F5® BIG-IQ® Centralized Management: Authentication, Roles, and User Management

Version 5.4

Table of Contents

Use my LDAP server to authenticate BIG-IQ users..... 5
Before integrating BIG-IQ with your LDAP server for authentication.....5
Set up BIG-IQ to use your LDAP server for user authentication..... 6
Add a BIG-IQ user authenticated by my RADIUS server and assign it a role.....7
Create an LDAP-authenticated user group..... 8

Use my RADIUS server to authenticate and authorize BIG-IQ users.....9
Before integrating BIG-IQ with your RADIUS server for authentication and authorization..... 9
Set up BIG-IQ to use my RADIUS server for user authentication.....9
Update BIG-IQ dictionary with vendor-specific RADIUS attributes..... 10
Add a user authenticated by my LDAP server and associate it with a role..... 10
Create a user group authorized by your RADIUS server..... 11

Use my TACACS+ server to authenticate and authorize BIG-IQ users..... 13
Before integrating BIG-IQ with your TACACS+ server for authentication and authorization..... 13
Set up BIG-IQ to use my TACACS+ server for user authentication..... 13
Add a TACAS+ authenticated user and associate it with a role..... 14
Create a TACACS+ authenticated user group..... 15

Limit a user's access to BIG-IP devices based on a their role 17
About built-in and custom roles.....17
Built-in roles/role types shipped with BIG-IQ.....17
Add a user and assign them a built-in role.....19
Custom roles based on job responsibilities.....20
Create a custom role type to give permissions to BIG-IP object types..... 21
Create a resource group and associate it with a role type..... 21
Add new custom role.....22
Add a user to a custom role..... 22

User roles in the Access configuration workflow.....25

Remove a BIG-IQ user from a role.....27

Synchronize new users and user groups with secondary BIG-IQ..... 29

Legal Notices..... 31
Legal notices.....31

Use my LDAP server to authenticate BIG-IQ users

F5® BIG-IQ® Centralized Management can verify user credentials against your company's LDAP server (LDAP server versions 2 and 3, and OpenLDAP directory, Apache Directory Server, and Active Directory). After you set up BIG-IQ to use your LDAP server, you can add users and user groups that authenticated by your LDAP server.

Before integrating BIG-IQ with your LDAP server for authentication

Before integrating LDAP authentication with the F5® BIG-IQ® Centralized Management system, you must complete these tasks.

Task	Notes	For my LDAP server
Use an LDAP browser to review the groups and users in your directory's structure and determine where they are located in the organizational units (OUs). Then, decide how you want to map those names.	There are two ways you can do this. The first option is to map users directly to their Distinguished Name (DN) in the directory with a user bind template in the form of `uid=<username>, ou=people, o=sevenSeas`. For example, you'd map John Smith's user name to his DN as `uid=<jsmith>, ou=people, o=sevenSeas` and he would log in as `jsmith` and would be correctly authenticated with his user name in the directory through his DN. The second option is to allow users to log in with names that do not map directly to their DN by specifying a `userSearchFilter` in the form of `(&(uid=%s))` when creating the provider. For example, if John Smith's DN is `cn=John Smith,ou=people,o=sevenSeas`, but you would like him to be able to log in with `jsmith`, specify a `userSearchFilter` in the form of `(&(jsmith=%s))`. If your directory does not allow anonymous binds, you must also specify a `bindUser` and `bindPassword` so that the BIG-IQ system can validate the user's credentials.	
Decide which groups in your directory to map with BIG-IQ groups.	If you configured a `bindUser` and `bindPassword` for users, the BIG-IQ system displays a list of groups from which to choose. If you haven't configured this for your users, you must know the DN for each group.	
Find out the DN where you can query or view for all users and groups.	This is the root bind DN for your directory, defined as `rootDN`, when you create a provider. The BIG-IQ system uses the root	

Task	Notes	For my LDAP server
	bind DN as a starting point when it searches for users and groups.	
Find the host IP address for the LDAP server.	The default port is 389, if not specified otherwise, or 636 if SSL is enabled.	

Set up BIG-IQ to use your LDAP server for user authentication

Before you can set up BIG-IQ to authenticate users against your LDAP server, you have to specify your LDAP server settings on F5® BIG-IQ® Centralized Management and perform all the tasks outlined in the section titled, *Before integrating BIG-IQ with your LDAP server*.

You can configure BIG-IQ to use one or more of your company's LDAP server(s) to authenticate users.

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Auth Providers**.
3. Click the **Add** button.
4. From the **Provider Type** list, select **LDAP**.
5. In the **Name** field, type a name for this new provider.

   This must be a unique name, and can be a maximum of 152 characters.
6. In the **Host** field, type the IP address of your LDAP server.
7. For the **Servers** setting, type in the **Port** that your Active Directory server uses.

   If you want BIG-IQ to use an SSL port to communicate with your LDAP server, type port `636` , otherwise leave it at the default port, **389**.
8. To use an SSL port to communicate with the LDAP server, for the **SSL Enabled** setting, select the **Enabled** check box.
9. If your LDAP server does not allow anonymous binds, in the **Bind User** and **Bind User Password** fields, type the full distinguished names and passwords for users with query access.
10. In the **Root DN** field, type the root context that contains users and groups.

    The root context must be a full distinguished name.
11. For the **Authentication Method** setting, specify a method.
    - **Simple** - Select this option to require a user name and password for authentication.
    - **None** - Select this option to prompt the LDAP server to ignore the user name and password.

