F5® BIG-IQ® Centralized Management: Access

Version 5.2

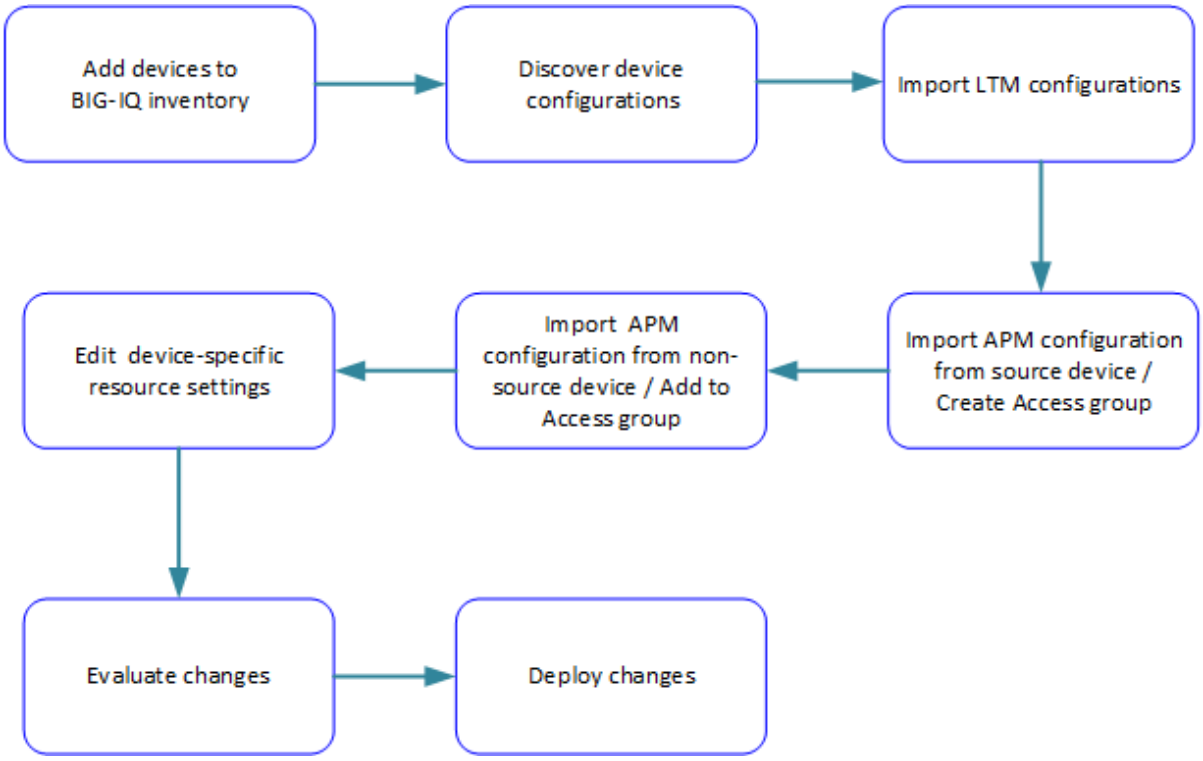
Table of Contents

BIG-IQ Configuration Management: Access Overview

About Access

The BIG-IQ® system offers you centralized management for BIG-IP ®Access Policy Manager® (APM) and F5 Secure Web Gateway (SWG) configurations. Centralized management gives you easy-to-deploy sets of access policies, and access policy configuration objects. This means you don't need to repeat the configuration on each BIG-IP system individually. Access also offers you centralized reporting, which allows you to compare and monitor BIG-IP APM® usage across many groups of devices.

Access configuration workflow



What are Access groups?

Each *Access group* is a group of BIG-IP® devices across which you plan to share the same Access configuration. When you import an APM service configuration from a device, the device must join an Access group.

About the types of resources that Access imports

When you import an APM® service configuration from a device, the device must join an Access group.

- If the device joins a new Access group, Access imports both shared resources and device-specific resources from the device.
- If the device joins an existing Access group, Access imports only the device-specific resources from the device.

About shared resources

In an Access group on the BIG-IQ® system, *shared resources* are a set of configuration objects that are expected to be the same on every device in an Access group.

How do shared resources work in the configuration?

Initially, shared resources are imported with the APM® service configuration from the device. After import, they are read-only on the BIG-IQ® system. The deployment process configures the shared resources on all devices in the Access group. This can result in major configuration changes on the devices, with resources being overwritten, deleted, or added on them.

About device-specific resources

In an Access group on the BIG-IQ® system, *device-specific resources* are a set of configuration objects that are expected to exist on every device in the Access group. However, the properties of these resources can differ from device to device.

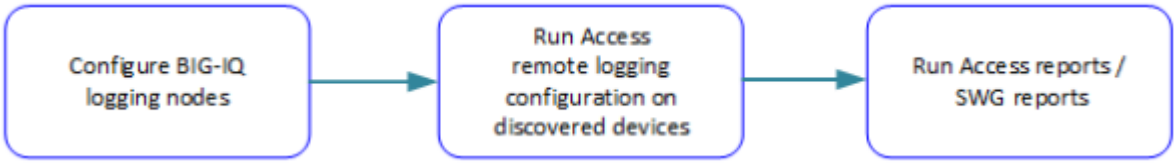
For example, an access policy could use an Active Directory server for user authentication. Device `apm_north_america.xyz.com` must use an Active Directory server configured in a North American domain or data center, while device `apm_south_america.xyz.com` must use an Active Directory server configured in a South American domain or data center.

How do device-specific resources work in the configuration?

When you add a device to an Access group, device-specific resources are created from the device's APM® service configuration. Or, if particular resources do not exist on a device, Access creates device-specific resources that match those in the device configuration. After import, you are instructed to review and change device-specific resources if needed; in addition, you can change them at your option. You can also make a device-specific resource shared, so that its properties can only be configured in the shared resources. At deployment, device-specific resources are configured on the specific devices.

Reporting configuration workflow

BIG-IQ logging nodes are required for Access and SWG reporting. To set up a discovered device so that it sends report data to a logging node, you must run the remote logging configuration. Then, you can run reports.



Upgrading BIG-IQ Access version 5.1 to 5.2

After upgrading from BIG-IQ® Centralized Management version 5.1 to version 5.2, send out a POST request to a REST API in order to restore session data after an upgrade. If you do not perform this step, then the sessions that you created before upgrading will not display in either the Sessions report or in the Active Sessions report after the upgrade. You take this action after restoring the elastic snapshot.

Enter this command: `restcurl -X POST -u admin:admin http://localhost:8100/mgmt/cm/access/reports/access-es-upgrade-task -d '{ }'`.

Users, User Groups, and Roles

About 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 who 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.

User roles in the Access configuration workflow

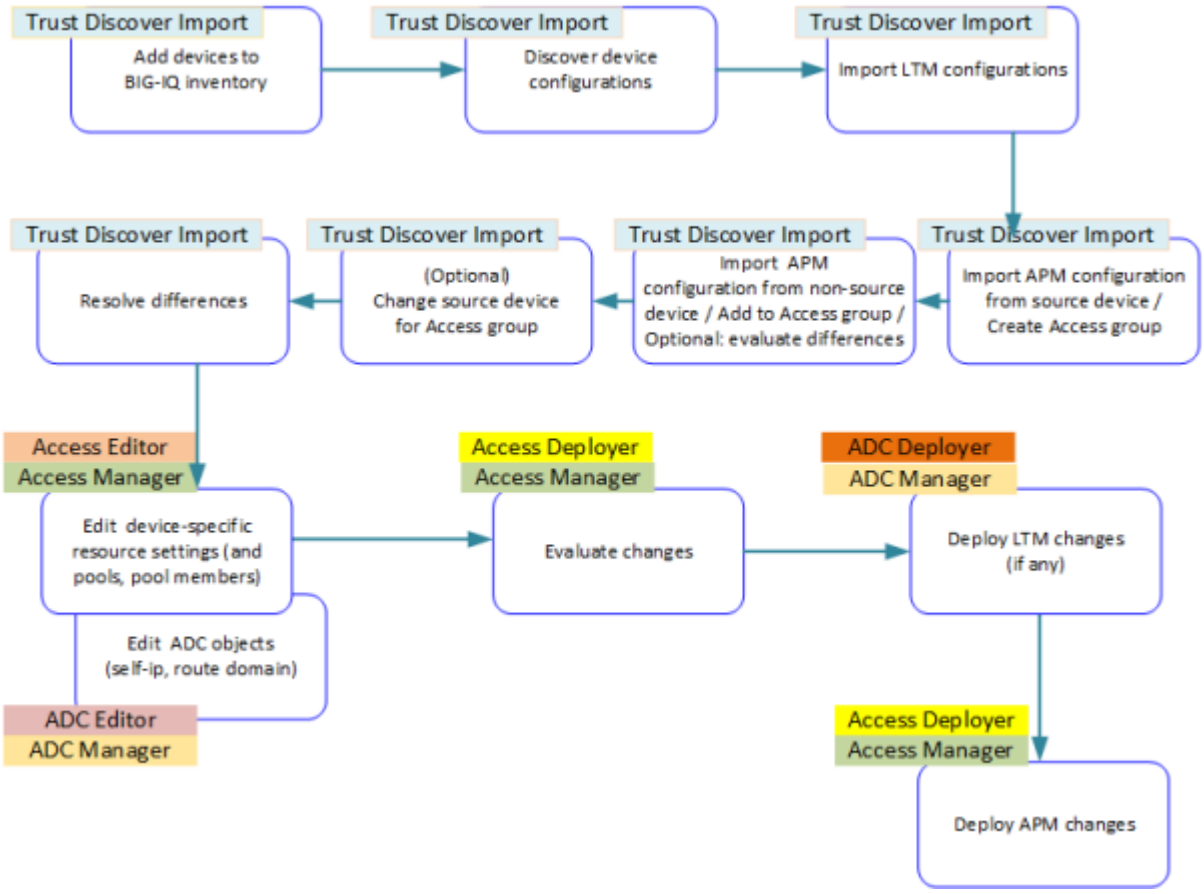


Figure 1: Access configuration workflow with possible user roles

User roles in the reporting configuration workflow

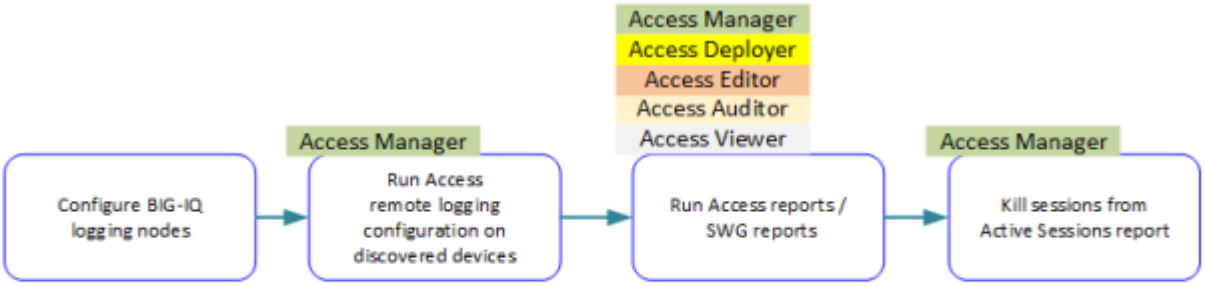


Figure 2: Reporting workflow with possible user roles

Adding a BIG-IQ user

Create a user to provide access to the BIG-IQ system.

