	WS1-HTTP				
HTTP Proxy Connect Profile	None				
FTP Profile	None				
RTSP Profile	None				
SSL Profile (Client)	<table border="1"> <thead> <tr> <th>Selected</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td></td> <td> /Common WS1-ClientSSL WorkspaceOne-SSL clientssl clientssl-insecure-compatible </td> </tr> </tbody> </table>	Selected	Available		/Common WS1-ClientSSL WorkspaceOne-SSL clientssl clientssl-insecure-compatible
Selected	Available				
	/Common WS1-ClientSSL WorkspaceOne-SSL clientssl clientssl-insecure-compatible				
SSL Profile (Server)	<table border="1"> <thead> <tr> <th>Selected</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td></td> <td> /Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl </td> </tr> </tbody> </table>	Selected	Available		/Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl
Selected	Available				
	/Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl				
SMTSP 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				

- a) **Protocol Profile (Client):** select **tcp-wan-optimized**.
- b) **Protocol Profile (Server):** select **tcp-lan-optimized**.
- c) **HTTP Profile:** select the HTTP profile previously created above.
- d) **Source Address Translation:** select **Auto Map**.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

4. In the Resource section.

The screenshot shows the 'Resources' configuration window. It is divided into several sections:

- iRules:** Contains two lists: 'Enabled' and 'Available'. The 'Enabled' list contains the iRule `_sys_https_redirect`. The 'Available' list contains several system iRules: `_sys_auth_radius`, `_sys_auth_ssl_cc_idap`, `_sys_auth_ssl_cridp`, `_sys_auth_ssl_ocsp`, and `_sys_auth_tacacs`. There are '<<' and '>>' buttons between the lists, and 'Up' and 'Down' buttons below the 'Enabled' list.
- Policies:** Contains two empty lists: 'Enabled' and 'Available', with '<<' and '>>' buttons between them.
- Default Pool:** A dropdown menu currently set to 'None'.
- Default Persistence Profile:** A dropdown menu currently set to 'None'.
- Fallback Persistence Profile:** A dropdown menu currently set to 'None'.

At the bottom of the window are three buttons: 'Cancel', 'Repeat', and 'Finished'.

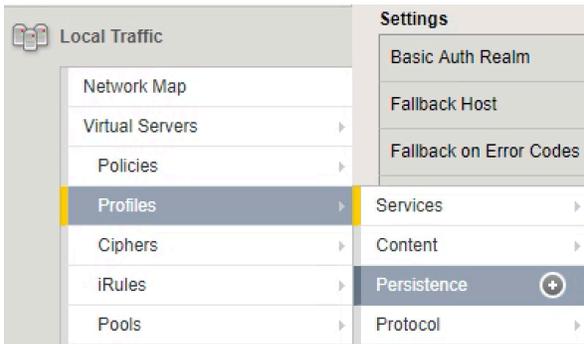
- iRules:** use the (<<) button to move the redirect iRule (`_sys_https_redirect`) to the **Active** list.
- Click the **Finished** button.

MobileSSO F5 Configurations (Optional)

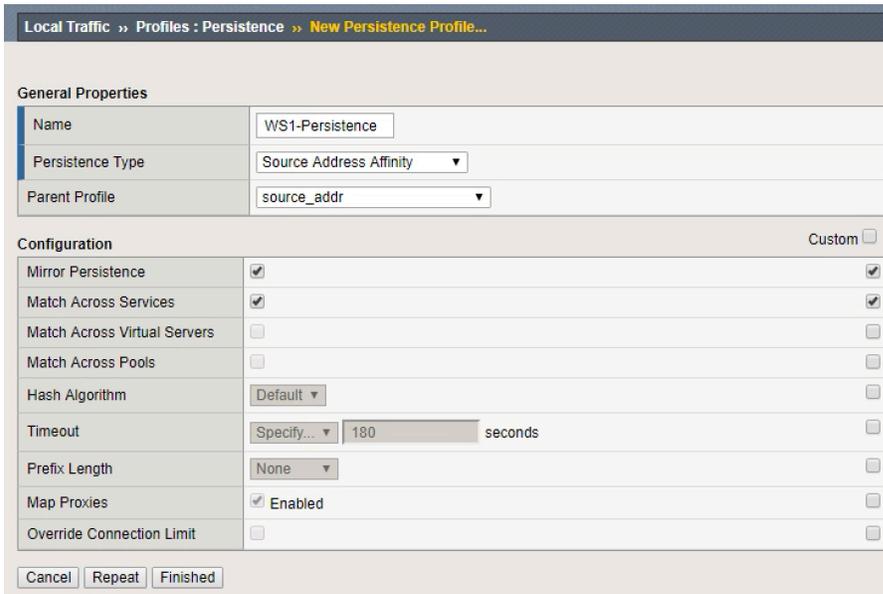
Create Persistence Profile

Note: Use the Persistence Profile mentioned in this section for both the 443 Virtual IP and the 88 Virtual IPs. If previous configuration was used change/replace Non-MobileSSO Persistence Profile with this one.

1. In the Local Traffic menus go to Profiles → Persistence → (+) plus icon to create a new Persistence Profile



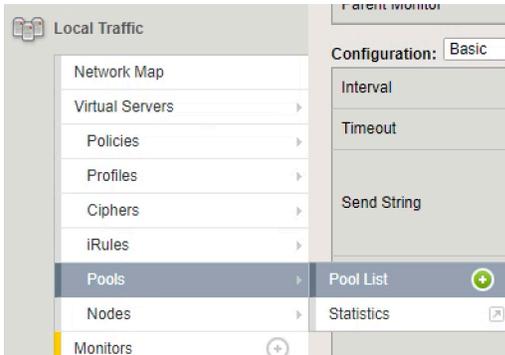
2. In the “New Persistence Profile...”



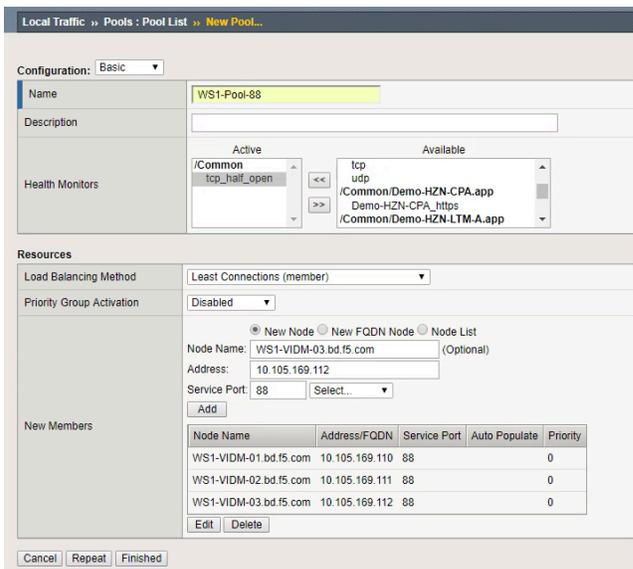
- a. **Name:** Provide a unique name.
- b. **Persistence Type:** select **Source Address Affinity**.
- c. Check the **Custom** checkbox and the **enable** Checkbox for **Mirror Persistence**.
- d. Check the **Custom** checkbox and the **enable** Checkbox for **Match Across Services**.
- e. Click **Finished**.

