F5® BIG-IQ® Centralized Management: Access

Version 5.4

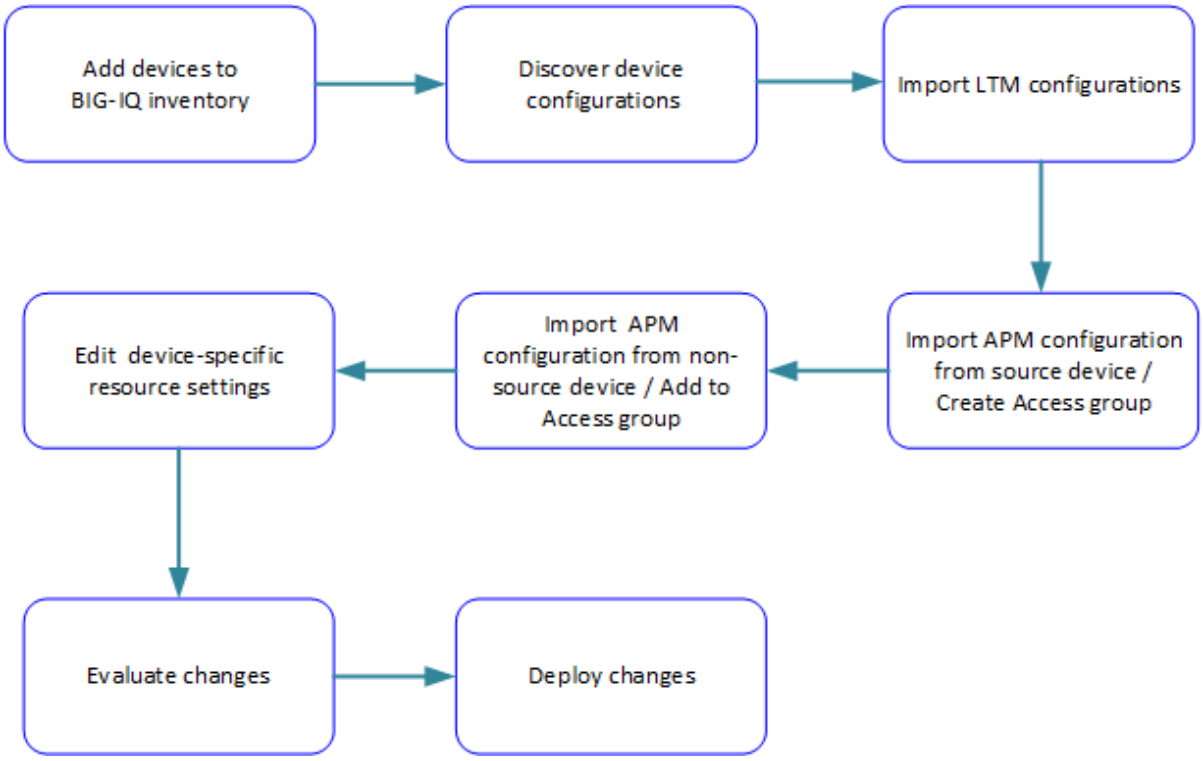
Table of Contents

BIG-IQ Centralized Management: Access Overview

About Access

Access in BIG-IQ® Centralized Management 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 lets you to compare and monitor BIG-IP APM® usage across many device groups.

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.

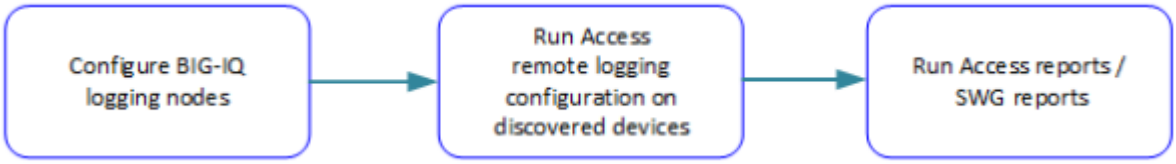
For example, an access policy could use an Active Directory server for user authentication. Device `apm_north_america.xyz.com` must use an Active Directory server configured in a North American domain or data center, while device `apm_south_america.xyz.com` must use an Active Directory server configured 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 Centralized Management from version 5.1

After upgrading from BIG-IQ® Centralized Management version 5.1 to version 5.2 or newer, send out a POST request to restore session data after an upgrade. Execute this command after restoring the elastic snapshot. If you do not perform this step, then after the upgrade, the sessions that you created before the upgrade displays incorrectly in either the Sessions report or in the Active Sessions report.

The command to send the post request is `restcurl -X POST -u admin:admin http://localhost:8100/mgmt/cm/access/reports/access-es-upgrade-task -d '{ }'`.

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. After creating a machine account, you can renew the machine account password.

Configuring a machine account

You configure a machine account so that Access can establish a secure channel to a domain controller.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** > **NTLM** and click **Machine Account** > **Create**.
   The New Machine Account screen displays.
5. In the **Name** field, type a name for the configuration..
6. From **Device**, select the associated BIG-IP device.
7. In the Configuration area, in the **Machine Account Name** field, type a name.
8. In the **Domain FQDN** field, type the fully qualified domain name (FQDN) for the domain that you want the machine account to join.
9. (Optional) In the **Domain Controller FQDN** field, type the FQDN for a domain controller.
10. In the **Admin User** field, type the name of a user who has administrator privilege.
11. In the **Admin Password** field, type the password for the admin user.

    Access uses these credentials to create the machine account on the domain controller. However, Access does not store the credentials and you do not need them to update an existing machine account configuration later.
12. Click **Join**.

This creates a machine account and joins it to the specified domain. This also creates a non-editable **NetBIOS Domain Name** field that is automatically populated.

Note: *If the* ***NetBIOS Domain Name*** *field on the machine account is empty, delete the configuration and recreate it. The field populates.*

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 Centralized Managment: Device" 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.
- The management address of the BIG-IP device must be open (typically this is port 22 and 443), or any alternative IP address used to add the BIG-IP device to the BIG-IQ inventory. Ports 22 and 443 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 a 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 version 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 the BIG-IP device 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

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 on the left side of the screen, click **ACCESS** > **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.

Note: *If you add a second device to an access group, the system does not automatically create sub-collections or pool members that are associated with a device-specific object. You must manually add or create these sub-collections or pool members.*

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **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**, select the check box **Create a snapshot of the current configuration before importing**.
6. Click **Add**.

The popup screen closes, displaying the Access Groups screen. The new device displays under the Devices list.

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 on the left side of the screen, click **ACCESS** > **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 on the left side of the screen, click **ACCESS** > **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 on the left side of the screen, click **ACCESS** > **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 discover at least one device. You must import the LTM® service configuration from a device before you can add that device to an Access group

You create an Access group to start managing 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 displays. 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 add an APM® device, you must discover at least one device with the APM® service. You must also import 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

Working with device-specific resources

Find, edit, and share device-specific resources with the Access module of BIG-IQ® Centralized Management.

Finding a device-specific resource

BIG-IQ® Centralized Management allows you to 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

BIG-IQ® Centralized Management allows you to can update the properties of a device-specific resource in the working configuration.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **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

BIG-IQ® Centralized Management allows you to 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 on the left side of the screen, click **ACCESS** > **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.

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 on the left side of the screen, click **ACCESS** > **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.

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.
    - NetTunnels Fec MUST be associated with Connectivity Profile in BIG-IQ, and deployed to other devices in Access Group.
- 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.
- Import SSL Keys and Certs
    - These are used in SAML configurations, SAML IdP connectors, OAM access gates, and OCSP responders.
- CA Profile
    - This is used in MachineCertAuthAgent.
    - Configure CA Profile in BIG-IP, import, and deploy to other devices in Access Group.
    - Associate CA Profile in "Machine Cert Auth" Agent either in BIG-IP or in BIG-IQ.
- SMTP Server
    - This is used in email agents.
    - Configure SMTP Server, and associate with Email Agent in policy in BIG-IP, import, and deploy to other devices in Access Group.
    - If you add the email agent to the access policy in BIG-IQ, create the SMTP Server in BIG-IQ if one does not exists and then choose it in the email agent.

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 on the left side of the screen, click **ACCESS** > **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 authorization.
13. For ADFS Proxy, select this check box to use this virtual server in an APM ADFS proxy configuration.

    For more information, see the "BIG-IP Access Policy Manager: Third-Party Integration" guide on the AskF5 web sites
14. From the **PingAccess Profile** list, select an already configured Ping Access Profile for authentication with a Ping Access policy server.
15. 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

LTM Object	Access Object
	• 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

About access policies

In an access policy, you define the criteria for granting access to various servers, applications, and other resources on your network. An access policy can be either a per-session policy or a per-request policy. You create an access policy by creating an access profile, which automatically creates a blank access policy. Every access profile has an access policy associated with it. You configure an access policy through the access profile, using the Visual Policy Editor.

About per-session and per-request policies

Access in BIG-IQ® Centralized Management provides two types of policies.

Per-session policy
The per-session policy runs when a client initiates a session. Depending on the actions you include in the access policy, it can authenticate the user and perform other actions that populate session variables with data for use throughout the session.

Per-request policy
After a session starts, a *per-request policy* runs each time the client makes an HTTP or HTTPS request. A per-request policy can include a subroutine, which starts a subsession. Multiple subsessions can exist at one time.

One per-session policy and one per-request policy are specified in a virtual server.

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 properties of the actions and the flow of actions in the 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 on the left side of the screen, click **ACCESS** > **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. Use the vertical and horizontal scrollbars to move to another section of the policy.
7. To save your changes, click the **Save** button.
8. To close the screen, click the **Close** button.

Create an access profile and per-session policy

You must create a access profile and its accompanying per-session policy before you can configure it in the 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 on the left side of the screen, click **ACCESS** > **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 **Per-Session Policies**.
   The Per-Session Policies (Shared) screen opens, displaying a list of access policies associated with this Access group.
5. Click **Create**.
   The New Access Policy screen opens.
6. In the **Name** field, type a name for the access profile.

Note: *A access profile name must be unique among all access profile and any per-request policy names.*

7. From the **Profile Type** list, select one these options:
   - **LTM-APM**: Select for a web access management configuration.
   - **SSL-VPN**: Select to configure network access, portal access, or application access. (Most access policy items are available for this type.)
   - **ALL**: Select to support LTM-APM and SSL-VPN access types.
   - **SSO**: Select to configure matching virtual servers for Single Sign-On (SSO).

     Note: *No access policy is associated with this type of access profile*
   - **RDG-RAP**: Select to validate connections to hosts behind APM when APM acts as a gateway for RDP clients.
   - **SWG - Explicit**: Select to configure access using Secure Web Gateway explicit forward proxy.
   - **SWG - Transparent**: Select to configure access using Secure Web Gateway transparent forward proxy.
   - **System Authentication**: Select to configure administrator access to the BIG-IP® system (when using APM as a pluggable authentication module).
   - **Identity Service**: Used internally to provide identity service for a supported integration. Only APM creates this type of profile.

     Note: *You can edit Identity Service profile properties.*

   Note: *Depending on licensing, you might not see all of these profile types.*

   Additional settings display.
8. From the **Scope** list, retain the default value or select another.
   - **Profile**: Gives a user access only to resources that are behind the same per-session profile. This is the default value.
   - **Virtual Server**: Gives a user access only to resources that are behind the same virtual server.
   - **Global**: Gives a user access to resources behind any per-session profile that has global scope.
9. In the Language Settings area, add and remove accepted languages, and set the default language. This setting does not display if the profile type is RDG-RAP

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
10. To save the profile and display the policy diagram, click the **Save & Close** button.

The policy name appears on the Per-Session Policies (Shared) screen.

Create a per-request policy

You must create a per-request policy before you can configure it in the 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 on the left side of the screen, click **ACCESS** > **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 **Per-Request Policies**.
   The Per-Request Policies (Shared) screen opens, displaying a list of access policies associated with this Access group.

5. Click **Create**.
   The Create per-req policy screen opens.
6. In the Name field, type a name for the policy and click **Save**.

   A per-request policy name must be unique among all per-request policy and access profile names.

The policy name appears on the Per-Request Policies (Shared) screen.

Editing an access policy

You can edit an existing access policy using the 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.
- Modifying any policy ending or macro terminal.

These actions can't be undone and also can't be undone if there are any pending diagram changes.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **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 diagram to the state before you made any changes to the diagram.
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**.

Adding a policy item

You can add a policy item using the 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 on the left side of the screen, click **ACCESS** > **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 the **Save** button.

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

Adding an action item or macro-call to a policy

You can modify an existing policy or sub-policy by adding additional action items and macro-calls. When modifying a policy, such as a macro, all diagram operations, insertions, deletions, modifications, and branch swaps are the same from the policy or sub-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 on the left side of the screen, click **ACCESS** > **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 macros that you can insert are in the Insertion dialog that displays when you click the + button.
6. Hover your cursor over a branch line between two items.
   An add icon (+) displays.
7. Click the icon **+**.
   The Item Insertion Selection popup screen opens.
8. From the Item Insertion Selection screen, select a macro or an action item.
   A new screen opens if you select an action item.
9. Fill in the relevant parameters and fields.
10. Click **Branch Rules**.
11. Click **Add**.
    The Branch Rules popup section displays more settings.
12. On the left, select either **Simple** or **Advanced** to create a branch rule configuration.

13. Fill in the relevant parameters and fields.
14. Click **OK**.
    The new branch rule displays in the Branch Rules screen.
15. Click the **Save** button.

    The **Save** button is only enabld if the form is valid.

The Access policy now includes the new action item.

Swapping policy branches

When examining the policy workflow, you can swap one branch with another. You swap branches as an easy way to change the policy workflow without deleting the existing branches and creating new ones. 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 on the left side of the screen, click **ACCESS** > **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 the **Save** button when you are done editing the policy.

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® Centralized Management 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.

Per-Session and per-request policy comparison

The table summarizes per-session policy and per-request policy similarities and differences.

Feature	Per-Session policy	Per-request policy
Supports macros	Yes	Yes
Requires that users click an Apply Access Policy link to go into effect.	Yes	No
When run	At session start.	After session is created, on every request.
Policy ending types	Allow, Deny, Redirect; endings apply to the session.	Allow, Redirect, Reject; endings apply to URL requests processed in the per-request policy. A Reject ending triggers the Deny ending in the access policy.
Supports variables	Creates session variables that are available throughout a session.	Reads available session variables. Creates per-flow variables that are available only while the per-request policy runs.

