BIG-IP® Access Policy Manager®: Secure Web Gateway

Version 13.1

Table of Contents

BIG-IP APM Secure Web Gateway Overview

About APM Secure Web Gateway

BIG-IP® Access Policy Manager® (APM®) implements a Secure Web Gateway (SWG) by adding access control, based on URL categorization, to forward proxy. With APM, you can create a configuration to protect your network assets and end users from threats, and enforce a use and compliance policy for Internet access. Users that access the Internet from the enterprise go through APM, which can allow or block access to URL categories or indicate that the user should confirm the URL before access can be allowed.

About APM benefits for web access

BIG-IP® Access Policy Manager® (APM®) supports basic web site access control purely based on user-defined URL categories. This feature is a part of base APM functionality, without requiring an SWG subscription. The benefits include:

- URL filtering capability for outbound web traffic.
- Monitoring and gating outbound traffic to maximize productivity and meet business needs.
- User identification or authentication (or both) tied to logging, and access control compliance and accountability.
- Visibility into SSL traffic.
- Reports on blocked requests and all requests. (Reports depend on event logging settings.)
- Ability to interactively request additional authentication for sensitive resources and provide time-limited access to them in subsessions.
- Ability to interactively request confirmation before allowing or blocking access to resources that might not, in all instances, provide benefit to the business. Confirmation and access take place in a subsession with its own lifetime and timeout values.

About Secure Web Gateway subscription benefits

A BIG-IP® system with Access Policy Manager® (APM®) and a Secure Web Gateway (SWG) subscription provides these benefits over those provided by APM alone:

- A database with over 150 predefined URL categories and 60 million URLs.
- A service that regularly updates the URL database as new threats and URLs are identified.
- Identification of malicious content and the means to block it.
- Web application controls for application types, such as social networking and Internet communication in corporate environments.
- Support for Safe Search, a search engine feature that can prevent offensive content and images from showing up in search results.
- A dashboard with statistical information about traffic logged by the BIG-IP system for SWG. Graphs, such as Top URLs by Request Count and Top Categories by Blocked Request Count, summarize activities over time and provide access to underlying statistics.

SWG subscription benefits extend these APM benefits:

- URL filtering capability for outbound web traffic.
- Monitoring and gating outbound traffic to maximize productivity and meet business needs.

- User identification or authentication (or both) tied to logging, and access control compliance and accountability.
- Visibility into SSL traffic.
- Reports on blocked requests and all requests. (Reports depend on event logging settings.)
- Ability to interactively request additional authentication for sensitive resources and provide time-limited access to them in subsessions.
- Ability to interactively request confirmation before allowing or blocking access to resources that might not, in all instances, provide benefit to the business. Confirmation and access take place in a subsession with its own lifetime and timeout values.

About the URL database URL categories

Note: *A URL database is available only on a BIG-IP® system with an SWG subscription.*

The Secure Web Gateway URL database supplies over 150 URL categories and identifies over 60 million URLs that fit within these categories. In addition, you can create custom categories if needed and add URLs to any category, custom or otherwise. You can also use custom categories to define blacklists and whitelists.

About user-defined URL categories

Without a URL database, an administrator tasked with treating only a few URLs differently can specify criteria for matching those few URLs in a simple **URL Branching** action in a per-request policy. An administrator who must categorize and filter a large number of URLs can, however, accomplish this with Access Policy Manager® (APM®) user-defined URL categories.

About APM session management cookies and forward proxy

When Access Policy Manager® (APM®) acts as a forward proxy, APM does not use session management cookies. If presented with an APM session management cookie while acting as a forward proxy, APM ignores the cookie.

Explicit Forward Proxy Configuration

Overview: Configuring APM to act as an explicit forward proxy

For explicit forward proxy, you configure client browsers to point to a forward proxy server. A forward proxy server establishes a tunnel for SSL traffic. Other virtual servers (wildcard SSL and wildcard forwarding IP virtual servers) listen on the tunnel. The listener that best matches the web traffic directed to the forward proxy server handles the traffic.