1. At the top of the screen, click **System**.
2. On the left, click **USER MANAGEMENT** > **Users**.
3. Click the **Add** button.
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.
   To associate the user with additional groups, click the plus [+] icon and select another group.
8. From the **User Roles** list, select a user role to associate with this user.
   Each role has a set of unique privileges.
   To associate the user with additional roles, click the plus [+] icon and select another role.
9. Click the **Save & Close** button at the bottom of the screen.

Creating a user group

You create a user group to offer individual users access to the same resources.

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 **Add**.

4. In the **Name** field, type a name for this new user group.
5. From the **Auth Provider** list, select **local (Local)**.
6. From the **Users** list, select a user to add to this group.
   To add additional users, click the plus [+] icon.
7. From the **User Roles** list, select a user role to give its associated system access to this user group.
   To add additional roles, click the plus [+] icon.
8. Click the **Save** button at the bottom of the screen.

User role access descriptions

The table lists standard BIG-IQ® system user roles you might need to assign to your users, depending on their responsibilities in working with Access.

Role	Role Description / Access
Access Auditor	This role provides access to BIG-IQ® Access reports.
Access Deployer	This role has deploy access to Access configuration objects. This role cannot discover and edit devices or policies.
Access Editor	This role has edit access to Access configuration objects. This role cannot discover and deploy devices or policies. This role includes the ability to add, update, and delete pools and pool members from the Access configuration object editor.
Access Manager	This role has deploy and edit access to Access configuration objects, and has access to Access Reports and Dashboard. This role cannot add or remove devices and device groups, and cannot discover, import or delete services.
Access Viewer	This role has view-only access to Access configuration objects and tasks for Access devices that have been discovered. This role cannot edit, discover, or deploy devices or policies.
ADC Deployer	This role has deploy access to ADC configuration objects. This role cannot discover and edit devices or configuration objects. At deployment, Access notifies you if it finds changes in ADC that you must deploy first,
ADC Editor	This role has edit access to ADC configuration objects. A user needs this role to be able to edit or create a self-IP address or a route domain and to view other ADC configuration objects. This role includes the ability to add, update, and delete pools and pool members from ADC; however, you can configure pools and pool members within Access without having this role.
ADC Manager	This role manages the ADC module with full privilege. This role works for a user who needs to: Deploy ADC; edit or create a self-IP address or a route domain; view other ADC configuration objects. This role includes the ability to add, update, and delete pools and pool members from ADC; however, you can configure pools and pool members within Access without having this role.
ADC Viewer	This role permits read-only access to the ADC module. A user who needs to view configuration objects from ADC needs this role.
Trust Discover Import	This role can add and delete devices, discover services and import them, and remove services.
Administrator	This role has access to all aspects of the BIG-IQ system, which can include BIG-IQ Security, BIG-IQ System, and BIG-IQ ADC management. This access includes areas involved in adding individual users, assigning roles,

Role	Role Description / Access
	device discovery, installing updates, activating licenses, and configuring a BIG-IQ high availability (HA) configuration.

BIG-IP Devices, HA Pairs, and Clusters

Preliminary tips for putting an Access group together

As you start to think about how to group BIG-IP® devices into Access groups that share a configuration, there are a few things you might want to keep in mind. When you select a device for an Access group, you are selecting the shared configuration for all of the devices in the group.

When you add BIG-IP devices to an Access group, Access evaluates the differences between the devices in the group. Access reports the differences for your information. If you need to make configuration changes on any of the devices, Access lets you know which device to change, and which object to update, delete, or add.

Things to know about machine accounts

Machine accounts support Microsoft Exchange clients that use NTLM authentication. An NTLM Auth Configuration object refers to a machine account. If the APM® configurations on the BIG-IP® systems include machine accounts, you might want to be aware of the following information.

In an Access group, the machine accounts on the devices must each have been created with the same name. If this is not the case, the deployment fails. The deployment differences will include the names of the devices on which you must reconfigure the machine accounts before you can successfully deploy.

Things to know about bandwidth controller configurations

On a BIG-IP® device, bandwidth controller configuration objects (policies and priority groups) are configured at the system level. In APM ®, they are used to provide traffic shaping for Citrix clients that support MultiStream ICA. In an access policy, a *BWC policy* item refers to a bandwidth controller policy. If the APM configurations on the BIG-IP systems refer to bandwidth controller objects, you should be aware of the following information.

The bandwidth controller configuration objects on the device are treated as if they were part of the Access shared configuration. That means when you import the APM service configuration from a device, the bandwidth controller objects are imported and cannot be updated in the BIG-IQ® system. When you deploy the configuration, deployment creates the bandwidth controller objects on the devices.

Access requirements for HA pairs and clusters

For BIG-IP® system high availability, APM ® supports two devices in a Sync-Failover group; these devices can also be referred to as an *HA pair*.

Access has these requirements for HA pairs on BIG-IQ® system configuration:

- If you import a device that is part of an HA pair, you must import the other device in the pair as well. Access must manage the configuration for both devices.
- When you import the devices that are an HA pair, you must place both devices in a cluster that contains only that pair.

Note: *This is not enforced when you add devices to a cluster. But when you try to deploy the configuration, Access reports errors and deployment fails.*

- When you add devices to an Access group, you must add both members of a cluster to the same Access group. (You can add all clusters to one Access group or add clusters to multiple Access groups.)

  Note: *Access enforces this requirement.*

To avoid problems after you create Access configurations on the BIG-IQ system, you should know which devices constitute each HA pair.

Important: *F5® recommends that you make a list of HA pairs, and keep it available for ready reference while you work in the BIG-IQ system.*

Managing Access Groups

How do I start to centrally manage APM configurations from BIG-IQ?

Here is an overview of your first steps for setting up an Access Policy Manager® (APM®) configuration once, and then being able to deploy that configuration from the BIG-IQ® system to other BIG-IP® devices.

Step 1. Add the BIG-IP device to the inventory list on the BIG-IQ system. You enter the IP address and credentials of the BIG-IP device you're adding, and associate it with a cluster (if applicable).

Step 2. Manage the APM configuration by adding to the existing Access Group or creating a new Access Group.

Note: *For more information, refer to the "BIG-IQ Device: Device Management" guide.*

What is the best way to create an Access group?

After you add devices to the BIG-IQ® system and discover them, you can create an Access group in either of two ways. Use whichever you prefer, based on your requirements.

- Select one device and create an Access group or add it to existing group. The Access group automatically discovers and imports the LTM and APM configurations.
- From the Device Management user interface, you can add one device at a time to an Access group when you import the APM service from each device. This requires that you discover the BIG-IP® Access Policy Manager® (APM)and the Local Traffic Manager™ (LTM) configurations manually. You must discover LTM first, because APM uses some resources that are managed by LTM. Afterwards, import the LTM configuration into the BIG-IQ system

Adding devices to the BIG-IQ inventory

Before you can add BIG-IP® devices to the BIG-IQ® inventory:

- The BIG-IP device must be located in your network and running a compatible software version. Refer to *https://support.f5.com/kb/en-us/solutions/public/14000/500/sol14592.html* for more information.
- Port 22 and 443 must be open to the BIG-IQ management address, or any alternative IP address used to add the BIG-IP device to the BIG-IQ inventory. These ports and the management IP address are open by default on BIG-IQ.

Note: *A BIG-IP device running versions 10.2.0 - 11.5.0 is considered a legacy device and cannot be discovered from BIG-IQ version 5.2. If you were managing a legacy device in previous version of BIG-IQ and upgraded to version 5.2, the legacy device displays as impaired with a yellow triangle next to it in the BIG-IP Devices inventory. To manage it, you must upgrade it to 11.5.0 or later. For instructions, refer to the section titled, Upgrading a Legacy Device.*

Note: *Access supports BIG-IP system software version 12.1 and 13.0 only.*

You add BIG-IP devices to the BIG-IQ system inventory as the first step to managing them.

1. At the top of the screen, click **Devices**.
2. Click the **Add Device** button.
3. In the **IP Address** field, type the IPv4 or IPv6 address of the device.
4. In the **User Name** and **Password** fields, type the user name and password for the device.
5. To add this device to a new cluster:

   Important: *If a device is not a member of a Sync-Failover group that you configured to support an Active-Standby configuration for APM, do not add it to a cluster.*

   If the device is the first member of a Sync-Failover group that you have added to the BIG-IQ system, add it to a new cluster. It does not matter whether this device is the Active or the Standby member of the group.

   a) From the **Cluster Display Name** list, select **Create New**, and then type a new name for this new cluster.

      A cluster name must be unique on the BIG-IQ system. It does not need to match the name of the Sync-Failover group on the BIG-IP device. However, ensuring some similarity between the names might be useful to you, because when you add the second member of the group, you must add it to the same cluster.

   b) Select an option from the **Deployment Settings**:

   - **Initiate BIG-IP DSC sync when deploying configuration changes (Recommended)** Select this option to prompt BIG-IQ to start the DSC synchronization process so that any configuration change made to this device is synchronized with other members of the DSC. This option makes sure all members of the DSC have the most current configuration.
   - **Ignore BIG-IP DSC sync when deploying configuration changes** Select this option to have BIG-IQ deploy any configuration changes for this device to all cluster members. Use this option only if this device is not configured in a DSC Sync-Failover device group, or if any members of the cluster are disabled.

6. To add this device to an existing cluster:

   If the device is the second member of a Sync-Failover group that you have added to the BIG-IQ system, add the device to the existing cluster for that Sync-Failover group.

   a) From the **Cluster Display Name** list, select **Use Existing**, and then select the cluster from the list.
   b) Select an option from the **Deployment Settings**:

   - **Initiate BIG-IP DSC sync when deploying configuration changes (Recommended)** Select this option to prompt BIG-IQ to push any configuration changes to this device to other members of the DSC. This option makes sure all members of the DSC have the most current configuration.
   - **Ignore BIG-IP DSC sync when deploying configuration changes** Select this option to have BIG-IQ deploy any configuration changes for this device to all cluster members. Use this option only if this device is not configured in a DSC Sync-Failover device group, or if any members of the cluster are disabled.

7. Click the **Add** button at the bottom of the screen.
   The BIG-IQ system opens communication to the BIG-IP device, and checks its framework.

   Note: *The BIG-IQ system can properly manage a BIG-IP device only if the BIG-IP device is running a compatible version of the REST framework.*

8. Click the **Add** button at the bottom of the screen.
   When complete, a popup screen displays a status and options to discover device service configurations immediately.
9. To discover configurations for APM® and LTM® now, select **Access Policy Manager (APM)**, and the **Local Traffic Manager (LTM)** check box is selected automatically; click **Discover**.