Create Pool

1. In the Local Traffic menus go to Pools → Pool List → (+) plus icon to create a new Pool



2. In the “New Pool...”



- a. **Name:** Provide a unique name.
- b. **Health Monitors:** use the Add (<<) button to move the **tcp_half_open** monitor to the **Active** list.
- c. **Load Balancing Method:** select **Least Connections (node)**.
- d. In the **New Members** area, complete the following for each Identity Manager node
 - i. **Node Name:** (Optional) Provide the FQDN or Identifier of the Node.
 - ii. **Address:** Provide the IP address of the First Identity Manager Node (Node 1).
 - iii. **Service Port:** type **88**.
 - iv. Click the **Add** button.
 - v. Repeat this step for each additional VMware Identity Manager node (Nodes 2 and 3 so when they are cloned they are available in the cluster).
- e. Click the **Finished** button.

Create Port 88 TCP VIP

1. In the Local Traffic menus go to Virtual Servers → Virtual Servers List → (+) plus icon to create a new Virtual Server



2. In the General Properties section.

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

General Properties

Name	WS1-VS-88-TCP
Description	
Type	Performance (Layer 4) ▼
Source Address	
Destination Address/Mask	10.105.169.11
Service Port	88 Other: ▼
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled ▼

- a. **Name:** Provide a unique name.
- b. **Destination Address/Mask:** type the IP Address associated to the FQDN for the virtual server.
- c. **Service Port:** type 88

3. In the Configuration section.

Configuration: Advanced ▾	
Protocol	TCP ▾
Protocol Profile (Client)	fastL4 ▾
HTTP Profile	None ▾
HTTP Proxy Connect Profile	None ▾
WebSocket Profile	None ▾
SplitSession Client Profile	None ▾
SplitSession Server Profile	None ▾
QoE Profile	None ▾
FIX Profile	None ▾
Statistics Profile	None ▾
VLAN and Tunnel Traffic	All VLANs and Tunnels ▾
Source Address Translation	Auto Map ▾
Bandwidth Controller	None ▾
Traffic Class	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>Enabled</p> <div style="border: 1px solid #ccc; width: 100px; height: 40px;"></div> </div> <div style="text-align: center;"> <p>Available</p> <div style="border: 1px solid #ccc; width: 100px; height: 40px;"></div> </div> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> << >> </div>
Connection Limit	0
Eviction Policy	None ▾
Connection Rate Limit	0
Connection Rate Limit Mode	Per Virtual Server
Connection Mirroring	<input type="checkbox"/> (May degrade performance when enabled.)
Address Translation	<input checked="" type="checkbox"/> Enabled
Port Translation	<input checked="" type="checkbox"/> Enabled

- a. Change the Configuration section from **Basic** to **Advanced**
- b. **Protocol**: select **TCP**.
- c. **Protocol Profile (Client)**: select **FastL4** from the pull-down menus.
- d. **Source Address Translation**: select **Auto Map**.
- e. **Address Translation**: check the **Enabled** checkbox.
- f. **Port Translation**: check the **Enabled** checkbox.

- 4. Scroll down to the Resources section.

The screenshot shows a configuration window titled "Resources". It features a table with two columns: "Enabled" and "Available". The "iRules" row is currently empty in the "Enabled" column, while the "Available" column contains a list of resources: "/Common", "HTML5-HZN74-Fix-2", "Origin-Header-LTM", "_sys_APM_ExchangeSupport_OA_BasicAuth", and "_sys_APM_ExchangeSupport_OA_NtlmAuth". Navigation buttons include "<<", ">>", "Up", and "Down". Below the table, there are three rows for configuration: "Default Pool" with a plus sign and a dropdown menu showing "WS1-Pool-88"; "Default Persistence Profile" with a dropdown menu showing "WS1-Persistence"; and "Fallback Persistence Profile" with a dropdown menu showing "None". At the bottom, there are three buttons: "Cancel", "Repeat", and "Finished".

- a. **Default Pool:** select the pool for MobileSSO previously created from the pull-down menus.
- b. **Default Persistence Profile:** select the persistence profile for MobileSSO previously created from the pull-down menus.
- c. Click the **Finished** button.

Create Port 88 UDP VIP

1. In the Local Traffic menus go to Virtual Servers → Virtual Servers List → (+) plus icon to create a new Virtual Server



2. In the General Properties section.

The screenshot shows the 'Local Traffic >> Virtual Servers : Virtual Server List >> New Virtual Server...' configuration page. The 'General Properties' section is visible with the following fields:

Name	WS1-VS-88-UDP
Description	
Type	Performance (Layer 4) ▼
Source Address	
Destination Address/Mask	10.105.169.11
Service Port	88 Other: ▼
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled ▼

- a. **Name:** Provide a unique name.
- b. **Destination Address/Mask:** type the IP Address associated to the FQDN for the virtual server.
- c. **Service Port:** type 88

3. In the Configuration section.

Configuration: **Advanced** ▼

Protocol	UDP ▼
Protocol Profile (Client)	fastL4 ▼
HTTP Profile	None ▼
HTTP Proxy Connect Profile	None ▼
WebSocket Profile	None ▼
SplitSession Client Profile	None ▼
SplitSession Server Profile	None ▼
QoE Profile	None ▼
FIX Profile	None ▼
Statistics Profile	None ▼
VLAN and Tunnel Traffic	All VLANs and Tunnels ▼
Source Address Translation	Auto Map ▼
Bandwidth Controller	None ▼
Traffic Class	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>Enabled</p> <div style="border: 1px solid #ccc; width: 100px; height: 100px;"></div> </div> <div style="text-align: center;"> <p>Available</p> <div style="border: 1px solid #ccc; width: 100px; height: 100px;"></div> </div> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> << >> </div>
Connection Limit	0
Eviction Policy	None ▼
Connection Rate Limit	0
Connection Rate Limit Mode	Per Virtual Server ▼
Connection Mirroring	<input type="checkbox"/> (May degrade performance when enabled.)
Address Translation	<input checked="" type="checkbox"/> Enabled
Port Translation	<input checked="" type="checkbox"/> Enabled

- a. Change the Configuration section from **Basic** to **Advanced**
- b. **Protocol**: select **UDP**.
- c. **Protocol Profile (Client)**: select **FastL4** from the pull-down menus.
- d. **Source Address Translation**: select **Auto Map**.
- e. **Address Translation**: check the **Enabled** checkbox.
- f. **Port Translation**: check the **Enabled** checkbox.

- 4. Scroll down to the Resources section.

The screenshot shows a configuration window titled "Resources". It features a table with two columns: "Enabled" and "Available".

	Enabled	Available
iRules	<input type="text"/>	<ul style="list-style-type: none">/CommonHTML5-HZN74-Fix-2Origin-Header-LTM_sys_APM_ExchangeSupport_OA_BasicAuth_sys_APM_ExchangeSupport_OA_NtlmAuth
Default Pool	<input type="text" value="WS1-Pool-88"/>	
Default Persistence Profile	<input type="text" value="WS1-Persistence"/>	
Fallback Persistence Profile	<input type="text" value="None"/>	

At the bottom of the window are three buttons: "Cancel", "Repeat", and "Finished".

- a. **Default Pool:** select the pool for MobileSSO previously created from the pull-down menus.
- b. **Default Persistence Profile:** select the persistence profile for MobileSSO previously created from the pull-down menus.
- c. Click the **Finished** button.

Configuring Root/Primary CA's on BIG-IP and Identity Manager

After configuring the F5 BIG-IP appliance to load balance the Identity Manager appliances, the next task is to upload the appliance's Primary or Root CA certificate to the BIG-IP.

