

BIG-IQ[®] Cloud: VMware NSX Administration

Version 1.0



Table of Contents

Legal Notices.....	5
Legal notices.....	5
BIG-IQ System Introduction.....	7
Overview: BIG-IQ system.....	7
Additional resources and documentation for BIG-IQ systems.....	7
About incorporating BIG-IQ system securely into your network.....	7
Open ports required for device management.....	8
Software Licensing and Initial Configuration.....	9
About software licensing and initial configuration.....	9
Automatic license activation.....	9
Manual license activation.....	10
Confirming the Management Address.....	10
Defining DNS and NTP servers for the BIG-IQ system.....	11
Changing the default passwords.....	11
Users, User Groups, and Roles.....	13
Overview: Users, user groups, and roles.....	13
About default passwords for pre-defined users.....	13
Changing the default password for the administrator user.....	13
Adding a locally-authenticated BIG-IQ user.....	14
About user roles.....	14
Roles definitions.....	14
Associating a user or user group with a role	15
Disassociating a user from a role.....	15
Device Discovery.....	17
About device discovery and management.....	17
Discovering a BIG-IP device in your network by its IP address.....	17
License Management.....	19
Overview: Licensing options.....	19
About pool licenses.....	19
Automatically activating a pool license.....	19
Manually activating a pool license.....	19
Assigning a pool license to a BIG-IP VE.....	21
Revoking a pool license from a BIG-IP VE.....	21

Integrating with VMware NSX.....	23
Network requirements for communication with VMware cloud services	23
Discovering devices located in the VMware cloud.....	23
About configuring the BIG-IQ device for a VMware integration.....	24
Prepare the BIG-IQ devices for NSX integration.....	24
Prepare VMware NSX for integration.....	28
Prepare the new BIG-IP devices for integration.....	30
Complete the NSX integration.....	32
 Cloud Tenant Management.....	 35
About creating cloud tenants	35
Creating a tenant.....	35
Creating a cloud user.....	35
Associating a user with a tenant's role.....	36
 Glossary.....	 37
BIG-IQ Cloud terminology.....	37

Legal Notices

Legal notices

Publication Date

This document was published on January 7, 2016.

Publication Number

MAN-0605-00

Copyright

Copyright © 2015-2016, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, AskF5, ASM, BIG-IP, BIG-IP EDGE GATEWAY, BIG-IQ, Cloud Extender, Cloud Manager, CloudFucious, Clustered Multiprocessing, CMP, COHESION, Data Manager, DDoS Frontline, DDoS SWAT, Defense.Net, defense.net [DESIGN], DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Mobile, Edge Mobility, Edge Portal, ELEVATE, EM, ENGAGE, Enterprise Manager, F5, F5 [DESIGN], F5 Agility, F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FCINCO, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, iCall, iControl, iHealth, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LROS, LTM, Message Security Manager, MobileSafe, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Ready Defense, Real Traffic Policy Builder, SalesXchange, ScaleN, SDAS (except in Japan), SDC, Signalling Delivery Controller, Solutions for an application world, Software Designed Application Services, Silverline, SSL Acceleration, SSL Everywhere, StrongBox, SuperVIP, SYN Check, SYNTHESIS, TCP Express, TDR, TechXchange, TMOS, TotALL, TDR, TMOS, Traffic Management Operating System, Traffix, Traffix [DESIGN], Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: <https://f5.com/about-us/policies/patents>

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

BIG-IQ System Introduction

Overview: BIG-IQ system

The BIG-IQ® system is a tool that streamlines the management of F5 devices in your network. Because it is based on the same platform as BIG-IP® devices, it includes full product support, security patches, and internal and external security audits (AuthN and AuthZ checks). The specific functionality offered is dependent on your software license.

Cloud administrators use BIG-IQ Cloud to provide cloud tenants self-service access to shared computing resources such as networks, servers, storage, applications, and services. Cloud resources can be private or public, depending on the customer's requirements. Each tenant has restricted and dedicated access to cloud resources based on a specific user account or tenant role, ensuring that tenants have access only to their own resources. Cloud resources are easily expanded and reallocated as needed, providing flexible resource balancing.

Additional resources and documentation for BIG-IQ systems

You can access all of the following BIG-IQ® system documentation from the AskF5™ Knowledge Base located at <http://support.f5.com/>.

Document	Description
BIG-IQ® Systems Virtual Editions Setup guides	BIG-IQ® Virtual Edition (VE) runs as a guest in a virtual environment using supported hypervisors. Each of these guides is specific to one of the hypervisor environments supported for the BIG-IQ system.
Release notes	Release notes contain information about the current software release, including a list of associated documentation, a summary of new features, enhancements, fixes, known issues, and available workarounds.
Solutions and Tech Notes	Solutions are responses and resolutions to known issues. Tech Notes provide additional configuration instructions and how-to information.

About incorporating BIG-IQ system securely into your network

To successfully manage devices in your network, including BIG-IQ® peer systems, the BIG-IQ system requires communication over HTTPS port 443. The BIG-IQ administrator can provide fine-grained access to various roles, which are verified by authorization checks (AuthN and AuthZ). Authenticated users have access only to the resources explicitly granted by the BIG-IQ administrator.

Open ports required for device management

The BIG-IQ® system requires bilateral communication with the devices in your network in order to successfully manage them. For this communication, the following ports are open by default to allow for the required two-way communication.

Open Port	Purpose
TCP 443 (HTTPS)	Discovering, monitoring, and configuring managed devices
TCP 443 (HTTPS) and TCP 22 (SSH)	Upgrade BIG-IP® devices running version 11.5.3 and later
TCP 443 (HTTPS)	Upgrade BIG-IP devices running version 12.0.0
TCP 443 (HTTPS)	Replicating and synchronizing BIG-IQ systems

Software Licensing and Initial Configuration

About software licensing and initial configuration

BIG-IQ® Cloud runs as a virtual machine in specifically-supported hypervisors. After you set up your virtual environment or your platform, you can download the BIG-IQ software, and then license the BIG-IQ system. You initiate the license activation process with the base registration key.

The *base registration key* is a character string that the license server uses to verify the functionality that you are entitled to license.

There are two methods for activating the product.

- If the system has access to the internet, you select the option to automatically contact the F5 license server and activate the license.
- If the system is not connected to the internet, you manually retrieve the activation key from a system that is connected to the internet, and transfer it to the BIG-IQ system.

Task List

Confirming the Management Address

Defining DNS and NTP servers for the BIG-IQ system

Changing the default passwords

Automatic license activation

You must have a base registration key to license the BIG-IQ® system. If you do not have a base registration key, contact the F5 Networks sales group (<http://www.f5.com>).

If the BIG-IQ® system has outbound access to the public internet, you can use this procedure to activate its license.

