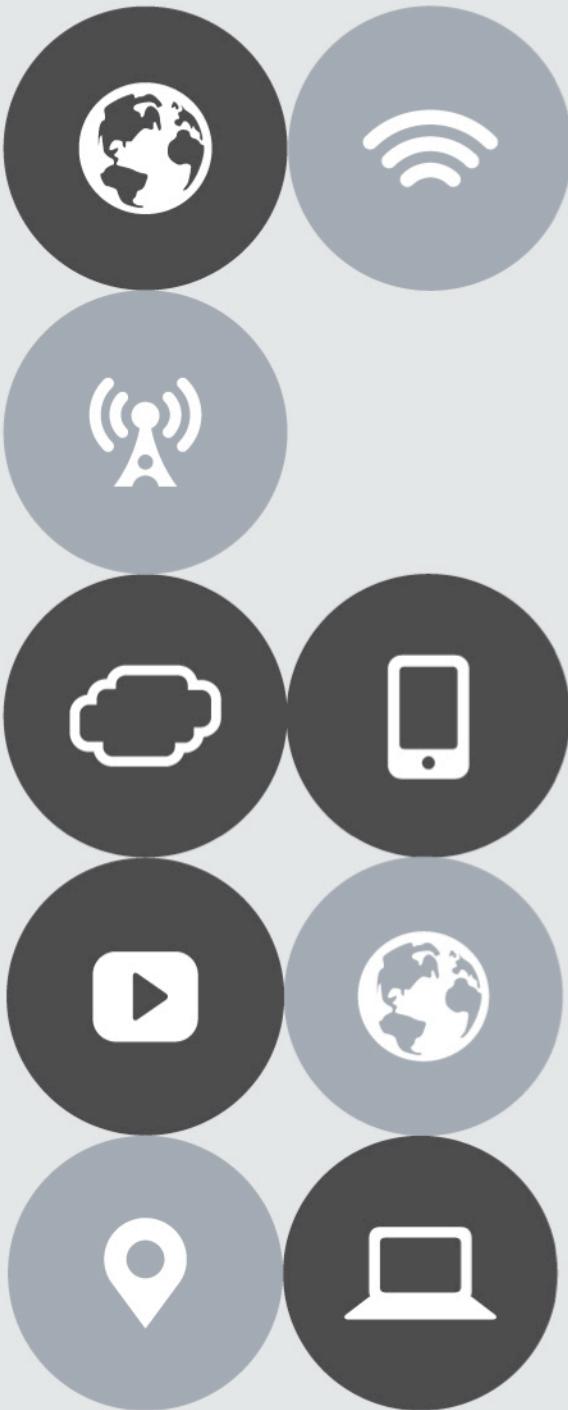




INTEGRATION GUIDE

vmware®

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.



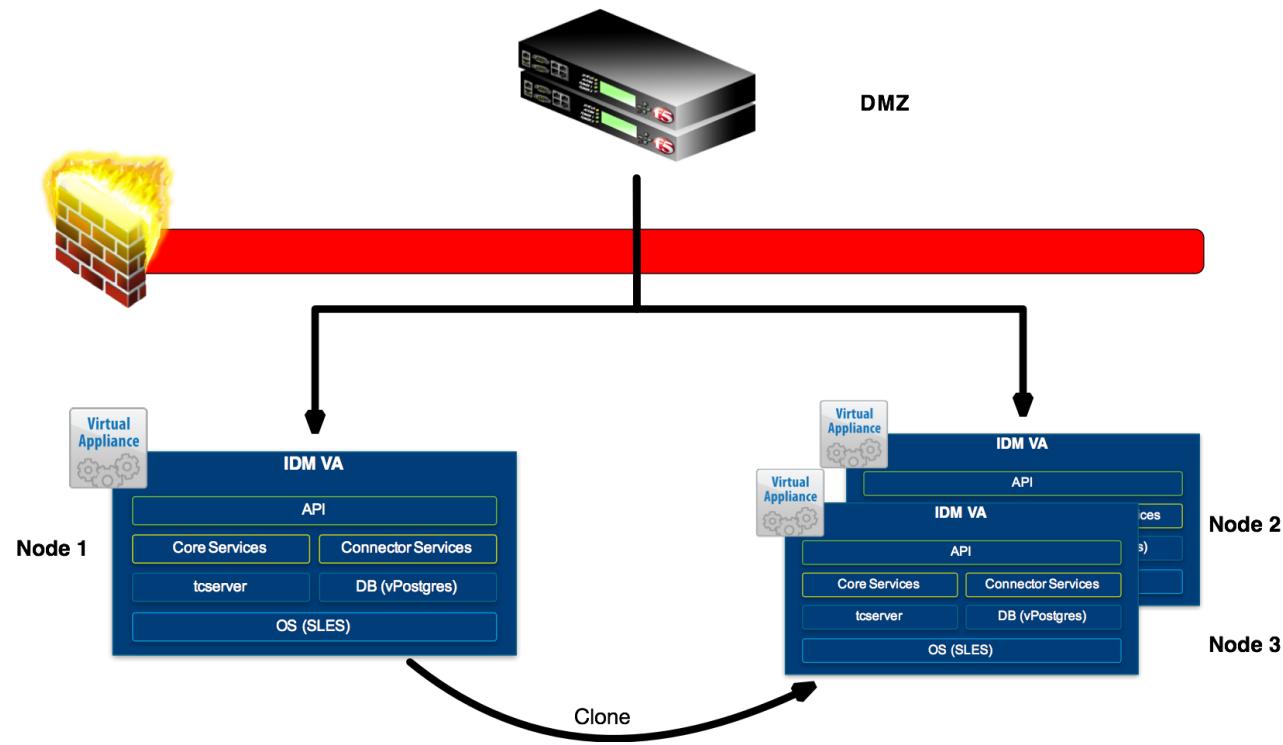
Contents

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

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

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

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

The screenshot shows the F5 BIG-IP Local Traffic interface. On the left, the navigation menu under 'Local Traffic' includes 'Network Map', 'Virtual Servers', 'Policies', 'Profiles' (which is selected), 'Ciphers', 'iRules', 'Pools', 'Nodes', 'Monitors', and 'Traffic Class'. Under 'Profiles', there are sub-options: 'SSL' (selected), 'Authentication', and 'Message Routing'. On the right, the 'SSL' configuration screen is displayed. It has sections for 'Type' (Performance (Layer 4)), 'Source Address' (0.0.0.0/0), 'Destination Address/Mask' (209.194.169.138), 'Service Port' (88), 'Services' (checkbox checked), 'Content' (Assisted), 'Persistence' (None), 'Protocol' (Available (Enabled)), and 'Client' (Client section with a green '+' button). Below these sections are 'Authentication' and 'Message Routing' sections.

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

- In the General Properties section

The screenshot shows the 'General Properties' dialog box. It has two fields: 'Name' (containing 'WS1-ClientSSL') and 'Parent Profile' (containing 'clientssl').