   You can discover service configurations now or do it later.

BIG-IQ discovers the configurations for the APM and LTM services.

BIG-IQ displays a discovering message in the Services column of the inventory list.

Creating an Access group from the Configuration tab

Before you can create an Access group, you must have at least one device discovered. You must have imported the LTM® service configuration from a device before you can add that device to an Access group

You create an Access group to start to manage the Access configuration for a group of devices.

Note: *When you create an Access group, the service configurations for the devices are imported.*

Important: *You, or any other BIG-IQ system user, cannot perform any tasks on the BIG-IQ system while it is importing a service configuration. Large configurations can take a while to import, so let other BIG-IQ users know before you start this task.*

1. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
2. Click the **Create** button.
   The New Group screen opens.
3. In the **Name** field, type a name for the Access group.
4. From **Device**, select the device to be the source of the shared configuration for other devices in the group.
5. For the **Snapshot** option, click the check box to create a snapshot at the time this Access group is created.
6. Click **Create**.
   The Access Groups screen opens. Progress information displays in the Status column.

Adding a device to an Access group from the Configuration tab

Before you start, you must have at least one device with the APM® service discovered. You must also have imported the LTM® service configuration from the device before you can add that device to an Access group.

You add a device to an Access group so you can manage its configuration from Access. When you add a device to an existing Access group, its device-specific configuration resources are imported into Access. A device can only belong to one Access group.

1. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
2. Click the name of the Access group you want to change.
   The General Properties screen for the access group displays, listing the devices in the Access group.
3. Click **Add Device**.
   The Add Device popup screen displays.
4. For **Device**, select the device from the dropdown menu.
5. (Optional) To create a snapshot of the existing configuration, for **Snapshot**, click the check box **Create a snapshot of the current configuration before importing**.
6. Click **Add**.
   The popup screen closes, showing the Access Groups screen. Progress information displays in the Status column.

Reimporting an Access group configuration or device-specific configuration

You must have an existing Access group.

You can reimport a shared Access group configuration or a device-specific configuration from any device in an Access group. This reduces the need to manually edit the configuration by hand.

Note: *You can an reimport from the Access groups UI screen.*

---

1. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
2. Click **Reimport**.
3. For the **Configuration Type** option, Select whether you want to import a **Shared Access Group and Device Specific configuration** or just a **Device specific configuration**.
4. (Optional) For the **Snapshot** option, select whether you want to create a snapshot of the current configuration before importing.
5. Click **Reimport**.

You now have reimported an existing configuration.

Removing a device from an Access group

You remove a device from an Access group if you no longer want to manage the Access configuration for the device, or if you want to add the device to a different Access group. An Access group can exist in the BIG-IQ system without any devices. You can remove all devices from an Access group, leave it empty, and then add new devices later.

1. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
2. Click the name of the Access group you want to change.
   The properties screen for that group opens, listing the devices in the Access group.
3. Select the check box for the device you want to remove and click **Remove**.
   A confirmation popup screen opens.
4. Confirm that you want to remove the device.
   The device no longer displays in the Access group. The APM service configuration on the device is no longer managed.

Before you can see new data from the device in Access reports or add the device to another Access group, you must discover the APM service configuration on the device.

Removing an Access group

You remove an Access group that you previously created.

1. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
2. Click the check box next to an existing Access group.
   The **Remove** button becomes available and a message displays.
3. In the Remove Access Group Configuration? message windows, click **OK**.

You have removed an Access group from your BIG-IQ system.

Creating an Access group from the Devices tab

Before you can create an Access group, you must have at least one device discovered. You must have imported the LTM® service configuration from a device before you can add that device to an Access group

You create an Access group to start to manage the Access configuration for a group of devices.

Note: *When you create an Access group, the service configurations for the devices are imported.*

Important: *You, or any other BIG-IQ system user, cannot perform any tasks on the BIG-IQ system while it is importing a service configuration. Large configurations can take a while to import, so let other BIG-IQ users know before you start this task.*

1. At the top of the screen, click **Devices** > **BIG-IP CLUSTERS** > **Access Groups**.
   The Access Groups screen displays.
2. Click the **Create** button.
   The New Group screen opens.
3. In the **Name** field, type a name for the Access group.
4. From **Device**, select the device to be the source of the shared configuration for other devices in the group.
5. For the **Snapshot** option, click the check box to create a snapshot at the time this Access group is created.
6. Click **Create**.
   The Access Groups screen opens. Progress information displays in the Status column.

Discovering the LTM and APM service configurations

Before you can import configurations from a device, you must first discover them. To prepare to create an Access configuration on the BIG-IQ ®system, you must discover the Local Traffic Manager™ (LTM®) service configuration, and then discover the Access Policy Manager® (APM) service configuration.

1. At the top of the screen, click **Devices**.
2. Click the name of the device you want to discover the service configuration from.
3. On the left, click **Services**.
4. For Local Traffic Manager (LTM), click **Discover**.
   You must wait for discovery to complete before you continue.
5. For Access Policy Manager (APM), click **Discover**.

Importing the LTM service configuration

You must discover a service configuration before you can import it.

Before you can import the Access Policy Manager® (APM) service configuration from a discovered device, you must import the Local Traffic Manager™ (LTM®) service configuration.

Important: *You, or any other BIG-IQ system user, cannot perform any tasks on the BIG-IQ system while it is importing a service configuration. Large configurations can take a while to import, so let other BIG-IQ users know before you start this task.*

1. At the top of the screen, click **Devices**.

2. Click the name of the device you want to import the service configuration from.
3. On the left, click **Services**.
4. For Local Traffic Manager (LTM), select the **Create a snapshot of the current configuration before importing** check box to save a copy of the device's current configuration.

   You're not required to create a snapshot, but it is a good idea in case you have to revert to the previous configuration for any reason.
5. For Local Traffic Manager (LTM), click **Import**.
   The LTM Import screen displays.
6. Click **Proceed to Import**.

The LTM service configuration is imported. Click the back arrow to return to the previous screen.

Importing the APM configuration into an Access group

You must discover a service configuration before you can import it.

You import Access Policy Manager® (APM) configuration objects from a device to manage the device configuration from the BIG-IQ® system. As part of the import process, you select an Access group.

Important: *You, or any other BIG-IQ system user, cannot perform any tasks on the BIG-IQ system while it is importing a service configuration. Large configurations can take a while to import, so let other BIG-IQ users know before you start this task.*

1. Click the name of the device you want to import the service configuration from.
2. On the left, click **Services**.
3. For Access Policy (APM), select the **Create a snapshot of the current configuration before importing.** check box to save a copy of the device's current configuration.

   You're not required to create a snapshot, but it is a good idea in case you have to revert to the previous configuration for any reason.
4. For Access Policy (APM), click **Import**.
5. On the Add to Access Group popup screen, specify either a new or existing Access group:
   - Select **Create New**, in the **Name** field, type a name, and click **Add**.
   - Select **Add to existing**, select a name from the **Name** list, and click **Add**.

   Important: *You must add both members of an HA pair to the same Access group.*

The APM service configuration is imported.

Adding a device to an Access group from the Devices tab

Before you start, you must have at least one device with the APM® service discovered. You must also have imported the LTM® service configuration from the device before you can add that device to an Access group.

You add a device to an Access group so you can manage its configuration from Access. When you add a device to an existing Access group, its device-specific configuration resources are imported into Access. A device can only belong to one Access group.

1. At the top of the screen, click **Devices** > **BIG-IP Devices**.
   The BIG-IP Devices screen displays.
2. Click **Add Device**.
   The Add Device popup screen displays.
3. Type an IP address.

4. Type a user name.
5. Type a password.
6. From the **Cluster Display Name** list, select either a a new DSC group or an existing DSC group.
7. Click **Add**.

Viewing and Editing the Access Configuration

Finding a device-specific resource

In BIG-IQ® Centralized Management Access, you can find a device-specific resource by searching for it in the search field, or under the specific device to which it belongs.

1. To search for a resource among the shared resources, click the question mark at the top right of the screen.
2. In the Search field, type all or part of the name of the object, and press Enter.
   The Search screen displays each shared object type, with the number of matching resources it has found, marked in parentheses. For example, ACCESS PROFILES (1), PORTAL ACCESS (0), and so on.
3. To search among device-specific resources, expand the Access group name, click the name of a device, then use the Filter field to sort the resources.
4. If you do not know the name of the resource you want to find, to find it you must browse through the shared resource types and device-specific resource types for the devices.

Editing a device-specific resource

In BIG-IQ® Access, you can update the properties of a device-specific resource in the working configuration.

1. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
2. In the Access Groups screen, click the name of an Access group.
   The screen displays a list of resource types.
3. Expand the resource types and select the particular type of resource that you want to change.
   A screen displays a list of resources displays.
4. Click the name of the resource that you want to edit.
   The properties screen for that resource opens.
5. Edit the resource properties.

   Note: *Click the question mark (?) icon for help on each property.*

6. Click **Save**.

The change is distributed to the BIG-IP® device when you deploy the configuration.

Sharing a device-specific resource

In BIG-IQ® Access, you can make a device-specific resource act like a shared resource.

Note: *When you make a device-specific resource shared, the resource takes the properties defined for it on the source device*

1. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
2. Select an existing Access group.

3. Select the type of resource that you want to change.
   The screen displays a list of resources of that type on the right.
4. From the list, select the check box for the resource that you want to make shared.
5. Click **Mark Shared**.
   The resource no longer displays on the list of device-specific resources.

You can now find the resource on the **Shared resources** list.

What local traffic objects does Access support?

In BIG-IQ® Centralized Management, you can associate various local traffic objects without manually configuring the objects in individual BIG-IP® devices before deploying the Access configuration on these devices. You must create these objects in either the BIG-IQ local traffic component or in BIG-IP local traffic. :

- Virtual Server
  - You can configure sections of a virtual server specific to BIG-IQ system in the BIG-IQ system. This includes configuring Access profiles, connectivity profiles, per-request policies, VDI profiles, enabling App Tunnels, enabling OAM support, and PingAccessProfile.
  - You can configure the SAML artifact resolution service with the virtual server for each BIG-IP device in BIG-IQ Access.
- SSL Certificate and SSL Key
  - On the BIG-IP device, you can export the certificate and key files for each CERT and KEY object, and manually import them to the same object in BIG-IQ system.
  - On the BIG-IP device, you can configure SAML, SAML IdP Connector, and OCSP Respond with SSL Cert and SSL Key.
  - You can configure OamAccessGate for each device with SSL Key and Cert in BIG-IQ system.
- Net Tunnels Fec
  - You can create the connectivity profile on a BIG-IP device with a Fec profile.
- Route Domains
  - You can create route domains for each BIG-IP device in BIG-IQ system.
  - You can configure the Route Domain Selection Agent for each BIG-IP device in BIG-IQ system by editing the Access policy.
- iRules
  - You can create iRules® in BIG-IP Access, and configure them in the virtual server.
  - If you are using iRules in an OAuth server, create the iRule first, then associate the OAuth server in the BIG-IP device.
- DNS Resolver
  - You can create DNS resolvers in either the BIG-IP device or BIG-IQ system.
  - The best practice is to create the DNS resolver in the BIG-IP device, then associate the DNS resolver with the OAuth server.
- SSL Client Profile and HTTP Profile
  - You can create either profile in BIG-IQ system, and configure it in the local traffic virtual server.
- Server SSL Profile
  - You can create this in either the BIG-IP device or in BIG-IQ system.
  - The best practice is to create the server SSL profile in the BIG-IP device, and associate it with the SAML IdP connector.
  - You can configure LDAP and Endpoint Management systems with a server SSL profile in either the BIG-IP device or in BIG-IQ system.