About access policy endings

An ending provides a result for an access policy branch. An ending for an access policy branch is one of three types.

Allow
Starts the SSL VPN session and loads assigned resources and a webtop, if assigned, for the user. Typically, you assign this when the user passes specific checks.

Deny
Disallows the SSL VPN session and shows the user an access denied web page. Typically, you assign this when the user does not have access to resources, or fails authentication. Alternatively after a session starts, shows a URL filter denied web page after a per-session policy rejects a request for a URL.

Redirect
Redirects the client to the URL specified in the ending configuration. You can define a redirect URL for each redirect ending. Typically, you can assign a redirect when the user requires remediation, or a separate resource. For example, a user who fails the antivirus check because virus definitions are out of date can be redirected to the software manufacturer's site to get an antivirus update.

What is a terminal?

A terminal is a sub-policy ending in an access policy. Differing from a policy ending, terminals do not have types and you can re-order them. The order of a terminal in a sub-policy determines the order of the branches in the macro-calls. Similar to policy endings, you can't create, change, or delete a terminal if there are pending changes in the policy.

Creating a policy ending

Every branch in a workflow has one of three policy endings: 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. Alternatively, you can assign an ending as the default ending.

Note: *Creating a policy ending 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 on the left side of the screen, click **ACCESS** > **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)** .
   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 a policy ending

You can edit a policy ending 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 on the left side of the screen, click **ACCESS** > **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 a policy ending

You can delete any policy ending 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 on the left side of the screen, click **ACCESS** > **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.

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 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.*

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 on the left side of the screen, click **ACCESS** > **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.

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. Log in to F5® BIG-IQ® Centralized Management with your user name and password.
2. At the top left of the screen, select **Change Management** from the BIG-IQ menu.
3. Under **SNAPSHOT & RESTORE**, select **Access**.
   The screen displays a list of Access snapshots that have been created on this device.
4. Select the check box to the left of the snapshot that you want to use as the source snapshot.
5. Click the **Compare** button.
   The Differences screen opens.
6. Analyze the configuration differences between the snapshot and the comparison target. When you are finished, click **Cancel** to close the Differences screen, and then click **Close**.
   The screen closes and you return to the Snapshot screen.

Authentication and Single Sign-On

About AAA server support

Access in BIG-IQ® Centralized Management interacts with authentication, authorization, and accounting (AAA) servers that contain user information. Access supports the following AAA servers:

- RADIUS (authentication and accounting)
- LDAP (authentication and query)
- Active Directory (authentication and query)
- SecurID
- HTTP
- Oracle Access Manager
- OCSP Responder
- CRLDP
- TACACS+ (authentication and accounting)
- Kerberos (authentication and authorization)

A typical configuration includes:

- An AAA server configuration object that specifies information about the external AAA server.
- An access policy that includes a logon item to obtain credentials and an authentication item that uses the credentials to authenticate against a specific AAA server.

Note: *For more information, refer to the BIG-IP Access Policy Manager: Authentication and Single Sign-On guide.*

About RADIUS authentication

BIG-IQ® Access supports authenticating and authorizing the client against external RADIUS servers. When a client connects with the user name and password, BIG-IQ Access authenticates against the external server on behalf of the client, and authorizes the client to access resources if the credentials are valid.

Configure a RADIUS AAA server

You create a RADIUS AAA server to authenticate and authorize a client with a valid user name and password.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **RADIUS**.
5. From either RADIUS (Shared) or RADIUS (Device-Specific), click **Create**.
   The New RADIUS screen displays
6. In the **Name** field, type a unique name for the authentication server.

7. From **Device**, select the associated BIG-IP device. This only displays when you create a device-specific RADIUS server.
8. For the **Mode** setting, select **Authentication**, **Accounting**, or **Authentication & Accounting**.
9. For **Authentication Service Port**, type the authentication port number of your server. The default is `1812`.
10. For the **Server Connection** setting, select one of these options:
    - Select **Use Pool** to set up high availability for the AAA server.
    - Select **Direct** to set up the AAA server for standalone functionality.
11. If you selected **Use Pool**, type a name in the **Server Pool Name** field.

    You create a pool of servers on this screen.
12. Provide the addresses required for your server connection:
    - If you selected **Direct**, type an IP address in the **Server Address** field.
    - If you selected **Use Pool**, for each pool member you want to add, type an IP address in the **Server Addresses** field and click **Add**.

    Note: *When you configure a pool, you have the option to type the server address in route domain format:* `IPAddress%RouteDomain`.
13. From the **Server Pool Monitor** dropdown menu, select a monitor to track the health of your AAA RADIUS server.
14. In the **Secret** field, type the shared secret password of the server.
15. In the **Confirm Secret** field, re-type the shared secret password of the server.
16. For **NAS IP Address**, type an an IP address as a RADIUS attribute 4, NAS-IP-address, that you can configure without changing the source IP address in the IP header of the RADIUS packets.
17. For **NAS IPV6 Address**, type an IPV6 address as a RADIUS attribute 4, NAS-IP-address, that you can configure without changing the source IP address in the IP header of the RADIUS packets.
18. For **NAS Identifier**, type a string that identifies the NAS that originates the Access-Request.
19. For **Timeout**, type the interval of time, in seconds, to wait for a response from the RADIUS AAA server before timing out. The default is `5`.
20. For **Retries**, type the number of times the BIG-IP system tries to make a connection to the RADIUS AAA server after the first attempt fails. The default is `3`.
21. From the **Character Set** dropdown menu, select the character encoding for the username and password.
    - **Windows-1252** - APM RADIUS Auth agent decodes the username and password into CP-1252 before sending it to the RADIUS server. This is the default.
    - **UTF-8** - RADIUS Auth sends the username and password unmodified.
22. From the **Service Type** dropdown menu, select the type of service used for the RADIUS server. f you retain **Default**, the service type is set to **Authenticate Only**.
23. Click **Save**.

The new AAA server displays on the RADIUS list.

About LDAP authentication

Use BIG-IQ Access to configure an LDAP AAA server You can use LDAPS in place of LDAP when the authentication messages between BIG-IP APM and the LDAP server must be secured with encryption. However, there are instances where you will not need LDAPS and the security it provides. For example, authentication traffic happens on the internal side of Access, and might not be subject to observation by

unauthorized users. Another example of when not to use LDAPS is when authentication is used on separate VLANs to ensure that the traffic cannot be observed by unauthorized users.

LDAPS is achieved by directing LDAP traffic over a virtual server that uses server side SSL to communicate with the LDAP server. Essentially, the system creates an LDAP AAA object that has the address of the virtual server. That virtual server (with server SSL) directs its traffic to a pool, which has as a member that has the address of the LDAP server.

Configure an LDAP AAA server

You create an LDAPS AAA server when you need to encrypt authentication messages between Access and the LDAP server.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **LDAP**.
5. From either LDAP (Shared) or LDAP (Device-Specific), click **Create**.
   The New LDAP screen displays
6. In the **Name** field, type a unique name for the authentication server.
7. From **Device**, select the associated BIG-IP device. This only displays when you create a device-specific LDAP server.
8. For the **Server Connection** setting, select one of these options:
   - Select **Use Pool** to set up high availability for the AAA server.
   - Select **Direct** to set up the AAA server for standalone functionality.
9. If you selected **Use Pool**, type a name in the **Server Pool Name** field.

   You create a pool of servers on this screen.
10. Provide the addresses required for your server connection:
    - If you selected **Direct**, type an IP address in the **Server Address** field.
    - If you selected **Use Pool**, for each pool member you want to add, type an IP address in the **Server Addresses** field and click **Add**.

    Note: *When you configure a pool, you have the option to type the server address in route domain format:* `IPAddress%RouteDomain`.

    ---
11. From the **Server Pool Monitor** dropdown menu, select a monitor to track the health of your AAA RADIUS server.
12. For the **Mode** setting, select **LDAP** or **LDAPS**.
13. For the **Service Port** setting, accept the default or type the port number of your AAA server. The default is `389` for LDAP and `636` for LDAPS.
14. For **Base Search DN**, type a base distinguished name from which to search.
15. In the **Admin DN** field, type the distinguished name (DN) of the user with administrator rights.

    Type the value in this format:
    `CN=administrator,CN=users,DC=sales,DC=mycompany,DC=com`.
16. In the **Admin Password** field, type the administrative password for the server.
17. In the **Verify Admin Password** field, re-type the administrative password for the server.
18. For **Group Cache Lifetime**, type the lifetime of a group cache. The default lifetime is 30 days.

19. For **SSL Profile (Server)**, select your SSL server profile from the list. LDAPS is achieved by directing LDAP traffic over a virtual server that uses a server side SSL to communicate with the LDAP server. This only displays for LDAPS.
20. For **Timeout**, type the number of seconds to reach the LDAP server initially. Accept the default (`15`) or type a number.
21. To save your changes, click the **Save & Close** button at the bottom of the screen.

The new AAA server displays on the LDAP servers list.

About Active Directory authentication

Use BIG-IQ Access to configure an Active Directory AAA server. You can authenticate using Active Directory authentication with BIG-IQ Access, which supports using Kerberos-based authentication through Active Directory.

Configure an Active Directory AAA server

You configure an Active Directory AAA server to specify domain controllers for Access to use for authenticating users.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **Active Directory**.
5. From either Active Directory (Shared) or Active Directory (Device-Specific), click **Create**.
   The New Active Directory screen displays
6. In the **Name** field, type a unique name for the authentication server.
7. From **Device**, select the associated BIG-IP device. This only displays when you create a device-specific Active Directory server.
8. In the **Domain Name** field, type the name of the Windows domain.
9. For the **Server Connection** setting, select one of these options:
   - Select **Use Pool** to set up high availability for the AAA server.
   - Select **Direct** to set up the AAA server for standalone functionality.
10. If you selected **Direct**, type a name in the **Domain Controller** field.
11. If you selected **Use Pool**, configure the pool:
    a) Type a name in the **Domain Controller Pool Name** field.
    b) Specify the **Domain Controllers** in the pool by typing the IP address and host name for each, and clicking the + button.
    c) To monitor the health of the AAA server, you have the option of selecting a health monitor. You can select it from the **Server Pool Monitor** list.
12. In the **Admin Name** field, type a case-sensitive name for an administrator who has Active Directory administrative permissions.

    An administrator name and password are required for an AD Query access policy item to succeed when it includes particular options. Credentials are required when a query includes an option to fetch a primary group (or nested groups), to prompt a user to change password, or to perform a complexity check for password reset.
13. In the **Admin Password** field, type the administrator password associated with the Domain Name.

14. In the **Verify Admin Password** field, retype the administrator password associated with the **Domain Name** setting.
15. In the **Group Cache Lifetime** field, type the number of days.

    The default lifetime is 30 days.
16. In the **Password Security Object Cache Lifetime** field, type the number of days.

    The default lifetime is 30 days.
17. From the **Kerberos Preauthentication Encryption Type** list, select an encryption type.

    The default is **None**. If you specify an encryption type, the BIG-IP® system includes Kerberos preauthentication data within the first authentication service request (AS-REQ) packet.
18. In the **Timeout** field, accept the default value or type a number of seconds.

    The timeout specifies the number of seconds to reach the AAA Active Directory server initially. After the connection is made, the timeout for subsequent operations against the AAA Active Directory server is 180 seconds and is not configurable.
19. Click **Save**.

The new AAA server displays on the Active Directory servers list.

About SecurID authentication

RSA SecurID is a two-factor authentication mechanism based on a one-time passcode (OTP) that is generated by using a token code provided by a software or hardware authenticator. A token is a one-time authentication code generated every 60 seconds by an authenticator (hardware or software) assigned to the user.

Configure a SecurID AAA server

You create a SecurID server for AAA authentication to request RSA SecurID authentication from an RSA Manager authentication server.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **SecurID**.
5. Click **Create**.
   The New SecurID screen displays
6. In the **Name** field, type a unique name for the authentication server.
7. From **Device**, select the associated BIG-IP device.
8. In the Configuration area, for the **Agent Host IP Address (must match the IP address in SecurID Configuration File)** setting, select an option as appropriate:
   - **Select from Self IP List**: Choose this when there is no NAT device between APM and the RSA Authentication Manager. Select an IP from the list of those configured on the BIG-IP® system (in the Network area of the Configuration utility).
   - **Other**: Choose this when there is a NAT device in the network path between Access Policy Manager and the RSA Authentication Manager server. If selected, type the address as translated by the NAT device.

Note: *This setting does not change the source IP address of the packets that are sent to the RSA SecurID server. (Layer 3 source addresses remain unchanged.) The agent host IP address is used only in Layer 7 (application layer) information that is sent to the RSA SecurID server.*

9. For **File Name**, browse to upload the configuration file from the RSA SecurID console.

   Consult your RSA Authentication Manager administrator to generate this file for you.
10. Click **Save**.

The new AAA server displays on the SecurID servers list.

About HTTP authentication

An HTTP AAA server directs users to an external web-based server to validate credentials. BIG-IQ Access supports these HTTP authentication types:

- HTTP form-based authentication - Directs users to a form action URL and provides the specified form parameters
- HTTP basic authentication - Directs users to a URI
- HTTP NTLM authentication - Directs users to a URI
- HTTP custom post - Directs users to a POST URL, a submit URL, or a relative URL and provides the specified content

Tip: *Use HTTPS instead of HTTP authentication for improved security, because HTTP authentication passes user credentials as clear text.*

Configuring an HTTP server for form-based authentication

You create a form-based HTTP AAA configuration to use HTTP form-based authentication from an 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 on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **HTTP**.
5. From either HTTP (Shared) or HTTP (Device-Specific), click **Create**.
   The New HTTP screen displays
6. In the **Name** field, type a unique name for the authentication server.
7. From **Device**, select the associated BIG-IP device. This only displays when you create a device-specific HTTP server.
8. For **Authentication Type**, select `Form-Based`.
9. In the **Start URI** field, type the complete URI that returns the logon form.

   The URI resource must respond with a challenge to a non-authenticated request.
10. Click **Save**.