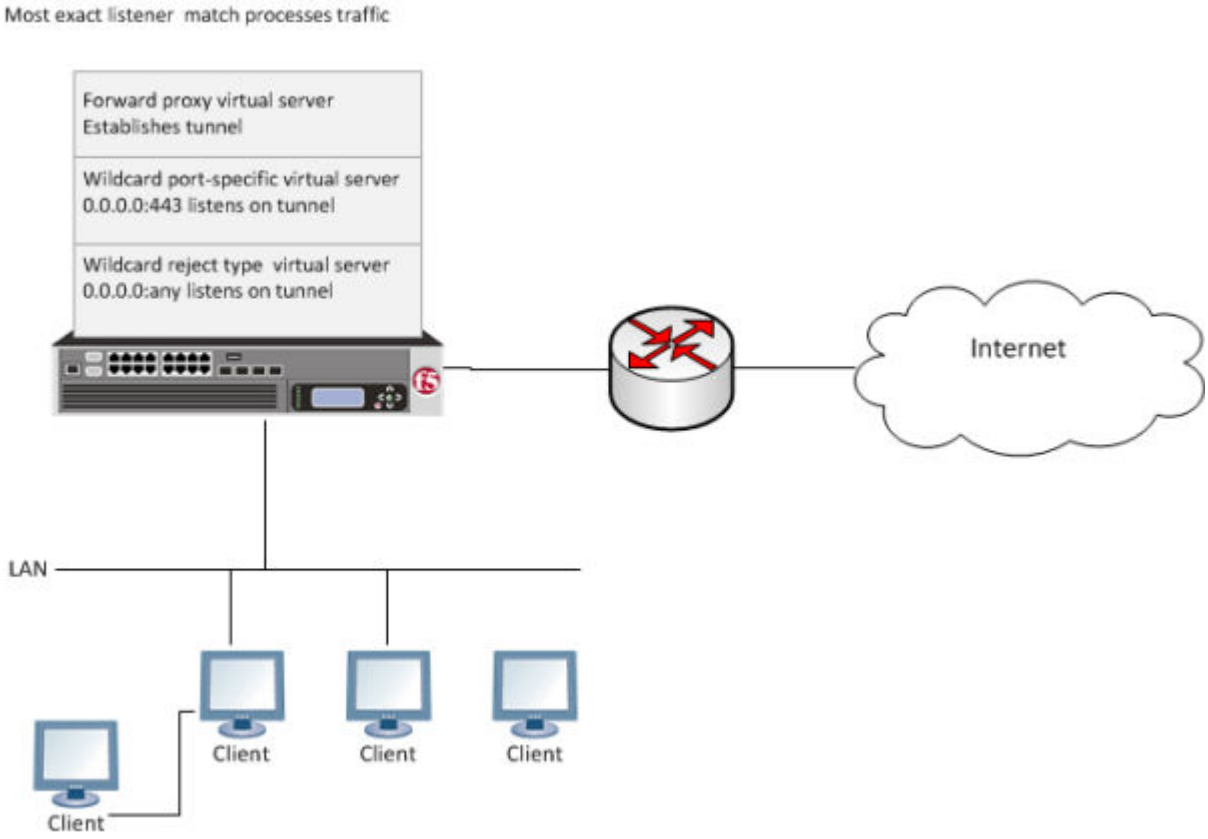


Figure 1: Explicit forward proxy configuration

Task summary

Use these procedures to configure the virtual servers, SSL profiles, access profile, and tunnel, that you need to support explicit forward proxy. When you are done, you must add an access policy and a per-request policy to this configuration to process traffic as you want.

Task list

Browser and firewall configuration best practices for explicit forward proxy
Creating a DNS resolver
Adding forward zones to a DNS resolver
Creating a tunnel for SSL forward proxy traffic
Creating a custom HTTP profile for explicit forward proxy
Creating an access profile for explicit forward proxy
Creating a virtual server to use as the forward proxy server

Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
Creating a virtual server for SSL forward proxy traffic
Creating a virtual server to reject traffic

About the iApp for Secure Web Gateway configuration

When deployed as an application service, the Secure Web Gateway (SWG) iApps® template can set up either an explicit or a transparent forward proxy configuration. The template is designed for use on a system provisioned and licensed with SWG. To download a zipped file of iApp templates from the F5 Downloads site at (`downloads.f5.com`), you must register for an F5 support account. In the zipped file, a README and template for F5 Secure Web Gateway are located in the RELEASE_CANDIDATE folder.

Browser and firewall configuration best practices for explicit forward proxy

In any deployment of explicit forward proxy, you must consider how best to configure browsers on client systems to point to the proxy server and how to configure your firewall to prevent users from bypassing the proxy. Here are some best practices to consider.

Table 1: Client browser and firewall configuration

Configuration	Recommendation
Client browser	Consider using a group policy that points to a Proxy Auto-Configuration (PAC) file to distribute the configuration to clients and periodically update it.
Firewall	A best practice might be to configure the firewall to trust outbound connections from Access Policy Manager® (APM®) only. Note that possibly not all applications will work with a firewall configured this way. (APM uses ports 80 and 443.)