    Warning: *No password authentication is used if you select* ***None****.*
12. For the **Search Scope** setting, select an option to specify the depth at which searches are made.
13. In the **Search Filter** field, type the LDAP filter expression that determines how users are found.

    The search filter depends on your LDAP implementation.
14. In the **Connect Timeout** field, type the number of milliseconds after which the BIG-IP system stops trying to connect to the LDAP server.
15. In the **Read Timeout** field, type the number of seconds the BIG-IP system will wait for a response to a query.
16. In the **User Display Name Attribute** field, type the LDAP field to use for the name that BIG-IQ displays.

    When using Active Directory, this is typically `displayName`.
17. To direct bind to a distinguished name, in the **User Bind Template** field, type the name.

For example, `cn={username},ou=people,o=sevenSeas`.

Now, when a user logs in, BIG-IQ inserts the user name into the template in place of the token, and the resulting distinguished name is used to bind to the directory.

18. To prompt the LDAP provider to search for groups based on a specific display name attribute, in the **Group Display Name Attribute** field, type an attribute.

    This attribute is typically `cn`.

19. Leave the **Group Search Filter** at its default query to return all groups under the provided rootDN.

    Alternatively, if you have a large number of groups (more than 100), you can base the search on a specific term by typing a query with a `{searchterm}` token in this field.

    For example: `(&(objectCategory=group)(cn={searchterm}*))`

20. To specify a query for finding a users group, in the **Group Membership Filter** field, type a query string.

    Use the token `{userDN}` anywhere that the user's distinguished name should be supplied in the LDAP query.

    You can use a `{username}` token as a substitute for the user's login name in a query.

    Leave this setting at the default `(|(member={username})(uniqueMember={username}))` unless the provider is Active Directory.

21. To specify a query attribute for finding users in a particular group, in the **Group Membership User Attribute** field, type the attribute.

    When using Active Directory, use `memberof`. For example:
    `(memberOf=cn=group_name,ou=organizational_unit,dc=domain_component)`

    For other LDAP directories, use `groupMembershipFilter`. For example:
    `(groupMembership=cn=group_name,ou=organizational_unit,o=organization)`

22. Select the **Perform Test** check box to test this provider.
23. Click the **Save & Close** button at the bottom of the screen.

Add a BIG-IQ user authenticated by my RADIUS server and assign it a role

If you want to add a user authenticated against your RADIUS server, you first have to set up F5® BIG-IQ® Centralized Management with your RADIUS server settings.

Once you understand exactly who you want to perform certain tasks, you can provide them access to particular areas of BIG-IQ by adding them as a user user and assigning the appropriate standardized role. You can assign as many roles as required to cover the user's responsibilities.

Important: *You must associate this user with a RADIUS-authenticate role, or authentication will fail.*

---

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Users**.
3. Click the **Add** button.
4. From the **Auth Provider** list, select **RADIUS**.
5. In the **User Name** field, type the user name for this new user.
6. 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.

7. From the **Available** list, select each user role you want to associate it with this user, and move it to the **Selected** list.

Important: *Be sure to let your users know that their access to certain parts of the BIG-IQ user interface depends on which role they are assigned.*

8. Click the **Save & Close** button at the bottom of the screen.

Create an LDAP-authenticated user group

Before you can add an LDAP-authenticated user group, you must set up BIG-IQ® to use your company's LDAP server for user authentication (using the **USER MANAGEMENT** > **Auth Providers** screen).

You create a user group to offer a set of individual users authentication from the same LDAP server.

Important: *If a user does not belong to an LDAP-authenticated user group, authentication will fail.*

1. At the top of the screen, click **System**.
2. At the left, click **USER MANAGEMENT** > **User Groups**.
   The User Groups screen opens.
3. Click the **Add** button.
4. In the **Name** field, type a name for this new user group.
5. From the **Auth Provider** list, select **LDAP**.
6. In the **Remote Group** field, type a term to search for remote groups.
7. In the **Group DN** field, type the domain name for this group.
8. From the **User Roles** list, select the user role that has the privileges you want to grant to this user group.
9. Click the **Save & Close** button at the bottom of the screen.

Use my RADIUS server to authenticate and authorize BIG-IQ users

F5® BIG-IQ® Centralized Management can verify user credentials against your company's RADIUS server. After you set up BIG-IQ to use your RADIUS server, you can add users and user groups authorized by that server.

Before integrating BIG-IQ with your RADIUS server for authentication and authorization

Before you set up BIG-IQ® Centralized Management for authentication and authorization with your RADIUS server, gather the following information.

Required Information	This is	For my RADIUS server
Name	The name of your RADIUS server.	
Host	The IP address or host name of your RADIUS server.	
Port	The port number of your RADIUS server.	
Secret	The case-sensitive text string used to validate communication.	
Test user name and password	A user name and password, authenticated on your RADIUS server.	
Key and Value properties for your RADIUS server	The RADIUS server uses this for authentication and encryption.	

Set up BIG-IQ to use my RADIUS server for user authentication

Before you can set up authentication, you must have specified your DNS settings. You usually do this when you license F5® BIG-IQ® Centralized Management.

You can set up BIG-IQ to use your company's RADIUS server. You can add two additional backup RADIUS servers in case the primary server is not available for authentication.

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Auth Providers**.
3. Click the **Add** button.
4. From the **Provider Type** list, select **RADIUS.**
5. In the **Name** field, type a name for this new provider.

   This must be a unique name, and can be a maximum of 152 characters.
6. For the **Servers** setting, In the **Host** and **Port** fields, type the RADIUS server's IP address (or fully qualified domain name) and port number for each of the servers you want to configure.