The new HTTP server, configured for form-based authentication, displays on the HTTP servers list.

To put this authentication into effect, add this AAA server to an HTTP Auth action in an access policy.

Configuring an HTTP server for Basic/NTLM authentication

You configure an HTTP AAA server when you want to use Basic/NTLM authentication.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **HTTP**.
5. From either HTTP (Shared) or HTTP (Device-Specific), click **Create**.
   The New HTTP screen displays
6. In the **Name** field, type a unique name for the authentication server.
7. From **Device**, select the associated BIG-IP device. This only displays when you create a device-specific HTTP server.
8. For **Authentication Type**, select `Basic/NTLM`.
9. (Optional) In the **Start URI** field, type a URI, for example, `http://plum.tree.lab2.sp.companynet.com/`.

   This resource must respond with a challenge to a non-authenticated request.

   Note: *This field is optional. If you type a URI in this field and you type a relative URL in the* ***Form Action*** *field, Access Policy Manager® (APM®) uses the value of the* ***Start URI*** *as the base URL; APM uses the base URL to resolve the relative URL and produce the final URL for HTTP POST.*

   ---

10. From the **Form Method** list, select either **GET** or **POST**.

    If you specify **GET**, the authentication request converts as HTTP GET.
11. In the **Form Action** field, type a URL that specifies where to process the form and perform form-based authentication. If you specified a **Start URI**, you can type a relative URL, otherwise you must type an absolute URL:
    - relative URL - When specified, form-based authentication is performed after the URL is resolved using the base URL that is specified in the **Start URI** field.
    - absolute URL -When specified, form-based authentication is performed at this URL.
12. In the **Form Parameter For User Name** and **Form Parameter For Password** fields, type the parameter name and password used by the form to which you are sending the POST request.
13. In the **Hidden Form Parameters/Values** field, type the hidden form parameters required by the authentication server logon form at your location.

    You must provide hidden form parameters and values if there are any. When present, these values are required by the authentication server logon form at your location.

    Specify a parameter name, a space, and the parameter value, if any. Start each parameter on a new line. If you use a session variable as a value, format it as shown in this example: `%{session.client.platform}`.
14. In the **Number Of Redirects To Follow** field, type how far from the landing page, in pages, the request should travel before failing.
15. For the **Successful Logon Detection Match Type** setting, select the method your authenticating server uses, and type the option definition in the **Successful Logon Detection Match Value** field.
16. Click **Save**.

The new HTTP server, configured for Basic/NTLM authentication, displays on the HTTP servers list.

To put this authentication into effect, add this AAA server to an HTTP Auth action in an access policy.

Configure an HTTP server for custom post authentication

You create a custom post configuration when there is no form and when body encoding is different from form encoding. (This can happen when POST is generated by JavaScript or ActiveX.) Using a custom post, you can specify the entire post body and any non-default HTTP headers.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **HTTP**.
5. From either HTTP (Shared) or HTTP (Device-Specific), click **Create**.
   The New HTTP screen displays
6. In the **Name** field, type a unique name for the authentication server.
7. From **Device**, select the associated BIG-IP device. This only displays when you create a device-specific HTTP server.
8. For **Authentication Type**, select `Custom Post`.
9. In the **Start URI** field, type in a URL resource, for example, `http://plum.tree.lab2.sp.companynet.com/`.

   If you do not specify a Start URI, Access Policy Manager® will likely detect that the absolute URI based on the Form Action parameter should be used for HTTP POST. If you specify a Start URI, Access Policy Manager uses both the Start URI and the Form Action parameters as the final URL for HTTP POST.
10. In the **Form Action** field, type the POST URL, the submit URL, or a relative URL.
11. For the **Successful Logon Detection Match Type** setting, select the method that the authenticating server uses.
12. For the **Successful Logon Detection Match Value**, type a value depending on the **Successful Logon Detection Match Type** that you selected:
    - **By Resulting Redirect URL** - Specify a URL if you selected this type.
    - **By Presence of Specific String in Cookie** - Specify a single string if you selected this type.

      Note: *With this option, when APM® receives a duplicate cookie, it adds it to the existing cookie list. As a result, multiple cookies with the same name, domain, and path can exist and can be searched.*
    - **By Presence of Cookie That Exactly Matches** - Specify the exact key fields (name, path, and domain) that are present in the HTTP response cookie if you select this type. Failure to supply the exact number of keys and the exact values for the HTTP response cookie results in a `No matching cookie found` error.

      Note: *This option supports cookie merge functionality. When APM receives a cookie that has the same name, domain, and path as an existing cookie, it merges it into the existing cookie.*
    - **By Specific String in Response** - Specify a string if you select this option.
13. In the **Number Of Redirects To Follow** field, type how far from the landing page, in pages, the request should travel before failing.
14. From the **Content Type** list, select an encoding for the HTTP custom post.

    The default setting is **XML UTF-8**.

***Note:** If you select **None**, you must add a header in the **Custom Headers** setting and you must apply your own encoding through an iRule.*

15. In the **Custom Body** field, specify the body for the HTTP custom post.
16. For **Custom Headers**, specify names and values for header content to insert in the HTTP custom post.
17. Click **Save**.

The new HTTP server, configured for custom post authentication, displays on the HTTPs servers list.

To put this authentication into effect, add this AAA server to an HTTP Auth action in an access policy.

About Oracle Access Manager integration with Access

You can configure only one AAA Oracle Access Manager (OAM) server, but it can support multiple AccessGates from the same Access server. When you create a AAA OAM server, its transport security mode must match the setting in the OAM access server.

Configure an OAM AAA server

You create an OAM server for AAA authentication to deploy Access in place of OAM 10g WebGates.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **Oracle Access Manager**.
5. From either Oracle Access Manager (Shared) or Oracle Access Manager (Device-Specific), click **Create**.
   The New Oracle Access Manager screen displays
6. In the **Name** field, type a unique name for the authentication server.
7. From **Device**, select the associated BIG-IP device. This only displays when you create a device-specific Oracle Access Manager server.
8. For **Access Server Name**, type the name that was configured in Oracle Access System for the access server.

   For the access server name, open the OAM Access System Console and select **Access system configuration** > **Access Server Configuration**.
9. For **Access Server Hostname**, type the fully qualified DNS host name for the access server system.
10. For **Access Server Port**, accept the default `6021`, or type the port number.

    For earlier versions of OAM, the default server port is `6021`. For later versions, the default server port is `5575`.
11. For **Admin Id**, type the admin ID.

    Admin Id and Admin Password are the credentials that are used to retrieve host identifier information from OAM. Usually, these are the credentials for the administrator account of both Oracle Access Manager and Oracle Identity Manager.
12. For **Admin Password**, type the admin password.
13. For **Verify Password**, retype the password.
14. For **Retry Count**, accept the default 0, or enter the number of times an AccessGate should attempt to contact the access server.

15. For **Transport Security Mode**, select the mode (open, simple, or cert) that is configured for the access server in Oracle Access System.
16. If Transport Security Mode is set to simple, type and re-type a **Global Access Protocol Passphrase**; it must match the global passphrase that is configured for the access server in OAM.
17. For **AccessGate Name**, type the name of an AccessGate; it must match the name of an AccessGate that is configured on the OAM access server.
18. For **AccessGate Password** and **Verify Password**, type the password; it must match the password that is configured for it on the OAM access server.
19. If transport security mode is set to cert, select the **Certificate**, **Key**, and **CA Certificate** that you imported for this particular AccessGate.
20. If transport security mode is set to cert and if a sign key passphrase is needed, type a **Sign Key Passphrase** and re-type it to verify it.
21. Click **Save**.

This adds the new AAA server to the AAA Servers list.

Add any other AccessGates that are configured for the OAM access server to this Oracle Access Manager AAA server. Then, for each AccessGate, configure a virtual server and enable OAM support on it for native integration with OAM.

About OCSP authentication

BIG-IQ Centralized Management supports authenticating a client using Online Certificate Status Protocol (OCSP). OCSP is a mechanism used to retrieve the revocation status of an X.509 certificate by sending machine or user certificate information to a remote OCSP responder. This responder maintains up-to-date information about the certificate's revocation status. OCSP ensures that the BIG-IQ system always obtains real-time revocation status during the certificate verification process.

Configure an OCSP responder

You create an OCSP responder for AAA authentication when you want to obtain revocation status for a user or machine certificate as part of your access control strategy.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **OCSP Responder** .
5. From either OCSP Responder (Shared) or OCSP Responder (Device-Specific), click **Create**.
   The New OCSP Responder screen displays
6. In the **Name** field, type a unique name for the authentication server.
7. From **Device**, select the associated BIG-IP device. This only displays when you create a device-specific OCSP Responder server.
8. From the **Configuration** list, select **Basic** or **Advanced**.
9. In the **URL** field, type the URL used to contact the OCSP service on the responder.

   You can skip this step if you did not select the **Ignore AIA** check box and all users have certificates with the correct AIA structure. (The **Ignore AIA** option is available when you select **Advanced** from the **Configuration** list; it is disabled by default.)
10. (Optional) From the **Certificate Authority File** list, select an SSL certificate.
11. If you selected **Advanced** from the **Configuration** list, do the following steps.

12. From the **Verify Other** list, select the name of the file to use to search for an OCSP response signing certificate when the certificate has been omitted from the response.
13. From the **VA File** list, select the name of the file that contains explicitly-trusted responder certificates.

    This parameter is required in the event that the responder is not covered by the certificates already loaded into the responder's CA store.
14. From the **Signer** list, select the name of the certificate used to sign an OCSP request and then from the Sign Key list, select the key used to sign an OCSP request, and, in the Sign Key Pass Phrase and Verify Sign Key Pass Phrase fields, type the key used to sign an OCSP request.

    If you specify a certificate, but not a key, the system reads the private key from the same file as the certificate. However, if you specify neither the certificate nor the key, then the request is not signed. Lastly, if you do not specify the certificate and you specify the key, then the configuration is considered to be invalid.
15. From the **CertID Digest** list select an algorithm to use to convert the client certificate and its issuer certificate to an OCSP cert ID.

    The cert ID is added to the OCSP request.
16. Click **Save**.
17. In the **Validity Period** field, type the number of seconds for the BIG-IP system to use in specifying an acceptable error range.

    The BIG-IP system uses this setting when the OCSP responder clock and a client clock are not synchronized to prevent a certificate status check from failing.
18. In the **Status Age** field, type the number of seconds to compare to the notBefore field of a status response.

    The system uses this parameter when the status response does not include the notAfter field.
19. To save your changes, click the **Save & Close** button at the bottom of the screen.

This adds the new OCSP responder to the OCSP list.

You can select this OCSP responder from an OCSP Auth access policy item.

About CRLDP authentication

BIG-IQ Centralized Management supports retrieving Certificate Revocation Lists (CRLs) from network locations (distribution points). A Certificate Revocation List Distribution Point (CRLDP) AAA server defines how to access a CRL file from a distribution point. A distribution point is either an LDAP Uniform Resource Identifier (URI), a directory path that identifies the location where the CRLs are published, or a fully qualified HTTP URL.

Configure a CRLDP AAA server

You create a CRLDP server for AAA authentication to determine how to access certificate revocation lists (CRLs).

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **CRLDP**.
5. From either CRLDP (Shared) or CRLDP (Device-Specific), click **Create**.
   The New CRLDP screen displays
6. In the **Name** field, type a unique name for the authentication server.

7. From **Device**, select the associated BIG-IP device. This only displays when you create a device-specific CRLDP server.
8. For the **Server Connection** setting, select one of these options:
   - Select **Use Pool** to set up high availability for the AAA server.
   - Select **Direct** to set up the AAA server for standalone functionality.
   - Select **No Server** to use a fully qualified HTTP URL as the CRL location.

   Note: *The ®BIG-IP system uses the URI from the user's certificate.*

   Note: *When you select **No Server**, the screen updates to omit the fields that are not necessary, such as **Server Addresses**, **Server Port**, and so on.*
9. If you selected **Use Pool**, type a name in the **Server Pool Name** field.

   You create a pool of servers on this screen.
10. Provide the addresses required for your server connection:
    - If you selected **Direct**, type an IP address in the **Server Address** field.
    - If you selected **Use Pool**, for each pool member you want to add, type an IP address in the **Server Addresses** field and click **Add**.

      Note: *When you configure a pool, you have the option to type the server address in route domain format:* `IPAddress%RouteDomain`.
11. If you selected **Use Pool**, you have the option to select a **Server Pool Monitor** to track the health of the server pool.
12. If you specified **Use Pool** or **Direct** for the server connection, the **Base DN** field displays; type a CRLDP base distinguished name into it.

    This setting applies for certificates that specify the CRL distribution point in directory name (dirName) format. Access Policy Manager® uses the Base DN when the value of the X509v3 attribute, `crlDistributionPoints`, is of type `dirName`. In this case, Access Policy Manager tries to match the value of the crlDistributionPoints attribute to the Base DN value. An example of a Base DN value is `cn=lxxx,dc=f5,dc=com`.

    Note: *If the client certificate includes the distribution point extension in LDAP URI format, the IP address, Base DN, and Reverse DN settings configured on the agent are ignored; they are specific to directory-based CRLDP. All other settings are applicable to both LDAP URI and directory-based CRL DPs.*
13. Click **Save**.

This adds the new CRLDP server to the CRLDP Servers list.

A CRLDP AAA server is available for use in a CRLDP Auth agent in an access policy.

About TACACS+ authentication

BIG-IQ Centralized Management supports authenticating and authorizing the client against Terminal Access Controller Access Control System (TACACS+) servers. TACACS+ is a mechanism used to encrypt the entire body of the authentication packet. If you use TACACS+ authentication, user credentials are authenticated on a remote TACACS+ server. If you use the TACACS+ Accounting feature, the accounting service sends `start` and `stop` accounting records to the remote server.

The Access feature of BIG-IQ supports TACACS+ authentication with the TACACS+ Auth access policy item and supports TACACS+ accounting with the TACACS+ Acct access policy item.