Log onto the Identity Manager Node's Portal Appliance Configuration Page

1. In a browser, type the FQDN of the first Identity Manager appliance you are configuring (for example, <https://ws1-vidm-01.bd.f5.com:8443/cfg/login>).



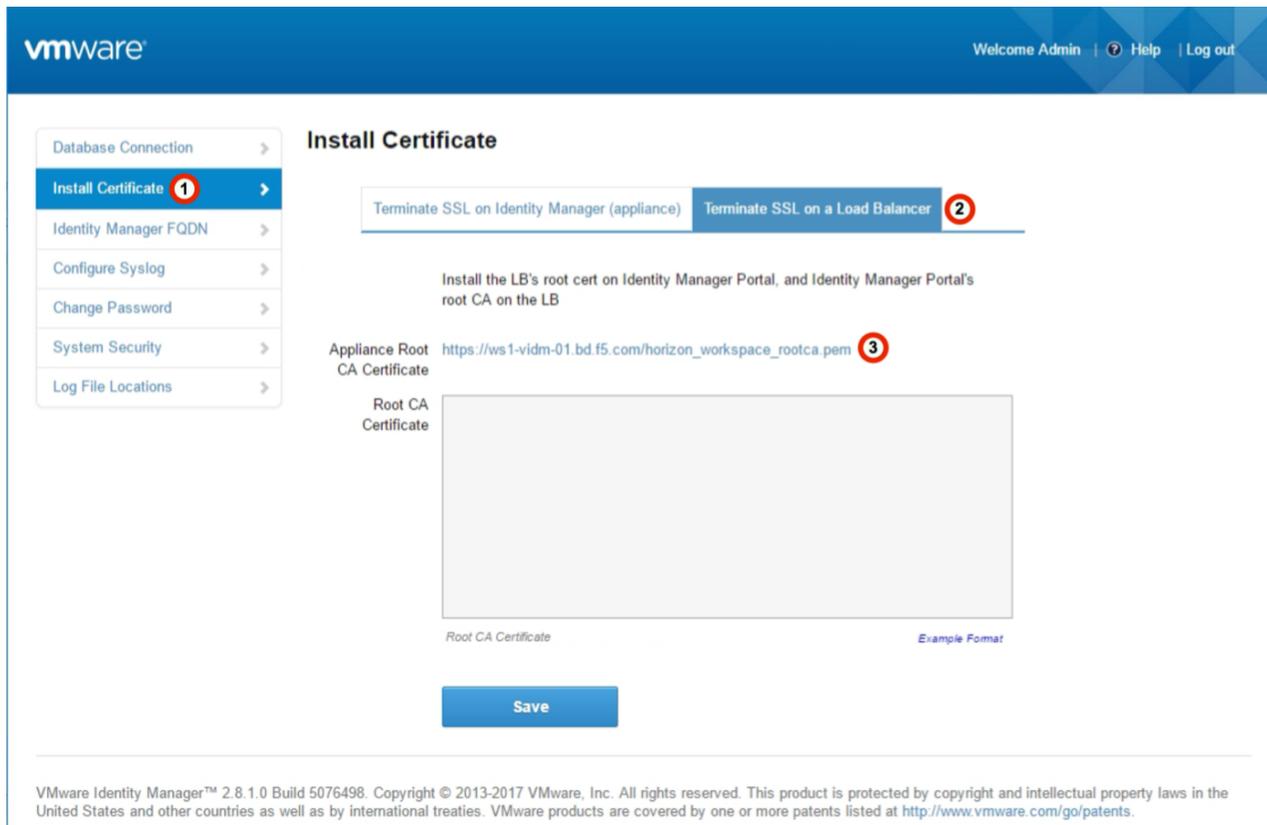
2. Login to the administrator interface with the password configured during the setup of the Identity Manager appliance.



Load the Identity Manager’s Root CA on the BIG-IP

In this step, you copy and load the Identity Manager’s Appliance Root CA to the BIG-IP. This example uses the appliance’s self-signed Root CA generated during the installation. If you have replaced the original self-signed certificates with other certificates, you must ensure the Root CA for the replacement certificates used for Identity Manager are uploaded to the BIG-IP.

Even though there may be three (3) Identity Manager appliances deployed for a production scenario, you only need to import one (1) Appliance Root CA. When you clone the Identity Manager Appliance Node 1 for redundancy, the Appliance Root CA does not change.



1. Click **Install Certificate** on the left side of the screen.
2. Click the **Terminate SSL on a Load Balancer** tab at the top right of the screen.
3. Click the link next to Appliance Root CA Certificate. A browser window opens with the Root CA's content.