1. Using a browser on which you have configured the management interface, type `https://management_IP_address>` where `<management_IP_address>` is the address you specified for device management.
This is the IP address that the BIG-IQ system uses to communicate with its managed devices.
2. Log in to BIG-IQ System with the default user name `admin` and password `admin`.
3. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
4. In the **Add-on Keys** field, paste any additional license key you have.
5. For the **Activation Method** setting, select **Automatic**, and click the **Next** button.
The End User Software License Agreement (EULA) displays.
6. To accept, click the **Agree** button.
7. Click the **Next** button.
8. In the **Old Password** fields, type the default admin and root passwords, and then type a new password in the **Password** and **Confirm Password** fields.
9. In the **Host Name** field, type a fully-qualified domain name (FQDN) for the system.

The FQDN can consist of letters and numbers, as well as the characters underscore (_), dash (-), or period (.).

10. Click the **Next** button to save your configuration.

Manual license activation

You must have a base registration key to license the BIG-IQ® system. If you do not have a base registration key, contact the F5 Networks sales group (<http://www.f5.com>).

If the BIG-IQ® system is not connected to the public internet, this procedure can activate its license.

1. Using a browser on which you have configured the management interface, type `https://<management_IP_address>` where `<management_IP_address>` is the address you specified for device management.
This is the IP address that the BIG-IQ system uses to communicate with its managed devices.
2. Log in to BIG-IQ System with the default user name `admin` and password `admin`.
3. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
4. In the **Add-on Keys** field, paste any additional license key you have.
5. For the **Activation Method** setting, select **Manual** and click the **Get Dossier** button.
The BIG-IQ system refreshes and displays the dossier in the **Device Dossier** field.
6. Copy the text displayed in the **Device Dossier** field, and click the **Access F5 manual activation web portal** link.
Alternatively, you can navigate to the F5 license activation portal at `https://activate.f5.com/license/`.
7. Click **Activate License**.
The Activate F5 Product page opens.
8. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
After a pause, the license key text displays.
9. Select the check box next to the **I have read and agree to the terms of this license** to agree to the license terms, and then click the **Next** button.
After a brief pause, the license key text displays.
10. Copy the license key.
11. On BIG-IQ Device, into the **License Text** field, paste the license key.
12. Click the **Next** button at the top of the page.

You still need to confirm the management address, set up your DNS and NTP services, and update your passwords before you can launch.

Confirming the Management Address

Before you confirm the management address, you must have activated the license.

You need to specify the details of how the BIG-IQ® device communicates.

1. In the **Host Name** field, type a fully-qualified domain name (FQDN) for the system.
The FQDN can consist of letters and numbers, as well as the characters underscore (_), dash (-), or period (.).

2. In the **Management Port IP Address** field, type the self IP address of your internal VLAN. The self IP address must be in Classless InterDomain Routing (CIDR) format. For example: 10.10.10.10/24. This is the self IP address that managed devices use to communicate with the BIG-IQ system. This address is also referred to as the *discovery address*.
3. In the **Management Port Route** field, type the default gateway address for the management port.
4. Select the **Use Management Address for HA Peer Communication** check box if you want to use the management port IP address for communication between peer BIG-IQ systems in a high availability configuration.
5. To specify a unique self IP address for communication between peer BIG-IQ systems in a high availability configuration, clear the **Use Management Address for HA Peer Communication** check box and type the self IP address for the HA IP Address in the **Self IP Address** field.

***Note:** The IP address must be specified in CIDR format.*

6. To save your configuration, click the **Next** button.

Defining DNS and NTP servers for the BIG-IQ system

After you license the BIG-IQ® system, you can specify the DNS and NTP servers.

Setting your DNS server and domain allows the BIG-IQ system to properly parse IP addresses. Defining the NTP server ensures that the BIG-IQ system's clock is synchronized with Coordinated Universal Time (UTC).

1. In the **DNS Lookup Servers** field, type the IP address of your DNS server.
You can click the **Test Connection** button to verify that the IP address is reachable.
2. In the **DNS Search Domains** field, type the name of your search domain.
The DNS search domain list allows the BIG-IQ system to search for local domain lookups to resolve local host names.
3. In the **Time Servers** fields, type the IP addresses of your Network Time Protocol (NTP) servers.
You can click the **Test Connection** button to verify that the IP address is reachable.
4. From the **Time Zone** list, select your local time zone
5. Click the **Next** button to save your configuration.

Changing the default passwords

After you initially license and configure the BIG-IQ system, you must confirm or change the administrator role password from the default, `admin`.

1. For the admin account, in the **Old Password** field, type `admin`.
2. In the **New Password** and **Confirm New Password** fields, type a new password.
3. For the root account, in the **Old Password** field, type `default`.
4. In the **New Password** and **Confirm New Password** fields, type a new password.
5. To save this configuration, click the **Next** button.

Users, User Groups, and Roles

Overview: Users, user groups, and roles

A *user* is an individual to whom you provide resources. You provide access to users for specific BIG-IQ® system functionality through authentication. You can associate a user with a specific role, or associate a user with a user group and then associate the group with a role.

A *role* is defined by its specific privileges. A *user group* is a group of individuals that have access to the same resources. When you associate a role with a user or user group, that user or user group is granted all of the role's corresponding privileges.

By default, the BIG-IQ® system provides the following default user types:

Default user type	Default password	Access rights
admin	admin	This user type can access all aspects of the BIG-IQ system from the system's user interface.
root	default	This user has access to all aspects of the BIG-IQ system from the system's console command line.

User types persist and are available after a BIG-IQ system failover.

About default passwords for pre-defined users

When you initially license the BIG-IQ® system, it creates the following administrative roles with a default password.

- admin
- root

Changing the default password for the administrator user

You must specify the management IP address settings for the BIG-IQ® system to prompt the system to automatically create the administrator user.

After you initially license and configure the BIG-IQ system, it is important to change the administrator role password from the default, `admin`.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. On the Users panel, for **Admin User**, click the gear icon and then **Properties**.
4. For the admin account, in the **Old Password** field, type `admin`.
5. In the **New Password** and **Confirm New Password** fields, type a new password.
6. For the root account, in the **Old Password** field, type `default`.

7. In the **New Password** and **Confirm New Password** fields, type a new password.
8. To save this configuration, click the **Next** button.

Adding a locally-authenticated BIG-IQ user

You create a user so you can then associate that user with a particular role to define access to specific BIG-IQ® system resources.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. In the Users panel, hover over a user, and click the gear icon when it appears.
The panel expands to display the User properties.
4. From the **Auth Type Provider** list, select **Local**.
5. In the **Full Name** field, type a name to identify this user.
The full name can contain a combination of symbols, letters, numbers and spaces.
6. In the **Password** and **Confirm Password** fields, type the password for the new user.
7. Click the **Add** button.

You can now associate this user with a role.

About user roles

As a system manager, you need a way to differentiate between users and to limit user privileges based on their responsibilities. To assist you, the BIG-IQ® system has created a default set of roles you can assign to a user. Roles persist and are available after a BIG-IQ system failover.

Roles definitions

BIG-IQ® system ships with several standard roles, which you can assign to individual users.