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

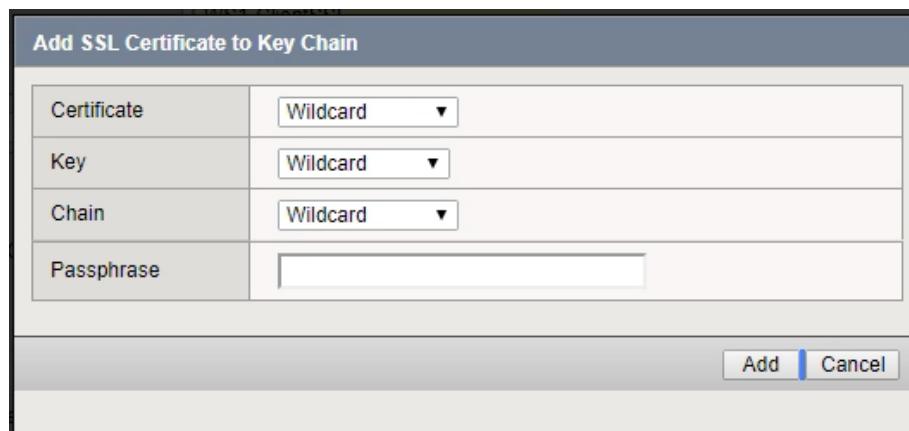
INTEGRATION GUIDE

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**.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

Create a HTTP Profile

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

The screenshot shows the 'Local Traffic > Profiles : SSL : Client' interface. On the left, there's a tree view with 'HTTP' selected. In the center, a table lists profiles: 'HTTP Compression', 'Web Acceleration', 'FTP', and 'TFTP'. On the right, there are tabs for 'Message Routing' and 'Other', and a 'Create...' button.

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

The screenshot shows the 'New HTTP Profile...' configuration dialog. It has two main sections: 'General Properties' and 'Settings'.

General Properties	
Name	WS1-HTTP
Proxy Mode	Reverse
Parent Profile	http

Settings	
Basic Auth Realm	
Fallback Host	
Fallback on Error Codes	
Request Header Erase	
Request Header Insert	
Response Headers Allowed	
Request Chunking	Preserve
Response Chunking	Selective
OneConnect Transformations	<input checked="" type="checkbox"/> Enabled
Redirect Rewrite	None
Encrypt Cookies	
Cookie Encryption Passphrase	
Confirm Cookie Encryption Passphrase	
Insert X-Forwarded-For	<input checked="" type="checkbox"/>

- a. **Name:** Provide a unique name for the instance
b. **Insert X-Forwarded-For:** Click the **Custom** checkbox and change to **Enabled**
c. 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.

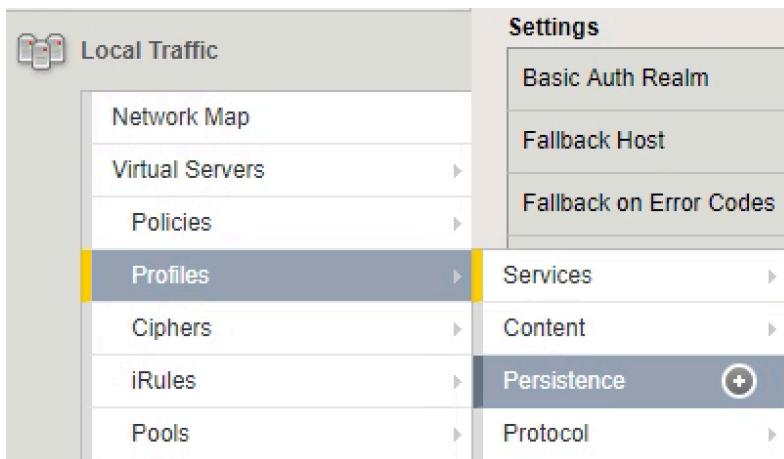
INTEGRATION GUIDE

Load Balancing VMware Identity Manager

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..."

This screenshot shows the 'New Persistence Profile...' configuration dialog. It has two main sections: 'General Properties' and 'Configuration'.

General Properties:

Name	WS1-Persistence
Persistence Type	Cookie
Parent Profile	cookie

Configuration:

Custom <input type="checkbox"/>	
Cookie Method	HTTP Cookie Insert
Cookie Name	[Redacted]
HTTPOnly Attribute	Enabled
Secure Attribute	Enabled
Always Send Cookie	<input type="checkbox"/>
Default Cookie Encrypt Pool-Name	<input type="checkbox"/>
Expiration	<input checked="" type="checkbox"/> Session Cookie
Cookie Encryption Use Policy	disabled
Encryption Passphrase	[Redacted]
Override Connection Limit	<input type="checkbox"/>

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

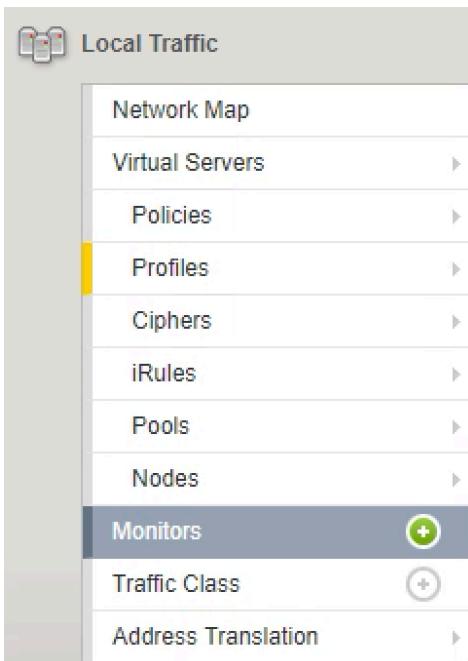
- a. **Name:** Provide a unique name.
- b. **Persistence Type:** select **Cookie**.
- c. Click **Finished**.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

Create Monitor

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



2. In the General Properties

The screenshot shows the 'General Properties' section of the 'New Monitor...' dialog. It includes fields for Name, Description, Type, and Parent Monitor.

General Properties	
Name	WS1-Monitor
Description	
Type	HTTPS
Parent Monitor	https

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

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

3. In the Configuration Section

Configuration: Basic ▾

Interval	5 seconds
Timeout	16 seconds
Send String	GET /SAAS/API/1.0/REST/system/health/heartbeat HTTP/1.1\r\nHost: \r\nConnection: Close\r\n\r\n
Receive String	ok\$
Receive Disable String	404
User Name	[]
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	*
Adaptive	<input type="checkbox"/> Enabled

Cancel **Repeat** **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**

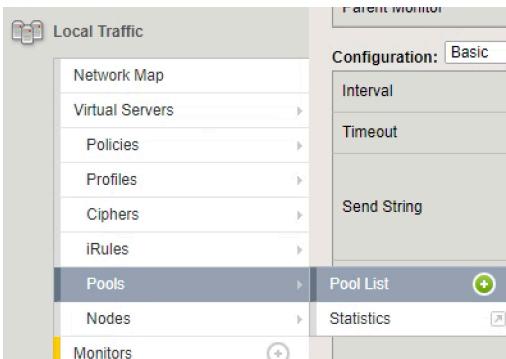
- d. Click **Finished**.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

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..."

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
WS1-VIDM-01.bd.f5.com	10.105.169.110	443	0	
WS1-VIDM-02.bd.f5.com	10.105.169.111	443	0	
WS1-VIDM-03.bd.f5.com	10.105.169.112	443	0	

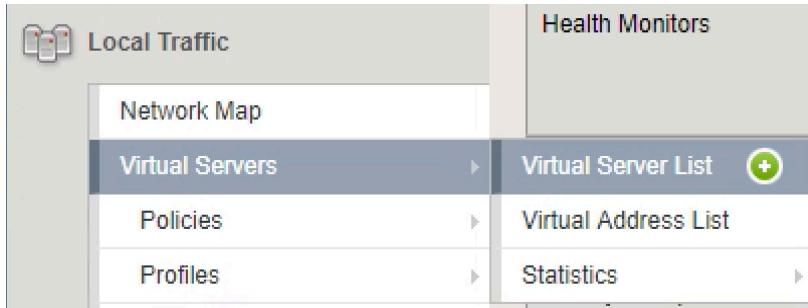
- a. **Name:** Provide a unique name.
- b. **Health Monitors:** use the Add (<>) button to move the monitor previously created to the **Active** list.
- c. **Load Balancing Method:** select **Least Connections (node)**.
- d. In the **New Members** area, complete the following for each Identity Manager 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.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

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.