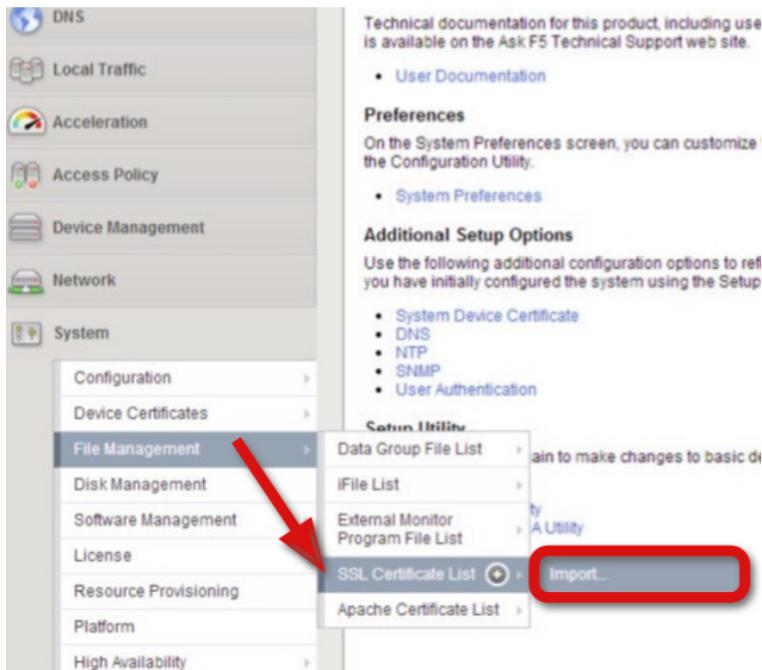
INTEGRATION GUIDE

Load Balancing VMware Identity Manager

4. Highlight the certificate and copy to your clipboard.

```
-----BEGIN CERTIFICATE-----
MIIDBTCCA1WgAwIBAgIQduwgBuL6NpxEJLZNJY7ZGzANBgkqhkiG9w0BAQUFADBI
MRUwEwYKZCIIm1ZPyLQGBGRYFbG9jYWwxFDASBggoJkiaJk/IsZAEZFgRjb3JwMRkw
FwYDVOQDExBDT05UUk9MQ0VOVEVSLUNBMCAXDTEOMDMwNjE3Mjg1MVoYDzIwNjQw
MzA2M2czODUwWjBIMRUwEwYKZCIIm1ZPyLQGBGRYFbG9jYWwxFDASBggoJkiaJk/Is
ZAEZFgRjb3JwMRkwFwYDVOQDExBDT05UUk9MQ0VOVEVSLUNBMIBIIBIjANBgkqhkiG
9w0BAQEFAAOCAQIBIICgKCAQEAzW2M2yICWn1IPNszLBqqVjWZ1kp2Ttq2xxYg
C6a4awIS1oCsdvrxEOP3wZfDYJF1LRj2aw9LrqqYQcLQAoIGBCDrQ3TVvZU+PmtC
akQyzYoe6+Hjb3hfc7FEBXjqfrEY3DMseu69CMeXqUW4vhyRvctQaDdbj3Z91+5vd
Ikkx0PwxyiBaHr8a6H8EgyXOY1112hpI4Vhg3j+h33fUbZe2HwM/sf81dfjTfmUI
pEvygztL4AnTt5UQb55XD0dsire/wNn7syYPQcMnO/HjHY5H8EpQlfEgadfwCHuM
ailvg853RDcnjJEgywxAMNq4XE+SRAECvN6VKldROVSP32qqhQIDAQABO1EwTzAL
BgNVH08EBAMCAYYwDwYDVR0TAQH/BAQwAwEB/zAdBgNVHQ4EFgQUrLH8z+nxYJnZ
7KtbVadCsV8WKh4wEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEFBQAoDggEB
AAMfoSJqS6JbTh1jIf0SBudXfLVkDVXhw1FtYaQWpw6wRGqMHbdEvaZGGg9y5UWt
H6Vr4JR8KGZY1xjY+D8ZC9t3VCuyGVY1MvtE8RA4sosaEC877P2c8TEoDniUtLnF
FifkpxFlnYWX4S/k1p2Q+e1lUpsS+63Ex/pHYjleBdIvMeY1tDeyY2tJ2IvITxmv
g4u1hHN8I56bCzmlOylGkNoZT+1UANwntUegX+4vuYuv3L580pD0qfxKi6icedNF
eT2maa61uq+WImns64mGsGvW7sdxkAeo8ALMYlhuy86OJFc+38v6hq321r8pa2SUZ
E7cY+nWeroGGd3OUHw39rGg=
-----END CERTIFICATE-----
```

Go to the BIG-IP Configuration utility and click **System > File Management > SSL Certificate List > Import**.



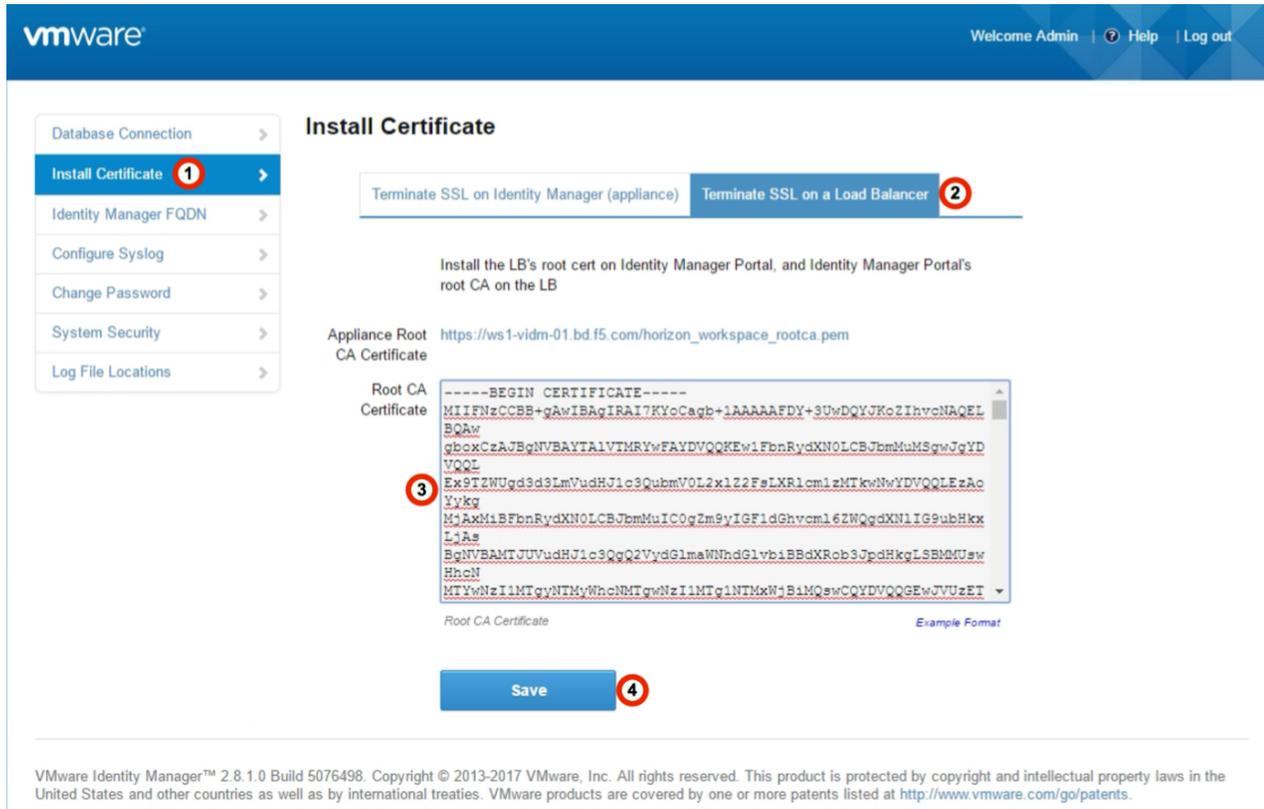
SSL Certificate/Key Source

Import Type	Certificate 1
Certificate Name	<input checked="" type="radio"/> Create New <input type="radio"/> Overwrite Existing WS1-PEM 3
Certificate Source	<input type="radio"/> Upload File <input checked="" type="radio"/> Paste Text 4 <pre>-----BEGIN CERTIFICATE----- MIIE7DCCA9SgAwIBAgIFFFJQnIkEwDQYJKoZIhvcNAQELBQAwgawxCzAJBgNVBAYT A1VTMRMwEQYDVQQIEwpjYWxpZm9ybmlhMRIwEAYDVQQHEw1QYWxvIEFsdG8xDzAN BgNVBAAoTB1ZNd2FyZTEaMBQGA1UECzMRSg9yaXpvbi1Xb3Jrc3BhY2UxJDAiBgNV BAMTQ01udGVybmlhIFJvb3Q0Q0EgMTQ5NDI3MjIOMTEhMB8GCSqGSIb3DQEJARYS dW5rbm93bkB2bXdhcmUuY29tMB4XDTE2MDUwODE5MzcyMVoXDTE2MDUwODE5Mzcy MlloZGawxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpjYWxpZm9ybmlhMRIwEAYDVQQH Ew1QYWxvIEFsdG8xDzANBgNVBAAoTB1ZNd2FyZTEaMBQGA1UECzMRSg9yaXpvbi1X b3Jrc3BhY2UxJDAiBgNVBAMTQ01udGVybmlhIFJvb3Q0Q0EgMTQ5NDI3MjIOMTEh MB8GCSqGSIb3DQEJARYSdW5rbm93bkB2bXdhcmUuY29tMIIBIjANBgkqhkiG9w0B AQEFAAOCAQ8AMIIBCGKCAQEAA7kH8c9jjZS/jOmPBoStt18j+QP1ZVaH+x1V+6i3G T1thJl2TotZyndSIFnbGwapd/PSdeT7Lda70lqDHTTBTGBIiPAOsqhTh5UE2PCob Ulrss8nw3bLbZICrTBLG3b4oaML4khqx53kDSwYiVI4EziaAofycKQWX1+ZXrEbS qTWXe5NpBSnjAdprvVALiKv18J6Y3vQ4VEULtgnu94Cct05XIcMBTlyAhfC72+Ii MxrzMA8/LUEif2uDbrjbZrV4eAmtU2zThb1DE265ss4nGxHZ6bKC9A7U+GMj9kBs URAwMvKDzwwBZVRCLoN4RksaKghuUnQyNOYsCmauivFSEQIDAQABo4IBETCCAQ0w DAYDVROTBANwAwEB/zAdBgNVHQ4EFgQUh8q2V6pET8oY8T7GPvmsiyKNXcMwgd0G A1UdIwSB1TCB0oAUh8q2V6pET8oY8T7GPvmsiyKNXcOhqbKkga8wgawxCzAJBgNV BAYTA1VTMRMwEQYDVQQIEwpjYWxpZm9ybmlhMRIwEAYDVQQHEw1QYWxvIEFsdG8x DzANBgNVBAAoTB1ZNd2FyZTEaMBQGA1UECzMRSg9yaXpvbi1Xb3Jrc3BhY2UxJDAi BgNVBAMTQ01udGVybmlhIFJvb3Q0Q0EgMTQ5NDI3MjIOMTEhMB8GCSqGSIb3DQEJ </pre> 5
Free Space on Disk	197 MB
<input type="button" value="Cancel"/> <input checked="" type="button" value="Import"/> 6	