Overview: Configuring APM to act as an explicit forward proxy
Overview: Configuring APM to act as an explicit forward proxy
Creating a DNS resolver

Creating a DNS resolver

You configure a DNS resolver on the BIG-IP® system to resolve DNS queries and cache the responses. The next time the system receives a query for a response that exists in the cache, the system returns the response from the cache.

1. On the Main tab, click **Network** > **DNS Resolvers** > **DNS Resolver List**.
   The DNS Resolver List screen opens.
2. Click **Create**.
   The New DNS Resolver screen opens.
3. In the **Name** field, type a name for the resolver.
4. Click **Finished**.

Note: *When you create an OAuth Server, creating a DNS Resolver with a forward zone named . (period) is mandatory to forward all requests.*

Adding forward zones to a DNS resolver

Before you begin, gather the IP addresses of the nameservers that you want to associate with a forward zone.

Add a forward zone to a DNS resolver when you want the BIG-IP® system to forward queries for particular zones to specific nameservers for resolution in case the resolver does not contain a response to the query.

Note: *Creating a forward zone is optional. Without one, a DNS resolver can still make recursive name queries to the root DNS servers; the virtual servers using the cache must have a route to the Internet.*

When you create an OAuth Server, creating a DNS Resolver with a forward zone named . (period) is mandatory.

1. On the Main tab, click **Network** > **DNS Resolvers** > **DNS Resolver List**.
   The DNS Resolver List screen opens.
2. Click the name of the resolver you want to modify.
   The properties screen opens.
3. On the menu bar, click **Forward Zones**.
   The Forward Zones screen displays.
4. Click the **Add** button.

   Note: *You add more than one zone to forward based on the needs of your organization.*

5. In the **Name** field, type the name of a subdomain or type the fully qualified domain name (FQDN) of a forward zone.

   Note: *To forward all requests (such as when creating an OAuth server), specify . (period) as the name.*

   For example, either `example` or `site.example.com` would be valid zone names.
6. Add one or more nameservers:
   a) In the **Address** field, type the IP address of a DNS nameserver that is considered authoritative for this zone.

      Based on your network configuration, add IPv4 or IPv6 addresses, or both.
   b) Click **Add**.
      The address is added to the list.

   Note: *The order of nameservers in the configuration does not impact which nameserver the system selects to forward a query to.*

7. Click **Finished**.

Creating a tunnel for SSL forward proxy traffic

You create a tunnel to support SSL traffic in a configuration where Access Policy Manager® (APM®) acts as an explicit forward proxy.

Note: *Alternatively, you can use a preconfigured tunnel, http-tunnel.*

1. On the Main tab, click **Network** > **Tunnels** > **Tunnel List**.
   The Tunnel List screen opens.
2. Click **Create**.

3. In the **Name** field, type a name.
4. From the **Encapsulation Type** menu, select **tcp-forward**.
5. Click **Finished**.
   The Tunnel List screen displays the tunnel with tcp-forward in the Profile column.

Creating a custom HTTP profile for explicit forward proxy

An HTTP profile defines the way that you want the BIG-IP® system to manage HTTP traffic.

Note: *To act an explicit forward proxy, Access Policy Manager® (APM®) requires a DNS resolver that you select in the HTTP profile.*

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **HTTP**.
   The HTTP profile list screen opens.
2. Click **Create**.
   The New HTTP Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Proxy Mode** list, select **Explicit**.
5. For **Parent Profile**, retain the **http-explicit** setting.
6. Select the **Custom** check box.
7. Scroll down to the Explicit Proxy area.
8. From the **DNS Resolver** list, select the DNS resolver you configured previously.
9. In the **Tunnel Name** field, you can retain the default value, **http-tunnel**, or type the name of a tunnel if you created one.

   APM requires a tunnel with tcp-forward encapsulation to support SSL traffic for explicit forward proxy.
10. From the **Default Connect Handling** list, retain the default setting **Deny**.

    Any CONNECT traffic goes through the tunnel to the virtual server that most closely matches the traffic; if there is no match, the traffic is blocked.
11. Click **Finished**.

The custom HTTP profile now appears in the HTTP profile list screen.

Creating an access profile for explicit forward proxy

Create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.

   Note: *An access profile name must be unique among all per-session profile and per-request policy names.*
4. From the **Profile Type** list, select **SWG-Explicit**.

   Selecting this type ensures that only access policy items that are valid for explicit forward proxy are available in the visual policy editor when you configure an access policy.
5. In the Configurations area for the **User Identification Method** list, select one of these methods:

- **IP Address**: Select this method only in an environment where a client IP address is unique and can be trusted.
- **Credentials**: Select this method to identify users using NTLM authentication.