The screenshot shows the 'New Virtual Server...' dialog box. At the top, the breadcrumb navigation is 'Local Traffic > Virtual Servers : Virtual Server List > New Virtual Server...'. Below the title, the section is labeled 'General Properties'. The form contains the following fields:

Name	WS1-VS-443
Description	(empty)
Type	Standard
Source Address	(empty)
Destination Address/Mask	10.105.169.11
Service Port	443
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.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

3. In the Configuration section.

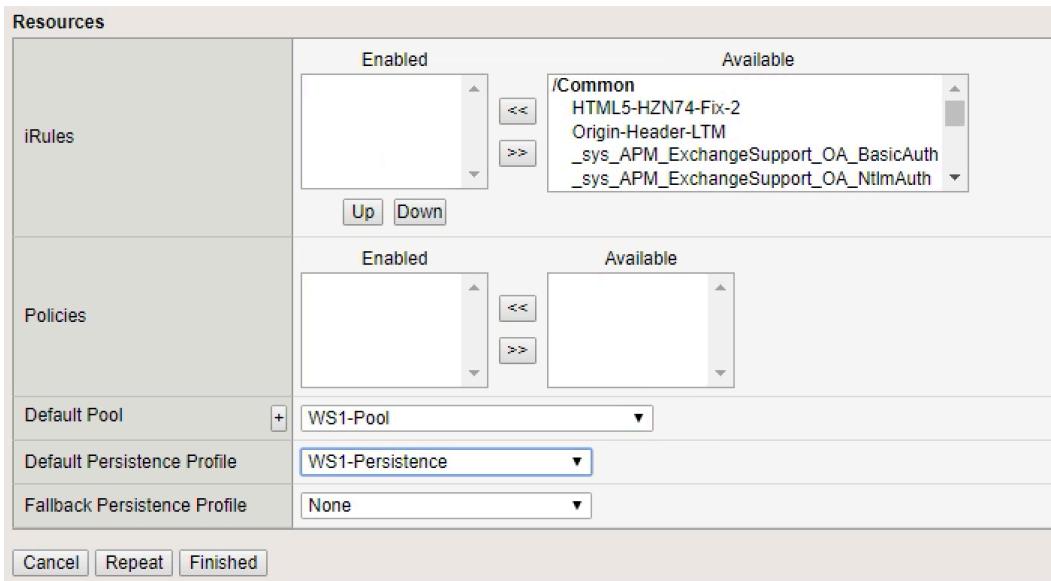
Configuration: Basic ▾					
Protocol	TCP ▾				
Protocol Profile (Client)	tcp-wan-optimized ▾				
Protocol Profile (Server)	tcp-lan-optimized ▾				
HTTP Profile	WS1-HTTP ▾				
HTTP Proxy Connect Profile	None ▾				
FTP Profile	None ▾				
RTSP Profile	None ▾				
SSL Profile (Client)	<table border="1"><thead>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

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

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

4. Scroll down to the Resources section.



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

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

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.

The screenshot shows the 'New Virtual Server...' configuration dialog. At the top, a breadcrumb navigation bar indicates the path: Local Traffic > Virtual Servers : Virtual Server List > New Virtual Server... Below this is a section titled 'General Properties' containing the following fields:

Name	WS1-VS-Redirect
Description	(empty text field)
Type	Standard
Source Address	(empty text field)
Destination Address/Mask	10.105.169.11
Service Port	80
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.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

3. In the Configuration section.

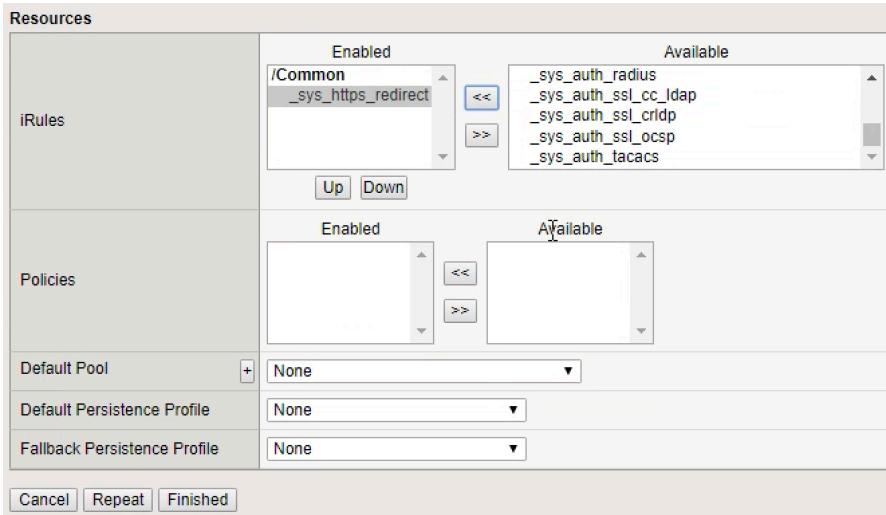
Configuration: Basic ▾					
Protocol	TCP ▾ tcp-wan-optimized				
Protocol Profile (Client)	tcp-lan-optimized ▾				
Protocol Profile (Server)	WS1-HTTP ▾				
HTTP Profile	None ▾				
HTTP Proxy Connect Profile	None ▾				
FTP Profile	None ▾				
RTSP Profile	None ▾				
SSL Profile (Client)	<table border="1"><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				
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 ▾				

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

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

4. In the Resource section.



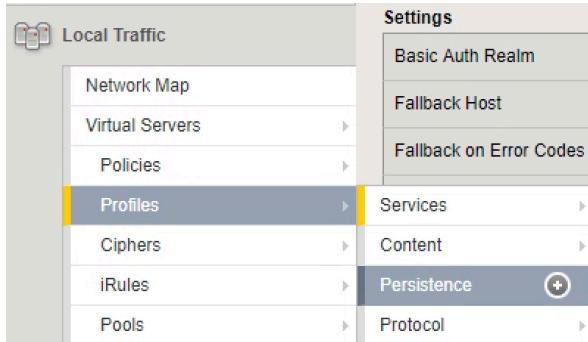
- a) **iRules:** use the (<<) button to move the redirect iRule (`_sys_https_redirect`) to the **Active** list.
- b) Click the **Finished** button.

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...”

The screenshot shows the 'New Persistence Profile...' configuration dialog. It has two main sections: 'General Properties' and 'Configuration'.