Note: *The BIG-IQ system must include a TACACS+ server configuration for every TACACS+ server that exists.*

Configure a TACACS+ AAA server

You create a TACACS+ AAA server to authenticate user credentials on a remote TACACS+ server.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **TACACS+**.
5. From either TACACS+ (Shared) or TACACS+ (Device-Specific), click **Create**.
   The New TACACS+ screen displays
6. In the **Name** field, type a unique name for the authentication server.
7. From **Device**, select the associated BIG-IP device. This only displays when you create a device-specific TACACS+ server.
8. For the **Server Connection** setting, select one of these options:
   - Select **Use Pool** to set up high availability for the AAA server.
   - Select **Direct** to set up the AAA server for standalone functionality.
9. If you selected **Use Pool**, type a name in the **Server Pool Name** field.
   You create a pool of servers on this screen.
10. Provide the addresses required for your server connection:
    - If you selected **Direct**, type an IP address in the **Server Address** field.
    - If you selected **Use Pool**, for each pool member you want to add, type an IP address in the **Server Addresses** field and click **Add**.

      Note: *When you configure a pool, you have the option to type the server address in route domain format:* `IPAddress%RouteDomain`.
11. If you selected **Use Pool**, you have the option to select a **Server Pool Monitor** to track the health of the server pool.
12. In the **Service Port** field, type a TACACS+ service port or select one from the list. The default is `49`.
13. In the **Secret** field, type a secret key to use to encrypt and decrypt packets sent or received from the server, and then re-type the secret key in the **Confirm Secret** field.
14. For the **Service** setting, select the name of the service for the user who is being authenticated to use.
    Identifying the service enables the TACACS+ server to behave differently for different types of authentication requests.
15. From the **Protocol** list, select the protocol associated with the value in the Service setting.
16. From the **Privilege Level** list, select the level of privilege to request.
17. From the **Authentication Type** and **Authentication Service** lists, select from the provided values.
18. To save your changes, click the **Save & Close** button at the bottom of the screen.

This adds the new TACACS+ server to the TACACS+ list.

About Kerberos authentication

BIG-IQ® Centralized Management® provides an alternative to the form-based login authentication method. Instead, an HTTP 401 (unauthorized) or HTTP 407 (proxy authentication required) response triggers a browser login screen to collect credentials.

This option is useful when a user is already logged in to the local domain and you want to avoid submitting an HTTP form for collecting user credentials. The browser automatically submits credentials to the server and bypasses the login box to collect the credentials again.

Note: *Because SPNEGO/Kerberos is a request-based authentication feature, the authentication process is different from other authentication methods, which run at session creation time. SPNEGO/Kerberos authentication can occur at any time during the session.*

The benefits of this feature include:

- Provides flexible login mechanism instead of restricting you to use only the form-based login method.
- Eliminates the need for domain users to explicitly type login information again to log in to BIG-IQ.
- Eliminates the need for user password transmission with Kerberos method.

Important: *Administrators should not turn off the* ***KeepAlive*** *setting on the web server because turning that setting off might interfere with Kerberos authentication.*

Configure a Kerberos AAA server

Configure a Kerberos AAA server so that you can add it to a Kerberos authentication action in an 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 on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **Kerberos**.
5. Click **Create**.
   The New Kerberos screen opens.
6. In the **Name** field, type a unique name for the authentication server.
7. From **Device**, select the associated BIG-IP device.
8. In the **Auth Realm** field, type a Kerberos authentication realm name (administrative name), such as `LAB.COMANYNET`.

   Type the realm name all uppercase; it is case-sensitive.
9. In the **Service Name** field, type a service name; for example, `HTTP`.
10. In the **File name** area, click **Choose File** to locate and upload a keytab file.

    A keytab file contains Kerberos encryption keys (these are derived from the Kerberos password).
11. To save your changes, click the **Save & Close** button at the bottom of the screen.

The new AAA server displays on the Kerberos list.

About SSO profiles

SAML 2.0 in BIG-IQ® Centralized Management® specifies an SSO profile that involves exchanging information among an identity provider (IdP), a service provider (SP), and a user. The IdP can be any SSO service offering SAML authentication services

Configure an SSO profile

Configure an SSO profile to configure the BIG-IQ system for single sign-on.

.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Single Sign-On** and click **SSO Profiles**.
5. Click **Create**.
   The New Profile screen opens.
6. In the **Name** field, type a name for this SSO profile. You cannot change the name if you are editing an exising profile.
7. From the **Scope** list, select the scope that is applicable for this SSO profile.
8. From the **SSO Configuration** list, select an existing SSO configuration.
9. Under **Log Settings**, move log settings from the Available list to the Active list.
10. To save your changes, click the **Save & Close** button at the bottom of the screen.

The new SSO profile displays.

Configure BIG-IQ for device posture checks with endpoint management systems

When you check the device posture of a mobile device from your endpoint management system, before allowing access to the corporate network, you can configure BIG-IQ Centralized Management to verify the mobile device posture. The verification comes from the endpoint management system before allowing access from the access policy. An endpoint management system also controls the corporate data on mobile devices. Edge Client establishes a VPN connection with BIG-IP® APM® and an endpoint management system (Airwatch, Maas360, or Microsoft Intune) manages and sends device details to APM.

Configure an endpoint management system

You can create an endpoint management system on BIG-IP APM with either Airwatch, MaaS360, or Microsoft Intune.

An endpoint system management system connector object on BIG-IQ Centralized Managemetn is an object that stores information about the device management server, such as IP addresses and API credentials. You can configure more than one endpoint management system profile on the same system.

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

2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Authentication** and click **Endpoint Management Systems**.
5. From either Endpoint Management Systems (Shared) or Endpoint Management Systems (Device-Specific), click **Create**.
   The New Endpoint Management Systems screen opens.
6. For **Name**, type the name for the endpoint management system. You cannot change the name if you are editing an existing configuration.
7. For **Type**, select **AirWatch**,**IBM Maas360**, or **Microsoft Intune**.
8. From **Server SSL Profile**, select a profile.
9. For **Update Interval (minutes)** type a number.

   This is the number of minutes between the start of periodic polling that APM performs to obtain enrollment and compliance information from the endpoint management system.

To set up API credentials for an Airwatch endpoint management system, do these steps.

10. In the **Username** and **Password** fields, type the user name for the administrator of the endpoint management system and the password that the administrator uses to log in.
11. For **API Token**, type the API token of the application.

To set up API credentials for an IBM Mass360 endpoint management system, do these steps.

12. In the **Username** and **Password** fields, type the user name for the administrator of the endpoint management system and the password that the administrator uses to log in.
13. For **Billing ID**, type the billing ID for the user's IBM Maas360 account.
14. For **Application ID**, type the application ID that you got from IBM Maas360.
15. For **Access Key**, type the access key that you got from IBM Maas360.
16. For **Platform**, type the platform version of the IBM Maas360 console.
17. For **App Version**, type the current version number of the application that corresponds to the account.

To set up API credentials for a Microsoft Intune endpoint management system, do these steps.

18. For **Tenant Id**, type the tenant ID that comes with a Microsoft Intune subscription, the domain name for the logon name.
19. For **Client Id**, type the client ID that becomes available after creating a web application
20. For **Client Secret**, type the client secret that becomes available after creating a web application.
21. To save your changes, click the **Save & Close** button at the bottom of the screen.

You have configured an endpoint management system.

Federation

Configure Access as an OAuth 2.0 authorization server

You can configure a BIG-IQ® Centralized Management with Access to act as an OAuth authorization server. OAuth client applications and resource servers can register to have Access authorize requests.

Registering a client application for OAuth services

For a client application to obtain OAuth tokens and OAuth authorization codes from the BIG-IQ® Centralized Management, you must register it with Access.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Federation** and click **OAuth Authorization Server** > **Client Application**.
5. Click **Create**.
   The New Client Application screen opens.
6. In the **Name** field, type a name for the object.
7. In the **Application Name** field, type the application name.
8. In the Customization Settings for English area in the **Caption** field, type a caption.

   Access displays this caption as the name of the application on an Authorization screen if you choose to display one.
9. In the Security Settings area, for **Authentication Type**, select one of the options:

   - **None** - This is typically used in conjunction with the Implicit grant type, which does not use a secret or a certificate. For grant types other than **Implicit**, the other options provide better security.
   - **Secret** - This is the default setting. If this is selected, Access generates this secret for the client and you can request that Access regenerate the secret.
   - **Certificate** - Uses the client certificate. If this is selected, the **Client Certificate Distinguished Name** field displays.
10. If the **Client Certificate Distinguished Name** field displays, leave it blank or type a name.

    If you leave it blank, Access accepts any valid client certificate. If you specify a name, Access accepts only the specific valid client certificate with the specified Distinguished Name.

    This is a sample Distinguished Name for the client certificate:
    ```
    emailAddress=w.smith@f5.com,CN=OAuth AS Project Client2 Cert,OU=Product Development,O=F5 Networks,ST=CA,C=US
    ```
11. For **Scope**, select one or more and move them to the **Selected** field.
12. From **Grant Type**, select one or more of the options:

    - **Authorization Code** - The client must authenticate with the authorization server (Access) to get a token.
    - **Implicit** - The client gets a token from the authorization server (Access) without authenticating to it. (Refresh tokens are not available with this grant type.)
    - **Resource Owner Password Credentials** - The client goes directly to the authorization server and uses the resource owner credentials to obtain a token.

13. For **Redirect URI(s)** (if displayed), type a fully qualified URI, click **Add**, and repeat as needed.

    Redirect URI(s) form a list of URIs to which the OAuth authorization server can redirect the resource owner's user agent after authorization is obtained for an authorization code or implicit grant type.

14. To apply the token management settings from an OAuth profile, perform these substeps:
    a) In the Token Management Configuration area, retain selection of the **Enabled** check box.

       The token management configuration settings in an OAuth profile apply to client applications assigned to that profile except when this setting is disabled.
    b) Skip to step 13.

15. To manage tokens in a manner that is distinct for this client application, perform these substeps:
    a) In the Token Management Configuration area, clear the **Enabled** check box.
       Additional fields display.
    b) Update any of the additional fields.

16. Click **Save**.

Access generates a client ID for the application. If the **Authentication Type** is set to **Secret**, Access generates a secret. The application displays on the Client Application screen.

Registering a resource server for OAuth services

For Access in BIG-IQ® Centralized Management as an OAuth authorization server to accept token introspection requests from a resource server for token validation, you must register the resource server with Access.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Federation** and click **OAuth Authorization Server** > **Resource Server**.
5. Click **Create**.
   The New Resource Server screen opens.
6. Click **Create**.
7. In the **Name** field, type a name for the object.
8. From **Device**, select the associated BIG-IP device.
9. For **Authentication Type**, select one of these:
   - **None** - This option requires no authentication when the resource server sends a token introspect request to the OAuth authorization server to get the token validated.
   - **Secret** - For this option, Access generates this secret and you can request that Access regenerate the secret.
   - **Certificate** - This is the default setting. If this is selected, **Resource Server Certificate Distinguished Name** field displays.
10. If **Resource Server Certificate Distinguished Name** displays, leave it blank or type a name.

    If you leave it blank, Access accepts any valid client certificate. If you specify a name, Access accepts only the specific valid client certificate with the specified Distinguished Name.

    This is a sample Distinguished Name for the client certificate:
    ```
    emailAddress=w.smith@f5.com,CN=OAuth AS Project Client2 Cert,OU=Product
    Development,O=F5 Networks,ST=CA,C=US
    ```
11. Click **Save**.

The new resource server displays on the list.

Configure an artifact resolution service

Before you configure the artifact resolution service (ARS), you need to have configured a virtual server. That virtual server can be the same as the one used for the SAML Identity Provider (IdP), or you can create an additional virtual server.

Note: *F5® highly recommends that the virtual server definition include a server SSL profile.*

You configure an ARS so that a BIG-IQ® system that is configured as a SAML IdP can provide SAML artifacts in place of assertions. With ARS, the BIG-IQ system can receive Artifact Resolve Requests (ARRQ) from service providers, and provide Artifact Resolve Responses (ARRP) for them.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Federation** and click **SAML Identity Provider** > **Artifact Resolution Services**.
5. Under Artifact Resolution Services (Shared) Artifact Resolution Services (Device-specific), click **Create**.
   The Create New SAML Artifact Resolution Service popup screen opens, showing general settings.
6. In the **Name** field, type a name for the artifact resolution service.
7. In the **Description** field, type a new description.
8. Click **Service Settings.**
9. From the **Virtual Server** list, select the virtual server that you created previously.

   ARS listens on the IP address and port configured on the virtual server.
10. In the **Artifact Validity (Seconds)** field, type the number of seconds for which the artifact remains valid. The default is 60 seconds.

    The system deletes the artifact if the number of seconds exceeds the artifact validity number.
11. For the **Send Method** setting, select the binding to use to send the artifact, either **POST** or **Redirect**.
12. In the **Host** field, type the host name defined for the virtual server, for example **ars.siterequest.com**.
13. In the **Port** field, type the port number defined in the virtual server. The default is `443`.
14. Click **Security Settings.**
15. To require that artifact resolution messages from an SP be signed, select the **Sign Artifact Resolution Request** check box.
16. To use HTTP Basic authentication for artifact resolution request messages, in the **User Name** field, type a name for the artifact resolution service request and in the **Password** field, type a password.

    These credentials must be present in all Artifact Resolve Requests sent to this ARS.
17. Click **OK**.
    The popup screen closes, leaving the Artifact Resolution Services list screen open.

The Artifact Resolution Service is ready to use.

Configure an OAuth profile

You configure an OAuth profile to specify the client applications, resource servers, token types, and authorization server endpoints that apply to the traffic that goes through a particular virtual server.

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

2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Federation** and click **OAuth Authorization Server** > **OAuth Profile**.
5. Click **Create**.
6. In the **Name** field, type a name for the object.
7. For **Device**, select the BIG-IP device attached to this application.
8. For **Client Application**, select the applications from the **Available** list and move them to the **Active** list.
9. For **Resource Server**, select the resource servers associated with this OAuth profile from the **Available** list and move them to the **Active** list.
10. Under**Token Management Configuration**, configure the following steps:
    a) For **Authorization Code Lifetime**, type a number.

       This specifies the number of minutes an authorization code is considered valid.
    b) For **Support Opaque Token**, select whether APM can issue opaque access tokens through this profile. The default setting is **Enabled**.
    c) From the Database Instance list, select a database instance to store the opaque access tokens that APM issues.
    d) For **Access Token Lifetime**, type a number.