The primary server is mandatory. A secondary server and tertiary server, which will be used if the primary or secondary servers fail, are optional.

7. In the **Secret** field, type the case-sensitive text string used to validate communication.
8. In the **Test User** and **Test Password** fields, type a user and password, then click the **Test** button to verify that BIG-IQ can reach the RADIUS server
9. Click the **Save & Close** button at the bottom of the screen.

You can now associate RADIUS server users and groups with BIG-IQ system roles.

Update BIG-IQ dictionary with vendor-specific RADIUS attributes

You must have root access to the BIG-IQ system's command line through SSH for this procedure.

Some RADIUS deployments include non-standard, vendor-specific attributes in the dictionary files. For these deployments, you must update the BIG-IQ system's default dictionary.

1. Copy the TinyRadius .jar file from the BIG-IQ system.
2. Extract the contents of the TinyRadius `.jar` file.
3. Update the file `org/tinyradius/dictionary/default_dictionary` file, by adding the vendor-specific attributes.
4. Repack the contents into a new `.jar` file.
5. Replace the old TinyRadius `.jar` on each BIG-IQ system with the new TinyRadius .jar file you created in step 4.

For example:

1. From a Linux machine, copy the TinyRadius `.jar` file to your BIG-IQ system by typing: `scp <big-iq-user>@<BIG-IQ-Address>:/usr/share/java/TinyRadius-1.0.jar ~/tmp/tinyrad-upgrade/`
2. Extract the file on your Linux Machine by typing: `jar -xvf TinyRadius-1.0.jar`
3. Edit the `org/tinyradius/dictionary/default_dictionary`, adding the vendor-specific attribute.

```
rm TinyRadius-1.0.jar
jar cvf TinyRadius-1.0.jar *
```

4. Update the jar on the BIG-IQ system by typing: `scp TinyRadius-1.0.jar <your_user>@<BIG-IQ address>:/var/tmp/`
5. SSH to the BIG-IQ system and type the following commands:

```
mount -o remount,rw /usr
cp /var/tmp/TinyRadius-1.0.jar /usr/share/java
mount -o remount,ro /usr
bigstart restart restjavad
```

6. Repeat steps 4 and 5 for each BIG-IQ in a HA configuration.

Now you can use the vendor-specific attributes RADIUS to create your user groups on BIG-IQ.

Add a user authenticated by my LDAP server and associate it with a role

If you want to add a user authenticated against your LDAP server, you first have to set up F5® BIG-IQ® Centralized Management with your LDAP server settings.

Once you understand exactly who you want to perform certain tasks, you can provide them access to particular areas of BIG-IQ by adding them as a user user and assigning the appropriate standardized role. You can assign as many roles as required to cover the user's responsibilities.

Important: *You must associate this user with a LDAP-authenticated role, or authentication will fail.*

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Users**.
3. Click the **Add** button.
4. From the **Auth Provider** list, select **LDAP**.
5. In the **User Name** field, type the user name for this new user.
6. 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.
7. In the **Password** and **Confirm Password** fields, type the password for this new locally-authenticated user.

   You can change the password any time.
8. From the **Available** list, select each user role you want to associate it with this user, and move it to the **Selected** list.

   Important: *Be sure to let your users know that their access to certain parts of the BIG-IQ user interface depends on which role they are assigned.*
9. From the **Available** list, select each user role you want to associate it with this user, and move it to the **Selected** list.

   Important: *Be sure to let your users know that their access to certain parts of the BIG-IQ user interface depends on which role they are assigned.*
10. Click the **Save & Close** button at the bottom of the screen.

Create a user group authorized by your RADIUS server

Before you can add a RADIUS-authenticated user group, you must set up BIG-IQ to use your company's RADIUS server for user authentication on the **USER MANAGEMENT** > **Auth Providers** screen

Create a user group to offer individual users the same privileges on F5® BIG-IQ® Centralized Management. This user group will be authorized by your RADIUS server.

Important: *If a user does not belong to a RADIUS-authenticated user group, authentication will fail.*

1. At the top of the screen, click **System**.
2. At the left, click **USER MANAGEMENT** > **User Groups**.
   The User Groups screen opens.
3. Click the **Add** button.
4. In the **Name** field, type a name for this new user group.
5. From the **Auth Provider** list, select **RADIUS**.
6. In the **Key** and **Value** fields, type the properties for your RADIUS server.
7. From the **User Roles** list, select the user role you want to associate with this user.

   You aren't required to associate a user role at this point; you can do that later. If you want to add another user role, click +.
8. Click the **Save & Close** button at the bottom of the screen.

You can now associate users with this user group.

Use my TACACS+ server to authenticate and authorize BIG-IQ users

F5® BIG-IQ® Centralized Management can verify user credentials against your company's TACACS+ server. After you set up BIG-IQ to use your TACACS+ server, you can add users and user groups that are authenticated by your TACACS+ server.

Before integrating BIG-IQ with your TACACS+ server for authentication and authorization

Before you set up BIG-IQ® Centralized Management for authentication and authorization with your TACACS+ server, you should gather this information.

Required Information	This is	For my TACACS+ server
Name	The name of your TACACS+ server.	
Host	The IP address or host name of your TACACS+ server.	
Port	The port number of your TACACS+ server.	
Secret	The case-sensitive text string used to validate communication.	
Primary Service	The service that the authorization requests are made for, such as system, shell, or connection.	
Protocol	An optional subset of a service, such as `telnet`, `ip`, or `http`.	
Test user name and password	A user name and password, authenticated on your TACACS+ server.	