1. From the **Import Type** list, select **Certificate**.
2. In the **Certificate Name** row, click the **Create New** radio button.
3. In the **Certificate Name** row, in the **Name** field, type a unique name for the Identity Manager Certificate.
4. In the **Certificate Source** area, click the **Paste Text** radio button.
5. In the **Certificate Source** area, paste the Appliance Root CA (or the CA used for the appliance certificate).
6. Click **Import**.

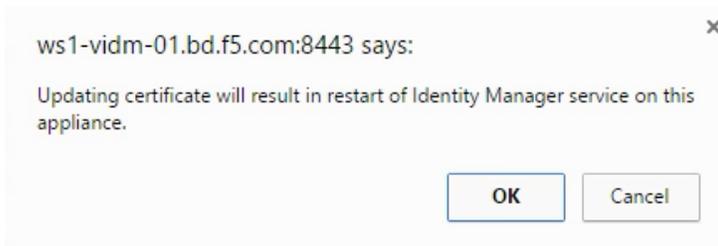
Load the FQDN Root/Primary CA Certificate into Identity Manager Node 1

Next, go to Identity Manager Appliance Node 1's appliance configuration interface.



From the appliance configuration page on Identity Manager Appliance Node 1:

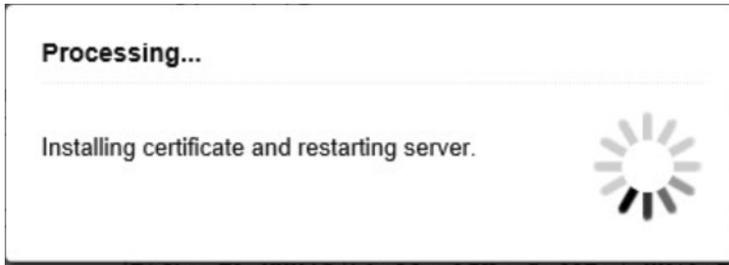
1. Click **Install Certificate** from the menu on the left side of the screen.
2. Click the **Terminate SSL on a Load Balancer** tab at the top right of the screen.
3. Open the FQDN's Root/Primary Certificate in WordPad or other text editing utility. Copy and paste the contents of this certificate into the **Root CA Certificate** window.
Note: The Root CA Certificate mentioned is the Root CA of the FQDN Certificate being used on the BIG-IP to load balance the VIDM Nodes. This is not the Device Certificate of the BIG-IP.
4. Click **Save**.
5. If prompted, click **OK** to continue.



6. The service will restart for the certificate to be successfully added to the Workspace/Identity Manager.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager



7. You will be returned to the VMware Workspace/Identity Manager Install Certificate screen once the process is complete.

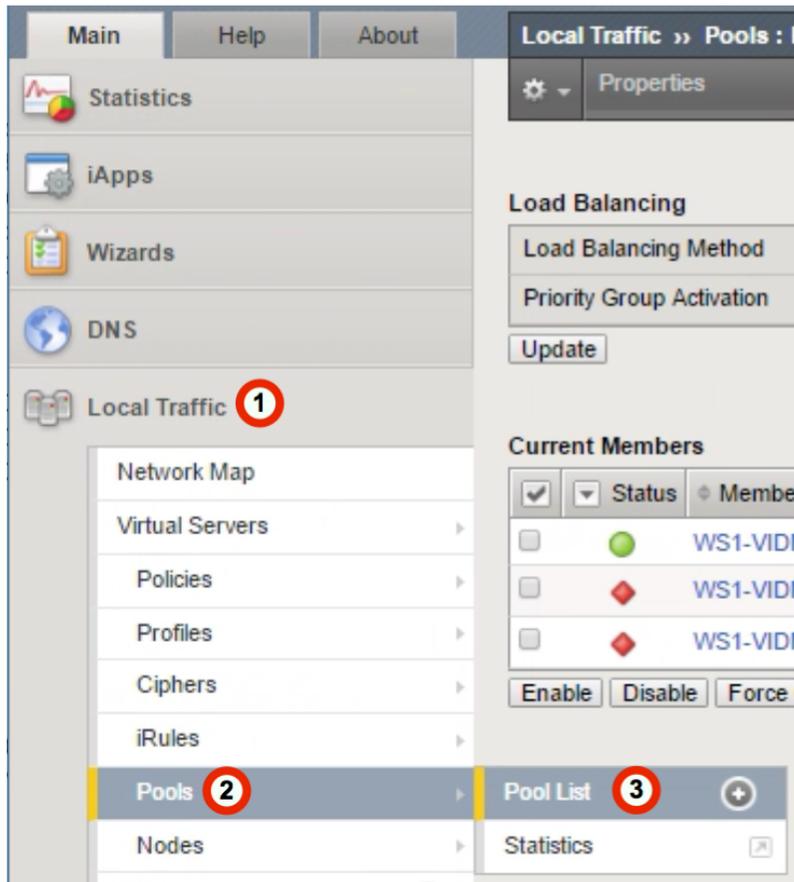
Configuring the FQDN for Identity Manager

After you have configured the appliance's root certificates on the F5 BIG-IP appliance, you must change the FQDN of node 1's appliance to point to the new load balanced FQDN.

Ensuring Node 1 is Online in the Pool

Before continuing, you must verify that Node 1 is Online in the pool of nodes. In this procedure, you check the BIG-IP to ensure that Node 1 is online. Nodes 2 and 3 (if added earlier) should be a part of the pool but marked as Offline (a red diamond icon).

1. Click **Local Traffic**.
2. Hover over **Pools**
3. Click **Pool List**.



4. Select the pool you created (**WorkspaceOne-Pool** in our example).
5. On the Menu bar, click **Members**.
6. In the Current Members area, you should see by the indicators that Node 1 (WS1-VIDM-01.bd.f5.com) has a green circle indicating it is online and available. Nodes 2 and 3 (WS1-VIDM-02.bd.f5.com and WS1-VIDM-03.bd.f5.com) have red triangles indicating that they are in an Offline State.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

NOTE: This is expected behavior as nodes 2 and 3 should not have been cloned yet.