       This specifies the number of minutes an access token is considered valid.
    e) For **Reuse Access Token**, select or clear the **Enabled** check box. If cleared, the server generates a new access token. If selected, the server extends the expiry time of the access token associated with the refresh token.

       Note: *For an access token to be reused, the* ***Enabled*** *check box must be selected for* ***Generate Refresh Token****.*

       ---
    f) From the **Access Token Limit Per User** field, type the maximum number of active opaque access tokens the OAuth authorization server provides to client applications on behalf of this user.
    g) For **Generate Refresh Token**, select or clear the **Enabled** check box. If selected, the OAuth authorization server generates a refresh token in addition to the access token for authorization code and resource owner credential grants.
    h) For **Refresh Token Lifetime**, type a number.

       This specifies the number of minutes that a refresh token is considered valid after it is generated.
    i) For **Reuse Refresh Token** select or clear the **Enabled** check box. When cleared and a new access token is obtained, the OAuth authorization server also generates a new refresh token value.
    j) For **Refresh Token Usage Limit**, type a number.

       This specifies the number of times an access token can be obtained using the refresh token.
    k) For **Support JWT Token**, select whether BIG-IQ can issue JSON web tokens (JWTs) through this profile. **Enabled** is cleared by default.
    l) From the **Issuer** field, type the issuer of the JWT.

       This must be a URI.
    m) From the **Subject** field, type the subject of the JWT.

       This value can be a string, URI, or session variable.
    n) From the **Trusted Certificate Authorities** list, select a certificate authority file stored on the BIG-IP device.
    o) For **Ignore Expired Certificate Validation,** enable to use the certificate for signing JWT access token even if it is expired.
    p) From the **Primary Key** list, select the primary signing key for the JWT.

q) For **Rotation Keys**, select one or more JWK configurations that contain public keys used as rotation keys.

r) For **Audience**, select the audience claim for which the JWT access token is intended.

s) For **Claim**, select the list of claims that are part of the JWT access token.

t) For **JWT Access Token Lifetime**, type a number.

This specifies the number of minutes a JWT access token is considered valid. In specifying this lifetime, consider that JWT access tokens cannot be revoked.

u) For **JWT Generate Refresh Token**, select **Enabled** so the OAuth authorization server generates a refresh token in addition to the access token for authorization code and resource owner credential grants.

v) For **JWT Refresh Token Lifetime**, type a number.

This specifies the number of minutes a refresh token is considered valid. In specifying this lifetime, consider that JWT refresh tokens cannot be revoked.

w) For the **JWT Refresh Token Encryption Secret** field, select the JWT refresh token encryption secret that is used to generate an encryption key.

BIG-IQ cannot import the JWT refresh token encryption from the BIG-IP device. After importing the BIG-IP device, reconfigure the encryption secret.

11. Under**Authorization Server Endpoints**, configure the following steps:

a) For **Authorization Endpoint**, type the endpoint that the OAuth authorization server uses to authenticate the resource owner and obtain authorization.

b) For **Token Issuance Endpoint**, type the endpoint that the client uses to obtain an access token or a refresh token.

c) For **Token Revocation Endpoint**, type the endpoint for the client to use to revoke a previously obtained opaque access token or refresh token.

d) For **OpenID Connect Configuration Endpoint**, type the path of the OpenID Connect endpoint that returns OpenID Connect configuration.

e) For **JWKS Endpoint**, type the path of the JSON Web Key Set (JWKS) endpoint that returns public signing keys.

12. To save your changes, click the **Save & Close** button at the bottom of the screen.

Connectivity

About connectivity profiles and Network Access

A connectivity profile defines connectivity and client settings for a Network Access session.

A connectivity profile contains:

- Compression settings for network access connections and application tunnels
- Citrix client settings
- Virtual servers and DNS-location awareness settings for BIG-IP® Edge Client® for Windows, Mac, and Linux
- Password caching settings for BIG-IP Edge Client for Windows, Mac, and mobile clients
- Settings for mobile clients

A connectivity profile is also associated with customizable client download packages for Edge Client for Windows and Edge Client for Mac.

About a connectivity profile and traffic handling

If a connectivity profile is assigned to a virtual server, it creates a secure connectivity (tunnel) interface. Traffic that is allowed through the tunnel is matched against any virtual servers enabled on the tunnel interface. If a matching virtual server is found, the traffic goes to the virtual server before going out to the network. Network access, portal access, iSession, and mobile app tunnel traffic are allowed through the tunnel and the same traffic handling is applied to all of them.

Creating a connectivity profile

You create a connectivity profile to configure client connections.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
3. Expand **Connectivity / VPN** and click **Connectivity** > **Profiles**.
4. Click **Create**.
   The Create New Connectivity Profile screen opens and displays General Settings.
5. Type a **Profile Name** for the connectivity profile.
6. Select a Parent Profile from the list.
   Access for BIG-IQ provides a default profile, connectivity.
7. To save your changes, click the **Save & Close** button at the bottom of the screen.

The connectivity profile displays in the list.

To provide functionality with a connectivity profile, you must add the connectivity profile and an access profile to a virtual server.

Connectivity profile general settings

You can configure the following general settings in a connectivity profile.

Profile setting	Value	Description
Profile Name	Text.	Text specifying name of the connectivity profile.
Parent Profile	A connectivity profile, selected from a list.	A profile inherits settings from its parent profile.
FEC Profile	A forward error correcting (FEC) profile, selected from a list.	A FEC profile applies to a network access tunnel. ***Note:*** *FEC profiles might not be available on all BIG-IP® systems.*
Description	Text.	Text description of the connectivity profile.

Configuring a connectivity profile for Edge Client for Windows

A connectivity profile automatically contains settings for BIG-IP® Edge Client® for Windows clients. You should configure the settings to fit your situation.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
3. Expand **Connectivity / VPN** and click **Connectivity** > **Profiles**.
4. Select the connectivity profile that you want to update from the list.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
5. Select **Win/Mac Edge Settings** in the left pane.
   Settings for the Windows Edge Client display in the right pane.
6. Set Edge Client action settings:
   a) Retain the default (selected) or clear the **Save Servers Upon Exit** check box.

      Specifies whether Edge Client maintains a list of recently used user-entered APM® servers. Edge Client always lists the servers that are defined in the connectivity profile, and sorts them by most recent access, whether this option is selected or not.
   b) To enable the client to try to use the Windows logon session for an APM session also, select the **Reuse Windows Logon Session** check box.

      This is cleared by default.
   c) To enable the client to try to use the credentials that they typed for Windows logon in an APM session also, select the **Reuse Windows Logon Credentials** check box.

      This is cleared by default.

      Note: *To support this option, you must also include the* ***User Logon Credentials Access Service*** *in the Windows client package for this connectivity profile and you must ensure that the access policy includes an uncustomized* ***Logon Page*** *action.*
7. To support automatic reconnection without the need to provide credentials again, allow password caching.

a) Select the **Allow Password Caching** check box.

This check box is cleared by default.

The remaining settings on the screen become available.

b) To require device authentication to unlock the saved password, select **Require Device Authentication.**

This option links the option to use a saved password to a device authentication method. Supported device authentication methods include PIN, passphrase, and biometric (fingerprint) authentication on iOS and Android. Android devices also support pattern unlocking.

c) From the **Save Password Method** list, select **disk** or **memory**.

If you select **disk**, Edge Client caches the user's password (in encrypted form) securely on the disk where it is persisted even after the system is restarted or Edge Client is restarted.

If you select **memory**, Edge Client caches the user's password within the BIG-IP Edge Client application for automatic reconnection purposes.

If you select **memory**, the **Password Cache Expiration (minutes)** field displays with a default value of 240.

d) If the **Password Cache Expiration (minutes)** field displays, retain the default value or type the number of minutes to save the password in memory.

8. To enable automatic download and update of client packages, from the **Component Update** list, select **yes** (default).

If you select **yes**, APM® updates Edge Client software automatically on the client system when newer versions are available. This option applies to updates for theses components only: BIG-IP Edge Client, component installer service, DNS relay proxy service, and user logon credentials access service.

9. Specify DNS suffixes that are considered to be in the local network.

Providing a list of DNS suffixes for the download package enables Edge Client to support the autoconnect option. With **Auto-Connect** selected, Edge Client uses the DNS suffixes to automatically connect when a client is not on the local network (not on the list) and automatically disconnect when the client is on the local network.

a) From the left pane of the popup screen, select **Location DNS List**.
Location DNS list information is displayed in the right pane.

b) Click **Add**.
An update row becomes available.

c) Type a name and click **Update**.

Type a DNS suffix that conforms to the rules specified for the local network.

The new row displays at the top of the table.

d) Continue to add DNS names and when you are done, click **OK**.

10. To save your changes, click the **Save & Close** button at the bottom of the screen.

You have now configured the security settings for BIG-IP Edge Client for Windows clients.

Configuring a connectivity profile for Edge Client for Mac

A connectivity profile automatically contains settings for BIG-IP® Edge Client® for Mac clients. You should configure the settings to fit your situation.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.

2. Click the name of the Access group that interests you.
A new screen displays the group's properties.

3. Expand **Connectivity / VPN** and click **Connectivity** > **Profiles**.

4. Select the connectivity profile that you want to update from the list.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
5. Select **Win/Mac Edge Settings** in the left pane.
   Settings for the Mac Edge Client display in the right pane.
6. Set Edge Client action settings:
   a) Retain the default (selected) or clear the **Save Servers Upon Exit** check box.

      Specifies whether Edge Client maintains a list of recently used user-entered APM® servers. Edge Client always lists the servers that are defined in the connectivity profile, and sorts them by most recent access, whether this option is selected or not.
   b) To enable the client to try to use the Mac logon session for an APM session also, select the **Reuse Mac Logon Session** check box.

      This is cleared by default.
   c) To enable the client to try to use the credentials that they typed for Mac logon in an APM session also, select the **Reuse Mac Logon Credentials** check box.

      This is cleared by default.

      Note: *To support this option, you must also include the* ***User Logon Credentials Access Service*** *in the Mac client package for this connectivity profile and you must ensure that the access policy includes an uncustomized* ***Logon Page*** *action.*

      ---
7. To support automatic reconnection without the need to provide credentials again, allow password caching.
   a) Select the **Allow Password Caching** check box.

      This check box is cleared by default.

      The remaining settings on the screen become available.
   b) To require device authentication to unlock the saved password, select **Require Device Authentication.**

      This option links the option to use a saved password to a device authentication method. Supported device authentication methods include PIN, passphrase, and biometric (fingerprint) authentication on iOS and Android. Android devices also support pattern unlocking.
   c) From the **Save Password Method** list, select **disk** or **memory**.

      If you select **disk**, Edge Client caches the user's password (in encrypted form) securely on the disk where it is persisted even after the system is restarted or Edge Client is restarted.

      If you select **memory**, Edge Client caches the user's password within the BIG-IP Edge Client application for automatic reconnection purposes.

      If you select **memory**, the **Password Cache Expiration (minutes)** field displays with a default value of 240.
   d) If the **Password Cache Expiration (minutes)** field displays, retain the default value or type the number of minutes to save the password in memory.
8. To enable automatic download and update of client packages, from the **Component Update** list, select **yes** (default).

   If you select **yes**, APM® updates Edge Client software automatically on the client system when newer versions are available. This option applies to updates for theses components only: BIG-IP Edge Client, component installer service, DNS relay proxy service, and user logon credentials access service.
9. Specify DNS suffixes that are considered to be in the local network.

   Providing a list of DNS suffixes for the download package enables Edge Client to support the autoconnect option. With **Auto-Connect** selected, Edge Client uses the DNS suffixes to automatically connect when a client is not on the local network (not on the list) and automatically disconnect when the client is on the local network.

a) From the left pane of the popup screen, select **Location DNS List**.
Location DNS list information is displayed in the right pane.
b) Click **Add**.
An update row becomes available.
c) Type a name and click **Update**.
Type a DNS suffix that conforms to the rules specified for the local network.
The new row displays at the top of the table.
d) Continue to add DNS names and when you are done, click **OK**.

10. To save your changes, click the **Save & Close** button at the bottom of the screen.

You have now configured the security settings for BIG-IP Edge Client for Mac clients.

Configuring a connectivity profile for Edge Client for Android

A connectivity profile automatically contains settings for BIG-IP® Edge Client® for Android clients. You should configure the settings to fit your situation.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
A new screen displays the group's properties.
3. Expand **Connectivity / VPN** and click **Connectivity** > **Profiles**.
4. Select the connectivity profile that you want to update from the list.
The Edit Connectivity Profile popup screen opens and displays General Settings.
5. Select **Mobile Client Settings** in the left pane.
Settings for the Android Edge Client display in the right pane.
6. To enable users to save their passwords for reconnection purposes within a specified time period, select the **Allow Password Caching** check box.
The additional fields in the area become available.
7. For **Save Password Method**, specify how to perform password caching:

- To allow the user to save the encrypted password on the device without a time limit, select **disk**.
- To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.

8. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
9. To enhance security on the client, retain the selection of the **Enforce Device Lock** check box (or clear the check box).
This check box is selected by default. Edge Portal® and Edge Client support password locking, but do not support pattern locking. If you clear this check box, the remaining settings in the area become unavailable.
10. For **Device Lock Method**, retain the default **numeric**, or select a different method from the list.
11. For **Minimum Passcode Length**, retain the default `4`, or type a different passcode length.
12. For **Maximum Inactivity Time (minutes)**, retain the default `5`, or type a different number of minutes.
13. To force the app to use a selected logon mode and prevent users from changing it:
a) Select the **Enforce Logon Mode** check box.
b) From the **Logon Method** list, select **web** or **native**.

Note: *Support for this feature will be announced in release notes for the individual Edge Apps (BIG-IP Edge Client for iOS, Edge Client for Android, Edge Portal for iOS, and Edge Portal for Android). Check the release notes for the Edge Apps to determine whether it is supported.*

14. To save your changes, click the **Save & Close** button at the bottom of the screen.

You have now configured the security settings for BIG-IP Edge Client for Android clients.