- Rewrite Profile and Classification Profile
  - You must create these in the BIG-IP device.
  - You can associate both these profiles with the local traffic virtual server in the BIG-IQ system.
  - You can associate the rewrite profile in portal mode with the Access group virtual server in the BIG-IQ system.

For more information about configuring BIG-IQ local traffic objects, refer to the online help, and to the guide, *F5 BIG-IQ Centralized Management: Local Traffic & Network*.

Editing a virtual server

You must create a virtual server in BIG-IP LTM. The created virtual servers are listed in the Access group for the corresponding Access group devices. You must manually configure a virtual server for each device in the Access group. During deployment, you must deploy the Access-specific virtual server properties.

A virtual server is an LTM resource that you can configure in BIG-IQ Access.

1. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
2. In the Access Groups screen, click the name of an Access group.
   The screen displays a list of resource types.
3. Expand the resource types and select the particular type of resource that you want to change.
   A screen displays a list of resources displays.
4. Click **Virtual Server**.
   The Virtual Server (Device-specific) screen displays on the right.
5. Select an existing virtual server to edit.
   A new screen displays.
6. Type a description.
7. From the **Access Profile** list, select a profile for managing secure access.
8. From the **Connectivity Profile** list, select a profile for managing specific connection options for a secure access connection.
9. From the **Per Request Policy** list, select an already configured per-request policy.
10. From the **Per Request Policy** list, select a VDI profile for use when you want to provide connections to virtual desktop resources.
11. For **Application Tunnels(Java & Per App VPN)**, select the check box to support connections from Java applications or to support a SOCKS tunnel from an iOS mobile device that initiates per-app VPN.
12. For **OAM Support**, select the check box to provide native integration with the OAM server for authentication and authorizatio.
13. From the **PingAccess Profile** list, select an already configured Ping Access Profile for authentication with a Ping Access policy server.
14. From the **Rewrite Profile** list, select a rewrite profile to rewrite web application data or to perform URI translation with the reverse proxy.

You have configured a virtual server.

Where are local traffic objects supported in Access?

This table describes the relationship between local traffic objects and APM objects. Specifically, this explains which local traffic objects are used in which Access objects.

Table 1: Local Traffic objects are supported in which Access objects?

LTM Object	Access Object
Virtual server	• Artifact Resolution Service • OAM Access gate
SSL Key	• SAML • SAML IDP connector • OAM Access gate • OCSP Responder
SSL Cert	• SAML • SAML IdP connector • OAM Access gate • OCSP Responder
SNAT Pool	• Network Access • RouteDomain Selection Agent
Server SSL Profile	• Endpoint management system • LDAP • SAML IdP connector
Net Tunnels Fec	• Connectivity Profile
Route Domain	• Route domain selection agent
iRules	• iRule Event Agent • OAuth Server
DNS Resolver	• OAuth Server
ReWrite Profile	• Portal access
LogPublisher	• Access log settings • Classification profile
Preset	• Classification profile

Returning a shared resource to device-specific resources

If you made a device-specific resource into a shared resource, you can return it to device-specific resources and configure its properties for each device in the Access group.

Note: *Device-specific resources are a system-defined subset of shared resources. Not all shared resources can be made device-specific.*

1. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
2. Select an existing Access group.
3. Select the type of resource that you want to change.
   The screen displays a list of resources of that type on the right.

4. From the list, select the resource that you want to return to its device-specific state.
5. Click **Make Device Specific**.
   The resource no longer displays on the list of shared resources.

The resource is now located with the device in **Device-specific resources**.

You can now change the resource properties to meet the device-specific requirements that you have.

Viewing an access policy

After you've imported a device, you can view the access policies that are configured on it. An access policy is either a per-session policy or a per-request policy. In either case, an access policy is made up of policy items, such as Start, Logon, Deny, and macros. A *macro* is a sub-policy with a beginning, one or more policy items, and one or more endings.

Note: *These policies are deployed to all the devices in the Access group. You can view the flow of actions in the policy, but not the properties of the actions.*

---

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. On the left, expand **Profiles / Policies**, click **Access Profiles (Per-Session Policies) (Shared)** or **Per-Request Policies(Shared)**.
   A new screen opens, showing a list of access policies associated with this Access group.
5. Select an access policy.
   The VPE screen opens.
6. (Optional) To move to another section of a large access policy more quickly than scrolling allows:
   - For Windows, hold the right mouse button down and drag the mouse.
   - For macOS, hold down the command key while dragging the mouse.
7. To close the screen, click **Close**.

About the access policy display

When you view an access policy in BIG-IQ® Access, the items in the policy are of a constant size. If an access policy item name is unusually long and does not include spaces, the name of the policy item will be truncated.

Editing an access policy

You can edit an existing access policy using the BIG-IQ® Access Visual Policy Editor (VPE) if the policy items are action, ending, or macro calls. Although Start and In are policy items, you cannot edit them. You can undo any edited actions, and if you cancel an editing session before saving, the Policy Editor makes no changes to the policy. However, some actions or objects cannot be undone or discarded. These include the following:

- Creating a per-session policy macro.
- Creating a per-request policy macro, subroutine, or subroutine macro.
- Creating new endings or terminals
- Deleting endings or terminals.
- Changing macros or subroutine properties.

- Updating the policy ending.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
3. Click the name of the Access group that interests you.
   A new screen displays the Access group properties.
4. On the left, expand **Profiles / Policies**, and click **Access Profiles (Per-Session Policies) (Shared)** or **Per-Request Policies(Shared)**.
   A new screen opens, showing a list of access policies associated with this Access group.
5. Select an access policy.
   The VPE screen opens.
6. Modify the policy by clicking the diagram to insert new items, modify existing items, delete items, or change endings.

   Undo returns you to the access policy before your most recent change.

   Redo allows you to redo an action you have undone.

   Revert returns the access policy to the state before you made any changes to the policy.
7. Click **Save**.

   Saving the policy saves all changes in the policy diagram, including all workflows and modified macros. You can also discard pending changes and macros by clicking **Discard**.

Editing a policy item

You can edit an existing policy item using the BIG-IQ® Access Visual Policy Editor (VPE).

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
3. Click the name of the Access group that interests you.
   A new screen displays the Access group properties.
4. On the left, expand **Profiles / Policies**, and click **Access Profiles (Per-Session Policies) (Shared)** or **Per-Request Policies(Shared)**.
   A new screen opens, showing a list of access policies associated with this Access group.
5. Select an access policy.
   The VPE screen opens.
6. Move your mouse over a policy branch, depicted by the blue line.
   An add icon (+) displays.
7. Click the (+) icon.
   The Item Insertion Selection popup screen opens.
8. From the selection list on the left, select the type of policy item.

   Example: **Logon**, or **Authentication**.

   The screen displays a list of policy items on the right.
9. From either the **Caption** or **Description** list, select a policy item.
   Another popup screen with properties and branch rules opens.
10. On the Properties tab, modify or fill in the fields.
11. To add a new branch rule or select an existing rule from the list, on the Branch Rules tab, click **Add**.
12. Click either **Simple** or **Advanced**, and modify the branch rule.
13. Click **Save**.

The policy item displays in the VPE at the location on the policy branch where you clicked the add icon (+).

About timeouts and crashes

During an editing session, if you remain inactive for a prolonged period of time, the session times out. Other times, the browser might freeze. In either case, you might have to prematurely terminate an editing session without a chance to save your changes. However, regardless of why you had to terminate a session, BIG-IQ® Access saves a draft of the policy and saves any unsaved macro when you make a modification. The next time you log in, locate the policy, and open the editing screen. The system notifies you that an unsaved draft exists, and prompts you to select whether you want to continue editing the draft or start over.

The system saves the change history in the draft, so actions such as Undo and Redo work for all changes you make before the session was interrupted. Lastly, if someone else was the previous editor, you can see the user and the time of the last edit. This allows you to choose whether or not to resume that person's editing session.

What is a macro sub-policy?

A *macro* is a sub-policy with a beginning, one or more policy items, and one or more endings. You can create or edit a macro as you would a policy. In a policy, a macro-call in the workflow represents the macro. When you insert a macro-call in a policy or another macro, it displays as a node in the workflow diagram. Typically, you use a macro in multiple branches of the workflow.

Macros are specific to an access policy. You cannot create a macro if there are pending changes to the access policy. You can also create special macros. These have the same workflow as the base macro type. However, you can only use subroutines in per-request policies and subroutine macros in subroutines.

Creating a macro sub-policy

You can create a macro sub-policy by using the Access visual policy editor.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
3. Click the name of the Access group that interests you.
   A new screen displays the Access group's properties.
4. On the left, expand **Profiles / Policies**, and click **Access Profiles (Per-Session Policies) (Shared)** or **Per-Request Policies(Shared)**.
   A new screen opens, showing a list of access policies associated with this Access group.
5. Select an access policy.
   The VPE screen opens.
6. At the lower left, ensure that **Macros** shows on the drop-down menu.

   Macros should be the default option. Macros always appear in the lower area of the VPE screen. This is where you edit them. You can change the properties of a macro in Edit Properties and manage macro terminals (endings) in Edit Terminals. You cannot modify properties or terminals that have pending changes.
7. Click **New**.
   The Create New popup screen opens.
8. From the **Template** drop-down list, select an existing template or an empty macro.
9. In the **Caption** field, type a name for the macro.
10. Click **OK**.
    The macro template displays in the VPE screen.

After creating a macro, you can edit the macro sub-policy by inserting actions or macros in the branches, or by selecting either the default ending or different endings.

Adding an action item or macro-call to a sub-policy

You can modify an existing sub-policy by adding additional action items and macro-calls. When modifying a sub-policy, such as a macro, all diagram operations, insertions, deletions, modifications, and branch swaps are the same from the sub-policy and the main Access policy.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. On the left, expand **Profiles/Policies**, and click **Access Profiles (Per-Session Policies) (Shared)** or **Per-Request Policies(Shared)**.
   A new screen opens, showing a list of access policies associated with this Access group.
5. Select an access policy.
   The VPE screen opens. The existing macro displays under the Macro sub-window.
6. Select the macro that you want to modify.
   The macro policy displays with actions and branches.
7. Hover your cursor over a branch line between two items.
   An add icon (+) displays.
8. Click the icon +.
   The Item Insertion Selection popup screen opens.
9. From the Caption list, select a policy item.
   A new screen opens.
10. Fill in the relevant parameters and fields.
11. Click **Branch Rules**.
12. Click **Add**.
    The Branch Rules popup section displays more settings.
13. On the left, select either **Simple** or **Advanced** to create a branch rule configuration.
14. Fill in the relevant parameters and fields.
15. Click **OK**.
    The new branch rule displays in the Branch Rules screen.
16. Click **Save**.