General Properties:

Name	WS1-Persistence
Persistence Type	Source Address Affinity
Parent Profile	source_addr

Configuration:

Mirror Persistence	<input checked="" type="checkbox"/>	Custom <input type="checkbox"/>
Match Across Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Match Across Virtual Servers	<input type="checkbox"/>	<input type="checkbox"/>
Match Across Pools	<input type="checkbox"/>	<input type="checkbox"/>
Hash Algorithm	Default	<input type="checkbox"/>
Timeout	Specify... 180 seconds	<input type="checkbox"/>
Prefix Length	None	<input type="checkbox"/>
Map Proxies	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Override Connection Limit	<input type="checkbox"/>	<input type="checkbox"/>

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

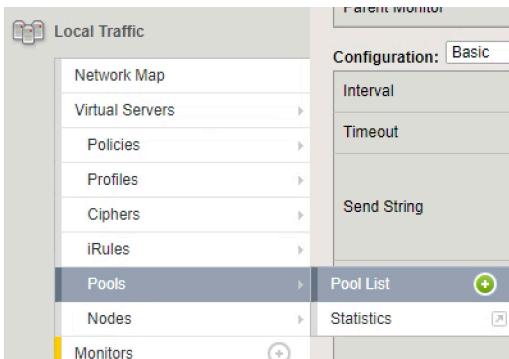
- Name:** Provide a unique name.
- Persistence Type:** select **Source Address Affinity**.
- Check the **Custom** checkbox and the **enable** Checkbox for **Mirror Persistence**.
- Check the **Custom** checkbox and the **enable** Checkbox for **Match Across Services**.
- Click **Finished**.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

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..."

The screenshot shows the 'New Pool...' configuration dialog. The 'Name' field is filled with 'WS1-Pool-88'. Under 'Health Monitors', the 'tcp_half_open' monitor is listed under 'Active' with a double-left arrow button to move it there. The 'Available' list includes 'tcp', 'udp', and several application monitors. In the 'Resources' section, 'Least Connections (member)' is selected as the load balancing method. The 'Priority Group Activation' is set to 'Disabled'. The 'New Members' section lists three nodes: 'WS1-VIDM-01.bd.f5.com' (Address: 10.105.169.110, Service Port: 88), 'WS1-VIDM-02.bd.f5.com' (Address: 10.105.169.111, Service Port: 88), and 'WS1-VIDM-03.bd.f5.com' (Address: 10.105.169.112, Service Port: 88). Each node has a priority of 0. Buttons at the bottom include 'Cancel', 'Repeat', and 'Finished'.

- 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.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

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.

A screenshot of the 'New Virtual Server...' configuration dialog. At the top, it shows the navigation path: Local Traffic > Virtual Servers : Virtual Server List > New Virtual Server... Below that is a section titled 'General Properties' containing the following fields:

Name	WS1-VS-88-TCP
Description	(empty)
Type	Performance (Layer 4) ▾
Source Address	(empty)
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**

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

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							
Traffic Class	<table border="1"><tr><td style="text-align: center;">Enabled</td><td style="text-align: center;">Available</td></tr><tr><td style="height: 100px;"></td><td style="height: 100px;"></td></tr><tr><td style="text-align: center;"><<</td><td style="text-align: center;">>></td></tr></table>	Enabled	Available			<<	>>
Enabled	Available						
<<	>>						
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						

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

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

4. Scroll down to the Resources section.

Resources

	Enabled	Available
iRules		/Common HTML5-HZN74-Fix-2 Origin-Header-LTM _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth
	Up Down	
Default Pool	+ WS1-Pool-88	
Default Persistence Profile	WS1-Persistence	
Fallback Persistence Profile	None	

Cancel **Repeat** **Finished**

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

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

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 'New Virtual Server...' dialog under 'General Properties'. The fields are as follows:

General Properties	
Name	WS1-VS-88-UDP
Description	(empty)
Type	Performance (Layer 4)
Source Address	(empty)
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

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

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	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td><input type="button" value="<<"/></td><td><input type="button" value=">>"/></td></tr></tbody></table>	Enabled	Available	<input type="button" value="<<"/>	<input type="button" value=">>"/>
Enabled	Available				
<input type="button" value="<<"/>	<input type="button" value=">>"/>				
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				

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

INTEGRATION GUIDE

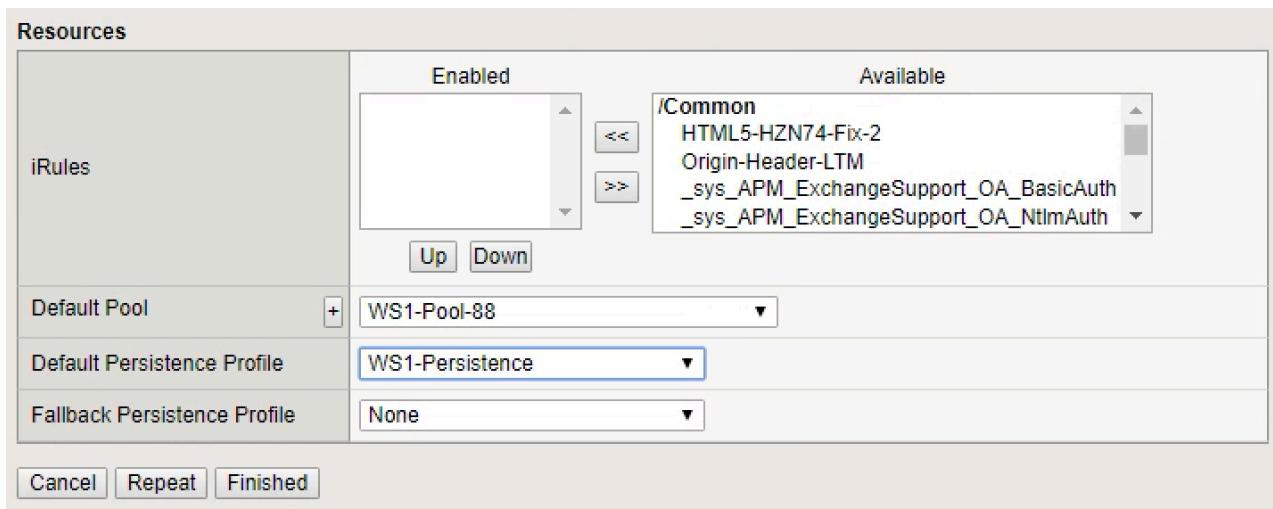
Load Balancing VMware Identity Manager

4. Scroll down to the Resources section.

Resources

	Enabled	Available
iRules		/Common HTML5-HZN74-Fix-2 Origin-Header-LTM _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth
	Up Down	
Default Pool	+ WS1-Pool-88	
Default Persistence Profile	WS1-Persistence	
Fallback Persistence Profile	None	

Cancel **Repeat** **Finished**



- Default Pool:** select the pool for MobileSSO previously created from the pull-down menus.
- Default Persistence Profile:** select the persistence profile for MobileSSO previously created from the pull-down menus.
- 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).

https://ws1-vidm-01.bd.f5.com:8443/cfg/ssl

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



INTEGRATION GUIDE

Load Balancing VMware Identity Manager

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.

The screenshot shows the 'Install Certificate' page of the VMware Identity Manager interface. The left sidebar has a 'Database Connection' section and a 'Install Certificate' item highlighted with a red circle containing the number 1. Below it are 'Identity Manager FQDN', 'Configure Syslog', 'Change Password', 'System Security', and 'Log File Locations'. The main content area has two tabs at the top: 'Terminate SSL on Identity Manager (appliance)' (selected) and 'Terminate SSL on a Load Balancer' (highlighted with a red circle containing the number 2). A note below the tabs says 'Install the LB's root cert on Identity Manager Portal, and Identity Manager Portal's root CA on the LB'. Underneath, there is a section for 'Appliance Root CA Certificate' with a link 'https://ws1-vidm-01.bd.f5.com/horizon_workspace_rootca.pem' (highlighted with a red circle containing the number 3) and a large text input field for the certificate content. A 'Save' button is at the bottom. At the very bottom of the page, a copyright notice reads: '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>.