Set up BIG-IQ to use my TACACS+ server for user authentication

Before you can set up authentication, you must have specified your DNS settings. You usually do this when you license F5® BIG-IQ® Centralized Management. You must also complete all the tasks outlined in *Before integrating BIG-IQ with your TACACS+ server*.

You can set up BIG-IQ to use your company's TACACS+ server for user authentication.

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Auth Providers**.
3. Click the **Add** button.
4. From the **Provider Type** list, select **TACACS+.**
5. For the **Servers** setting, in the **Host** and **Port** fields, type the TACACS+ server's IP address (or fully qualified domain name) and port number for each of the servers you want to configure.

   To add more servers, just click the + button.

6. In the **Name** field, type a name for this new provider.

   This must be a unique name, and can be a maximum of 152 characters.
7. In the **Primary Service** field, specify what type of authorization requests will be made for this service.

   For example: `system`, `connection`, or `PPP`.
8. In the **Protocol** field, specify an optional subset of a service.

   For example: `ip`, `telnet`, or `http`.
9. To encrypt the data, select the **Yes** check box for the **Encrypt** setting.
10. To verify that BIG-IQ can reach the TACACS+ server, in the **Test User** and **Test Password** fields, type a valid user name and password, and click the **Test** button.
11. Click the **Save & Close** button at the bottom of the screen.

You can now associate TACACS+ server users with BIG-IQ system roles.

Add a TACAS+ authenticated user and associate it with a role

You must set up F5® BIG-IQ® Centralized Management with your TACAS+ server settings before you can add a TACAS+ authenticated user.

Once you understand exactly who you want to perform certain tasks, you can provide them access to particular areas of BIG-IQ by adding them as a user and assigning the appropriate standardized role. You can assign as many roles as required to cover the user's responsibilities.

Important: *You must associate this user with a TACAS+ authenticated role, or authentication will fail.*

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Users**.
3. Click the **Add** button.
4. From the **Auth Provider**rlist, select **TACAS+**.
5. From the **Auth Provider** list, select **LDAP**.
6. In the **User Name** field, type the user name for this new user.
7. 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.
8. In the **Password** and **Confirm Password** fields, type the password for this new locally-authenticated user.

   You can change the password any time.
9. From the **Available** list, select each user role you want to associate it with this user, and move it to the **Selected** list.

   Important: *Be sure to let your users know that their access to certain parts of the BIG-IQ user interface depends on which role they are assigned.*
10. From the **Available** list, select each user role you want to associate it with this user, and move it to the **Selected** list.

    Important: *Be sure to let your users know that their access to certain parts of the BIG-IQ user interface depends on which role they are assigned.*
11. Click the **Save & Close** button at the bottom of the screen.

Create a TACACS+ authenticated user group

Before you can add a TACACS+ authenticated user group, you must set up BIG-IQ® to use your company's TACACS+ server for user authentication.

You can create a user group for multiple users to authenticate through a TACACS+ server.

Important: *If a user does not belong to a TACACS+ authenticated user group, authentication will fail.*

1. At the top of the screen, click **System**.
2. At the left, click **USER MANAGEMENT** > **User Groups**.
   The User Groups screen opens.
3. Click the **Add** button.
4. In the **Name** field, type a name for this new user group.
5. From the **Auth Provider** list, select **TACACS+**.
6. For the **Authorization Attributes** setting, in the **Attribute** and **Value** fields, type the attribute and value pair for this group's TACACS+ server.
7. From the **User Roles** list, select the user role that has the privileges you want to grant to this user group.
8. Click the **Save & Close** button at the bottom of the screen.

Limit a user's access to BIG-IP devices based on a their role

BIG-IQ® Centralized Management gives you the tools you need to customize user access to managed devices by letting you assign role-based access based on job responsibilities. When you associate a role with a user (or a group of users), they have access only to the areas within BIG-IQ that you explicitly grant.

The responsibilities and roles each of your users has probably depends on the number of people who have access to BIG-IQ.

Assigning more than one role to a user

For example, if you have only two people managing your devices from BIG-IQ, they both most likely need to have full access to all aspects of BIG-IQ at one time or another. For these users, you'd assign them both the Administrator role.

Assigning more granular/specialized privileges to a user

On the other hand, if you're working for a larger company that has specialized roles to manage different services, or different parts of services, you can provide more granular access.

For example, if you have two people who manage BIG-IP devices used only for network security purposes, you could assign them both the role of Network Security Manager. Or, if you have two people managing devices used for network security, but you want only one of them to write and edit policies, and the other to (only) deploy the policies, you could assign the first person the Network Security Editor role, and the other person the Network Security Deployer role. In this case, the person with the Network Security Editor role can only create, view, and edit policies, but not deploy them. The person assigned to the Network Security Deployer can view and deploy policies, but cannot create or edit them.

About built-in and custom roles

You can assign role-based user access one of two ways:

- Built-in user roles - BIG-IQ ships with several built-in user roles that correlate to common job responsibilities. This makes it easy for you to quickly assign users with permissions to access the BIG-IP objects they need to do their job.
- Custom user roles - allow you to grant access to users at a granular level in a way that fits your business needs. You can provide specific permissions to as many BIG-IP objects as needed, even across multiple services.

Built-in roles/role types shipped with BIG-IQ

As a system manager, you'll need a way to limit a user's access to certain areas of F5® BIG-IQ® Centralized Management and to its managed devices. The easiest way to do this is to base user access on the responsibilities, or role, the user has in your company. To help you do that, BIG-IQ ships with a set of built-in roles (associated with a role type) with certain privileges that you can assign to specific users. Since responsibilities and duties for certain roles are specialized, users assigned to some roles have access to only specific parts of BIG-IQ. These restrictions are outlined in the role description.