Role	Description
Administrator	Responsible for overall administration of all licensed aspects of the BIG-IQ system. These responsibilities include adding individual users, assigning roles, discovering BIG-IP® systems, installing updates, activating licenses, and configuring a BIG-IQ high availability (HA) configuration.
Tenant	<p>A tenant is an entity that can consist of one or more users accessing resources provided by an administrator. Responsibilities include: customizing and deploying application templates, and monitoring the health statistics and performance of applications and servers.</p> <hr/> <p>Note: The BIG-IQ system creates a new role when an administrator creates a new tenant. The</p>

Role	Description
	<i>connectors each tenant can access are specified when the tenant is created. The name of the new role is based on the tenant name. For example, creating a new tenant named <code>headquarters-user</code>, produces a new role named <code>headquarters-user</code> (Cloud Tenant).</i>

Associating a user or user group with a role

Before you can associate a user or user group with a role, you must create a user or user group.

When you associate a user or user group with a role, you define the resources users can view and modify. You can associate multiple roles with a given user.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. At the top of the screen, click **Access Control**.
3. In the Users or User Groups panel, click the name you want to associate with a role, and drag and drop it on a role in the Roles panel.
A confirmation pop-up screen opens.
4. Click the **Confirm** button to assign the user or user group to the selected role.

This user or user group now has access to the resources associated with the role you specified.

Disassociating a user from a role

Use this procedure to disassociate a user from an assigned role.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. At the top of the screen, click **System > Users**.
3. Click the name of the user you want to edit.
4. For the User Roles property, delete the user role that you want to disassociate from this user.
5. Click the **Save** button to save your changes.

This user no longer has the privileges associated with the role you deleted.

Device Discovery

About device discovery and management

You use BIG-IQ® Device to centrally manage resources located on BIG-IP® devices.

The first step to managing devices is making BIG-IQ Device aware of them through the discovery process. To discover a device, you provide BIG-IQ Device the device IP address, user name, and password. Alternatively, you can upload a CSV file to discover a large number of devices. When you discover a device you place it into a group. These groups help you organize devices with similar features, like those in a particular department or running a certain software version.

After you discover devices, you can view and export inventory details about those devices for easy asset management, and you can modify device configurations as required without having to log in to each device individually.

Discovering a BIG-IP device in your network by its IP address

After you license and perform the initial configuration for the BIG-IQ® system, you can discover BIG-IP™ devices running version 11.5.3 HF3 and later or 11.6 HF6 and later. For proper communication, you must configure the BIG-IQ system with a route to each F5 device you want to manage. If you do not specify the required network communication route between the devices, then device discovery fails.

Important: *The BIG-IQ system will attempt discovery of BIG-IP devices running versions other than those noted (above) as fully supported. Discovering unsupported devices is not recommended.*

There are two ways to discover F5 devices in your network.

- You can discover a device you previously imported to the BIG-IQ system.
- You can discover a device in your local network.

Important: *When you discover a device, BIG-IQ software will install necessary components on the device, which can cause the traffic management interface (TMM) on the BIG-IP device to restart. Therefore, before discovering a device, verify that no critical network traffic is targeted to the BIG-IP device.*

1. Hover over the Devices header, click the + icon when it appears, and then select **Discover Device**. The Devices panel expands to show the Discover Device screen.
2. To discover a device:
 - If you previously imported the device to the BIG-IQ system:
 1. For **Source**, select the **BIG-IQ Inventory** option.
 2. Click the device located in the **Available** field, and click the Move button to move it to the **Include** field.
 3. Click **Save** to start the discovery task
 - If the device is in your local network:
 1. For the **Source**, select **IP Address**.

2. For the **IP Address**, specify the device's internal self-IP address.
3. For the **Device Group**, select the group to which you want to add the device.
4. In the **User Name** and **Password** fields, type the administrator user name and password for the managed device.

Important: For successful device discovery, you must use the admin account; not the root account. If root access is needed, the system prompts you for it.

3. Click **Save** to start the discovery task.

The BIG-IQ system populates the properties of the device that you added in the Devices panel.

License Management

Overview: Licensing options

You can centrally manage BIG-IP® virtual edition (VE) licenses for a specific set of F5 offerings (for example, BIG-IP LTM® 25M, BIG-IP LTM 200G, and BIG-IP LTM 1G). When a device is no longer needed, you can revoke the license instance and assign it to another BIG-IP VE device. This flexibility keeps operating costs fixed, and allows for a variety of provisioning options. *Pool licenses* are purchased once, and you assign them to a number of concurrent BIG-IP VE devices, as defined by the license. These licenses do not expire.

About pool licenses

Pool licenses are purchased for a particular product offering for a fixed number of devices, but are not permanently tied to a specific device. As resource demands change, you can use BIG-IQ® Device to revoke and reassign those licenses to other BIG-IP® VE devices as required. Pool licenses do not expire.

Automatically activating a pool license

You must have a base registration key before you can activate the license pool.

If the resources you are licensing are connected to the public internet, you can automatically activate the license pool.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. Hover over the Licenses header, and click the + icon when it appears.
The New License screen opens.
3. In the **License Name** field, type the name you want to use to identify this license.
4. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
5. In the **Add-on Keys** field, paste any additional license key you have.
6. For the **Activation Method** setting, select **Automatic**.
The End User Software License Agreement (EULA) displays.
7. To accept, click the **Accept** button.
The system reads your license key and adds the activated license to the License panel.

Manually activating a pool license

You must have a base registration key before you can activate the pool license.

If the BIG-IQ® Device you are licensing is not connected to the public internet, you can activate the pool license manually.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. Hover over the Licenses header, and click the + icon when it appears.
The New License screen opens.
3. In the **License Name** field, type the name you want to use to identify this license.
4. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
5. In the **Add-on Keys** field, paste any additional license key you have.
6. For the **Activation Method** setting, select **Manual** and click the **Get Dossier** button.
The BIG-IQ system refreshes and displays the dossier in the **Device Dossier** field.
7. Copy the text displayed in the **Device Dossier** field, and click the **Access F5 manual activation web portal** link.
Alternatively, you can navigate to the F5 license activation portal at <https://activate.f5.com/license/>.
8. Click **Activate License**.
The Activate F5 Product page opens.
9. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
After a pause, the license key text displays.
10. Copy the license key.
11. On BIG-IQ Device, into the **License Text** field, paste the license key.
12. Click the **Activate** button.
If the license does not display as activated in the Licenses panel after several minutes, click the arrow next to the license to contract the list, then click it again to expand. The screen should refresh and display the license as activated.

Manually activating offering licenses

Before you can activate the individual offering licenses, you must first activate the license itself.

Activating the offering licenses makes them available for assignment.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Licenses panel, click the arrow next to the license you previously activated.
The list expands to display the license offerings associated with this license.
4. Hover over an offering license and click the gear icon when it appears.
5. Copy the text displayed in the **Device Dossier** field, and click the **Access F5 manual activation web portal** link.
Alternatively, you can navigate to the F5 license activation portal at <https://activate.f5.com/license/>.
6. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
After a pause, the license key text displays.
7. Copy the license key.
8. On BIG-IQ Device, into the **License Text** field, paste the license key.
9. Click the **Activate** button.
If the license does not display as activated in the Licenses panel after several minutes, click the arrow next to the license to contract the list, then click it again to expand. The screen should refresh and display the license as activated.