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.

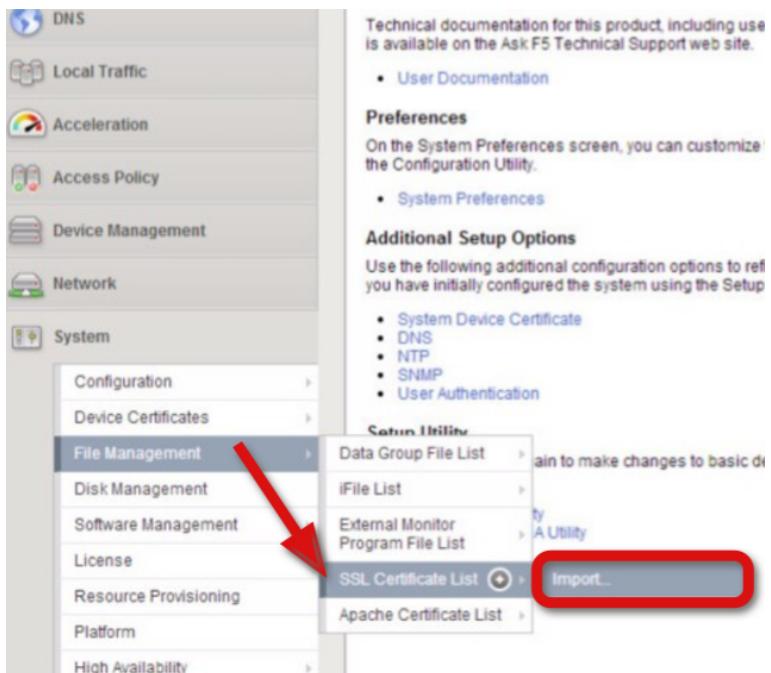
INTEGRATION GUIDE

Load Balancing VMware Identity Manager

4. Highlight the certificate and copy to your clipboard.

```
-----BEGIN CERTIFICATE-----  
MIIDbTCQCAwIBAgI0duwgBuL6NpxEJLZNJY7ZGeANBgkqhkiG9w0BAQFADBI  
MRUwEwYKCzImi2PyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IzZAEZfgrjb3UwMRkw  
FwYDVQQDExBDT0SUk9M0Q0V0VEVSLSUNEMCAXDTE0MDMwNjE3Mjg1MVoYDzlwNjQw  
MzA2MTczODUwNjBIMRUwEwYKCzImi2PyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/Iz  
ZAEZfgrjb3JwMRkwFwYDVQQDExBDT0SUk9M0Q0V0VEVSLSUNEMIIBiJANBgkqhkiG  
9w0BAQEFAOCAsAMIIIBCqECAQEArW2M2yICWn1IPNaxLBqqVjW2lkp2Ttq2xxYg  
C6aiawISicCsdvxrxEOP3wZFDYJF1LRjZaw9LrqkYQtLQaoIGBCDrQ3TVyZU+PmtC  
akQyzYoe6+Hjb3fc7FBXjqfrEY3DMseu69CMexqUW4vhvRvctQaDdbj3Z91+5vd  
Ikxq0PwsyiBaHr8a6H8EgyXOYl1I2hpI4Vhg3j+h33fUbZe2HWm/af8ldfjTfmUI  
pEvyygztL4AnTt5Uqb5SXD0dixre/wlh7syYPQoMnO/HjHYSH8EpQlfEgadfWCChuM  
ailvg853RDcnjJEgywxAMNq4XE+SRAECvN6VK1dROVSP32qqhQIDAQABc1EwTzAL  
BgNVHQ8EBAMCAYYwDwYDVROTAQH/BADwAwEB/zAdBgNVHQ4EFgQUrLH8z+nxYJnZ  
7KtbVadCaV8WKh4wEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvvcNAQEFBQADggEB  
AAMfoSJqS6JbTH1jIf0SBUdxfLVkDVXHwlFtYaQWpw6wRGqMHbdEvaZGGg9y5UWt  
H6Vr4JR8KGZYixjt+D8ZC9t3VCuyGVYLMvtE8RA4zoaaEC877P2c8TEcDniUtLnf  
FifkpxFlnYWX4S/kip2Q+elliUpaS+63Ex/pHYjleBdIvNeYltDeyY2tJ2IvTTxm  
g4u1hHN8I56bCrm1Oy1GkNo2T+1UAwWntUegX+4vuYuv3L580pDQfxKi6icedNP  
eT2maa6iuq+WImns64mGsGw7sdkaeo8ALMYlhuy86QJFc+j8v6hq3Zlr8pa2SUZ  
E7cY+nNeroGGd3OUHw39rGg-----  
-----END CERTIFICATE-----
```

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



INTEGRATION GUIDE

Load Balancing VMware Identity Manager

SSL Certificate/Key Source

Import Type	<input style="width: 100px; height: 25px; border: none; border-radius: 5px; padding: 2px 10px; margin-right: 5px;" type="button" value="Certificate"/> 1
Certificate Name	<input checked="" type="radio"/> Create New <input type="radio"/> Overwrite Existing <input type="text" value="WS1-PEM"/> 3
Certificate Source	<input type="radio"/> Upload File <input checked="" type="radio"/> Paste Text 4 <pre>-----BEGIN CERTIFICATE----- MIIE7DCCA9SgAwIBAgIFFFJQnIkEwDQYJKoZIhvcNAQELBQAwgawxCzAJBgNVBAYT A1VTMRMwEQYDVQQIEwpjYWxpZm9ybmlhMRIwEAYDVQQHEw1QYWxvIEFsdG8xDzAN BgNVBAcTB1ZNd2FyZTEaMBqGA1UECxMRSG9yaXpvbi1Xb3Jrc3BhY2UxJDAiBgNV BAMTG01udGVybmfISFJvb3QqQ0EqMTQ5NDI3M1I0MTEhMB8GCSqGSIb3DQEJARYS dW5rbm93bkB2bXdhcmUuY29tMB4XDTE2MDUwODE5Mzc1MVoXDTQ0MDkvMjE5Mzc1 MlwgaawxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpjYWxpZm9ybmlhMRIwEAYDVQQH Ew1QYWxvIEFsdG8xDzANBgNVBAcTB1ZNd2FyZTEaMBqGA1UECxMRSG9yaXpvbi1X b3Jrc3BhY2UxJDAiBgNVBAMTG01udGVybmfISFJvb3QqQ0EqMTQ5NDI3M1I0MTEh MB8GCSqGSIb3DQEJARYsdW5rbm93bkB2bXdhcmUuY29tMIIBIjANBgkqhkiG9w0B AQEEFAOCQAQ8AMIIBCgKCAQEAt7kH8c9jjZs/jOmPBeStt18j+QF1ZVaH+xIV+6i3G TjthJ12TotZYndSIFnbGwad/P8deI7LDa70laDHTTBtGBIIPAOsghTh5UE2PCob Ulrss8nw3bLb2ICrTBLG3b4caML4khgx53kDSwYiVI4EzisAofycKOWXl+ZKrEbS gTWXe5NpbBSn1AdprvVALiKv18J6Y3vQ4VEULtanu94CcT05Xi0MBT1vAhfC72+Ii MxrzMAs/LUEif2uDbribZrV4eAmtU2zThb1DE265ss4nGxHZ6bKC9A7U+GM19kB8 UPAwMvKDzwwBZVRCLcN4RksaKGhuUnQyNOYsCmauivFSEQIDAQABo4IBETCCAQ0w DAYDVROTBauAwEB/zAdBgNVHQ4EFgQUh8a2V6pET8oY8T7GPvmsiyKNXcMwgd0G A1UdIwSB1ICB0oAUh8g2V6pET8oY8T7GPvmsiyKNXcOhgbKkg8wgawxCzAJBgNV BAYTA1VTMRMwEQYDVQQIEwpjYWxpZm9ybmlhMRIwEAYDVQQHEw1QYWxvIEFsdG8xD zANBgNVBAcTB1ZNd2FyZTEaMBqGA1UECxMRSG9yaXpvbi1Xb3Jrc3BhY2UxJDAi BgNVBAMTG01udGVybmfISFJvb3QqQ0EqMTQ5NDI3M1I0MTEhMB8GCSqGSIb3DQEJ </pre> 5
Free Space on Disk	197 MB
<input type="button" value="Cancel"/> <input type="button" value="Import"/> 6	