6. If you selected **Credentials** for the **User Identification Method**, you must select an entry from the **NTLM Auth Configuration** list.
7. If you selected **IP Address** for the **User Identification Method**, you can also select an entry from the **NTLM Auth Configuration** list to use NTLM authentication before a session starts.

   In the case of a shared machine, an IP address might already be associated with a user or a session. Using NTLM authentication ensures that the system can associate the IP address with the correct session (new or existing) or with a new user each time a user logs on to a shared machine.
8. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
9. Click **Finished**.
   The Access Profiles list screen displays.

The access profile displays in the Access Profiles List. Default-log-setting is assigned to the access profile.

Creating a virtual server to use as the forward proxy server

You specify a virtual server to handle forward proxy traffic. In an explicit proxy configuration, client browser configurations specify this virtual server as the proxy server.

Note: *Use this virtual server for forward proxy traffic only. You should not try to use it for reverse proxy too; do not add a pool to it. This virtual server is, in effect, a bastion host.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.

   Type a destination address in this format: `162.160.15.20`.
5. From the **Configuration** list, select **Advanced**.
6. In the **Service Port** field, type the port number to use for forward proxy traffic.

   Typically, the port number is `3128` or `8080`.
7. From the **HTTP Profile** list, select the HTTP profile you configured earlier.
8. For the **HTTP Connect Profile** setting, be sure to retain the default value **None**.
9. From the **VLAN and Tunnel Traffic** list, select **Enabled on**.
10. For the **VLANs and Tunnels** setting, move the VLAN on the BIG-IP® system that connects to the internal networks to the **Selected** list.
11. From the **Source Address Translation** list, select **Auto Map**.
12. Click **Finished**.

After you configure an access policy and a per-request policy, update this virtual server to specify them.

Creating a custom Client SSL forward proxy profile

Creating a Client SSL forward proxy profile makes it possible for client and server authentication, while still allowing the BIG-IP® system to perform data optimization, such as decryption and encryption. This profile applies to client-side SSL forward proxy traffic only.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client SSL profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **clientssl**.
5. To avoid issues with privacy concerns, you might need to enable SSL forward proxy bypass for URLs that expose personal user information, such as those for financial or government sites.
   a) Scroll down to the **SSL Forward Proxy** list, and select **Advanced**.
   b) Select the **Custom** check box for the SSL Forward Proxy area.
   c) From the **SSL Forward Proxy** list, select **Enabled**.
      You can update this setting later but only while the profile is not assigned to a virtual server.
   d) From the **CA Certificate** list, select a certificate.
   e) From the **CA Key** list, select a key.
   f) In the **CA Passphrase** field, type a passphrase.
   g) In the **Confirm CA Passphrase** field, type the passphrase again.
   h) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
   i) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
   j) (Optional) For the **Certificate Extensions List** setting, select the extensions that you want in the **Available extensions** field, and move them to the **Enabled Extensions** field using the **Enable** button.
   k) From the **SSL Forward Proxy Bypass** list, select **Enabled**.
      You can update this setting later but only while the profile is not assigned to a virtual server.
      Additional settings display.
   l) For **Default Bypass Action**, retain the default value **Intercept**.
      You can override the value of this action on a case-by-case basis in the per-request policy for the virtual server.

   Note: *Bypass and intercept lists do not work with per-request policies. Retain the setting* ***None*** *for the remainder of the fields.*
6. Click **Finished**.

The custom Client SSL forward proxy profile now appears in the Client SSL profile list screen.

Creating a custom Server SSL profile

Create a custom server SSL profile to support SSL forward proxy.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The Server SSL profile list screen opens.
2. Click **Create**.
   The New Server SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For **Parent Profile**, retain the default selection, **serverssl**.

5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. From the **SSL Forward Proxy** list, select **Enabled**.

   You can update this setting later, but only while the profile is not assigned to a virtual server.
8. From the **SSL Forward Proxy Bypass** list, select **Enabled** (or retain the default value **Disabled**).

   The values of the **SSL Forward Proxy Bypass** settings in the server SSL and the client SSL profiles specified in a virtual server must match. You can update this setting later but only while the profile is not assigned to a virtual server.
9. Scroll down to the **Secure Renegotiation** list and select **Request**.
10. Click **Finished**.

The custom Server SSL profile is now listed in the SSL Server profile list.