Role	This role can:
Administrator	Perform all tasks for setting up and maintaining BIG-IQ and managing devices. This includes discovering devices, adding individual users, assigning roles, installing updates, activating licenses, and so forth.
Access Auditor	Only view Access configuration objects and managed Access devices. This role cannot edit, discover, or deploy devices or policies.
Access Deployer	Deploy Access configuration objects. This role cannot discover and edit devices or policies.
Access Editor	View and edit Access configuration objects, including the ability to add, update, and delete pools and pool members from the Access configuration object editor. This role cannot discover or deploy devices or policies.
Access Manager	Deploy and edit Access configuration objects, and view the Access Reporting and dashboard. This role cannot add or remove devices and device groups, and cannot discover, import, or delete services.
Access Viewer	Only view Access configuration objects and discovered Access devices. This role cannot edit, discover, or deploy devices or policies.
Application Editor	View Local Traffic & Network objects and create, view, and modify applications via Service Catalog templates.
Device Manager	Perform all tasks for device management, including device discovery, licensing, software image management, and UCS backups.
Device Viewer	Only view aspects of device management including device discovery, licensing, software image management, and UCS backups.
DNS Viewer	Only view aspects of device management associated with DNS.
Fraud Protection Manager	Perform all tasks for managing the Fraud Protection Service functionality.
Fraud Protection Viewer	Only view Fraud Protection Service objects.
License Manager	Perform all tasks related to BIG-IP licensing.
Local Traffic & Network Deployer	View and deploy Local Traffic & Network configuration objects for managed Local Traffic & Network devices.
Local Traffic & Network Editor	Create, view, modify, and delete Local Traffic & Network configuration objects.
Local Traffic & Network Manager	Perform all tasks for managing Local Traffic & Network, including creating, viewing, modifying, and deleting Local Traffic & Network objects.
Local Traffic & Network Viewer	Only view Local Traffic & Network objects.
Network Security Deployer	View and deploy Network Security objects.
Network Security Editor	Create, view, modify, and delete Network Security objects.
Network Security Manager	Perform all tasks associated with Network Security, including areas involved in creating, viewing, modifying, and deleting shared and firewall-specific security objects.
Network Security Viewer	Only view Network Security firewall objects. This role cannot edit, discover, or deploy devices or policies.

Role	This role can:
Pool Member Operator	Enable, disable, or force offline pool members for all pools. To limit access to select pools, create a custom resource group and role based on the Pool Member Operator type.
Security Manager	Perform all tasks associated with Network Security, Web Application Security, and Fraud Protection Service, including areas involved in device discovery, creating, viewing, modifying, and deleting Web Application Security, shared and firewall-specific security objects.
Service Catalog Editor	View Local Traffic & Network objects and create, view, modify, and delete Service Catalog templates.
Service Catalog Viewer	Only view Local Traffic & Network objects and Service Catalog templates.
Trust Discovery Import	Manage device trust establishment, service discovery, service import, removal of services and removal of trust.
Virtual Server Operator	Enable or disable all virtual servers. To limit access to select virtual servers, create a custom resource and role based on the Virtual Server Operator role type.
Web App Security Deployer	View and deploy Web Application Security and shared security configuration objects for Web Application Security devices.
Web App Security Editor	Create, view, modify, and delete Web Application Security and shared security configuration objects.
Web App Security Manager	Create, view, modify, delete and deploy Web Application Security and shared security configuration objects.
Web App Security Viewer	Only view Web Application Security and shared security configuration objects.

Add a user and assign them a built-in role

If you want to authentication users with an LDAP, RADIUS, or TACAS+ server, you must first configure that before adding a user.

Once you understand exactly who you want to perform certain tasks, you can provide them access to particular areas of F5® BIG-IQ® Centralized Management by adding them as a user and assigning the appropriate standardized role. You can assign as many roles as required to cover the user's responsibilities.

Important: *Since some roles have access only to certain areas or screens in the BIG-IQ user interface, it's important to communicate that to the user. When you assign a role to a user, be sure you outline the responsibilities and restrictions for their role. Clarifying this helps avoid any potential confusion. Also note,these roles do not have access to the global search functionality: Network Security Manager, Network Security Edit, Network Security View, and Trust Discovery Import.*

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Users**.
3. Click the **Add** button.
4. From the **Auth Provider** list, select the authentication method you want to use for this user.

   Important: *A user must belong to a group or have an assigned role, or authentication will fail.*

5. In the **User Name** field, type the user name for this new user.
6. 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.
7. In the **Password** and **Confirm Password** fields, type the password for this new locally-authenticated user.

   You can change the password any time.
8. To associate this user with an existing user group, select the group from the **User Groups** list.

   You aren't required to associate a user group at this point; you can do that later if you want. If you want to associate another user group with this user, click +.
9. From the **Available** list, select each user role you want to associate it with this user, and move it to the **Selected** list.

   Important: *Be sure to let your users know that their access to certain parts of the BIG-IQ user interface depends on which role they are assigned.*
10. Click the **Save & Close** button at the bottom of the screen.