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

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

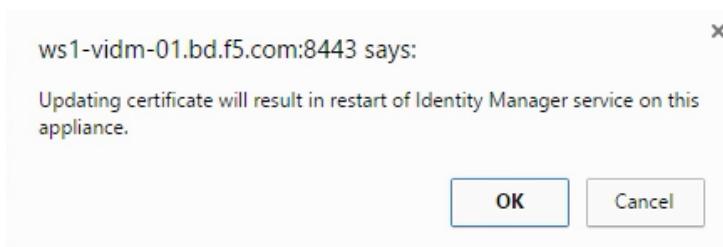
Load the FQDN Root/Primary CA Certificate into Identity Manager Node 1

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

The screenshot shows the 'Install Certificate' screen in the VMware Identity Manager appliance configuration interface. The left sidebar menu has 'Install Certificate' selected (marked with a red circle 1). The top navigation bar shows 'Welcome Admin | Help | Log out'. The main content area has two tabs: 'Terminate SSL on Identity Manager (appliance)' (selected) and 'Terminate SSL on a Load Balancer' (marked with a red circle 2). A note below the tabs says 'Install the LB's root cert on Identity Manager Portal, and Identity Manager Portal's root CA on the LB'. Below this, there is a section for 'Appliance Root CA Certificate' with a text input field containing a certificate snippet (marked with a red circle 3). A 'Save' button is at the bottom (marked with a red circle 4). A note at the bottom of the page states: '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>.

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

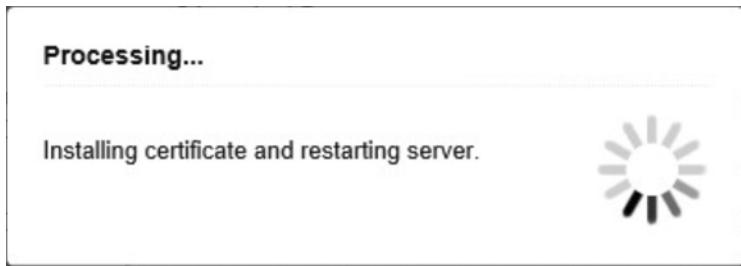
1. Click **Install Certificate** from the menu on the left side of the screen.
2. Click the **Terminate SSL on a Load Balancer** tab at the top right of the screen.
3. Open the FQDN's Root/Primary Certificate in WordPad or other text editing utility. Copy and paste the contents of this certificate into 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.

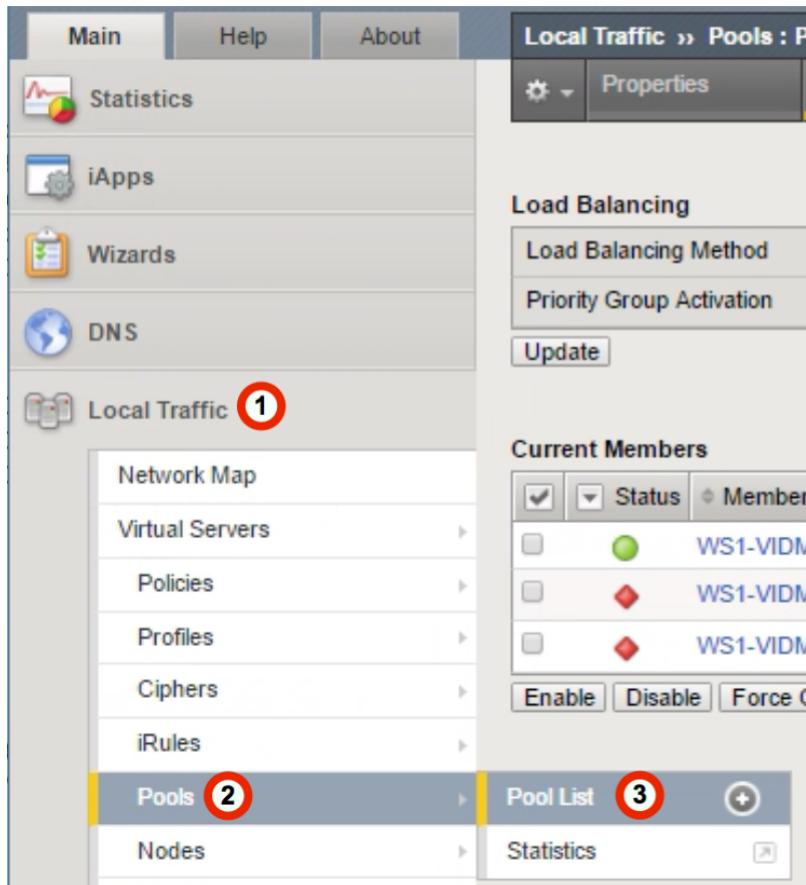
Configuring the FQDN for Identity Manager

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.

The screenshot shows the 'Local Traffic' interface with the 'Pools' section selected. Under 'Pool List', the 'WorkspaceOne-Pool' is chosen. The 'Members' tab is active, highlighted in yellow. The interface includes sections for 'Load Balancing' and 'Current Members'. In the 'Load Balancing' section, the 'Load Balancing Method' is set to 'Least Connections (member)' and 'Priority Group Activation' is set to 'Disabled'. Below this is an 'Update' button. The 'Current Members' section lists three nodes: WS1-VIDM-01.bd.f5.com:443 (IP 10.105.169.110, Port 443), WS1-VIDM-02.bd.f5.com:443 (IP 10.105.169.111, Port 443), and WS1-VIDM-03.bd.f5.com:443 (IP 10.105.169.112, Port 443). Each node has a status indicator (green for Node 1, red for Nodes 2 and 3) and a checkbox. Below the table are buttons for 'Enable', 'Disable', 'Force Offline', and 'Remove'.

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	

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

INTEGRATION GUIDE

Load Balancing VMware Identity Manager

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>).