Configuring a connectivity profile for Edge Portal for Android

A connectivity profile automatically contains settings for BIG-IP® Edge Portal® for Android clients. You should configure the settings to fit your situation.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
3. Expand **Connectivity / VPN** and click **Connectivity** > **Profiles**.
4. Select the connectivity profile that you want to update from the list.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
5. Select **Mobile Client Settings** in the left pane.
   Settings for the Android Edge Portal display in the right pane.
6. To enable users to save their passwords for reconnection purposes within a specified time period, select the **Allow Password Caching** check box.
   The additional fields in the area become available.
7. For **Save Password Method**, specify how to perform password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.
   - To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

   If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.
8. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
9. To enhance security on the client, retain the selection of the **Enforce Device Lock** check box (or clear the check box).

   This check box is selected by default. Edge Portal® and Edge Client support password locking, but do not support pattern locking. If you clear this check box, the remaining settings in the area become unavailable.
10. For **Device Lock Method**, retain the default **numeric**, or select a different method from the list.
11. For **Minimum Passcode Length**, retain the default `4`, or type a different passcode length.
12. For **Maximum Inactivity Time (minutes)**, retain the default `5`, or type a different number of minutes.
13. To force the app to use a selected logon mode and prevent users from changing it:
    a) Select the **Enforce Logon Mode** check box.
    b) From the **Logon Method** list, select **web** or **native**.

Note: *This feature is supported with F5 Access for iOS and F5 Access for Android.*

14. To save your changes, click the **Save & Close** button at the bottom of the screen.

You have now configured the security settings for BIG-IP Edge Portal for Android clients.

Configuring a connectivity profile for Edge Client for iOS

A connectivity profile automatically contains settings for BIG-IP® Edge Client® for iOS clients. You should configure the settings to fit your situation.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
3. Expand **Connectivity / VPN** and click **Connectivity** > **Profiles**.
4. Select the connectivity profile that you want to update from the list.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
5. Select **Mobile Client Settings** in the left pane.
   Settings for the iOS Edge Client display in the right pane.
6. To enable users to save their passwords for reconnection purposes within a specified time period, select the **Allow Password Caching** check box.
   The additional fields in the area become available.
7. To enable device authentication on the client, select **Require Device Authentication**.
8. For **Save Password Method**, specify how to perform password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.
   - To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

   If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.
9. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
10. In the **On Demand Disconnect Timeout (minutes)** field, retain the default `2`, or type a different number of minutes before VPN on demand times out.
11. To force the app to use a selected logon mode and prevent users from changing it:
    a) Select the **Enforce Logon Mode** check box.
    b) From the **Logon Method** list, select **web** or **native**.

    Note: *This feature is supported with F5 Access for iOS and F5 Access for Android.*
12. To save your changes, click the **Save & Close** button at the bottom of the screen.

You have now configured the security settings for BIG-IP Edge Client for iOS clients.

Configuring a connectivity profile for Edge Portal for iOS

A connectivity profile automatically contains settings for BIG-IP® Edge Portal® for iOS clients. You should configure the settings to fit your situation.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
3. Expand **Connectivity / VPN** and click **Connectivity** > **Profiles**.
4. Select the connectivity profile that you want to update from the list.

The Edit Connectivity Profile popup screen opens and displays General Settings.

5. Select **Mobile Client Settings** in the left pane.
   Settings for the iOS Edge Portal display in the right pane.
6. To enable users to save their passwords for reconnection purposes within a specified time period, select the **Allow Password Caching** check box.
   The additional fields in the area become available.
7. To enable users to save their passwords for reconnection purposes within a specified time period, select the **Allow Password Caching** check box.
   The additional fields in the area become available.
8. For **Save Password Method**, specify how to perform password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.
   - To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

   If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.
9. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
10. Specify security by keeping **Enforce PIN Lock** set to **Yes**.
    Edge Portal supports PIN locking, but does not support pattern locking.
11. For **Maximum Grace Period (minutes)**, retain the default `2`, or type a different number of minutes.
12. To force the app to use a selected logon mode and prevent users from changing it:
    a) Select the **Enforce Logon Mode** check box.
    b) From the **Logon Method** list, select **web** or **native**.

    Note: *Support for this feature will be announced in release notes for the individual Edge Apps (BIG-IP Edge Client for iOS, Edge Client for Android, Edge Portal for iOS, and Edge Portal for Android). Check the release notes for the Edge Apps to determine whether it is supported.*
13. To save your changes, click the **Save & Close** button at the bottom of the screen.

Configuring a connectivity profile for F5 Access for Chrome OS

A connectivity profile automatically contains default settings for F5® Access for Chrome OS. You should configure the connectivity profile settings to fit your situation.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
3. Expand **Connectivity / VPN** and click **Connectivity** > **Profiles**.
4. Select the connectivity profile that you want to update from the list.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
5. Select **Mobile Client Settings** in the left pane.
   Settings for F5 Access for Chrome OS display in the right pane.
6. To enable users to save their passwords for reconnection purposes within a specified time period, select the **Allow Password Caching** check box.
   The additional fields in the area become available.
7. For **Save Password Method**, specify how to perform password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.

- To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.

8. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
9. To force the app to use a selected logon mode and prevent users from changing it:
   a) Select the **Enforce Logon Mode** check box.
   b) From the **Logon Method** list, select **web** or **native**.

Note: *Support for this feature will be announced in release notes for the individual Mobile and App Store apps (BIG-IP® Edge Client® for iOS, Edge Client for Android, F5 Access for Chrome OS, Edge Portal for iOS, and Edge Portal for Android). Check the release notes for the Apps to determine whether it is supported.*

---

10. To save your changes, click the **Save & Close** button at the bottom of the screen.

You have now configured the security settings for F5 Access for Chrome OS.

Configuring a connectivity profile for F5 Access for Mac OS

A connectivity profile automatically contains default settings for F5® Access for Mac OS. You should configure the connectivity profile settings to fit your situation.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
3. Expand **Connectivity / VPN** and click **Connectivity** > **Profiles**.
4. Select the connectivity profile that you want to update from the list.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
5. Select **Mobile Client Settings** in the left pane.
   Settings for F5 Access for Mac OS display in the right pane.
6. To enable users to save their passwords for reconnection purposes within a specified time period, select the **Allow Password Caching** check box.
   The additional fields in the area become available.
7. For **Save Password Method**, specify how to perform password caching:
   - To allow the user to save the encrypted password on the device without a time limit, select **disk**.
   - To specify that the user password is cached in the application on the user's device for a configurable period of time, select **memory**.

   If you select **memory**, the **Password Cache Expiration (minutes)** field becomes available.
8. If the **Password Cache Expiration (minutes)** field displays, type the number of minutes you want the password to be cached in memory.
9. To force the app to use a selected logon mode and prevent users from changing it:
   a) Select the **Enforce Logon Mode** check box.
   b) From the **Logon Method** list, select **web** or **native**.

Note: *Support for this feature will be announced in release notes for the individual Mobile and App Store apps (BIG-IP® Edge Client® for iOS, Edge Client for Android, F5 Access for Chrome OS, Edge Portal for iOS, and Edge Portal for Android). Check the release notes for the Apps to determine whether it is supported.*

---

10. To save your changes, click the **Save & Close** button at the bottom of the screen.

Configuring a connectivity profile for Edge Client for Windows

A connectivity profile automatically contains settings for BIG-IP® Edge Client® for Windows clients. You should configure the settings to fit your situation.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
3. Expand **Connectivity / VPN** and click **Connectivity** > **Profiles**.
4. Select the connectivity profile that you want to update from the list.
   The Edit Connectivity Profile popup screen opens and displays General Settings.
5. Select **Win/Mac Edge Settings** in the left pane.
   Settings for the Windows Edge Client display in the right pane.
6. Set Edge Client action settings:
   a) Retain the default (selected) or clear the **Save Servers Upon Exit** check box.

      Specifies whether Edge Client maintains a list of recently used user-entered APM® servers. Edge Client always lists the servers that are defined in the connectivity profile, and sorts them by most recent access, whether this option is selected or not.
   b) To enable the client to try to use the Windows logon session for an APM session also, select the **Reuse Windows Logon Session** check box.

      This is cleared by default.
   c) To enable the client to try to use the credentials that they typed for Windows logon in an APM session also, select the **Reuse Windows Logon Credentials** check box.

      This is cleared by default.

      Note: *To support this option, you must also include the* ***User Logon Credentials Access Service*** *in the Windows client package for this connectivity profile and you must ensure that the access policy includes an uncustomized* ***Logon Page*** *action.*

      ---
7. To support automatic reconnection without the need to provide credentials again, allow password caching.
   a) Select the **Allow Password Caching** check box.

      This check box is cleared by default.

      The remaining settings on the screen become available.
   b) To require device authentication to unlock the saved password, select **Require Device Authentication.**

      This option links the option to use a saved password to a device authentication method. Supported device authentication methods include PIN, passphrase, and biometric (fingerprint) authentication on iOS and Android. Android devices also support pattern unlocking.
   c) From the **Save Password Method** list, select **disk** or **memory**.

      If you select **disk**, Edge Client caches the user's password (in encrypted form) securely on the disk where it is persisted even after the system is restarted or Edge Client is restarted.

      If you select **memory**, Edge Client caches the user's password within the BIG-IP Edge Client application for automatic reconnection purposes.

      If you select **memory**, the **Password Cache Expiration (minutes)** field displays with a default value of 240.

d) If the **Password Cache Expiration (minutes)** field displays, retain the default value or type the number of minutes to save the password in memory.

8. To enable automatic download and update of client packages, from the **Component Update** list, select **yes** (default).

If you select **yes**, APM® updates Edge Client software automatically on the client system when newer versions are available. This option applies to updates for theses components only: BIG-IP Edge Client, component installer service, DNS relay proxy service, and user logon credentials access service.

9. Specify DNS suffixes that are considered to be in the local network.

Providing a list of DNS suffixes for the download package enables Edge Client to support the autoconnect option. With **Auto-Connect** selected, Edge Client uses the DNS suffixes to automatically connect when a client is not on the local network (not on the list) and automatically disconnect when the client is on the local network.

a) From the left pane of the popup screen, select **Location DNS List**.
Location DNS list information is displayed in the right pane.

b) Click **Add**.
An update row becomes available.

c) Type a name and click **Update**.

Type a DNS suffix that conforms to the rules specified for the local network.

The new row displays at the top of the table.

d) Continue to add DNS names and when you are done, click **OK**.

10. To save your changes, click the **Save & Close** button at the bottom of the screen.

You have now configured the security settings for BIG-IP Edge Client for Windows clients.

Network Access

Configuring Lease Pools

What is a lease pool?

A *lease pool* specifies a group of IPv4 or IPv6 IP addresses as a single object. You can use a lease pool to associate that group of IP addresses with a network access resource. When you assign a lease pool to a network access resource, network access clients are automatically assigned unallocated IP addresses from the pool during the network access session.

Important: *Network access with IPv6 alone is not supported. An IPv6 tunnel requires a simultaneous IPv4 tunnel, which is automatically established when you assign IPv4 and IPv6 lease pools, and set the version to* ***IPv4&IPv6****.*

Create an IPv4 lease pool

Create a lease pool to provide internal network addresses for network access tunnel users.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Connectivity / VPN** and click **Network Access** > **IPV4 Lease Pools**.
5. Click the **Create** button.
6. In the **Name** field, type a name for the resource.
7. Add IPv4 addresses to the lease pool.
   - To add a single IP address, in the Member List area, select **IP Address** for the type. In the **IP Address** field, type the IP address.
   - To add a range of IP addresses, in the Member List area, select **IP Address Range** for the type. In the **Start IP Address** field, type the first IP address, and in the **End IP Address** field, type the last IP address.
8. To save your changes, click the **Save & Close** button at the bottom of the screen.

A lease pool is created with the IP address or IP address range you specified.

To delete an IP address or IP address range, select the IP address or IP address range in the member list, and click the **Delete** button.

Create an IPv6 lease pool

Create a lease pool to provide internal network addresses for network access tunnel users.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.

3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Connectivity / VPN** and click **Network Access** > **IPV6 Lease Pools**.
5. Click the **Create** button.
6. In the **Name** field, type a name for the resource.
7. Add IPv4 addresses to the lease pool.
   - To add a single IP address, in the Member List area, select **IP Address** for the type. In the **IP Address** field, type the IP address.
   - To add a range of IP addresses, in the Member List area, select **IP Address Range** for the type. In the **Start IP Address** field, type the first IP address, and in the **End IP Address** field, type the last IP address.
8. To save your changes, click the **Save & Close** button at the bottom of the screen.

A lease pool is created with the IP address or IP address range you specified.

To delete an IP address or IP address range, select the IP address or IP address range in the member list, and click the **Delete** button.

About Windows client traffic shaping

Used together, client traffic classifiers and client rate classes provide client-side traffic shaping features on Windows® network access client connections. You configure a *client traffic classifier*, which defines source and destination IP addresses or networks, and can also specify a protocol. The client traffic classifier is then associated with a *client rate class*, which defines base and peak rates for traffic to which it applies, and other traffic shaping features. A client traffic classifier is assigned in a network access resource.

Important: *Client traffic classifiers support IPv4 addresses only.*

Configuring client traffic shaping

Client rate shaping allows you to shape client-side traffic from Windows® client systems, based on traffic parameters.

1. Create a client rate class.
2. Create a client traffic classifier.
   When you create the client traffic classifier, you select the previously created client rate class.

Together, the client rate class and client traffic classifier work to provide client-side traffic control to Windows clients to which the traffic control is applied.

Select the client traffic classifier in the **Network Settings** configuration of a network access resource. The client traffic classifier is then applied to Windows clients, for client-side traffic on the VPN tunnels defined by that network access resource.

Creating a client traffic classifier

You must create at least one client rate class before you create a client traffic classifier. You select client rate classes to define rules in the client traffic classifier.

Create a client traffic classifier to define traffic control rules for the virtual and physical network interfaces on a network access tunnel.

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

2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Connectivity / VPN** and click **Network Access** > **Client Traffic Classifiers**.
5. Click **Create**.
   The New Client Traffic Classifier screen opens.
6. In the **Name** box, type a name for the client traffic classifier, and click **Save & Close**.
   The Client Traffic Classifiers list screen opens.
7. Click the name of the client traffic classifier you just created.
8. Add rules for the appropriate interface.