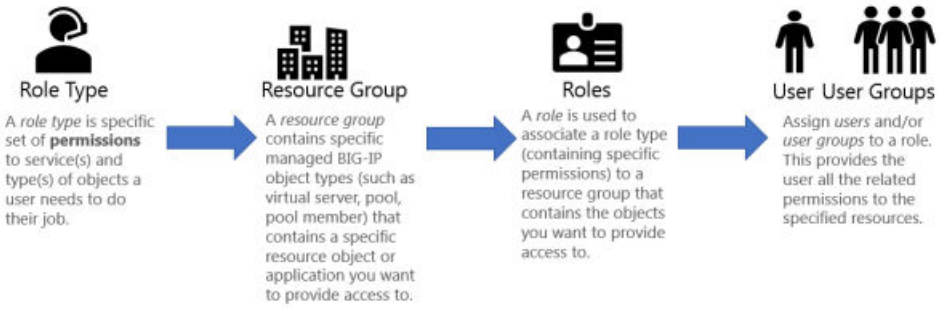
This user now has the privileges associated with the role(s) you selected and BIG-IQ will authenticate this user locally

You can now tell this user how their BIG-IQ access aligns with their responsibilities. Make sure they understand they might not see every screen you or one of their peers does. Also let them know that if they try to log in more than 5 times in 5 minutes with the wrong user name and/or password, they might get the following error: `Maximum number of login attempts exceeded.` If that happens, the user must wait 5 minutes before trying to log back in.

Note: *If your BIG-IQ is in an HA pair, you must synchronize this change by refreshing the secondary BIG-IQ.*

Custom roles based on job responsibilities

Here is an overview of the different concepts you need to understand when creating custom roles based on job responsibilities.



BIG-IQ® Centralized Management makes it easy for you to give users specific permissions for access only to those BIG-IP® objects they need to do their job. Role-based access allows you to create a custom role with specific privileges to view or edit only those BIG-IP objects (resources) you explicitly assign to the role.

There are several built-in roles shipped with BIG-IQ, but there might be a reason you want to give a person permissions to interact only in a clearly defined way with specific resources. To do that, you need to add each of the following to BIG-IQ:

1. **Custom role type** - Select a one or more services and define a set of permissions (read, add, edit, delete) for interacting with the objects associated with selected services.
2. **Custom resource group** - Select the specific type of resources you want to provide a user access to—for example, BIG-IP virtual servers.
3. **Custom role** - Associate this custom role with the custom role type and resource group you created, to combine the permissions you specified in the custom role type with the resources you defined for the custom resource group.
4. **Custom user** - Associate this user with the custom role you created to provide that person access and permissions to the resources you specified.

Create a custom role type to give permissions to BIG-IP object types

Creating a custom role type is the first step to providing custom role-based access to users.

1. At the top of the screen, click **System**.
2. On the left, click **ROLE MANAGEMENT** > **Custom Role Types**.
3. Near the top of the screen, click the **Add** button.
4. In the **Name** field, type a name to identify this new role type.

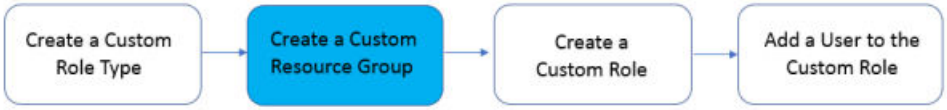
   A description is optional.
5. From the **Services** list, select each service you want to associate with this role type, then scroll through the **Object Type** list and select the check box next to each object type you want to provide access to.

   Important: *As you know, interactions and relationships between resource objects in your network can be complex. Because of that, it's best to leave all of these object types selected. This ensures you don't unintentionally limit this role type's ability to manage all of the objects they need to, for them to do their job.*

   ---
6. After you've finished adding objects types, for each object type, select the check box beneath the permissions you want to grant for this role type.
7. Click the **Save & Close** button at the bottom of the screen.

Create a resource group and associate it with a role type

Create a resource group with all of the BIG-IP objects you want to provide access to, and assign a role type to it.



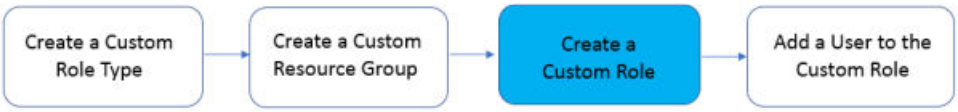
1. At the top of the screen, click **System**.
2. On the left, click **ROLE MANAGEMENT** > **Custom Resource Groups**.
3. Near the top of the screen, click the **Add** button.
4. In the **Name** field, type a name to identify this group of resources.
5. From the **Role Type** list, select the role type you want to provide access to for this group of resources.
6. From the **Select Service** list, select the service(s) you want to provide access to for this group of resources.

7. From the **Object Type** list, select the type of object you want to add to this group of resources.
8. For the **Source** setting:
   - **Selected Instances** - Select this option to put only the source objects you selected into this resource group. If you select this option, the associated role will not have access to any new objects of the same type added in the future unless you explicitly add it to this resource group.
   - **Any Instance** - Select this option if you want the associated role to have any instance of the specified object type, including future instances (newly configured objects of this type).
9. Select the check box next to the name of each object you want to add to this group of resources, and click the **Add Selected** button.
10. Click the **Save & Close** button.

Now you can associate this role type and resource group to a role.

Add new custom role

In addition to the built-in roles that ship with BIG-IQ, you can create a custom role with specific privileges to particular areas of BIG-IQ and BIG-IP devices.