~~https://ws1-vidm-01.bd.f5.com:8443/cfg/ssl~~

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



INTEGRATION GUIDE

Load Balancing VMware Identity Manager

Change Identity Manager Node 1's FQDN

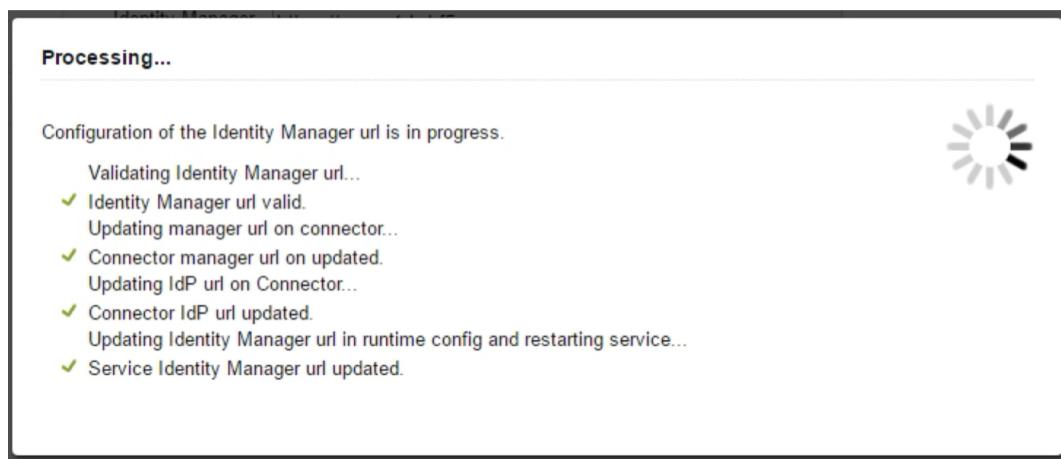
Once in the Workspace Portal/Identity Manager Appliance Configuration Page:

The screenshot shows the VMware Identity Manager configuration interface. On the left, a sidebar menu lists several options: Database Connection, Install Certificate, Identity Manager FQDN (with a red circle containing the number 1), Configure Syslog, Change Password, System Security, and Log File Locations. The main content area is titled "Identity Manager FQDN". It contains a brief description of what FQDN is, a note about load balancers, and a text input field labeled "Identity Manager FQDN*" with the value "https://myws1.bd.f5.com" (circled with a red 2). Below the input field is a placeholder "e.g. https://mycompany.identitymanager.com:444". At the bottom of the page, there is a "Save" button (circled with a red 3) and a copyright notice at the bottom.

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

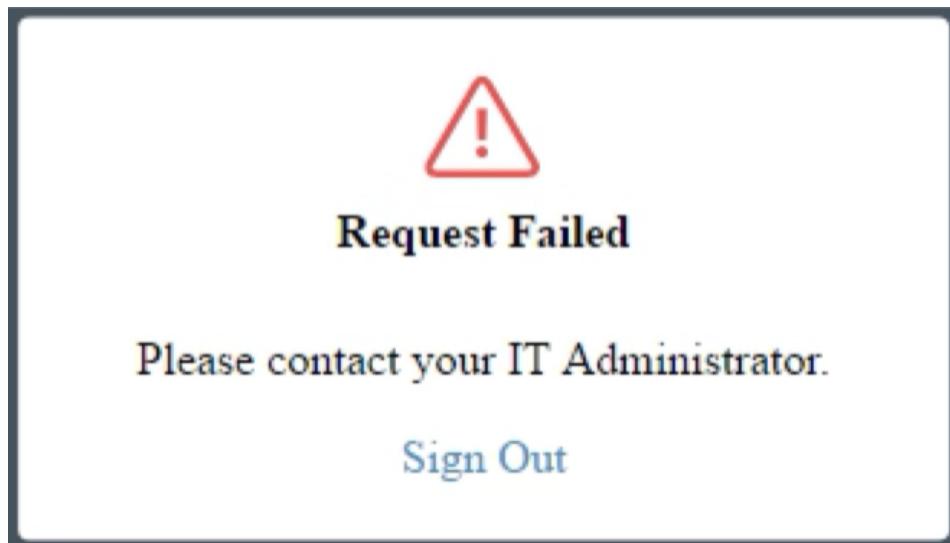
Once the FQDN update starts, you should be prompted with a screen that displays the progress.



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.



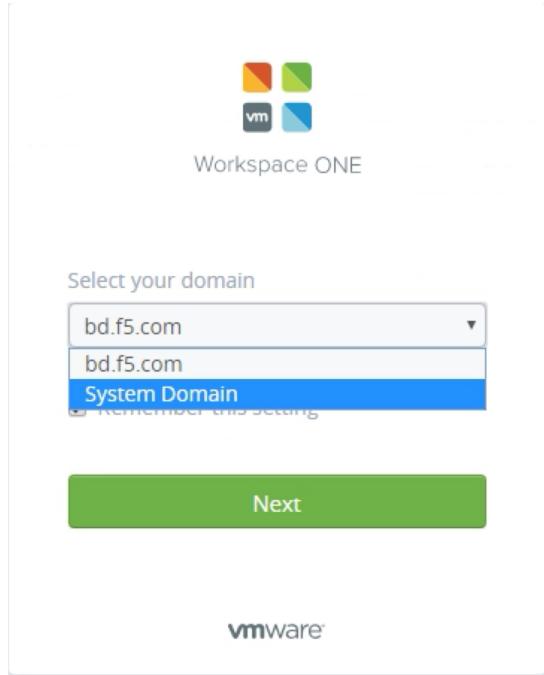
1. In a browser, type the FQDN of the first Identity Manager appliance you are configuring (for example, https://ws1-vidm-01.bd.f5.com)



INTEGRATION GUIDE

Load Balancing VMware Identity Manager

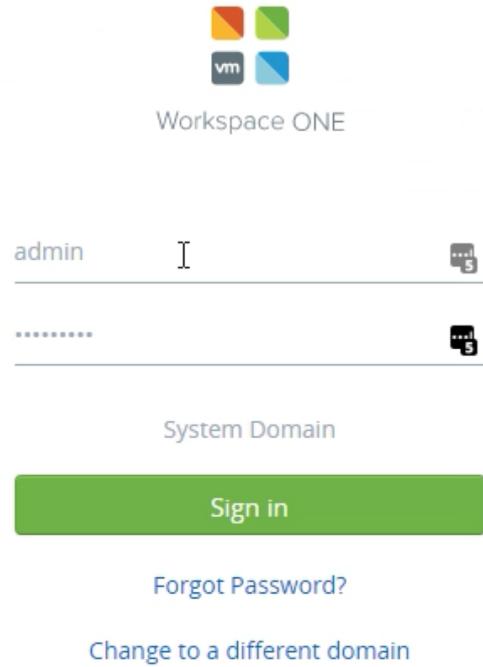
2. Clear the check from the **Remember this Setting** box, and then select **System Domain** from the list.
3. Click **Next**.



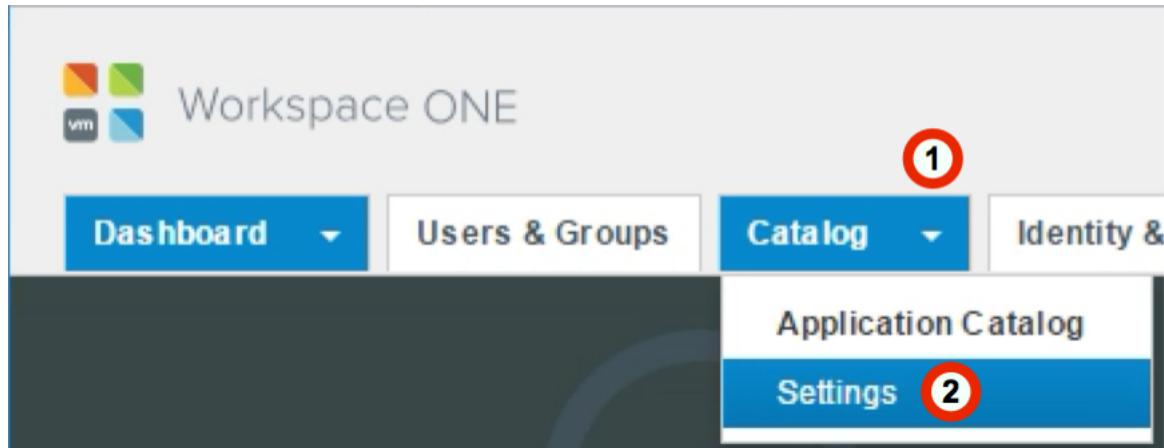
4. Login to the Workspace One Portal with the Local Admin Username and Password, ensure that **System Domain** is marked as the domain. If it is the incorrect domain select **Change to a different domain** and follow the previous steps.