The Access policy now includes the new action item.

Creating an ending policy item

Every branch in a workflow has one of three ending policy items: Deny, Redirect, or Allow. Macro endings are called *terminals*. As with action items, you can create, modify, or delete endings. You must include at least one ending for a policy or a macro, with one ending as the default. The default ending cannot be deleted. If you delete an ending that is in-use, the ending changes to the default ending.

Note: *Creating an ending policy item can only be done if there are no pending changes to the policy flows.*

1. Log in to the BIG-IQ system with your user name and password.

2. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. On the left, expand **Profiles/Policies**, and click **Access Profiles (Per-Session Policies) (Shared)** or **Per-Request Policies(Shared)**.
   A new screen opens, showing a list of access policies associated with this Access group.
5. Select an Access policy.
   The VPE screen opens.
6. At the top of the screen, click **Edit Endings**.
   The Manage Policy Endings popup screen opens.
7. Click **New**.
   The popup screen displays New Ending settings.
8. In the **Name** field, type a name for this policy ending.
9. In the **Color** field, select a color that the Policy Editor displays to represent this policy ending.
10. For the **Type** setting, select one of the options:
    - **Success** if the policy branch ends in success.
    - **Fail** if the policy branch ends in failure.
    - **Redirect** if the policy branch redirects to a new URL, and then type a valid URL in the **URL** field.
11. Click **Save**.
12. Click **Close**.

You have created a new policy ending.

Editing an ending policy item

You can edit an ending policy item by changing the color, caption, type, and redirect URL (if the sub-policy is a Deny ending).

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
3. On the left, click **Access Groups**.
   The Access Groups screen opens.
4. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
5. On the left, expand **Profiles/Policies**, and click **Access Profiles (Per-Session Policies) (Shared)** or **Per-Request Policies(Shared)**.
   A new screen opens, showing a list of access policies associated with this Access group.
6. Select an access policy.
   The VPE screen opens.
7. At the top of the screen, click **Edit Endings**.
   The Manage Policy Endings popup screen opens.
8. From the list under Policy Endings, select an existing ending.
   The popup screen displays configurable fields.
9. In the **Name** field, type a name for this policy ending.
10. In the **Color** field, select a color that the Policy Editor displays to represent this policy ending.
11. For the **Type** option, select one of the options:
    - **Success** if the policy branch ends in success.

- **Fail** if the policy branch ends in failure.
- **Redirect** if the policy branch redirects to a new URL ,and then type a valid URL in the **URL** field.

12. If you are editing the Deny ending, modify the fields under Customization.
13. Click **Save**.
14. Click **Close**.

You have edited a policy ending.

Deleting an ending policy item

You can delete any ending policy item except for the Deny ending.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. On the left, expand **Profiles/Policies**, click **Access Profiles (Per-Session Policies) (Shared)** or **Per-Request Policies(Shared)**.
   A new screen opens, showing a list of access policies associated with this Access group.
5. Select an access policy.
   The VPE screen opens.
6. At the top of the screen, click **Edit Endings**.
   The Manage Policy Endings screen opens.
7. From the list under Policy Endings, click the ending you want to delete.

   You cannot delete the Deny ending.

   An **X** button displays next to the ending.
8. Click the **X** button.
   The Delete Diagram Component Confirmation popup screen opens.
9. Click **OK**.
10. Click **Close**.

You have deleted a policy ending.

Swapping policy branches

When examining the policy workflow, you can swap one branch with another. Swapping branches does not change the order of the branch rule, only the destination of the two branches involved in the swap. When moving a branch, a highlighted bold blue line indicates that the swap is allowed. You cannot swap branches from an agent's upstream and downstream agent branches.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. On the left, expand **Profiles/Policies**, and click **Access Profiles (Per-Session Policies)s (Shared)** or **Per-Request Policies(Shared)**.
   A new screen opens, showing a list of access policies associated with this Access group.
5. Select an access policy.
   The VPE screen opens*.

6. Click on a branch and hold your mouse button.
7. Drag the branch up or down.
   A red dotted line previews where the branch ends up.
8. Release your mouse button.
   The VPE displays an access policy with swapped branches.
9. Click **Save**.

About editing conflicts

If you and other users can edit a policy, then multiple users can attempt to modify the same policy at the same time. As a result, changes made by another user can override your changes. However, in BIG-IQ® Access, if you start an editing session while another user is still editing, the system notifies you that you won't be able to make changes to the policy. The policy appears to you as read-only, and the warning message shows you who is currently editing the policy. You can then choose one of the following actions:

- Contact the other editor.
- Try again another time.
- Take over the original user's session. You can then choose to save or discard the original user's changes or continue editing.

Note: *When you choose a policy that has pending changes, the system displays a warning message tell you who was the last editor, and when the last edit was made. You can then choose to either resume the editing session or view the policy in read-only mode.*

Note: *If you choose to continue editing, the screen displays an orange line indicating that the policy has unsaved changes. The Details screen shows a summary of where the changes are.*

Managing Configuration Snapshots

What is snapshot management?

You can manage configuration snapshots for the configurations you have created on the BIG-IQ® Centralized Management system. A *snapshot* is a backup copy of a configuration. Configuration snapshots are created manually. This type of snapshot does not include events or alerts.

Note: *If an Access group version changes to a later BIG-IQ version and you attempt to restore a snapshot created during the previous version, then restoring that snapshot can cause working configuration changes that can cause a deployment failure.*

Comparing snapshots

You can compare two snapshots, or compare a snapshot to the configuration on the BIG-IQ® Centralized Management system to view their differences.

1. Under **SNAPSHOT & RESTORE**, select **Access**.
   The screen displays a list of Access snapshots that have been created on this device.
2. Select the check box to the left of the snapshot that you want to use as the source snapshot.
3. Click the **Compare** button.
   The Differences screen opens.

4. Analyze the configuration differences between the snapshot and the comparison target. When you are finished, click **Cancel** to close the Differences screen, then click **Close**.
   The screen closes and you return to the Snapshot screen.

Evaluating and Deploying Changes

How do I evaluate changes made to managed objects?

To change the object settings on a managed device, there are four tasks to perform.

This figure illustrates the workflow you perform to manage the objects on BIG-IP® devices. Evaluating the changes you have made is the third step in this process.

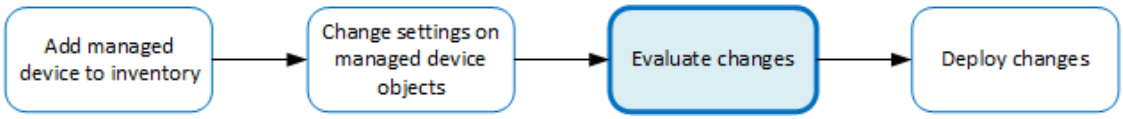


Figure 3: Overview of evaluating changes made to managed objects

Note: *If you need to make an urgent change, you can skip the evaluation step. However, we highly recommend evaluation in all but emergency situations. See Making an urgent deployment for details.*

How do I deploy changes made to managed objects?

Deploying changes applies the revisions that you have made on the BIG-IQ® Centralized Management system to the managed BIG-IP® devices.

This figure illustrates the workflow you perform to manage the objects on BIG-IP devices. Deploying the settings is the last step in this process.

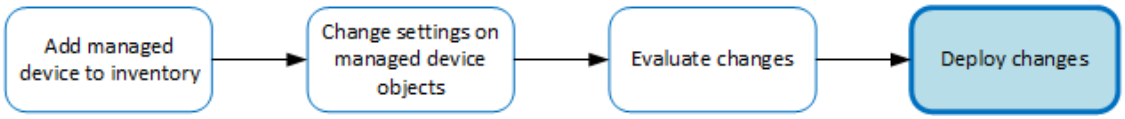


Figure 4: Change managed object workflow

How does deployment to devices in a cluster work?

When you created a cluster in BIG-IQ® inventory, you chose a deployment option for the devices in that cluster.

If you chose to initiate BIG-IP® DSC® sync, and the Sync-Failover group on the BIG-IP system is configured for manual sync, after deployment to either device in the HA pair, Access kicks off manual sync to the other device. If manual sync succeeds, the deployment is successful. Otherwise, the deployment status shows an error.

If you chose to initiate BIG-IP DSC sync and the Sync-Failover group on the BIG-IP system is configured for automatic sync, after deploying to either device in the HA pair, automatic sync propagates the configuration to the other device. If automatic sync succeeds, the deployment is successful. Otherwise, the deployment status shows an error.

If you chose to ignore BIG-IP DSC sync, you must deploy the configuration from BIG-IQ to both devices in the cluster.

Note: *It is possible that after this, conflicts in DSC sync for these devices will occur.*

Evaluating Access configuration changes

Evaluating your changes gives you a chance to spot critical errors and review your revisions one more time before deploying them.

Note: *When BIG-IQ® Centralized Management evaluates configuration changes, it first re-discovers the configuration from the managed device to ensure that there are no unexpected differences. If there are issues, the default behavior is to discard any changes made on the managed device, and then deploy the configuration changes.*

- To accept the default, proceed with the evaluation. The settings from the managing BIG-IQ overwrite the settings on the managed BIG-IP® device.
- To override the default, re-discover the device and re-import the service. The settings from the managed BIG-IP device overwrite any changes that have been made using the BIG-IQ.

Note: *Critical errors are issues with a configuration change that cannot be deployed successfully. Verification warnings are less serious in that they might not cause the deployment to fail, but you should review them,nonetheless.*

Note: *If you have Local Traffic & Network (LTM) changes to deploy, deploy the LTM changes before deploying changes to other components, or those deployments might fail.*

1. Log in to the BIG-IQ system with your user name and password.
2. Click **Deployment**.
3. Under **EVALUATE & DEPLOY**, select **Access**.
   The screen opens a list of Access evaluations and deployments that have been created on this device.
4. Under Evaluations, click **Create**.
   The New Evaluation screen opens.
5. In the **Name** field, type in a name for the evaluation task you are creating.
6. In the **Description** field, type in a brief description for the evaluation task you are creating.
7. For the **Source**, select what you want to evaluate.
   - To compare the object settings currently on the managed device with the object settings in the pending version, select **Current Changes**.
   - To compare the object settings currently on the managed device with the object settings in a stored snapshot, select **Existing Snapshot**, then choose the snapshot you want to use.
8. For **Supporting Objects**, select **Include associated LTM Objects** to deploy an Access configuration with associated LTM objects.
9. In the **Target** settings, from the **Group** list, select the Access group that you want to evaluate.
   Devices in the group display in the **Available** field.
10. Move the devices that you want to evaluate to the **Selected** field.