You can now assign this offering license to a BIG-IP® VE device.

Assigning a pool license to a BIG-IP VE

Before you can assign a pool license to a BIG-IP® VE device, you must activate the license on the BIG-IQ® system and discover the BIG-IP VE device to which you want to assign the license.

Pool licenses provide you with the flexibility to easily manage resources and operating costs. Use this procedure if you have activated a pool license, but have not yet assigned it to a BIG-IP VE.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Devices panel, expand the device group that contains the device you want to license by clicking the arrow next to it.
The panel expands to display the list of devices contained in this group.
4. Click the gear icon next to the device you want to license, and then click **License Device**.
5. In the **Name** field, type a name for this license.
6. From the **Licensing** list, select **Use a Pool License**.
7. From the **Pool License** list, select the pool license you want to assign to this device.
8. Click the **Deploy** button.
9. To confirm that the license was successfully deployed, click the gear icon next to the license you deployed, click **Properties**, and then click **Assignments**.
The device you licensed displays with the license status and the last contact from the BIG-IQ system.

Revoking a pool license from a BIG-IP VE

If traffic decreases to the applications on some of your managed BIG-IP® devices, you can use BIG-IQ® Device to revoke those licenses and assign them to other resources as needed.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. At the top of the screen, click **Provisioning**.
3. On the Devices panel, expand the device group that contains the device for which you want to revoke a license by clicking the arrow next to it.
4. Click the gear icon next to the device for which you want to revoke a license, and then click **License Device**.
5. From the **Licensing** list, select **Revoke a License**.
6. Click the **Deploy** button.

You can now assign this license to another BIG-IP® device.

Integrating with VMware NSX

Network requirements for communication with VMware cloud services

For proper communication, BIG-IQ® Cloud must have network access to the resources on which VMware software is installed. Before you can manage cloud resources, you must define a network route between the BIG-IQ Cloud device's VLAN and the management VLAN on the VMware.

Discovering devices located in the VMware cloud

After you license and perform the initial configuration for the BIG-IQ® system, you can discover BIG-IP® devices running version 11.5 or later. For proper communication between the managing BIG-IQ device and the devices it manages, you must configure the BIG-IQ system with a route to each F5 device you want to manage. If you do not specify the required network communication route between the devices, then device discovery fails.

You must know the IP address that the BIG-IQ device will use to access the BIG-IP device.

Discover a device by providing the BIG-IQ® system with the device's IP address, user name, and password.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. Hover over the Devices header, click the + icon when it appears, and then select **New Device**.
The Devices panel expands to show the New Device screen.
3. In the **IP Address** field, type the device's IP address.
The preferred address for discovering a BIG-IP device is its management IP address.
4. If the BIG-IQ system and the BIG-IP device are on different subnets, then you need to specify an IP route between them.
 - If the BIG-IQ device and the BIG-IP device communicate using the management IP address, then use SSH to issue a `route` command.
 1. Use SSH to log in to the BIG-IQ system's management IP address as the root user.
 2. Type the following command: `route <route name> {gw <x.x.x.x> network default}`
 - If the BIG-IQ device and the BIG-IP device use something other than the management IP address to communicate, then use SSH to issue a `tmsh route` command.
 1. Use SSH to log in to the BIG-IQ system's management IP address as the root user.
 2. Type the following command: `tmsh create net route <route name> {gw <x.x.x.x> network default}`

Note: Where `<route name>` is a user-provided name to identify the new route, and `<x.x.x.x>` is the IP address of the default gateway for the internal network.

5. In the **User Name** and **Password** fields, type the administrator user name and password for the managed device.
6. For the **Auto Update Framework** setting, select the **Update Automatically** check box to direct the BIG-IQ system to perform any required REST framework updates on the BIG-IP device.
For the BIG-IQ system to properly manage a BIG-IP device, the BIG-IP device must be running the most recent REST framework.
7. Click the **Add** button.

The BIG-IQ system populates the properties of the device that you added, and displays the device in the Devices panel and its configuration files display in the Configuration panel.

To complete discovery of BIG-IP® devices and populate the Devices panel, provide the administrator user name and password when requested. You can then associate tenants with this resource.

About configuring the BIG-IQ device for a VMware integration

The BIG-IQ® device facilitates the integration between the VMware NSX and the BIG-IP® device or device cluster. The work flow for configuring this integration takes you back and forth between the two participants in this integration.

You can either integrate with a standalone BIG-IP virtual machine, or with a high availability (HA) cluster of BIG-IP virtual machines. The process for setting up the two configurations is nearly identical. Optional steps and settings to enable HA are noted where applicable.

You can ensure that the traffic management function is always available by configuring two or more BIG-IP systems in a high availability (HA) configuration. Any configuration change that occurs on one BIG-IP system is immediately synchronized with its peer devices. If one BIG-IP system in an HA configuration fails, a peer BIG-IP system takes over the traffic management.

The BIG-IP HA cluster that you create with this process is a single failover group that uses the default traffic group and automatic sync. For a complete discussion of the significance of these details, refer to the *BIG-IP® Device Service Clustering: Administration* guide, which is available on <http://support.f5.com/kb/en-us.html>.

Prepare the BIG-IQ devices for NSX integration

To begin the process of preparing the BIG-IQ® device for integration, you set up one or more BIG-IQ devices, create an NSX call back user, and a new server image, and then create an NSX connector.

Configuring a high availability configuration

You must perform basic system setup and activate a license on two or more BIG-IQ® systems before you can configure a high availability cluster.

Configuring BIG-IQ® Cloud as part of a high availability (HA) cluster ensures that you do not lose management capability of the BIG-IP® devices in your network because one BIG-IQ Cloud system fails.

Important: Do not confuse the BIG-IQ HA cluster you create in this process with a BIG-IP device cluster. Although the concept is similar, this process creates a cluster of BIG-IQ devices. BIG-IP HA cluster configuration is a separate process.

Note: Configuring an HA cluster is an optional task in this process.

If you have a primary BIG-IQ system (it can either be brand new, or one that you have been using for a while), and you want to add one or more new BIG-IQ Cloud systems as backup, you simply add the new systems to the primary system's `cm-cloud-all-big-iqs` group.

Important: To synchronize properly, the BIG-IQ systems must be running the same version of software. The exact configuration in terms of hardware is not required; however, the systems should have comparable resources. This is required because, in the event of a fail over, the peer must be able to maintain the process requirements for both systems. This is especially important in terms of disk space and data collection.

Important: The device that you add as an HA peer must be in an unconfigured state. That is, you should complete only the basic setup tasks. Specifying configuration details beyond those covered in the licensing and initial configuration process is likely to complicate the synching process.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. In System, hover over the BIG-IQ Systems header, and click the + icon when it appears. The New Device screen opens.
3. In the **IP Address** field, type the BIG-IQ System's self IP address.
4. In the **User name** and **Password** fields, type the administrative user name and password for the system.
5. For the **Group** setting, select **HA Peer Group**.
6. Click the **Add** button to add this device to this high availability cluster.