Local Traffic » Pools : Pool List » WorkspaceOne-Pool

Properties Members Statistics

Load Balancing

Load Balancing Method: Least Connections (member)

Priority Group Activation: Disabled

Update

Current Members

<input checked="" type="checkbox"/>	Status	Member	Address	Service Port	FQDN
<input type="checkbox"/>	●	WS1-VIDM-01.bd.f5.com:443	10.105.169.110	443	
<input type="checkbox"/>	◆	WS1-VIDM-02.bd.f5.com:443	10.105.169.111	443	
<input type="checkbox"/>	◆	WS1-VIDM-03.bd.f5.com:443	10.105.169.112	443	

Enable Disable Force Offline Remove

You are now ready to move onto update Node 1's Identity Manager appliance FQDN.

Log onto the Identity Manager Node's Portal Appliance Configuration Page

1. In a browser, type the FQDN of the first Identity Manager appliance you are configuring (for example, <https://ws1-vidm-01.bd.f5.com:8443/cfg/login>).

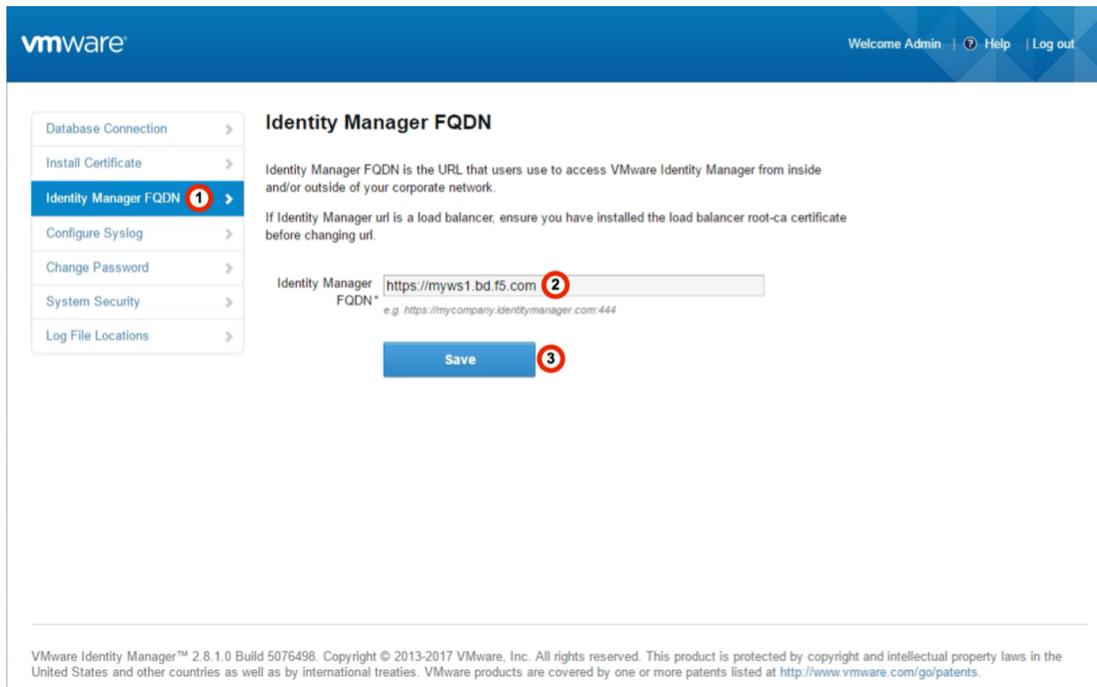


2. Login to the administrator interface with the password configured during the setup of the Identity Manager appliance.



Change Identity Manager Node 1's FQDN

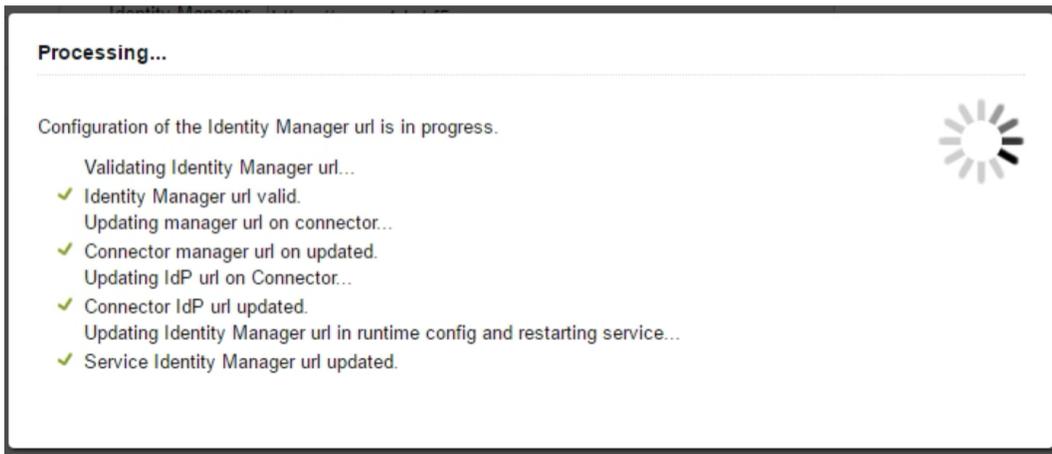
Once in the Workspace Portal/Identity Manager Appliance Configuration Page:



1. Select **Identity Manager FQDN** from the left-hand menu
2. Enter the Workspace Portal/Identity Manager FQDN: (i.e. https://myws1.bd.f5.com)
3. Click **Save**.

Confirming the FQDN Name change

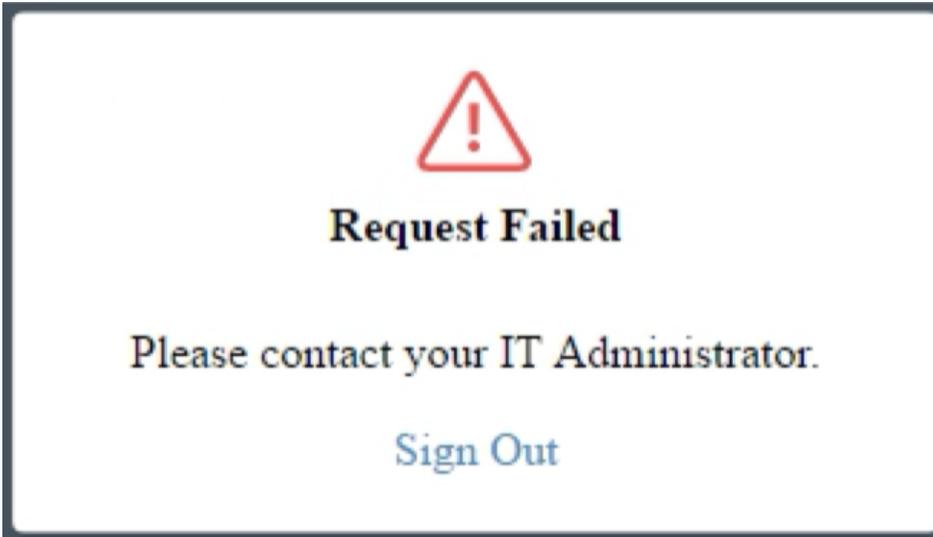
Once the FQDN update starts, you should be prompted with a screen that displays the progress.



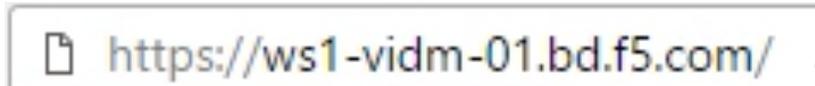
If you have completed every step successfully, you should see four (4) green checkmarks. If that is the case, please continue to the next step.