Rule type	Description
Rules for Virtual Network Access Interface	Add a rule to this section to apply the traffic shaping control only to traffic on the virtual network access interface.
Rules for Local Physical Interfaces	Add a rule to this section to apply the traffic shaping control only to traffic on the client computer's local physical interfaces.
Rules for Virtual Network Access and Local Physical Interfaces	Add a rule to this section to apply the traffic shaping control to traffic on both the virtual Network Access interface and the client's local physical interfaces.

9. To save your changes, click the **Save & Close** button at the bottom of the screen.

Configuring App Tunnel Access

What are app tunnels?

An *app tunnel* (application tunnel) provides secure, application-level TCP/IP connections from the client to the network. App tunnels are particularly useful for users with limited privileges who attempt to access particular web applications, as app tunnels do not require that the user has administrative privileges to install.

Additionally, optimization is available for app tunnels. With compression settings for app tunnels, you can specify the available compression codecs for client-to-server connections. The server compares the available compression types configured with the available compression types on the server, and chooses the most effective mutual compression setting. You configure compression for the server in the connectivity profile.

Note: *Because app tunnels do not require administrative rights, some features of Network Access and Optimized Application tunnels are not available with app tunnels. For example, the application tunnel cannot easily resolve domain names in applications without a client-side DNS redirector, or modification of the system hosts file.*

Important: *For tunnels that access backend servers by using DNS resolution, use Optimized Application Tunnels in the Network Access menus instead. Optimized Applications require administrative rights on the local system.*

Configuring an app tunnel object

When you create an app tunnel object, that object becomes a simple container that holds app tunnel resources. Once you specify those resources from within the app tunnel resource, you can then assign the resource to an 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 on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Connectivity / VPN** and click **App Tunnels**.
5. Click **Create**.
   The New App Tunnel screen opens.
6. Type a name and description for your app tunnel.
7. Although an ACL is automatically created for your application object, you can choose to determine the order of your ACL as it appears in the ACL list. Use the **ACL Order** list to select the placement you want.
8. Under Default Customization Settings, type a **Caption** for the app tunnel.
   This caption identifies the app tunnel and enables it to appear on a full webtop.
9. To save your changes, click the **Save & Close** button at the bottom of the screen.

You have just created an app tunnel object.

Resource Item properties

The application resource item specifies how to create a particular tunnel. The application field serves as a hint to the BIG-IQ system for special handling of specific protocols. Compression settings specify which compression codecs the tunnels can use, while the Launch Applications section allows you to define an application that will run after you establish the resource tunnel.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Connectivity / VPN** and click **App Tunnels**.
5. From the App Tunnels list, select an existing app tunnel.
6. On the left side of the new screen, select **Resource Items**.
7. Click **Add**.
   The New Resource Item screen opens.
8. In the **Description** field, type a description of the application access resource.
9. For the **Destination** setting, specify whether the application destination **Type** is a host or an IP address.

   You cannot use the fully qualified domain name to connect to an application resource that is configured with an IP address destination type.

   If you specify a hostname, make sure that it is DNS-resolvable. After the application tunnel is assigned to a full webtop in an access policy, the application tunnel does not appear on the full webtop if the hostname is not DNS-resolvable.
10. Specify your port or port range for the application.
11. From the **Application Protocol** list, select the application protocol.

Option	Description
None	Specifies that the app tunnel resource uses neither RPC or FTP protocols.
Microsoft RPC	Specifies that the resource uses the Microsoft® RPC protocol.
Microsoft Exchange RPC Server	Specifies that the resource uses the Microsoft Exchange RPC Server protocol.
FTP	Specifies that the resource uses FTP protocol.

12. From the **Log** list, select **Packet** to log activity to the packet log, or **None** to disable logging for the app tunnel.
13. From the **Operating System** list, select the platform on which a Java-based resource runs.

    The resource runs only on the platform that you select. This setting is applicable when Java Tunnel is enabled on the application tunnel.
14. From the **Compression** list, select **Enabled** to display compression types and enable or disable them.
15. From the **Deflate** list, select **Enabled** to enable Deflate compression. Deflate compression uses the least CPU resources, but compresses the least effectively.
16. From the **LZO** list, select **Enabled** to enable LZO compression. LZO compression offers a balance between CPU resources and compression ratio, compressing more than deflate, but with less CPU resources than Bzip2.

17. From the **Bzip2** list, select **Enabled** to enable Bzip2 compression. Bzip2 compression uses the most CPU resources, but compresses the most effectively.
18. From the **Adaptive** list, select **Enabled** to enable adaptive compression. Adaptive compression automatically selects the compression type based on network and traffic characteristics.
19. For the **Application Path** setting, optionally specify a path for an application to start after the application access tunnel is established.
20. For the **Parameters** setting, specify any parameters associated with the application that starts with the **Application Path**. The parameters you can add are:
    - `%host%` - This is substituted with the loopback host address, for example `http://%host%/application/`.
    - `%port%` - The loopback port. Use this if the original local port has changed due to conflicts with other software.
21. To save your changes, click the **Save & Close** button at the bottom of the screen.

Configuring Remote Desktop Access

What are remote desktops?

Remote desktops allow users to access the following types of internal servers in virtual desktop sessions:

- Microsoft® Remote Desktop servers
- Citrix® servers
- VMware View Connection servers

You can configure remote desktops by name or by their internal IP addresses, and grant or deny users the ability to set up their own favorites.

Configuring a resource for remote desktops

You can configure BIG-IQ so users can access internal servers in virtual desktop sessions. Refer to the online help for more information about the parameters you can configure for remote desktops.

1. Log in to the BIG-IQ system with your user name and password.
2. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
3. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
4. Expand **Connectivity / VPN** and click **VDI / RDP** > **Remote Desktops**.
5. Click **Create**.
   The New Remote Desktops List screen opens.
6. In the **Name** field, type a name for this desktop resource.
7. From the **Type** list, select **Citrix**, **RDP**, or **VMware View**.
8. For **Destination**, select a destination **Type** (**Host Name**, **IP Address**, or **Pool**) then specify destination servers for Citrix, Microsoft RDP, or VMware View:
   - **Host Name** - Type the host name and, in the **Port** field, type a port number.

     Note: *For Citrix and VMware View, the standard port is* `80` *and for Microsoft RDP, the standard port is* `3389`*.*
   - **IP Address** - Type the IP address and, in the **Port** field, type a port number.
   - **Pool** - Select, or create and then select, a pool of Citrix XML Brokers or View Connection servers.
9. To provide SSL capabilities between the BIG-IP system and the Citrix or the VMware View destination servers, for **Server Side SSL** select **Enable**.
10. From the **ACL Order** list, select **Last**, **After**, or **Specify**.
    This specifies where to add the ACL. Selecting **After** or **Specify** displays an additional list to select from.
11. To enable the system to log packets sent from any of the destination servers, from the **Log** list, select **Packet**.
12. To enable the first application from Citrix to run automatically, select the **Auto Launch** check box.

13. To open a cross-platform Java client for a Microsoft RDP connection, select the **Java Client** check box.

    When Java Client is enabled, Windows, Mac, and Linux clients can use RDP connections through the same connection. Also, these areas are disabled: Access to Local Resources and User Experience, and 32-bit color depth is disabled from Screen Properties.

14. To specify custom settings that affect the rendering of certain features for Citrix or Microsoft RDP, type text in the **Custom Parameters** field .

    The format of the value for each terminal resource is different.

    Custom parameters example for Citrix: `[Section1]Name1=Value1 Name2=Value2[Section2]`
    Custom parameters example for Microsoft RDP: `screen mode id:i:1use multimon:i:0desktopwidth:i:1440desktopheight:i:900session bpp:i:32`

Use these steps to enable Single Sign-On.

15. To configure Single Sign-On, for **Enable SSO** select **Enable**.
16. For RDP or VMware View remote desktop types, specify the **Username Source**, **Password Source**, and **Domain Source** fields.
17. For a Citrix remote desktop type, select from the **SSO Method** list and specify values for any additional fields that display.

Use these steps to configure additional settings for an RDP remote desktop resource type.

18. In the Application Properties area, to specify an **Application to Start**, type the full path to the application on the target server and prefix the application name with a pound (#) sign for published applications. For example, type `#app_name`.
19. In the Customization Settings for English area, in the **Caption** field type a caption for the remote desktop resource.
20. To save your changes, click the **Save & Close** button at the bottom of the screen.

Configuring Portal Access

Overview: What is portal access?

Portal access allows end users access to internal web applications with a web browser from outside the network. With portal access, the BIG-IP system managed by BIG-IQ communicates with back-end servers, and rewrites links in application web pages so that further requests from the client browser are directed back to the Access Policy Manager server. With portal access, the client computer requires no specialized client software other than a web browser.

Portal access provides clients with secure access to internal web servers, such as Microsoft OutlookWeb Access (OWA), Microsoft SharePoint, and IBM Domino Web Access. Using portal access functionality, you can also provide access to most web-based applications and internal web servers.

Portal access differs from network access, which provides direct access from the client to the internal network. Network access does not manipulate or analyze the content being passed between the client and the internal network. The portal access configuration gives the administrator both refined control over the applications that a user can access through Access Policy Manager, and content inspection for the application data. The other advantage of portal access is security. Even if a workstation might not meet requirements for security for full network access, such a workstation can be passed by the access policy to certain required web applications, without allowing full network access. In a portal access policy, the client computer itself never communicates directly with the end-point application. That means that all communication is inspected at a very high level, and any attacks originating on the client computer fail because the attack cannot navigate through the links that have been rewritten by the portal access engine.

Creating a portal access configuration

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
3. Expand **Connectivity / VPN** and click **Portal Access** > **Portal Access Lists**.
4. Click **Create**.
   The New Portal Access screen opens.
5. Type the name and an optional description.
6. From the **ACL Order** list, specify the placement for the resource.

Option	Description
Last	Select this option to place the new portal access resource last in the ACL list.
After	Select this option to select, from the list of configured ACLs, the ACL that this portal access resource should follow in sequence.
Specify	Select this option to specify an order number, for example, `0` or `631`for the ACL.

7. From **Configuration**, select **Basic** or **Advanced**.
   The **Advanced** option provides additional settings so you can configure a proxy host and port.
8. For the **Match Case for Paths** setting, select **Yes** to specify that portal access matches alphabetic case when matching paths in the portal access resource.

9. From the **Patching Type** list, select the patching type for the web application.

   For both full and minimal patching types, you can select or clear patching methods specific to your selection.

10. If you selected **Minimal Patching** and the **Host Patching** option, type a host search string, or multiple host search strings separated with spaces, and the host replace string, which must be the Access Policy Manager® virtual server IP address or fully qualified domain name.

11. To publish a link for the web application on the full webtop, or to use hosted content files, for the **Publish on Webtop** setting, select the **Enable** check box.

    Important: *Do not enable the* ***Publish on Webtop*** *setting if you are configuring the portal access resource for minimal patching.*

12. If you enabled **Publish on Webtop**, select whether the **Link Type** is an application URI or a file uploaded to the hosted content repository.

    - **Application URI:** This is the main URI used to start this portal access resource. You can configure other URIs with specific caching and compression settings by adding resource items to the portal access resource, after the main resource is configured.
    - **Hosted Content:** Use content uploaded to the hosted content repository to present on the webtop. When you select a hosted content file (typically a web-browser readable file), that file becomes the main destination for this webtop link.

      Note: *In the* ***Resource Items*** *area, you must add all resources that you have uploaded to the hosted content repository that apply to this particular hosted content link.*

13. In the Customization Settings for English area, in the **Caption** field, type a caption.

    The caption appears on the full webtop, and is required. This field is required even if you do not select the **Publish on webtop** option.

14. Optionally, in the **Detailed Description** field type a description for the web application.

15. In the **Image** field, specify an icon for the web application link. Click the **View/Hide** link to show the current icon.

16. If your application is behind a proxy server, to specify a proxy host and port, you must select **Advanced** for the configuration to display additional fields, and type the proxy host and proxy port.

    Important: *Portal access does not support forwarding HTTPS requests through the HTTPS proxy. If you specify the HTTPS scheme in the* ***Application URI*** *field and specify a proxy host, portal access does not forward the requests.*

17. To save your changes, click the **Save & Close** button at the bottom of the screen.

This completes the portal access resource configuration.

Add resource items to the portal access resource to provide functionality for your web applications.

Configuring Webtops

About webtops

There are three webtop types you can define on the Access module for BIG-IQ. You can define a network access only webtop, a portal access webtop, or a full webtop.

Important: *Do not assign a webtop for a portal access connection configured for minimal patching mode. This configuration does not work.*

- A network access webtop provides a webtop for an access policy branch to which you assign only a network access resource for starting a network access connection that provides full network access.
- A portal access webtop provides a webtop for an access policy branch to which you assign only portal access resources. When a user selects a resource, the BIG-IP device managed by BIG-IQ communicates with back-end servers and rewrites links in application web pages so that further requests from the client browser are directed back to the BIG-IP device managed by BIG-IQ.
- A full webtop provides an access policy ending for an access policy branch to which you can optionally assign portal access resources, app tunnels, remote desktops, and webtop links, in addition to network access tunnels. Then, the full webtop provides your clients with a web page on which they can choose resources, including a network access connection to start.

  Note: *If you add a network access resource with Auto launch enabled to the full webtop, the network access resource starts when the user reaches the webtop. You can add multiple network access resources to a webtop, but only one can have Auto launch enabled.*

Creating a webtop link

You can create and customize links that you can assign to full webtops. In this context, *links* are defined applications and websites that appear on a webtop, and can be clicked to open a web page or application. You can customize these links with descriptions and icons.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
3. Expand **Webtops** and click **Webtop Links**.
4. Click **Create**.
   The New Webtop Links screen opens.
5. From the **Link Type** list, select whether the link is a URI or hosted content.
   - If you selected **Application URI**, in the **Application URI** field, type the application URI.
   - If you selected **Hosted Content**, select the hosted file to use for the webtop link.
6. In the **Caption** field, type a descriptive caption.

   The **Caption** field is pre-populated with the text from the **Name** field. Type the link text that you want to appear on the web link.
7. If you want to add a detailed description, type it in the **Detailed Description** field.
8. To specify an icon image for the item on the webtop, click in the **Image** field and choose an image, or click the **Browse** button.