INTEGRATION GUIDE

Load Balancing VMware Identity Manager



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



- 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

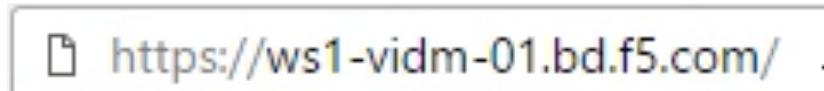
The screenshot shows the VMware Identity Manager (VIDM) interface. At the top, there's a navigation bar with tabs: Dashboard, Users & Groups, Catalog, Identity & Access Management (selected), and Appliance Settings. A search bar at the top right contains the placeholder "Search users, groups or applications". On the left, a sidebar lists various settings: Global Settings, Remote App Access, SAML Metadata, Approvals, Auditing, Horizon Air, User Portal Branding, ThinApp Application Alerts, and New End User Portal UI (which is highlighted with a blue background and circled with a red number 1). In the center, a callout box displays the message "New End User Portal UI" and "New End User Portal UI is enabled successfully" (circled with a red number 3). Below this, there's a button labeled "Enable New Portal UI" (circled with a red number 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>.

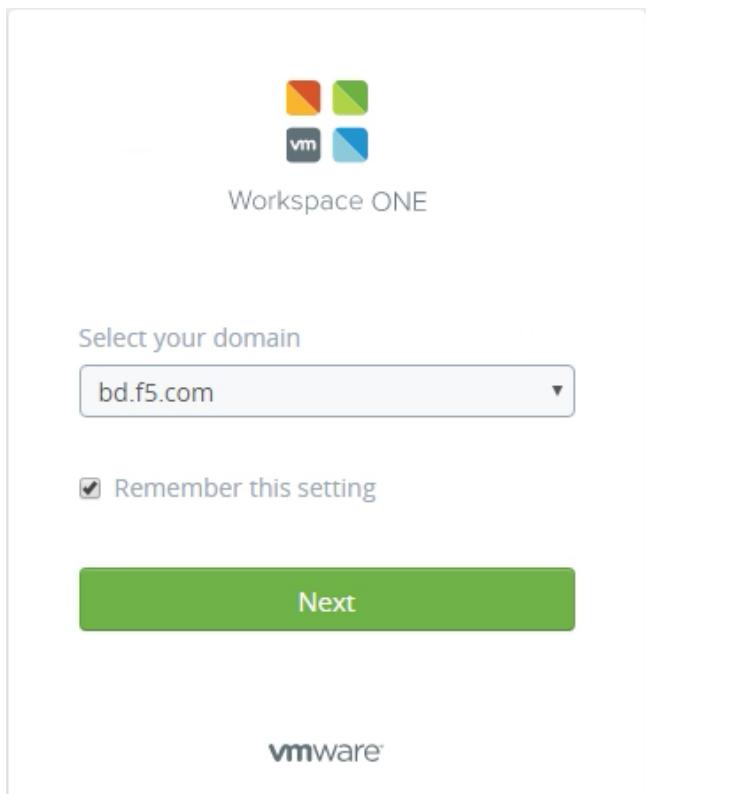
Logging into Identity Manager Portal

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).



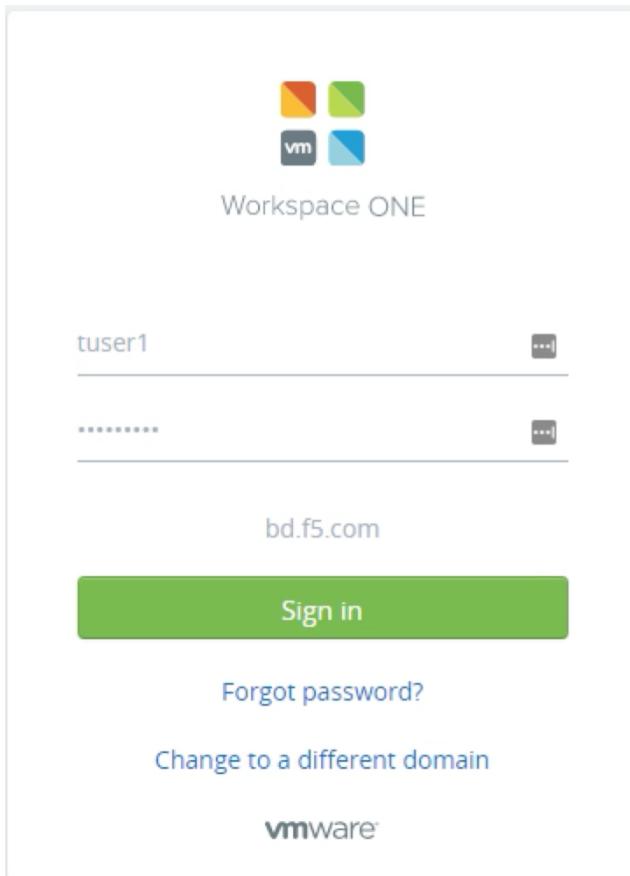
You should see the Workspace One Domain Selection Page. If you are taken directly to the Login page for System Domain or a domain where the user you wish to test is not selected appropriately, click the **Change to a different domain** button to get back to the domain selection page.



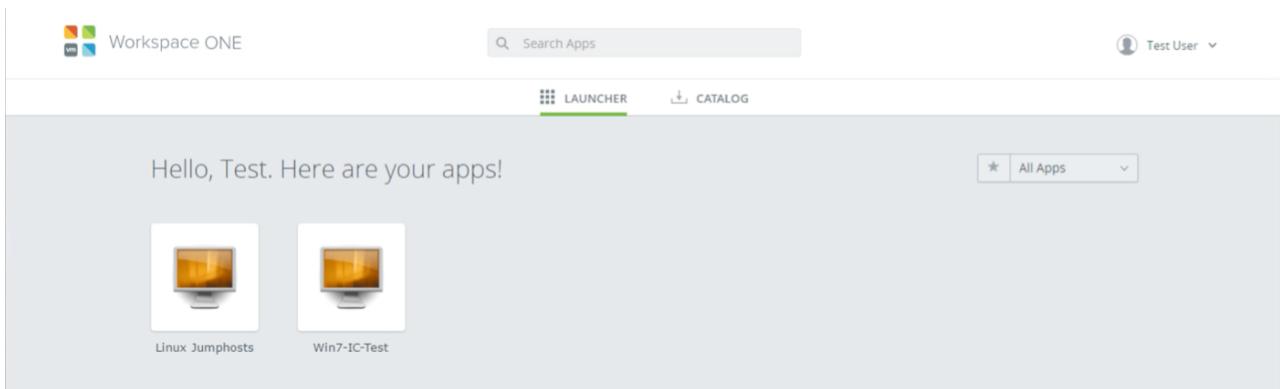
INTEGRATION GUIDE

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>