The system discovers its peer and displays its status.

If discovery of the newly configured BIG-IQ system fails, a **Delete** button displays. Verify the correct self IP address and credentials. Then click the **Delete** button to remove the incorrect information, and re-type the self IP address, user name, and password.

About activating a pool license

When you integrate with VMware NSX to create BIG-IP® VE virtual machines, you can activate a pool license so that BIG-IQ® software can use a license from that pool to license the BIG-IP VE systems that it creates.

You can choose not to use a pool license and skip to discovering devices. If you make this choice, the BIG-IQ device still creates BIG-IP VE systems, but you need to license them before they can be used.

You initiate the license activation process with a base registration key. The *base registration key* is a character string that the license server uses to verify the functionality that you are entitled to license. If the system has access to the internet, you select an option to automatically contact the F5 license server and activate the license. If the system is not connected to the internet, you must manually retrieve the activation key from a system that is connected to the internet, and then transfer it to the BIG-IQ system.

Note: If you do not have a base registration key, contact your F5 Networks sales representative.

Automatically activating a pool license

You must have a base registration key before you can activate the license pool.

If the resources you are licensing are connected to the public internet, you can automatically activate the license pool.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. Hover over the Licenses header, and click the + icon when it appears. The New License screen opens.
3. In the **License Name** field, type the name you want to use to identify this license.

4. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
5. In the **Add-on Keys** field, paste any additional license key you have.
6. For the **Activation Method** setting, select **Automatic**.
The End User Software License Agreement (EULA) displays.
7. To accept, click the **Accept** button.
The system reads your license key and adds the activated license to the License panel.

Manually activating a pool license

You must have a base registration key before you can activate the pool license.

If the BIG-IQ® Device you are licensing is not connected to the public internet, you can activate the pool license manually.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. Hover over the Licenses header, and click the + icon when it appears.
The New License screen opens.
3. In the **License Name** field, type the name you want to use to identify this license.
4. In the **Base Registration Key** field, type or paste the BIG-IQ registration key.
5. In the **Add-on Keys** field, paste any additional license key you have.
6. For the **Activation Method** setting, select **Manual** and click the **Get Dossier** button.
The BIG-IQ system refreshes and displays the dossier in the **Device Dossier** field.
7. Copy the text displayed in the **Device Dossier** field, and click the **Access F5 manual activation web portal** link.
Alternatively, you can navigate to the F5 license activation portal at <https://activate.f5.com/license/>.
8. Click **Activate License**.
The Activate F5 Product page opens.
9. Paste the dossier into the **Enter your dossier** field, and then click the **Next** button.
After a pause, the license key text displays.
10. Copy the license key.
11. On BIG-IQ Device, into the **License Text** field, paste the license key.
12. Click the **Activate** button.

If the license does not display as activated in the Licenses panel after several minutes, click the arrow next to the license to contract the list, then click it again to expand. The screen should refresh and display the license as activated.

Creating an NSX callback user

You need to create a user credential that the BIG-IQ® system can use to communicate with the VMware NSX system.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. Hover over the User header, and click the + icon when it appears.
The New User screen opens, displaying property fields for the new user.
3. In the **Username** field, type the name of the user account that VMware NSX will use when it interacts with the BIG-IQ system.
The entry can contain a combination of letters, numbers, periods, and hyphens.


Note: You need to recall this name when you configure the NSX.

4. From the **Auth Provider** list, select **Local**.
5. In the **Full Name** field, type a (human friendly) name to identify the NSX account.
The full name can contain a combination of symbols, letters, numbers and spaces.
6. In the **Password** and **Confirm Password** fields, type the password for the callback user account.
7. Click the **Add** button.

Creating a new server image

Before you create a new server image, you must know the accessible location of an F5 BIG-IP® VE installation file. The accessible location must be either an HTTP URL, or a VCenter datastore. These installation files use the .ovf file extension.

When VMware NSX creates a new server as part of the BIG-IQ® Cloud and VMware NSX integration, it uses the server image file you specify as the template.

1. In the BIG-IQ Cloud system Connectors panel, hover over the connector you created previously, click the gear icon () , and then select **Properties**.
The properties screen for that connector opens.
2. Scroll down to Server Images, and click **New**.
The New Server Image screen opens.
3. In the **Machine Image Name** field, type a name for the server image.
It is helpful if the image name identifies the version of the BIG-IP software you are using.
4. In the **OVF URL** field, specify the accessible location of an F5 BIG-IP VE installation file.
5. Click the **Save** button.

Creating a connection between BIG-IQ Cloud and NSX Manager

To enable integration between a third-party cloud provider and BIG-IQ® Cloud, you must configure a cloud connector. A *cloud connector* is a resource that identifies the local or virtual environment in which a tenant deploys applications and, when necessary, adds parameters required by third-party cloud providers.

For VMware NSX version 6.2 and later, BIG-IQ Cloud also helps you manage VMware resources required to run applications. Management tasks include discovering, creating, starting, and stopping VMware NSX application servers running in the private cloud. You can use this feature to accommodate seasonal traffic fluctuations by periodically adding and retracting devices and application servers as needed. Additionally, you can also provide tenants access to self-deployable iApps® through VMware integration.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.
2. Hover over the Connectors header, and click the + icon when it appears.
The New Connector screen opens.
3. In the **Name** and **Description** fields, type a name and description.
You can use the name and description to help you organize network resources into logical groups based on certain criteria, such as the location or application.

Important: You will need to recall the name you assign to this connector so that you can select it when you are configuring the VMware user interface. The name you specify is used as the service definition name in the VMware user interface.

4. From the **Cloud Provider** list, select **VMware NSX**.
The screen displays additional settings specific to VMware NSX.

5. From the **Devices** list, select the device you want to associate with this connector.
Most likely, the device you select will be the one you just added for use with this connector.
6. In the **VMware NSX Address** field, type the IP address of the VMware system.
The VMware IP address must be fully accessible from the BIG-IQ device.
7. In the **VMware NSX User Name** and **VMware NSX Password** fields, type the credentials that the BIG-IQ device will use to authenticate to the NSX Manager.
8. In the **VMware vCenter Server Address** field, type the IP address of the vCenter server.
9. In the **VMware vCenter Server User Name** and **VMware vCenter Server Password** fields, type the credentials that the BIG-IQ device will use to authenticate to vCenter.
10. In the Device Provisioning area, from the **Time Zone** list, select your local time zone.
11. In the **NTP Servers** fields, type the IP addresses of your Network Time Protocol (NTP) servers.
12. In the **DNS Servers** field, type the IP address of your DNS server.
13. In the **DNS Suffix(s)** field, type the name of your search domain.
The DNS search domain list allows the BIG-IQ system to search for local domain lookups to resolve local host names.
14. In the Callback Settings area, from the **BIG-IQ Callback User Name** list, select the user name that NSX Manager uses to authenticate to the BIG-IQ system.