Click the **View/Hide** link to show or hide the currently selected image.

9. To save your changes, click the **Save & Close** button at the bottom of the screen.

The webtop link is now configured, and appears in the list, and on a full webtop assigned with the same action. You can edit the webtop link further, or assign it to an access policy.

Before you can use this webtop link, it must be assigned to an access policy with a full webtop, using either an advanced resource assign action or a webtop, links and sections assign action.

Creating a webtop section

Create a webtop section to specify a caption to display on a full webtop for a list of resources. Specify the order of the webtop section relative to other webtop sections.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
3. Expand **Webtops** and click **Webtop Sections**.
4. Click **Create**.
   The New Webtop Sections screen opens.
5. In the **Name** field, type a name for the webtop section.
6. From the **Display Order** list, select one the options.

   Specify the display order of this webtop section relative to others on the webtop.

   - **First**: Places this webtop section first.
   - **After**: When selected, an additional list displays; select a webtop section from it to place this webtop section after it in order.
   - **Specify**: When selected, an additional field displays. Type an integer in it to specify the absolute order for this webtop section.
7. From the **Initial State** list, select the initial display state:

   - **Expanded**: Displays the webtop section with the resource list expanded.
   - **Collapsed**: Displays the webtop section with the resource list collapsed.
8. To save your changes, click the **Save & Close** button at the bottom of the screen.

The webtop section is created.

Specify resources for this webtop section.

About uploading custom files to Access

You can upload custom files to the Access module of BIG-IQ® Centralized Management® to provide resources directly to users.

For example, you can upload BIG-IP Edge Client® installers, antivirus or firewall update packages, or Citrix receiver files for your users to download. You can upload custom images, web pages, Java archives, JavaScript files, CSS files, archive files, and many other types of files as well.

Optionally, you can compress and upload multiple files as a single ZIP archive file. When you upload an archive file, you can choose to either upload the compressed file, or upload and extract the compressed file.

Upload Only

Select this option to upload an archived file that must remain in archive format. For example, you can upload a ZIP file for a user to download, containing a package of documents, or an application and

related files. Some applications also use archived files; for example, you will upload a JAR file without extracting it.

Upload and Extract
Select this option to upload an archived file and extract it to the specified location. The folder hierarchy of the extracted file is preserved when you use this action. Select this option when you are uploading a collection of files that must be separated on the server for use by the end user; for example, to upload a web application that includes top-level HTML files, and subdirectories containing scripts, images, CSS, and other files.

Uploading files to Access

Before you upload multiple files to Access module of BIG-IQ® Centralized Management®, you can compress and combine the files into a ZIP archive file. Then, you can upload and extract the files in one step.

You can upload files to Access to provide content for public viewing, to provide pages and content to Portal Access connections, or to provide customized webtop links.

1. At the top of the screen, select **Configuration**, then on the left side of the screen, click **ACCESS** > **Access Groups**.
2. Click the name of the Access group that interests you.
   A new screen displays the group's properties.
3. Expand **Webtops** and click **Hosted Content** > **Manage Files**.
4. Click the **Upload** button.
   Click the **New Hosted Content Configuration** screen opens.
5. For the **Select File** setting, click the **Browse** button and select the file to upload.
   - To upload each file separately, select the first file, then repeat this step for all remaining files.
   - To upload all files at once from a compressed file, select the compressed file.

   The **Select File** and **File Name** fields are populated with the file name.
6. If you are uploading a compressed file that you want to extract, from the **File Action** list, select **Upload and Extract**.
7. To save your changes, click the **Save & Close** button at the bottom of the screen.
   The file appears in the Managed Files list.

You must associate any access profiles that will access hosted content with the hosted content repository.

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.

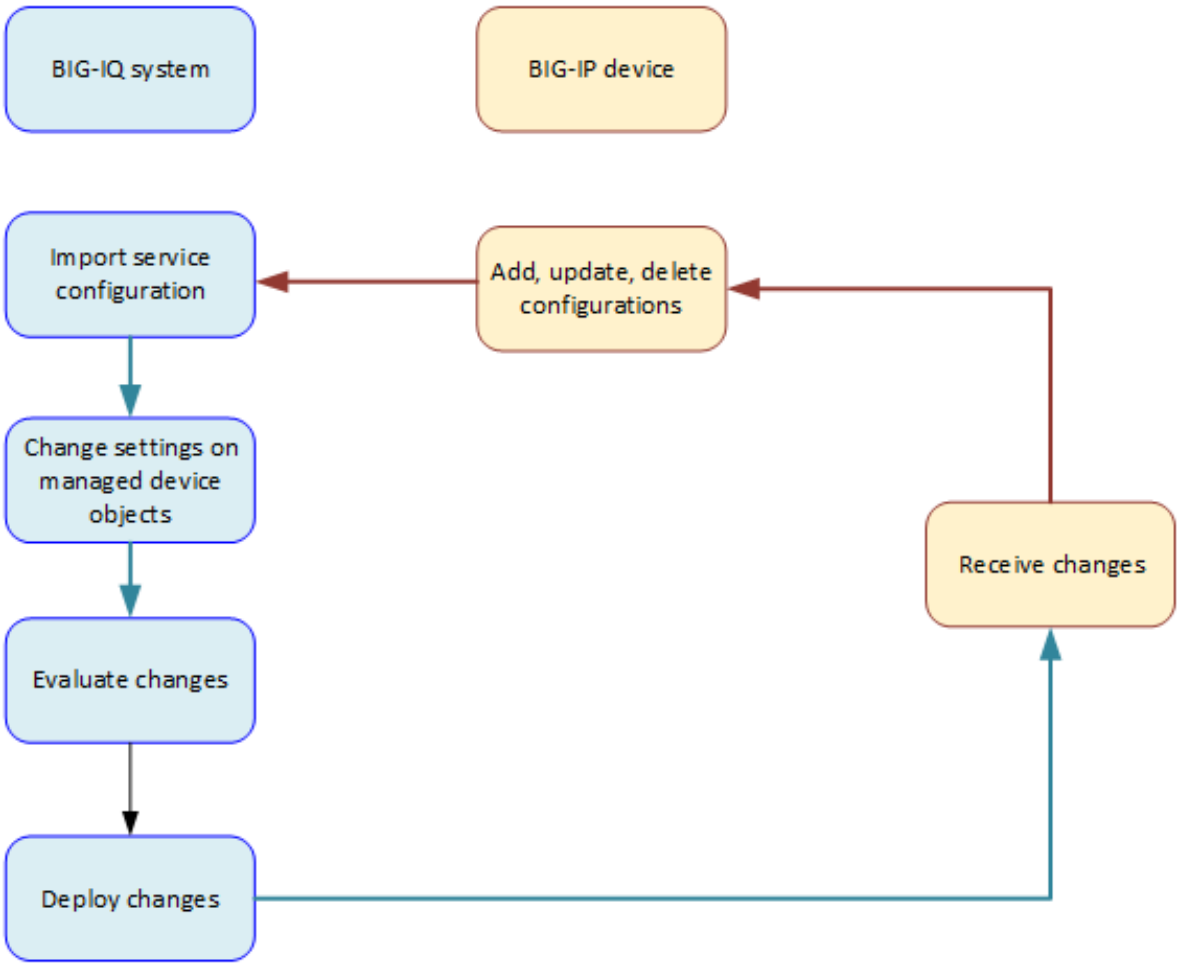


Figure 1: Ongoing change

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 on the left side of the screen, click **ACCESS** > **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® Centralized Management 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. ***Note:*** *Search results for a search on values in the Action column may match additional hidden values since the underlying metadata is being searched.*
Action: Task Status	Type the task status action name in the filter. Task status actions include: Start, Finish, Cancelled, and Failed. ***Note:*** *Search results for a search on values in the Action column may match additional hidden values since the underlying metadata is being searched.*
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.

Managing Object Pinning

What is object pinning?

You *pin* an object, such as a logging profile, to a pinning policy to have it included in a deployment. The pinning policy is associated with a BIG-IP® device and has the same name as the BIG-IP device. You do not create pinning policies. Pinning policies always exist to contain objects that get pinned to a policy.

You pin an object to a pinning policy for a BIG-IP device to mark the object as being used by the BIG-IP device configuration, and to have it deployed with that configuration and not deleted from the device. When an object is pinned for deployment to a BIG-IP device that is part of a cluster, the object is deployed to the other member of the cluster as well.

You use the Pinning Policies screen to pin policy objects so that they are deployed to a BIG-IP device, or to view the objects that are already pinned to be deployed to a BIG-IP device. The objects that can be selected for pinning differ depending on which service is being used. For example, only the Network Security service allows you to pin firewall policy objects, and only the Local Traffic service allows you to pin SMTP server objects. You can pin objects to, or unpin objects from, multiple BIG-IP device pinning policies at once.

Note: *Both the system and users can pin an object. But users can unpin only objects that are labeled as user pinned. For easy identification, objects pinned by a user are listed with the User identifier in the Pin Source Tags column on the Pinning Policy Properties screen. Any user can unpin a user pinned object.*

Pin objects to a BIG-IP device pinning policy

You pin objects, such as logging profiles, to BIG-IP®device pinning policies to ensure that the objects are deployed to BIG-IP devices. The process for pinning to a single BIG-IP device pinning policy differs from the process for pinning to several BIG-IP device pinning policies.

1. Open the Pinning Policies screen. How you access the screen depends on the service you are using.
   - To pin Local Traffic service objects, click **Configuration** > **LOCAL TRAFFIC** > **Pinning Policies**.
   - To pin Network Security service objects, click **Configuration** > **SECURITY** > **Network Security** > **Pinning Policies**.
   - To pin Shared Security service objects, click **Configuration** > **SECURITY** > **Shared Security** > **Pinning Policies**.
   - To pin Access service objects, click **Configuration** > **ACCESS** > **Access Groups** > **Pinning Policies**. An Access group must exist to see this menu item.
2. Decide whether to pin to a single BIG-IP device pinning policy, or multiple BIG-IP device pinning policies.
   - Go to Step 3 to pin objects to a single BIG-IP device pinning policy.
   - Go to Step 4 to pin objects to multiple BIG-IP device pinning policies.
3. To pin objects to a pinning policy for a single BIG-IP device:
   a) Click the name of the BIG-IP device pinning policy to which you will pin objects. (It has the same name as the associated BIG-IP device.)
   The properties screen opens.
   b) At the top of the area near the bottom of the screen, select the type of object to be pinned.

The screen lists objects of the type you selected.

c) Select the check box to the left of the objects to be pinned, and click **Add Selected**.

4. To pin objects to multiple BIG-IP device pinning policies:
   a) Select the check boxes for the BIG-IP device pinning policies to which to pin objects, and click **Pin to Multiple Policies**.
   The properties screen opens and displays the selected BIG-IP device pinning policies.
   b) In the area near the bottom of the screen, select the type of object to be pinned.
   The screen lists objects of the type you selected.
   c) Select the check box for objects to be pinned and click **Add Selected**.
5. Save your work.

A dialog box displays the success of the pinning operation. The object, or objects, are pinned to the pinning policy for the BIG-IP device, or devices, and will be deployed with them.

Unpin objects from a BIG-IP device pinning policy

You unpin objects, such as logging profiles, from a BIG-IP® device pinning policy when they no longer need to be deployed with the BIG-IP device. The process for unpinning from a single BIG-IP device pinning policy differs from the process for unpinning from several BIG-IP device pining policies.

Note: *Both the system and users can pin an object. But users can unpin only objects that are labeled as user pinned. For easy identification, objects pinned by a user are listed with the User identifier in the Pin Source Tags column on the Pinning Policy Properties screen. Any user can unpin a user pinned object.*

1. Open the Pinning Policies screen. How you access the screen depends on the service you are using.
   - To unpin Local Traffic service objects, click **Configuration** > **LOCAL TRAFFIC** > **Pinning Policies**.
   - To unpin Network Security service objects, click **Configuration** > **SECURITY** > **Network Security** > **Pinning Policies**.
   - To unpin Shared Security service objects, click **Configuration** > **SECURITY** > **Shared Security** > **Pinning Policies**.
   - To pin Access service objects, click **Configuration** > **ACCESS** > **Access Groups** > **Pinning Policies**. An Access group must exist to see this menu item.
2. Decide whether to unpin from a single BIG-IP device pinning policy, or from multiple BIG-IP device pinning policies.
   - Go to Step 3 to unpin objects from a single BIG-IP device pinning policy.
   - Go to Step 4 to unpin objects from multiple BIG-IP device pinning policies.
3. To unpin objects from a single BIG-IP device pinning policy:
   a) Click the name of the BIG-IP device pinning policy from which to unpin objects.
   The properties screen opens.
   b) In the Selected Resources area, expand the resource type of the object you want to unpin.
   The screen lists objects of the type you selected.
   c) Select the check box for the objects to be unpinned and click **Remove**.

   Both the system and users can pin an object. But users can unpin only objects that are labeled as user pinned. For easy identification, objects pinned by a user are listed with the User identifier in the Pin Source Tags column on the Pinning Policy Properties screen. Any user can unpin a user pinned object.
4. To unpin objects from multiple BIG-IP device pinning policies:

a) Select the check boxes for the BIG-IP device pinning policies from which to unpin objects, and click **Unpin from Multiple Policies**.
The properties screen opens and displays the selected BIG-IP device pinning policies.
b) In the lower area of the screen, select the type of object to be unpinned.
The screen lists objects of the type you selected.
c) Select the check box for the objects to unpin and click **Add Selected**.

The Selected Resources area lists the objects to be unpinned. Both the system and users can pin an object. But users can unpin only objects that are labeled as user pinned. For easy identification, objects pinned by a user are listed with the User identifier in the Pin Source Tags column on the Pinning Policy Properties screen. Any user can unpin a user pinned object.

5. Save your work.

A dialog box displays the success of the unpinning operation. The object or objects are unpinned from the BIG-IP device pinning policy and will no longer be deployed to it.

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 December 27, 2017.

Publication Number

MAN-0615-04

Copyright

Trademarks

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

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

Patents

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

Link Controller Availability

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

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a

residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

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

Canadian Regulatory Compliance

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

Standards Compliance

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

Index

A

B

C

D

E

F

H

I

K

L

M

O

P

R

S

T

U

V

W