    Note: *If you are evaluating a device that is a member of a cluster set to initiate BIG-IP DSC sync at deployment, you can select either member of the HA pair.*

    Note: *If you are evaluating a device that is a member of a cluster set to ignore BIG-IP DSC sync, you should select both devices in the cluster.*

11. If you want to apply access policies on each BIG-IP device after deployment, select **Automatically apply policies after deployment**.
12. Review the evaluation to determine whether you are going to deploy it or not.
    a) If there are critical errors, you cannot deploy these changes. Click each error to see what it is, and then go back to where you made the change to fix it.

       After resolving any critical errors, you can come back and repeat the evaluation.
    b) If there are verification warnings, you can still deploy your changes, but you will probably want to resolve the warnings first. Click each warning to see what it is, and then go back to where you made the change to fix it.

       After resolving any verification warnings, you can come back and repeat the evaluation.
    c) If there are no critical errors or verification warnings, review the changes by clicking the **view** link.

       Each change is listed. You can review each one by clicking the name.
    d) When you finish reviewing the differences, click **Cancel**.
13. If the evaluation shows that you must evaluate and deploy Local Traffic configurations, do that before you deploy this evaluation.

To apply these just-evaluated object changes to the managed device, they must be deployed. Refer to *Deploy configuration changes* for instructions.

Deploying the Access configuration

To apply the Access configuration on the BIG-IQ system to your managed devices, you deploy the configuration.

1. Log in to the BIG-IQ® system with your user name and password.

   Important: *You must log in as an Administrator, Access Manager, or Access Deployer user to perform this task.*
2. Click **Deployment**.
3. Under **EVALUATE & DEPLOY**, select **Access**.
   The screen displays a list of Access evaluations and deployments defined on this device.
4. Click the name of the evaluation that you want to deploy.
   The View Evaluation screen opens.
5. Specify whether you want to deploy the changes immediately or schedule deployment for later.
   - To deploy this change immediately:
     1. Select **Deploy Now**.
     2. Click **Deploy** to confirm.
   - To deploy this change later:
     1. Select the **Schedule for later** check box.
     2. Select the date and time.
     3. Click **Schedule Deployment**.

   The process of deploying changes can take some time, especially if there are a large number of changes. During this time, you can click **Cancel** to stop the deployment process.

   Important: *If you cancel a deployment, some of the changes might have already deployed.* ***Cancel*** *does not roll back these changes.*

The evaluation you chose is added to the list of deployments on the bottom half of the screen.

- If you chose to deploy immediately, the changes begin to deploy and the Status column updates as it proceeds.
- If you choose to delay deployment, the Status column displays the scheduled date and time.

Access deployment errors and warnings: causes and resolutions

Problem	Description	Resolution
Access profile type mismatch	The deployment process imports an access profile from a device to the other devices in the Access group. If an access profile of the same name exists on a device, the access profile types must match. If it does not, a critical error occurs and deployment fails.	On the BIG-IP® device, delete the access profile. Then, redeploy on the BIG-IQ® system.
Sandbox object outside of the `/Common` partition	If partitions exist on the device in addition to the `/Common` partition, they contain sandbox objects by default. When the deployment process tries to create the sandbox objects, if the same partitions do not exist on the device, a critical error occurs and deployment fails.	On each BIG-IP device, create the same partitions. Then, redeploy on the BIG-IQ system.
Pools, pool members, self IPs, route domains	Access objects refer to pools, pool members, self IP addresses, and route domains, all of which are managed in ADC. If any of these objects is not present on the device, evaluation provides a warning that LTM® must be deployed before Access can be deployed. If the warning is ignored, Access deployment fails.	Deploy LTM. Then re-discover LTM before trying to deploy Access.

Managing Ongoing Change

How to manage ongoing configuration change

If you make changes on a BIG-IP® device before you have deployed the configuration from the BIG-IQ® system, configuration conflicts can occur. If conflicts do exist, when you deploy the configuration from the BIG-IQ system, you will have to choose between the configuration on the BIG-IQ or on the BIG-IP. You cannot keep both.

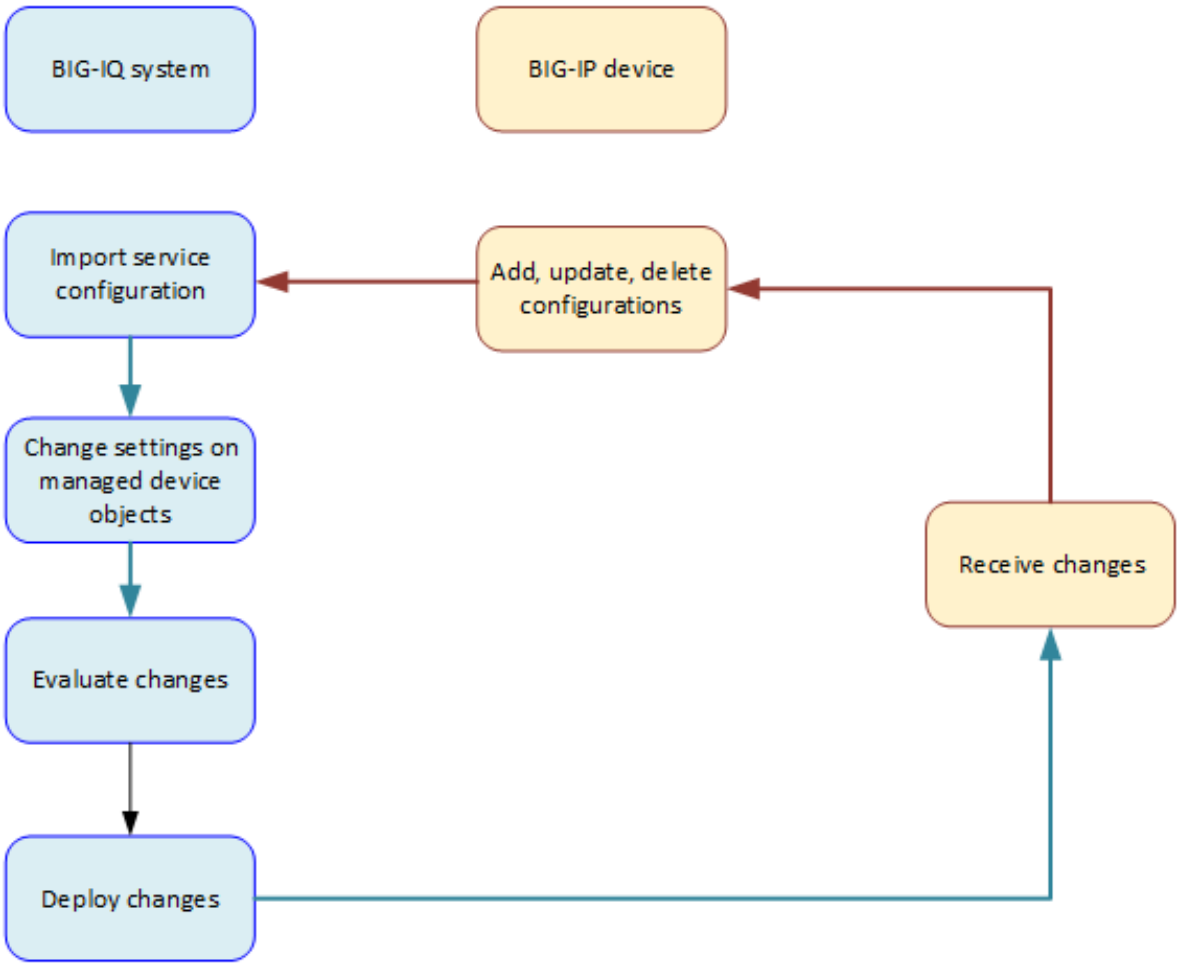


Figure 5: Ongoing change

How does re-import impact the device-specific resources?

When you re-import the APM® service configuration, the process adds and deletes any device-specific resources that were added and deleted on the device for the Access group. The process, however, does not overwrite any existing device-specific resources on the BIG-IQ® system.

Device-specific resources are processed like this whether you import the APM service configuration from the Device Management user interface.

Guidelines for making changes to the Access configuration

These are general guidelines for updating the configuration:

- You should make any needed change that you can from the Access user interface.
- If you still need to make changes, you should make them on the BIG-IP® device.

See the table for more specific guidelines.

Resource	Description
Access: Device-specific resource	• Modify device-specific resources on the BIG-IQ® system and deploy the changes. • Add or delete device-specific resources on the device; then re-import the service configuration into the BIG-IQ system.
Access: Shared resource	Add, modify, and delete shared resources on the device. Then re-import the service configuration into the BIG-IQ system.
Access: Pools and pool members	You can add and update pools and pool members when you configure some AAA servers in Access. Any changes you make are immediately available in ADC. To deploy these changes, you must deploy ADC before you deploy APM.
ADC: Pools and pool members	If you use ADC to add, update, or delete pools or pool members, you can create conflicts with the Access configuration. If you make changes in ADC, they are not available from Access.
ADC: Route domains and self-IP addresses	To add or edit route domains and self-IP addresses, do so in ADC. To make the changes available in Access, deploy the LTM® working configuration and then reimport the LTM configuration to the BIG-IQ system,
ADC: Virtual servers	Access configuration objects do not refer to virtual servers; however, you probably want to know how to configure them. You can add and edit virtual servers in ADC, but you can configure Access-specific settings, such as specifying an access profile, only on the BIG-IP system. You can add or edit virtual servers in either of these ways:

Resource	Description
	• Add or edit virtual servers in ADC. Deploy the LTM configuration to one or more devices. Edit Access-specific settings on the BIG-IP systems. Reimport the LTM configuration to the BIG-IQ system. • Add or edit a virtual server on the BIG-IP system. Reimport the LTM configuration.
ADC: iRule, nodes, interfaces, routes, VLANs, DNS resolvers	Access configuration objects do not refer to these objects directly. You do not need to worry about conflicts in the Access configuration.

Re-discovering and re-importing the APM service configuration

You can move any changes made to the Access Policy Manager® (APM®) service configuration on the device into the working configuration for the BIG-IQ® system.

Note: *When you use the* ***Reimport*** *option for an Access group, it re-discovers and re-imports the APM service configuration. It also detects whether changes were made to the LTM® service configuration and displays a message if you need to re-discover and re-import LTM first.*

1. At the top of the screen, select **Configuration**, then expand **ACCESS**and click **Access Groups** .
2. In the Access Groups list on the right, click the name of the Access group.
   The Properties screen displays.
3. Click **Reimport**.

   A confirmation message displays.

   Important: *Reimporting can cause major changes to the working configuration.*
4. To continue with re-discovery and re-import, click **Continue**.

The APM service configuration is imported. Importing the APM service configuration can change objects in the ADC configuration.

Re-discovering and re-importing the LTM service configuration

You can move any changes made to the Local Traffic Manager™ (LTM®) service configuration on the device into the working configuration for the BIG-IQ® system. You just re-discover and re-import the LTM service configuration.

Note: *If changes made to Local Traffic configuration objects in ADC dictate that you deploy LTM first, the system displays a message telling you to do that.*

1. At the top of the screen, click **Devices**.
2. Click the name of the device you want to discover a service configuration from.
3. On the left, click **Services**.
4. For Local Traffic (LTM), click **Re-discover**.
   If the current configuration on the BIG-IQ is different than the one on the BIG-IP® device, BIG-IQ displays a screen for you to resolve the conflicts.