Note: Select the user name you specified when you created an NSX callback user.

15. In the **BIG-IQ Callback Password** field, type the password that NSX Manager uses to authenticate to the BIG-IQ REST system.

Note: Specify the password you used when you created an NSX callback user.

16. From the **BIG-IQ Callback Address** list, select the IP address that this NSX Manager uses to access each BIG-IQ device in the HA cluster.
By default, the management IP address is used, but you can specify a self IP address if you choose.
17. From the **Licensing** list, select the name of the license pool that you created for the NSX integration.
18. Click the **Save** button.

As part of the connection creation process, the BIG-IQ system does the following:

- Creates a new default tenant for the new connector.
- Verifies connectivity to the NSX Manager and vCenter APIs, and registers the BIG-IQ system as an NSX Partner Service provider.
- Creates a callback user role that enables NSX to access the BIG-IQ software resources necessary for interaction with the BIG-IQ REST API.

Prepare VMware NSX for integration

After you finish preparing the BIG-IQ[®] device for integration, there are a couple of tasks to perform in the VMware NSX environment to complete the integration. You need to create an NSX Edge Service Gateway and enable a load balancing service for it.

Creating an NSX Edge Services Gateway

The NSX Edge Service Gateway establishes the network within which network services such as firewall, NAT, and load balancing are deployed. To integrate a BIG-IP® device with NSX, you must create at least one Edge Service Gateway.

Important: You perform the following task using the vSphere Web Client user interface. At time of release, these steps accurately describe the VMware user interface. For the most current instructions for performing these steps, refer to the VMware web site <http://pubs.vmware.com/>.

In the vSphere web client user interface, create a new NSX Edge.

Important: When you are configuring the Edge Services Gateway, make sure to observe the following:

- Choose to create the gateway in undeployed mode.
 - If you are configuring an HA cluster of BIG-IP virtual machines, select **Enable High Availability**, otherwise leave it cleared.
 - Choose the **X-Large** Appliance size.
 - Make sure that the NSX Edge you create identifies the Cluster/Resource Pool and the Datastore, but does not identify any interfaces. Otherwise, follow your standard practice for NSX Edge creation.
-

When you finish editing an Edge, it appears in the list under NSX Edges.

Enabling a service for the Edge

You must provision IP pools and port groups before you enable an Edge load balancer.

If you are configuring an HA cluster of BIG-IP® virtual machines for two-arm deployments, you need to configure four vnics (1 for management, 2 for data, and 1 for HA). For one-arm deployments, you need three vnics (management, data, and HA). If you are not using HA, you can use one less vnic in each case.

The NSX Edge Service Gateway establishes the network within which network services such as firewall, NAT, and load balancing are deployed. To integrate a BIG-IP® device with NSX, you must create at least one Edge Service Gateway.

Important: You perform the following step using the vSphere Web Client user interface. At time of release, these steps accurately describe the VMware user interface. For the most current instructions for performing these steps, refer to the VMware web site <http://pubs.vmware.com/>.

1. In the vSphere web client user interface, select the NSX Edge you just created.
2. On the **Manage** tab for the selected Edge, select the **Load Balancer** tab and click **Edit**.
The Edit Load balancer global configuration screen opens.
3. Select **Enable Load Balancer** and **Enable Service Insertion**.
Additional options are enabled, so that you can specify additional details.
4. For the **Service Definition**, select the BIG-IQ connector that you created previously.
5. For the **Service Configuration**, select **F5 ADC-Provision dedicated BIG-IP VE(s)**.
6. For the Deployment Specification, select the BIG-IP system server image you created previously.
7. Specify the configuration details for the Runtime NICs that you expect NSX to use as load balancers.

***Note:** The connectivity types you specify depend on whether you are configuring an HA cluster. For HA, you configure 1 management Vnic, 1 HA Vnic, and 1 or 2 data Vnics. For standalone, you configure 1 management Vnic and 1 - 3 data Vnics.*

a) Configure **vnic0**.

- For the **Connected To** setting, use the management port group you created as a prerequisite.
- For **Connectivity type**, use **Management**.
- For the **Primary IP Allocation Mode**, use **IP Pool**.
- For the **IP Pool**, use the management pool you created as a prerequisite.

b) Configure **vnic1**.

- For the **Connected To** setting, use the external port group you created as a prerequisite.
- For **Connectivity type**, use **Data**.
- For the **Primary IP Allocation Mode**, use **IP Pool**.
- For the **IP Pool**, use the external pool you created as a prerequisite.

c) Configure **vnic2**.

- For the **Connected To**, use the internal port group you created as a prerequisite.
- For the **Connectivity type**, use **Data**.
- For the **Primary IP Allocation Mode**, use **IP Pool**.
- For the **IP Pool**, use the internal pool you created as a prerequisite.

d) Configure **vnic3**.

- For the **Connected To** setting, use the HA port group you created as a prerequisite.
- For **Connectivity type**, use **HA** if you are configuring an HA cluster of BIG-IP virtual machines, otherwise use **Data**.
- For the **Primary IP Allocation Mode**, use **IP Pool**.
- For the **IP Pool**, use the HA pool you created as a prerequisite.

8. On the Edit Load balancer global configuration screen, select the **Typped Attributes** tab.

9. For the **Fully qualified host name of BIG-IP VE?** value, type a host name for the BIG-IP VEs that the NSX Edge will create.

The NSX Edge creates two new runtimes. These runtimes create BIG-IP virtual machines based on the specifications you provided. These virtual machines will be managed by the BIG-IQ® as an HA Cluster.

Prepare the new BIG-IP devices for integration

After the VMware NSX integration creates the BIG-IP® virtual devices, there are a couple of tasks to perform on the BIG-IP device environment to complete the integration. If the devices are configured in an HA cluster, you only perform these tasks on one device, after which the configuration is replicated on the other cluster members using Config sync.

Uploading a custom iApp to the BIG-IP device



After the NSX integration creates the BIG-IP® virtual edition instances, you may want to upload a custom iApp that more closely matches your application requirements.

1. Log in to BIG-IQ® Cloud with the administrator user name and password.

2. Download the iApp template.

This iApp template is available at

https://raw.githubusercontent.com/04hiteshPatel/appsvcs_integration_iapp/release/v1.0_001/appsvcs_integration_v1.0_003_001.tpl

3. On the Servers panel, hover over one of the BIG-IP VE servers created by the NSX integration, click the gear icon () , and then select **Properties**.
The Properties screen for the selected server opens.
4. Next to **Management Password**, click **Show**.
The screen displays the Management Password generated by the NSX integration process when it created the BIG-IP VE.
5. Copy the password to your clipboard and then click **Cancel** to close the screen.
6. On the Devices panel, click the gear icon () , and then select **Properties**.
The Properties screen for the selected device opens.
7. Next to **Address**, click the link that displays the IP address of the BIG-IP device.
The login screen for the device opens.
8. For the **Username**, type `Admin`; then, for the **Password** paste in the password copied to the clipboard in the step 4, and then click **Log in**.
9. On the BIG-IP device Main tab, click **iApps > Templates** and then click **Import**.
The Import File screen opens.
10. Click **Choose File** and then navigate to the iApp template and click **Open**.
11. Click **Upload**.
The iApp template is added to the list of installed templates. In about 60 seconds, it is imported to the managing BIG-IQ®. From there it is automatically imported to the NSX service.