Enable End User Portal UI for Load Balanced Configurations

After you have changed the FQDN of the Node 1 appliance, you must enable the End User Portal UI. This is natively disabled when any load balancer is configured with Identity Manager and must be re-enabled or you receive a “Please contact your IT Administrator” error when logging in as a user.



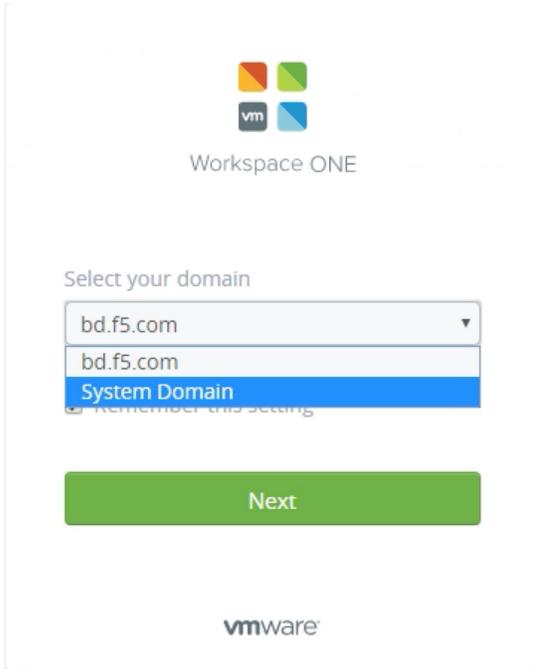
1. In a browser, type the FQDN of the first Identity Manager appliance you are configuring (for example, <https://ws1-vidm-01.bd.f5.com>)



INTEGRATION GUIDE

Load Balancing VMware Identity Manager

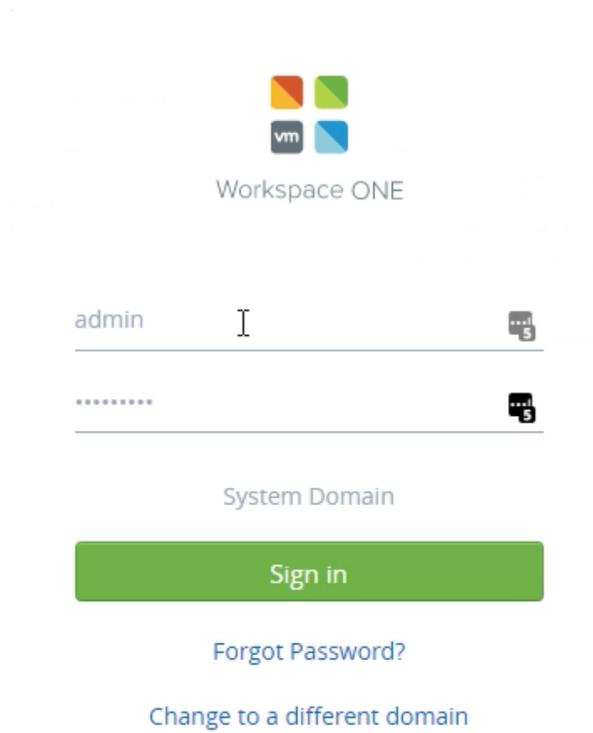
2. Clear the check from the **Remember this Setting** box, and then select **System Domain** from the list.
3. Click **Next**.



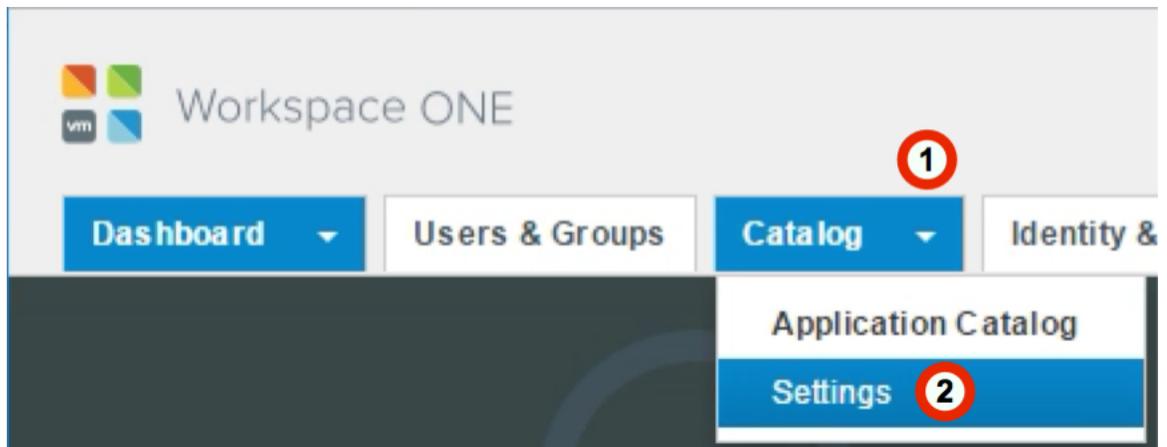
4. Login to the Workspace One Portal with the Local Admin Username and Password, ensure that **System Domain** is marked as the domain. If it is the incorrect domain select **Change to a different domain** and follow the previous steps.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager



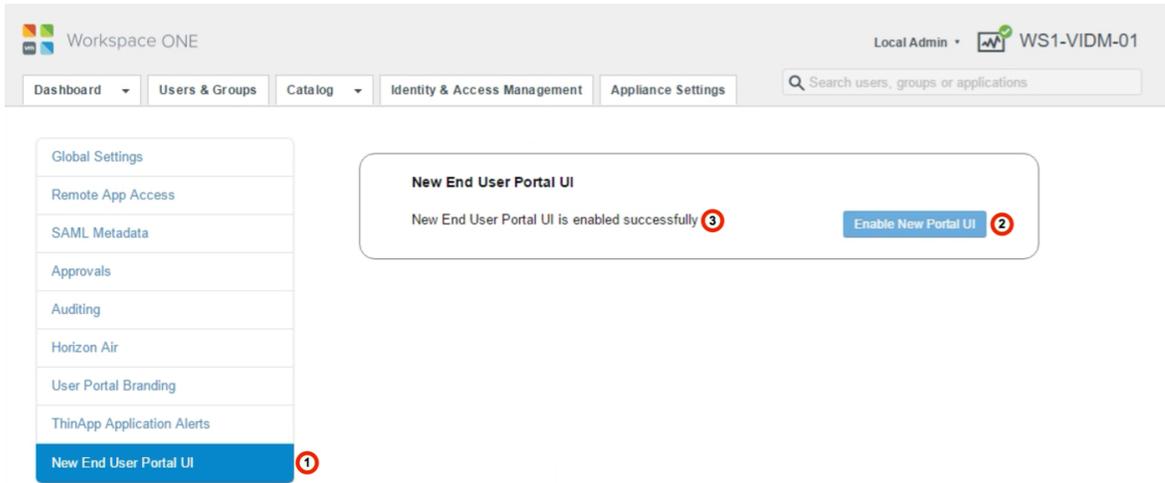
5. Once Logged into the Admin Portal, from the **Catalog** menu (1) select **Settings** (2).