5. If there are conflicts, select one of the following options for each object that is different, and then click the **Continue** button:
   - **Use BIG-IQ** to use the configuration settings stored on BIG-IQ.
   - **Use BIG-IP** to override the configuration setting stored on BIG-IQ with the settings from the BIG-IP device.
6. For Local Traffic (LTM), select the **Create a snapshot of the current configuration before importing.** check box to save a copy of the device's current configuration.

   You're not required to create a snapshot, but it is a good idea in case you have to revert to the previous configuration for any reason.
7. For Local Traffic (LTM), click **Re-import**.

The LTM service configuration is imported.

Managing Audit Logs in Access

About audit logs

You use audit logs to review changes in the BIG-IQ® system. All BIG-IQ system roles have read-only access to the audit log, and can view and filter entries. Any user with the appropriate privileges can initiate an action.

All API traffic on the BIG-IQ system, and every REST service command for all licensed modules, is logged in a separate, central audit log (`restjavad-audit.n.log`) which is located in `/var/log` on the BIG-IQ system.

Considerations when using the audit log

When using the audit log, consider the following:

- The audit log does not record an entry for every generation of a task. It only records an entry when the task status changes.
- When an object is deleted and then recreated with the same name, partition, and other information, the difference between those objects may show the deleted object as being the previous generation of the new object.
- By default, not all columns are displayed by the audit log to conserve space. To review what columns are displayed, click the gear icon in the upper right of the Audit Logging screen.

Actions and objects that generate audit log entries in Access

BIG-IQ® Centralized Management records in the audit log all user-initiated changes that occur on the management system. A change is defined as when certain objects are modified, when certain tasks change state, or when certain user actions are performed. For example, when the admin account is used to log in to the BIG-IQ system, the audit log records the time, the user (admin), the action (New) and the object type (Login). The log does not include changes that occurred on BIG-IP® devices that were imported.

Changes to working-configuration objects generate audit log entries. In addition, these actions generate log entries:

- Creating or deleting a user account.
- Users logging in and logging out, including when the user is logged out due to inactivity.
- Creating or cancelling a device discovery or a device reimport.
- Adding a new device to an access group.
- Creating or deleting an access group.
- Removing all services.
- Reimporting a device.
- Saving a configurable property in an existing device object.
- Stopping a session.
- Deleting a previously discovered device.
- Creating or deleting a deployment task.
- Creating a difference task.
- Creating, restoring, or deleting a snapshot.

- Editing some system information (such as editing a host name, a root password, a DNS entry, or an SNMP entry).

Audit log entry properties

The audit log displays the following properties for each log entry.

Property	Description
Source	IP address of the client machine that made the change. This property is blank for actions that were initiated by an internal process. For example, when a user invokes a deployment action, the deployment action then invokes a difference task to find the differences between the current configuration and the one to be deployed. The difference task has no Source IP address.
Time	Time that the event occurred. The time is the BIG-IQ system local time and is expressed in the format: mmm dd, yyyy hh:mm:ss (time zone); for example: `Apr 19, 2016 13:09:03(EDT)`.
User	Name of the account that initiated the action, such as an account named `Admin` for an administrative account.
Action	Type of modification. For operation changes, the action types include New, Delete, and Modify. For task changes, the action types include Start, Finish, Failed, and Cancelled.
Object Name	Object identified by a user-friendly name; for example: `newRule1`, `deploy-test`, or `Common/global`. When the name `RootNode` is listed, that indicates that the object is associated with a BIG-IP device. `RootNode` is typically seen when creating, deleting or updating log profiles, service policies, or firewall policies.
Changes	Indicates whether there was a change in the object. If **View** occurs in this column, there is a change to the object. To view the detailed differences of the change, click **View**.
Object Type	Classification for this action. When the type `Root Node` is listed, that indicates that the object is associated with a BIG-IP device. `Root Node` is typically seen when creating, deleting or updating log profiles, service policies, or firewall policies.
Parent Type	Class or group of the parent object.

Viewing audit entry differences

In the audit log, when potential changes to an object are logged, the **View** link is shown in the Changes column for that entry. You can click **View** to examine the differences between generations of that object.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **LOGS**, then expand **Audit Logs**, and then , click the component that you want to view audit entries for.
3. To display differences for an object, click **View** in the Changes column.

   A popup screen opens, showing two columns that compare the differences between the two generations of the object in JSON. In these columns, additions to an object generation are highlighted in green, and differences are highlighted in gold.

If the system cannot retrieve a generation of an object, the column displays either `Generation Not Available` or `Generation No previous generation`. Object information may not be available if it has been automatically purged from the system to conserve disk space, or if it has been deleted.

The JSON difference displayed for a delete entry in the audit log shows the JSON difference from the previous operation because the generation identifier is not incremented when an object is deleted.

4. When you are finished, click **Close** on the popup screen to return to the Audit Logging screen.

Filtering entries in the audit log

You can use the Filter field at the top right of the Audit Logging screen to rapidly narrow the scope displayed, and to more easily locate an entry in the audit log.

- Filtering is text-based.
- Filtering is not case-sensitive.
- You can use wild cards, or partial text.
- All BIG-IQ® roles can filter entries.
- To clear the filter, click the **X** to the right of the search string in the **Filtered by** field on the left.

1. At the top of the screen, click **Monitoring**.
2. On the left, expand **LOGS**, then expand **Audit Logs**, and then , click the component that you want to view audit entries for.
3. Use the Filter field in the upper right corner to narrow your search:
   a) Select the field that you want to specify filter options for.
   b) Type the information specific to the object you want to filter on.
   c) Select **Exact** if you want to view only logs that completely match the filtering content you typed. Or, if you want to view any logs that include the filtering content, select **Contains**.
   d) Press **Enter**.

Option	Description
All	Specifies that all objects should be filtered using the filter text. When this option is used, both the user-visible and the underlying data are searched for a match, so you may see matches to your filter text which do not appear to match it.
Client Address	For **Filter**, type the IP address of the device that generates the logs. Log entries from devices with a different IP address will not be displayed.
Time	Type both a date and a time. Displayed times are given in the local time of the BIG-IQ system. Supported time formats are highly Web browser-dependent. Time formats other than those listed might appear to filter successfully but are not supported. Entering a single date and time results in a filter displaying all entries from the specified date and time to the current date and time. For time formats that use letters and numbers, enter the date time in one of the following formats: • mmm dd yyyy hh:mm:ss. Example: `Jan 7 2014 8:30:00` • mmm dd, yyyy hh:mm:ss (time zone). Example: `Apr 28, 2016 13:09:03(EDT)` • mmm dd, yyyy. Example: `Apr 28, 2016` • mmm dd, yyyy hh:mm:ss. Example: `Apr 28, 2016 16:09:06` • ddd mmm dd yyyy hh:mm:ss. Example: `Thu Jan 16 2014 11:13:50`

Option	Description
	For time formats that use only numbers, enter the date time in one of the following formats: • mm/dd/yy hh:mm:ss. Example: `01/01/16 12:14:15` • m/d/yy hh:mm:ss. Example: `1/1/14 12:14:15` • mm/dd/yyyy hh:mm:ss. Example: `1/1/2014 12:14:15`
Node	Type the node name in the filter.
User	Type the user account name in the filter.
Action: Operation	Type the operation action name in the filter. Operation actions include: New, Delete, and Modify.
Action: Task Status	Type the task status action name in the filter. Task status actions include: Start, Finish, Cancelled, and Failed.
Object Name	Type the full or partial name of the object in the filter. If a partition name is displayed, do not include it in the filter. For example, Common/AddressList_4 would be entered as `AddressList_4`. Because the device-specific object name includes the BIG-IP® host name, you can enter a full or partial device name to get all objects for a specific BIG-IP device.
Object Type	Type the object type in the filter.
Parent	Type the parent name in the filter. Only appears for rules to show the rule list, firewall, or policy that contains the rule.
Parent Type	Type the Parent Type name in the filter. Only appears when the Parent field contains a value.
Contains	Specifies that the filter text is contained within the object specified. When you select **Contains**: • If the filter text is a string, the filter text matches an entire string or only a part of a string. • If the filter text is an IP address, the filter text matches an IPV4 or IPV6 address that is the same as the filter text, or matches an IPV4 address range or subnet that includes the filter text. IPV6 addresses can not be found within a range or subnet. • If the filter text is a port number, the filter text matches a port number that is the same as the filter text, or matches a port number range that includes the filter text.
Exact	Specifies that the filter text is exactly contained within the object specified. When **Exact** is selected: • If the filter text is a string, the filter text matches only the entire string. • If the filter text is an IP address, the filter text matches only an IPV4 or IPV6 address that is the same as the filter text. • If the filter text is a port number, the filter text matches only a port number that is the same as the filter text.

The result of a search filter operation is a set of entries that match the filter criteria, sorted by time.

Customizing the audit log display

You can customize the audit log display to assist you in locating information faster.

- To customize the order of columns displayed, click any column header and drag the column to the location you want.
- To sort by column, click the name of the column you want to sort. Not all columns can be sorted. When sorting items in the Object Name column, partition names are ignored. For example, the object name `Common/rule1` would be sorted without the common partition name, as if it were named `rule1`.
- To resize columns, click the column side and drag it to the preferred location.
- To select what columns are displayed, click the gear icon in the upper right of the Audit Logging screen. In the popup screen, select columns you want to display and clear columns you do not want to display. Move your cursor away from the screen to dismiss it.

Managing audit log archive settings

You can view or change the audit archive settings. The archived audit log files are stored in the `/var/config/rest/auditArchive/` directory on the BIG-IQ® system. You can view Access audit logs based on the following Access roles:

- Deployer.
- Editor.
- Viewer
- Manager.

You can view and configure Access archive settings with only the Access Manager role. The roles Auditor, Deployer, and Viewer cannot view or edit archive settings.

1. Log in to BIG-IQ Centralized Management system with Administrator or Security Manager credentials.
2. Select **Audit Logging** from the BIG-IQ menu.
3. Click the **Archive Settings** button in the upper left of the Audit Logging screen to display the audit log settings.
4. Complete or review the properties and status settings, and click **Save**.

Property	Description
Retain Entries	Specifies the number of days after the audit log entries are archived.
Weekly Update	Specifies which days of the week to update the audit log. Select the check box to the left of each day that you want the audit log to be updated. The default is every day.
Start Time	Specifies when the audit archiving should begin. The default is 12:00 am.
Items Expired	Displays the read-only number of entries that have expired.
Last Error	If an error has occurred, displays the read-only error text for any errors found.
Last Error Time	If an error has occurred, displays a read-only value that contains the time the last error was found. The time in the field is the BIG-IQ system local time and is expressed in the format: ddd mmm dd yyyy hh:mm:ss, for example, `Fri Jan 17 2014 23:50:00`.

About archived audit logs

You can view or change how audit logs are archived by clicking the **Archive Settings** button on the Audit Logging screen.