Creating a customized application template

Before you can customize the application template for the NSX integration, you must upload the template to the managed device and then wait for it to be exported to the managing BIG-IQ® device.

An *iApp* is an application template located on F5 devices. When you discover an F5 device, all iApps® templates installed on that device are imported to the BIG-IQ® system. You can customize iApp templates, specifying which parameters are displayed, and which are tenant-editable. Once deployed, these parameters are available in the NSX user interface.

Note: Once you customize and save an application as a catalog entry, you cannot modify it.

Important: To modify an iApp on the BIG-IP® device, you must save it with a new name. Once an iApp has been imported to a managing BIG-IQ device, it is not imported again. When an iApp with a new name is saved on a managed BIG-IQ device, BIG-IQ software imports it automatically.

1. Hover over the Catalog header and click the + icon when it appears.
The New Template screen opens and displays the application template properties.
2. In the **Name** field, type a name for this new template.
3. For the **Input Parameters** setting, select the option that displays the parameters you want to work with.
The setting you choose here determines which parameters, from the base template that you select, display in subsequent fields and areas on the screen.
 - Select **Accept Defaults** if you do not want to edit any parameters.
 - Select **Common Options** if you only want to edit a subset of the template parameters. This option displays parameters that:
 - are marked as tenant-editable

- that describe the virtual server or pool
 - Select **All Options** to view all of the parameters for the template you select. You can then expand individual template sections, or click **Expand All** to view every parameter in every section.
4. For the **Cloud Connector** setting, select **All Connectors**.
 5. From the **Application Type** list, select the base template that contains the parameters that provide the network settings and levels of services that you want to have available in your NSX environment.
 6. Expand sections as necessary and then specify parameter values as needed. You can provide default values in that column, and select which parameters the user can revise.

Important: You cannot specify pool member settings (other than the IP address) for the BIG-IP device using the NSX interface. Instead, select **Common Options**, and specify the pool member settings as default values.

Tip: The template options that you can view depend on which option you chose in step 3.

Important: There are two parameters that you must select as tenant editable: the parameter that identifies the pool address, and the parameter that defines the pool member table. You can specify default values and allow user revision for as many parameters as you want. The names of these two parameters vary from one template to the next.

7. Click the **Save** button.

You can now use this connector to complete the NSX integration.

Complete the NSX integration

After you finish preparing the BIG-IP® devices for integration, there are a couple of tasks to perform in the BIG-IP device environment to complete the integration. Because the devices are configured in an HA cluster, you only perform these tasks on one device, after which the configuration is replicated on the other cluster members using Config sync.

Configuring a pool of virtual machines to handle data plane traffic

Before you can create a pool of virtual machines, you must allow NSX integration to create the virtual machines. You also must create and configure the web servers for which the virtual machines will manage traffic.

The web server pool services the data plane traffic generated by your applications.

Use the VMware NSX user interface to create a web server pool.

Populate the pool using the previously created web servers.

Note: This task is performed entirely within the VMware NSX user interface. Refer to the appropriate VMware documentation for details on how to create a web server pool.

Configuring the NSX virtual server

The virtual server you create here resides on the BIG-IP® virtual machine created by the NSX integration.

1. Use the VMware NSX user interface to create a new virtual server.

***Note:** This task is performed entirely within the VMware NSX user interface. Refer to the appropriate VMware documentation for details on how to create a web server pool.*

2. On the New Virtual Server General tab, from the **Application Profile** list, choose the name of the custom application template you created on the BIG-IQ system .
The settings that can be specified on the Advanced tab are now determined by the parameters marked Tenant Editable in the application template.
3. For the **IP Address**, click **IP Pool**, and then select the external pool you created earlier to handle data plane traffic.
4. In the **Name** field, specify a name to identify this virtual server.
5. From the **Default Pool** list, select the just-created web server pool.
6. If you want to revise any of the tenant editable values, click the **Advanced** tab and make your changes.
7. Click **OK** to finish creating the new virtual server
VMware NSX creates the new server.

The new server status is indicated by the Service Profile Status. If the status is other than `In Service`, you can get more information under Detailed Status, or even more information by viewing the new server on the BIG-IQ® device.

Cloud Tenant Management

About creating cloud tenants

As a cloud administrator, you create tenants and allocate resources to them in the form of iApps® application templates. Tenants can then self-deploy the customized application templates to easily define network and application services for several devices, without requiring them to perform complicated networking procedures.

The process of providing resources for a tenant includes these tasks:

- Create a tenant - When you create a tenant, BIG-IQ® Cloud creates a unique role for the tenant and populates it in the Role panel.
- Create a user - When you create a user account, you assign a user name and a password.
- Associate a user with a tenant's role - You associate a user with a tenant to provide that user access to pre-defined cloud resources in the form of self-service customized applications. You can associate multiple users with a single tenant for access to specific resources.

Creating a tenant

You create a tenant to provide access to customized cloud resources and applications.

1. Hover over the Tenants header, and click the + icon when it appears.
The panel expands to display property fields for the new tenant.
2. In the **Name** and **Description** fields, type a name and an optional description for this tenant.
The name can consist of a combination of numbers and symbols, but cannot contain any spaces.
3. From the **Available Connectors** list, select the connector associated with the resources that you are going to provide to this tenant.
To add another connector, click the plus (+) sign and select a connector from the additional **Available Connectors** list.
4. In the **Address**, **Phone**, and **Email** fields, type optional contact information for this tenant.
5. Click the **Save** button.

You can now associate a user with this tenant to provide access to applications and services.

Creating a cloud user

When you create a cloud user you provide that individual with access to specific resources.

1. Hover over the User header, and click the + icon when it appears.
The panel expands to display property fields for the new user.

2. In the **Full Name** field, type a name to identify this user.
The full name can contain a combination of symbols, letters, numbers and spaces.
3. In the **Password** and **Confirm Password** fields, type the password for the new user.
4. Click the **Add** button.

You can now associate this user with an existing tenant to provide access to pre-defined cloud resources.

Associating a user with a tenant's role

Before you associate a user with a tenant's role, you must first create the tenant. You can associate multiple users with a tenant's role.

Attention: *The BIG-IQ system administrator creates roles from the **BIG-IQ System** > **Access Control** menu. For more information, refer to the **BIG-IQ® System: Licensing and Initial Configuration** guide.*

You associate user with a tenant's role to provide that user specific access to cloud resources in the form of self-service applications.

In the Users panel, click the user name that you want to associate with a role and drag and drop it onto that role, in the Roles panel.