6. From the left menu, click **New End User Portal UI** (1) and then click **Enable New Portal UI** (2).
This sends an update to the Identity Manager Portal and then **New End User UI is enabled successfully** (3) appears.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager



Workspace ONE

Local Admin • WS1-VIDM-01

Dashboard Users & Groups Catalog Identity & Access Management Appliance Settings

Search users, groups or applications

- Global Settings
- Remote App Access
- SAML Metadata
- Approvals
- Auditing
- Horizon Air
- User Portal Branding
- ThinApp Application Alerts
- New End User Portal UI** (1)

New End User Portal UI

New End User Portal UI is enabled successfully (3)

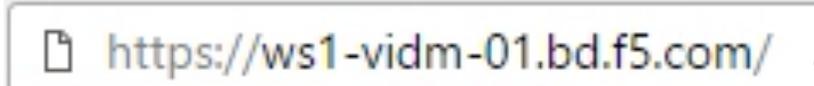
Enable New Portal UI (2)

VMware Identity Manager™ 2.8.1.0 Build 5076498. Copyright © 2013-2017 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

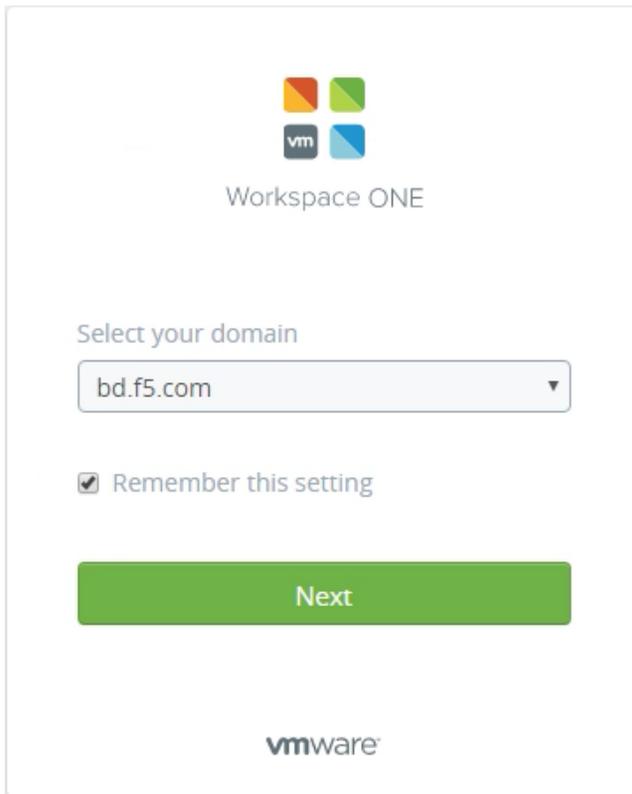
Logging into Identity Manager Portal

After Enabling the New UI, the next task is to login to the Identity Manager Portal as a user to ensure that everything is correct. In this case, you are now using the new FQDN site name to connect to the portal.

1. In a browser, type the FQDN of the first Identity Manager appliance you are configuring (for example, `https://ws1-vidm-01.bd.f5.com`).



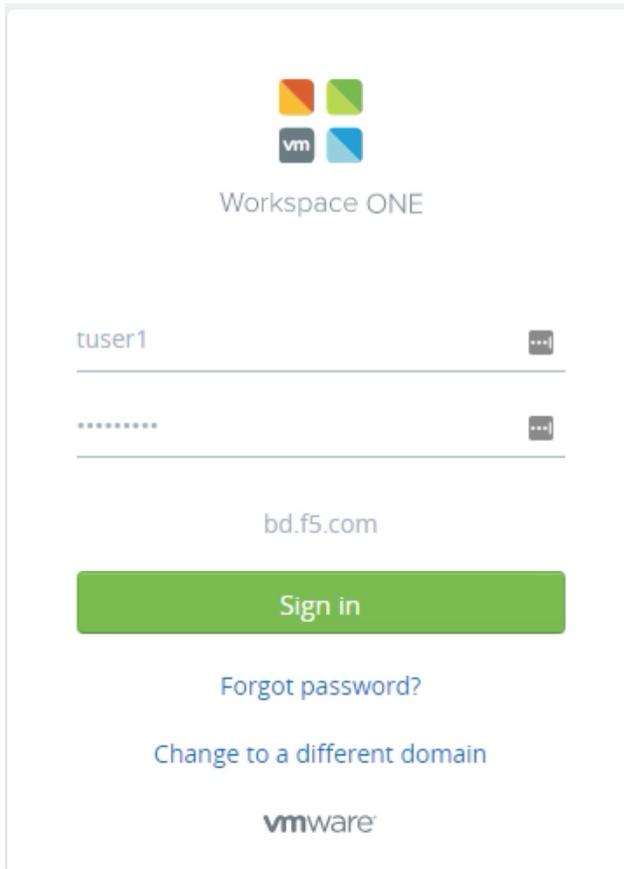
You should see the Workspace One Domain Selection Page. If you are taken directly to the Login page for System Domain or a domain where the user you wish to test is not selected appropriately, click the **Change to a different domain** button to get back to the domain selection page.



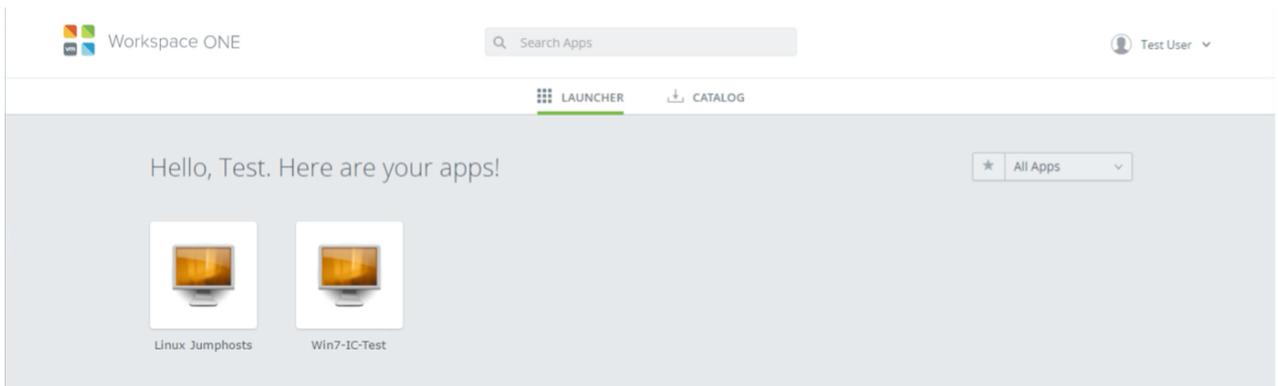
INTEGRATION GUIDE

Load Balancing VMware Identity Manager

2. Login to the Workspace One Portal with the Local Admin Username and Password. Ensure the domain is **System Domain**. If it is not, click **Change to a different domain** and follow the previous steps.



3. After logging in you should see the apps/desktops associated with the user that logged on. If there are no applications or desktops, you should still be able to get to the WS1 Portal page with no apps in it.



Cloning Nodes 2 and 3

After you have successfully tested the node under the load balanced FQDN, you have completed the steps necessary to be able to clone to Nodes 2 and 3. F5 does not provide guidance on the cloning of the additional nodes, as this is a VMware Appliance and there are recommended paths from VMware to clone the additional nodes. The following links/documents that can help the continuation of the deployment.

- VMware Identity Manager Documentation (Continue from Step 3 “Clone the Virtual Appliance”)
http://pubs.vmware.com/identity-manager-28/index.jsp#com.vmware.wsp-install_28/GUID-A29C51E5-6FF5-4F7F-8FC2-1A0F687F6DC5.html
- VMware EUC Customer Success Team, 3-Node Cluster (Page 16 – Creating IDM Node 2&3)
<https://communities.vmware.com/docs/DOC-33552>