Archived audit log files are stored in the `archive-audit.n.txt` file in the appropriate subdirectory of the `/var/config/rest/auditArchive` directory on the BIG-IQ® Centralized Management system:

- Network Security audit log: `/var/config/rest/auditArchive/networkSecurity/`
- Web Application Security audit log: `/var/config/rest/auditArchive/webAppSecurity/`
- Fraud Protection Service audit log: `/var/config/rest/auditArchive/websafe/`
- Local Traffic and Network audit log: `/var/config/rest/auditArchive/adc/`
- Device Management audit log: `/var/config/rest/auditArchive/device/`
- Access audit log:`/var/config/rest/auditArchive/access/`

Audit entries are appended to the `archive-audit.0.txt` file. When the `archive-audit.0.txt` file reaches approximately 800 MB, the contents are copied to `archive-audit.1.txt`, compressed into the `archive-audit.1.txt.gz` file, and a new empty `archive-audit.0.txt` file is created, which then has new audit entries appended to it.

Up to five compressed archived audit files can be created before those files begin to be overwritten to conserve space. The compressed audit log archive is named `archive-audit.n.txt.gz`, where n is a number from 1 to 5. As the audit log archives are created and updated, the content of the archives is rotated so that the newest archive is always `archive-audit.1.txt.gz` and the oldest is always the highest numbered archive, typically, `archive-audit.5.txt.gz`.

The file content rotation occurs whenever `archive-audit.0.txt` is full. At that time, the content of each `rchive-audit.n.txt.gz` file is copied into the file with the next higher number, and the content of `archive-audit.0.txt` is copied into `archive-audit.1.txt` and then compressed to create `archive-audit.1.txt.gz`. If all five `archive-audit.n.txt.gz`files exist, during the rotation the contents of `archive-audit.5.txt.gz` are overwritten, and are no longer available.

About audit logs in high-availability configurations

In high-availability (HA) configurations, there is a primary and secondary BIG-IQ® system. During failover, the audit log entries and the audit archive settings are copied from the primary to the secondary system before the secondary system becomes the new primary system.

However, archived audit logs are not copied from the primary to the secondary BIG-IQ system.

About the REST API audit log

The REST API audit log records all API traffic on the BIG-IQ® system. It logs every REST service command for all licensed modules in a central audit log (`restjavad-audit.n.log`) located on the system.

Note: *The current iteration of the log is named `restjavad-audit.0.log`. When the log reaches a certain user-configured size, a new log is created and the number is incremented. You can configure and edit settings in `/etc/restjavad.log.conf`.*

Any user who can access the BIG-IQ system console (shell) has access to this file.

Managing the REST API audit log

The REST API audit log contains an entry for every REST API command processed by the BIG-IQ® system, and is an essential source of information about the modules licensed under the BIG-IQ system. It

can provide assistance in compliance, troubleshooting, and record-keeping. With it, you can review log contents periodically, and save contents locally for off-device processing and archiving.

1. Using SSH, log in to the BIG-IQ Access system with administrator credentials.
2. Navigate to the `restjavad` log location: `/var/log`.
3. Examine files with the naming convention: `restjavad-audit.n.log`.

   The letter *n* represents the log number.
4. Once you have located it, you can view or save the log locally through a method of your choice.

Reference

About iApps and Access

On a BIG-IP® system, a configuration that is created using an iApp can be updated only by using the same iApp. Access does not support iApps®. Access does not import, manage, or deploy resources that were created using an iApp.

Shared configuration resources

The tables list configurations that are shared or can be made shared.

Table 2: Access policies and related resources

Resource	Description
Policies	Access policies
Profiles	Properties for the session
CAPTCHA configurations	Specifies the CAPTCHA service
NTLM Auth Configuration	Used to authenticate Exchange applications

Table 3: AAA servers

Resource	Description
RADIUS*	RADIUS accounting and RADIUS authentication
LDAP*	LDAP and LDAPs authentication; LDAP queries
Active Directory*	Active Directory authentication and query
Active Directory Trusted Domains	Authenticate users across all trusted domains or forests for a customer
SecurID*	RSA SecurID authentication
HTTP*	HTTPS authentication; HTTP Basic/NTLM authentication
Oracle Access Manager*	Native integration with Oracle Access Manager
OCSP Responder*	Machine certificate revocation status; user certificate revocation status
CRLDP*	Retrieve Certificate Revocation Lists from network locations (Distribution Points)
TACACS+*	TACACS+ authentication and accounting
Kerberos*	Kerberos end-user login; basic or Kerberos authentication

Resource	Description
SAML*	External SAML Identity Provider for the BIG-IP® system, as a SAML service provider, to communicate with
Endpoint Management Systems*	Server properties *This resource is device-specific but can be made shared

Table 4: ACLs

Resource	Description
User-defined ACLs*	ACLs that users create
All ACLs*	The order of system-defined and user-defined ACLs *This resource is device-specific but can be made shared

Table 5: SSO Configurations

Resource	Description
HTTP Basic	Single sign-on (SSO) using cached user identity and authorization header
NTLMV1	Challenge-response; proves user identity without sending password to server
NTLMV2	Challenge-response; proves user identity without sending password to server
Kerberos	Transparent authentication of users to Windows Web application servers (IIS) joined to Active Directory domain
Forms	Detects start URL match and uses cached user identity to construct and send HTTP form-based post request on behalf of the user
Forms - Client Initiated	Detects login page request, puts generated JavaScript code into login page, and returns it to client, where it is automatically submitted by the inserted JavaScript
SAML	SAML local Identity Provider (IdP) service is a type of SSO service that BIG-IP, configured as an IdP, provides

Table 6: SAML

Resource	Description
Local SP Services	BIG-IP system as Service Provider (SP) provides SP services
External IdP Connectors	BIG-IP system as SP relies on external Identity Providers (IdPs) for authentication

Resource	Description
Local IdP Services	BIG-IP system as IdP provides SSO authentication services
External SP Connectors	BIG-IP system as IdP works with external SPs
Artifact Resolution Services*	Supports SAML artifacts on a BIG-IP system configured as a SAML IdP
BIG-IP IdP Automation	Supports configuration automation
SAML Resources	Resources to support the SAML configuration
	*This resource is device-specific but can be made shared

Table 7: Local User DB

Resource	Description
Manage Instances	Local user database instances

Table 8: Hosted Content

Resource	Description
Manage Files	Hosted content files
Manage Profile Access	Access control for hosted content files using access profiles

Table 9: Webtops

Resource	Description
Webtops	Webtop used in Portal Access or Network Access
Webtop Links	Links for inclusion on a webtop
Webtop Sections	Sections to organize content on a webtop

Table 10: Secure Web Gateway

Resource	Description
URL Categories	URL categories
URL Filters	URL filters
Applications	System-defined list of applications
Application Filters	User-defined application filters
Report Settings	Sets up statistics (for use with SWG subscription service)

Table 11: Network Access

Resource	Description
Network Access resource*	A Network Access resource allows user access to the local network through a secure VPN tunnel

Resource	Description
Lease Pools*	IPV4 or IPV6 lease pools associate a group of IP addresses with a Network Access resource
Client Traffic Classifiers*	Used to shape traffic for Network Access client connections from Windows
Client Rate Classes	Base and peak rates for traffic; associated with a client traffic classifier
	*This resource is device-specific but can be made shared

Table 12: Application Access

Resource	Description
App Tunnels*	Provide secure, application-level TCP/IP connections from a client to the network
Remote Desktops*	Allow users to access internal servers (Citrix, VMware View Connection, or Microsoft Remote Desktop) in virtual desktop sessions
VDI Profiles	Virtual desktop interface profile for a remote desktop configuration
Citrix Bundles	Hosted content used to deliver a Citrix Receiver client to a user's Windows computer
Microsoft Exchange	Profile for Microsoft Exchange application authentication
	*This resource is device-specific but can be made shared

Table 13: Portal Access

Resource	Description
Portal Access resources*	Provide user access to internal web applications with a web browser from outside the network
Rewrite profiles	An LTM profile treated as a shared resource
	*This resource is device-specific but can be made shared

Table 14: Resources that are not grouped in the user interface

Resource	Description
Per-Request Policies	Policies that run for requests made after a session is established
Secure Connectivity	Connectivity profile for remote access
Event Logs Settings	Log settings for APM, components within APM, and SWG

Table 15: Bandwidth Controllers

Resource	Description
Policies	A resource configured outside of APM at the system level and that is treated as a shared resource in Access.
Priority Groups	A resource configured outside of APM at the system level and that is treated as a shared resource in Access.

Device-specific configuration resources

Theses tables list device-specific resources.

Table 16: AAA servers

Resource	Description
RADIUS*	RADIUS accounting and RADIUS authentication
LDAP*	LDAP and LDAPs authentication; LDAP queries
Active Directory*	Active Directory authentication and query
SecurID*	RSA SecurID authentication
HTTP*	HTTPS authentication; HTTP Basic/NTLM authentication
Oracle Access Manager*	Native integration with Oracle Access Manager
OCSP Responder*	Machine certificate revocation status; user certificate revocation status
CRLDP*	Retrieve Certificate Revocation Lists from network locations (Distribution Points)
TACACS+*	TACACS+ authentication and accounting
Kerberos*	Kerberos end-user login; basic or Kerberos authentication
SAML*	External SAML Identity Provider for the BIG-IP® system, as a SAML service provider, to communicate with
Endpoint Management Systems*	Server properties
	*This resource is device-specific but can be made shared

Table 17: ACLs

Resource	Description
User-defined ACLs*	ACLs that users create
All ACLs*	The order of system-defined and user-defined ACLs

Resource	Description
	*This resource is device-specific but can be made shared

Table 18: SAML

Resource	Description
Artifact Resolution Services*	Supports SAML artifacts on a BIG-IP system configured as a SAML IdP *This resource is device-specific but can be made shared

Table 19: Network Access

Resource	Description
Network Access resource*	A Network Access resource allows user access to the local network through a secure VPN tunnel
Lease Pools*	IPV4 or IPV6 lease pools associate a group of IP addresses with a Network Access resource
Client Traffic Classifiers*	Used to shape traffic for Network Access client connections from Windows *This resource is device-specific but can be made shared

Table 20: Application Access

Resource	Description
App Tunnels*	Provide secure, application-level TCP/IP connections from a client to the network
Remote Desktops*	Allow users to access internal servers (Citrix, VMware View Connection, or Microsoft Remote Desktop) in virtual desktop sessions *This resource is device-specific but can be made shared

Table 21: Portal Access

Resource	Description
Portal Access resources*	Provide user access to internal web applications with a web browser from outside the network *This resource is device-specific but can be made shared

Table 22: Portal Access resources that can be device-specific or made shared

Resource	Description
Machine Account	For Microsoft Exchange clients that use NTLM authentication

Legal Notices

Legal notices

Publication Date

This document was published on April 14, 2017.

Publication Number

MAN-0615-02

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*.

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.

Index

A

B

C

D

E

H

I

L

M

O

P

R

S

T

U

V