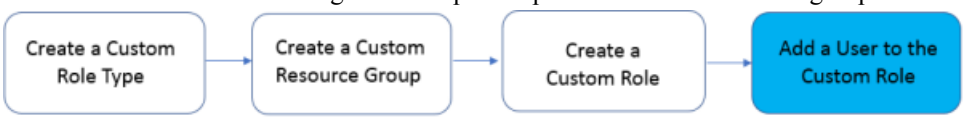
1. At the top of the screen, click **System**.
2. On the left, click **ROLE MANAGEMENT** > **Roles**.
3. Click the **Add** button.
4. In the **Name** field, type a name to identify this new role.
5. From the **Role Type** list, select the kind of role you want to add.

   You might have to resize the bottom half of the screen to see all of the following options.
6. For the **Role Mode** setting, select an option.
   - **Relaxed Mode** – If you select this option, the role can view and manage all objects you've given explicit permission to, and it can see (but won't be able to manage) related objects for associated services.
   - **Strict Mode** – If you select this option, this role can view and manage only the specific objects you've given explicit permission to.

   Tip: *It's a good idea to leave this in* ***Relaxed Mode*** *so you don't unintentionally limit an associated user's ability to see related objects.*
7. To view the type of user access granted for the resource groups associated with this role, click the **View Permissions** button.
8. Click the **Save & Close** button at the bottom of the screen.

Add a user to a custom role

Add a user to a custom role to give them specific permissions to a resource group.



1. On the left, click **USER MANAGEMENT** > **Users**.
2. Click the **Add** button.

3. From the **Auth Provider** list, select the authentication method you want to use for this user.

   Important: *A user must belong to a group or have an assigned role, or authentication will fail.*

4. In the **User Name** field, type the user name for this new user.
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 this new locally-authenticated user.

   You can change the password any time.
7. To associate this user with an existing user group, select the group from the **User Groups** list.

   You aren't required to associate a user group at this point; you can do that later if you want. If you want to associate another user group with this user, click +.
8. From the **Available** list, select each user role you want to associate it with this user, and move it to the **Selected** list.

   Important: *Be sure to let your users know that their access to certain parts of the BIG-IQ user interface depends on which role they are assigned.*

9. Click the **Close** button.

These users now have the privileges associated with the role(s) you selected.

User roles in the Access configuration workflow

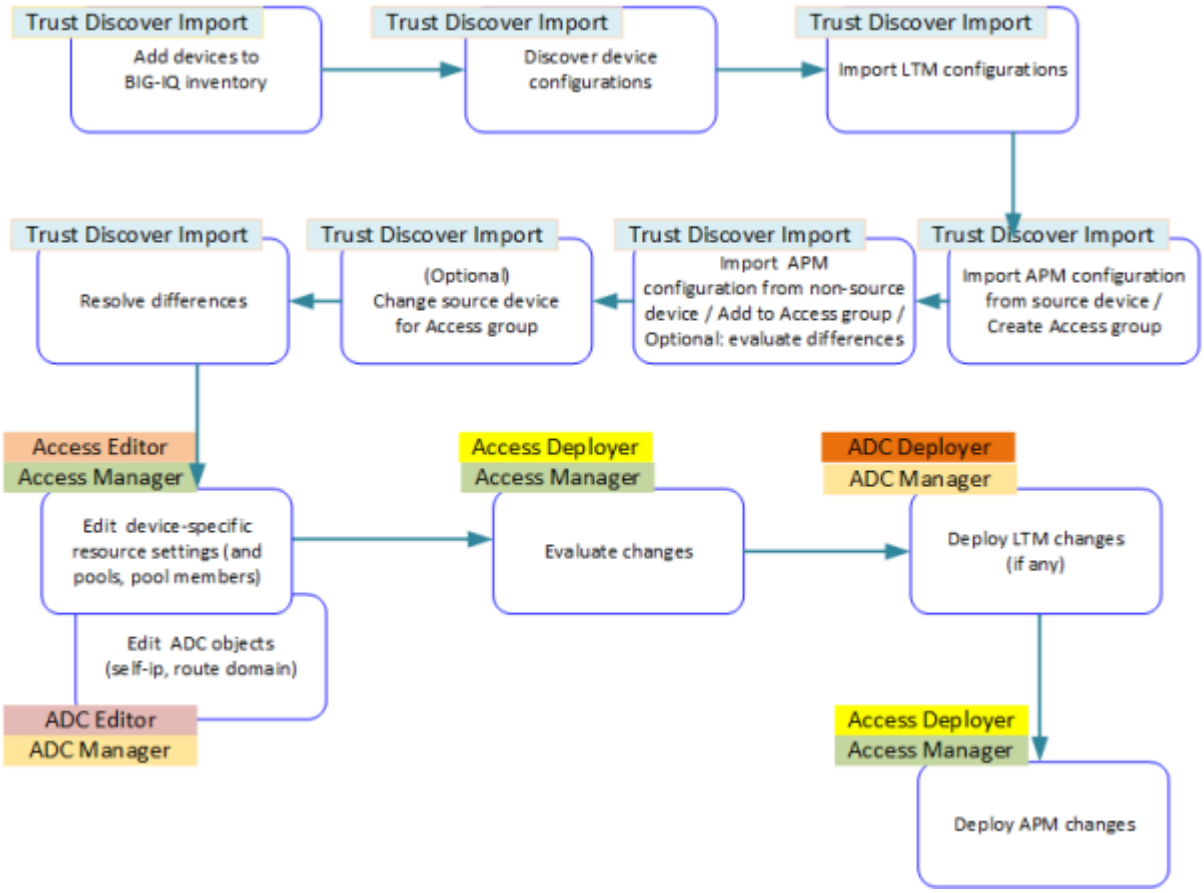


Figure 1: Access configuration workflow with possible user roles

---

Note: *This figure is only for roles that are built-in. You can modify the configuration to support the creation of custom roles.*

Remove a BIG-IQ user from a role

If a job or responsibilities change for an employee, you can use this procedure to disassociate that BIG-IQ user from an assigned role.