This user now has access to all of the resources defined for the associated role.

Glossary

BIG-IQ Cloud terminology

Before you manage cloud resources, it is important that you understand some common terms as they are defined within the context of the BIG-IQ® Cloud.

Term	Definition
<i>application templates</i>	An application template is a collection of parameters (in the form of F5 iApps® templates) that a cloud administrator defines to create a customized configuration for tenants. Cloud administrators add the configured application to a catalog from which a tenant can self-deploy it.
<i>BIG-IQ Cloud</i>	The BIG-IQ® Cloud system is a tool that streamlines management and access for tenants to services and applications hosted by local and/or cloud-based servers.
<i>cloud administrator</i>	Cloud administrators create application templates for tenants to centrally manage access to specific web-based applications and resources. Cloud administrators might also be referred to as cloud providers.
<i>cloud bursting</i>	Cloud bursting is a seamless way to manage an anticipated increase in application traffic by directing some traffic to another cloud resource. When demand falls back into normal parameters, traffic can be directed back to the original cloud resource. This elasticity enables efficient management of resources during periods of increased or decreased traffic to applications.
<i>cloud connector</i>	A cloud connector is a resource that identifies the local or virtual environment in which a tenant deploys applications and, when necessary, adds parameters required by third-party cloud providers.
<i>resources</i>	A resource is any managed object, including devices, web applications, virtual servers, servers, cloud connectors, and so forth.
<i>roles</i>	A role defines specific privileges to which you can associate one or more users. There are two default roles for BIG-IQ Cloud: cloud administrator and cloud tenant.
<i>tenant</i>	A tenant is an entity that can consist of one or more users accessing resources provided by a cloud administrator.

Term	Definition
<i>user</i>	A user is an individual who has been granted access to specific tenant resources.

Index

A

- active-active pair
 - configuring for the BIG-IQ system 24
- admin, *See* administrator
- Administrator role
 - defined 14
- administrator user
 - and default password 13
 - changing password for 11, 13
- administrator user password
 - changing 11, 13
- application catalog 31
- applications
 - customizing for tenants 31
- application templates
 - defined 37
 - using 31
- authorization checks
 - for secure communication 7

B

- base registration key
 - about 10
- BIG-IQ Cloud
 - about 7
 - defined 37
- BIG-IQ device
 - about preparation for NSX integration 24
 - configuring for VMware NSX integration 24
- BIG-IQ system
 - about activating 9
 - about licensing 9

C

- callback user
 - adding an NSX 26
- catalog
 - for applications 31
- cloud administrator
 - defined 37
- cloud bursting
 - defined 37
- cloud connector
 - defined 37
 - for VMware NSX 27
- cloud resources
 - providing for tenants 35
- cloud tenants
 - about creating 35
 - adding 35
- communication
 - between BIG-IQ and managed devices 7
- configuration
 - and initial setup 9–10

- configuring BIG-IP devices
 - about 30
- custom iApp
 - uploading 30

D

- data plane traffic
 - configuring a pool of virtual machines for 32
- device clusters
 - about 28
- device discovery
 - by scanning network 17
- device inventory
 - about 17
- device management
 - about 17
- devices
 - about discovering 17
 - adding 17
 - discovering VMware devices 23
- discovery address
 - defined 9
- DNS server
 - specifying for the BIG-IQ system 11
- documentation, finding 7
- dossier
 - providing 9–10

E

- Edge Services Gateway
 - creating for NSX 29
 - enabling for NSX 29

G

- glossary 37
- guides, finding 7

H

- high availability
 - configuring 24
- HTTPS port 443
 - required for communication 7

I

- initial configuration
 - for BIG-IQ system 9
- integration
 - about preparation of BIG-IQ devices for NSX 24
 - of BIG-IQ device and VMware NSX 24
- IP addresses
 - for managed devices 17

L

- license
 - activating automatically 9
 - activating manually 10
 - manually activate a pool license 19, 26
- license activation
 - for BIG-IQ system 9–10
- licenses
 - about managing for devices 19
 - about pool licenses 19
 - for pools 21
 - revoking for managed device 21
- licensing
 - activating pool license automatically 19, 25
 - activating pool license manually 19, 26
 - for managed devices 19
 - for pool license 19, 25
 - for pools for BIG-IP devices 21
- licensing process
 - for managed devices 25

M

- managed devices
 - about discovering 17
- manual activation
 - for pool license 19, 26
- manuals, finding 7

N

- network
 - incorporating BIG-IQ systems 9
- network configuration
 - and requirements for using VMware 23
- network configurationsiApps
 - customizing for tenants 31
- network security
 - about 7
- NSX callback user
 - adding 26
- NSX Edge Services Gateway
 - creating 29
 - enabling a service for 29
- NSX integration
 - about completion 32
- NSX virtual server
 - configuring 32

O

- offering licenses
 - activating for a license 20

P

- Pacific Standard Time zone
 - as default for the BIG-IQ system 11
- password
 - changing for administrator user 11, 13

- pool license
 - about activating 25
 - activating automatically 19, 25
 - activating manually 19, 26
 - revoking for a BIG-IP device 21
- pool licenses
 - about 19
 - assigning to a BIG-IP device 21
- port 22
 - using 8
- port 443
 - required for communication 7
 - using 8
- ports
 - required for communication with BIG-IQ 7
 - required open 8
- pre-defined users
 - and administrator role 13
 - and root role 13
- PST zone, See Pacific Standard Time zone

R

- release notes, finding 7
- resources
 - defined 37
 - providing access for user 36
- roles
 - associating with users and user groups 15
 - defined 13
 - for users 13–14
- root user
 - and default password 13

S

- security
 - for communication 7
- server image
 - creating 27
- system user
 - adding 14

T

- TCP port 22
 - using 8
- TCP port 443
 - using 8
- tenant
 - adding 35
- Tenant role
 - defined 14
- tenants
 - about creating 35
 - associating with a user 36
 - creating applications for 31
- tenants users
 - and tenants 35
 - and users 35
- terminology 37

- terms
 - defined [37](#)
- time zone
 - and default for the BIG-IQ system [11](#)
 - changing for the BIG-IQ system [11](#)
 - specifying a DNS server for the BIG-IQ system [11](#)
- time zone default
 - for the BIG-IQ system [11](#)

U

- user groups
 - defined [13](#)
- user roles
 - about [14](#)
 - associating with users and user groups [15](#)
- users
 - adding [14](#), [26](#), [35](#)
 - associating with a tenant [36](#)
 - defined [13](#), [35](#)
 - removing role from [15](#)

- utility license
 - activating an offering license for [20](#)

V

- virtual machines
 - configuring a pool to handle data plane traffic [32](#)
- virtual server
 - configuring NSX [32](#)
- VMware
 - and network configuration requirements [23](#)
- VMware devices
 - discovering [23](#)
- VMware integration
 - configuring the BIG-IQ device [24](#)
- VMware NSX
 - integrating with BIG-IQ Cloud [27](#)
- VMware NSX integration
 - about preparation [24](#)