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Users**.
3. On the Users inventory list, click the name of the user.
   The screen refreshes to display the properties for this user.
4. From the **User Roles** list, select the user role to disassociate from this user and click the **X**.
   The selected user role is removed from the list of privileges assigned to this user.
5. Click the **Save & Close** button at the bottom of the screen.

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

Synchronize new users and user groups with secondary BIG-IQ

You must configure two BIG-IQ® Centralized Management systems in a high availability (HA) pair before you can synchronize users and user groups with a secondary BIG-IQ

Users and user groups are handled differently than other data that's synchronized between BIG-IQ® systems in an HA pair. For that reason, you must refresh the secondary BIG-IQ system in an HA pair after you add a new user or user group. Refresh the secondary BIG-IQ system so new users and user groups can successfully log in to the secondary system.

1. At the top of the screen, click **System**.
2. On the left, click **BIG-IQ HA**.
3. At the top of the screen, click the **BIG-IQ HA Settings** button.
4. Click the **Log Out and Refresh** button.
5. Click **OK**, then **Log Out**.
   BIG-IQ logs you out of the system.

You should now be able to log in to the secondary BIG-IQ system with the new user and/or user group you added.

Legal Notices

Legal notices

Publication Date

This document was published on December 29, 2017.

Publication Number

MAN-0685-00

Copyright

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

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*.

Link Controller Availability

This product is not currently available in the U.S.

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.

Index

A

Access Administrator role
    defined *17*
Access Auditor role
    defined *17*
Access Deployer role
    defined *17*
Access Editor role
    defined *17*
Access Manager role
    defined *17*
Access Viewer role
    defined *17*
Administrator role
    defined *17*
authenticate user
    using an LDAP server *5*
authentication
    about using my TACACS+ server for *13*
    configuring BIG-IQ to use LDAP *6*
    configuring with RADIUS *9*
    configuring with TACACS+ *13*
authentication of users
    using a RADIUS server *9*
authorization of users
    using a RADIUS server *9*

B

BIG-IP resources
    providing access to *21*
BIG-IQ users
    and authenticating with RADIUS *9*
    authenticating with LDAP *5*
    authenticating with TACACS+ server *13*
built-in roles
    shipped with BIG-IQ *17*

C

configuration workflow
    and Access user roles *25*
    and ADC user roles *25*
    and Trust Discover Import user role *25*
custom role types
    creating *21*
custom roles
    adding users *22*

D

Device Manager role
    defined *17*
Device Viewer role
    defined *17*
DNS Viewer role
DNS Viewer role *(continued)*
    defined *17*

F

Fraud Protection Manager role
    defined *17*
Fraud Protection Viewer role
    defined *17*

L

LDAP
    before authenticating users *5*
    configuring authentication *6*
    info to collect before integrating *5*
    prerequisite info for integration *5*
LDAP authentication
    configuring for new user *10*
    creating user groups *8*
LDAP server
    using to authenticate BIG-IQ users *5*
Local Traffic & Network Deployer role
    defined *17*
Local Traffic & Network Editor role
    defined *17*
Local Traffic & Network Manager role
    defined *17*
Local Traffic & Network Viewer role
    defined *17*

N

Network Security Deployer role
    defined *17*
Network Security Editor role
    defined *17*
Network Security Manager roleSecurity Manager role
        License Manager role
    defined *17*
Network Security Viewer role
    defined *17*

P

permissions
    assigning to a role type *21*
Pool Member Operator
    defined *17*

R

RADIUS
    configuring authentication with *9*
    info to collect before integrating *9*
    prerequisite info for integration *9*
    using pre-defined RADIUS groups *10*

RADIUS authentication
configuring for new user 7
RADIUS authorization
for user groups 11
RADIUS server
for authenticating and authorizing BIG-IQ users 9
resource groups
creating 21
role types
about 21
creating custom 21
providing access to BIG-IP resources 21
role-based user access
about 17
roles
about 17
about using 20
adding 22
adding users to custom roles 22
defined for BIG-IQ users 17
for users 17

S

SCRIPT5007 error 29
Service Catalog Editor
defined 17
Service Catalog Viewer
defined 17
system user
adding 19
adding RADIUS authenticated user 7
authenticating with LDAP 10
authenticating with TACAS+ 14

T

TACACS+
configuring authentication with 13
info to collect before integrating 13
prerequisite info for integration 13
TACACS+ authentication
creating user groups 15
TACACS+ server
about using for authenticating users 13
TACAS+ authentication
configuring for new user 14
troubleshooting
errors logging into secondary BIG-IQ system 29
Trust Discovery Importer
defined 17

U

user access
about 17
about limiting 20
user authentication
configuring through RADIUS 9
configuring through TACACS+ 13
user groups
creating for LDAP authentication 8
user groups *(continued)*
creating for local authorization 11
creating for TACACS+ authentication 15
user roles
about 17
defined for BIG-IQ 17
in Access configuration workflow 25
users
adding 7, 10, 14, 19, 22
authenticating with LDAP 10
authenticating with TACAS+ 14
remotely-authenticated with RADIUS 7
users and user groups
synchronizing with secondary BIG-IQ system 29
usersroles
removing role from 27
removing users from 27

V

Virtual Server Operator role
defined 17

W

Web App Security Deployer role
defined 17
Web Security Editor role
defined 17
Web Security Manager role
defined 17
Web Security Viewer role
defined 17