Creating a virtual server for SSL forward proxy traffic

You specify a port-specific wildcard virtual server to handle SSL traffic. This virtual server listens on the tunnel that the forward proxy server establishes.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the custom Client SSL proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable proxy SSL functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the Proxy SSL settings.
   - Create new Client SSL and Server SSL profiles and configure the Proxy SSL settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable proxy SSL functionality.

   ---
9. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the custom Server SSL proxy profile you previously created and move the name to the **Selected** list.

   Important: *To enable SSL proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the Proxy SSL settings.
   - Create new Client SSL and Server SSL profiles and configure the Proxy SSL settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL proxy functionality.

   ---

10. From the **VLAN and Tunnel Traffic** list, select **Enabled on**.
11. For the **VLANs and Tunnels** setting, move either the tunnel you configured earlier or the default tunnel, **http-tunnel**, to the **Selected** list.

    This must be the same tunnel that you specified in the HTTP profile for the virtual server for forward proxy.
12. From the **Source Address Translation** list, select **Auto Map**.
13. For the **Address Translation** setting, clear the **Enabled** check box.
14. Click **Finished**.

The virtual server now appears in the Virtual Server List screen.

After you configure an access policy and a per-request policy, update this virtual server to specify them.

Creating a virtual server to reject traffic

You create a reject type virtual server to reject any IP traffic with URLs that are incomplete, or otherwise misconfigured for use with forward proxy. This virtual server listens on the tunnel that the forward proxy server establishes.

Note: *Secure Web Gateway does not support application access and network access tunnels.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. From the **Type** list, select **Reject**.
5. In the **Source Address** field, type `0.0.0.0/0`.
6. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
7. From the **Service Port** list, select ***All Ports**.
8. From the **Protocol** list, select **TCP**.
9. From the **VLAN and Tunnel Traffic** list, select **Enabled on**.
10. For the **VLANs and Tunnels** setting, select the tunnel you configured earlier, or select the default tunnel, **http-tunnel**, and move it to the **Selected** list.

    This must be the same tunnel that is specified in the virtual server for the forward proxy server.
11. Click **Finished**.

Implementation result

You now have the profiles and virtual servers that you need for explicit forward proxy.

Important: *Before you configure browsers to send traffic to this configuration, you need to configure an access policy and a per-request policy and specify them in the virtual servers.*

Access policy and per-request policy configuration depends on what you are trying to do. Look for configuration examples that categorize and filter traffic, intercept or bypass SSL traffic, forward traffic to a third-party proxy server, and so on.

About APM ACLs and explicit forward proxy

Only L7 ACLs work with Access Policy Manager® (APM®) explicit forward proxy.

Overview: Processing RDP traffic on a device configured for explicit forward proxy

If you configure Access Policy Manager® APM® as a gateway for RDP clients and configure APM to act as an explicit forward proxy on the same BIG-IP® system, you need to complete an additional configuration step to ensure that APM can process the RDP client traffic. The configuration F5 recommends for explicit forward proxy includes a catch-all virtual server, which listens on all IP addresses and all ports, on an HTTP tunnel interface.

When a programmatic API queries listeners for a specific IP and port, the query covers all interfaces and tunnels. As a result, the catch-all virtual server will always match. Sending traffic using this tunnel results in all packets being dropped because this virtual server is configured as a reject type of virtual server.

To prevent RDP client traffic from being dropped, add an additional wildcard port-specific virtual server on the HTTP tunnel interface.

Note: *Removing the catch-all virtual server from the HTTP tunnel interface is not recommended because doing so is counterproductive for security.*

Creating a virtual server for RDP client traffic

You specify a port-specific wildcard virtual server to match RDP client traffic on the HTTP tunnel interface for the Secure Web Gateway (SWG) explicit forward proxy configuration.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `3389`.
6. From the **Configuration** list, select **Advanced**.
7. From the **VLAN and Tunnel Traffic** list, select **Enabled on**.
8. For the **VLANs and Tunnels** setting, move the HTTP tunnel interface used in the SWG explicit forward proxy configuration to the **Selected** list.

   The default tunnel is **http-tunnel**.

   This must be the same tunnel specified in the HTTP profile for the virtual server for forward proxy.
9. For the **Address Translation** setting, clear the **Enabled** check box.
10. Click **Finished**.

The virtual server now appears in the Virtual Server List screen.

About wildcard virtual servers on the HTTP tunnel interface

In the recommended Secure Web Gateway explicit forward proxy configuration, client browsers point to a forward proxy server that establishes a tunnel for SSL traffic. Additional wildcard virtual servers listen on the HTTP tunnel interface. The listener that best matches the web traffic directed to the forward proxy server handles the traffic.

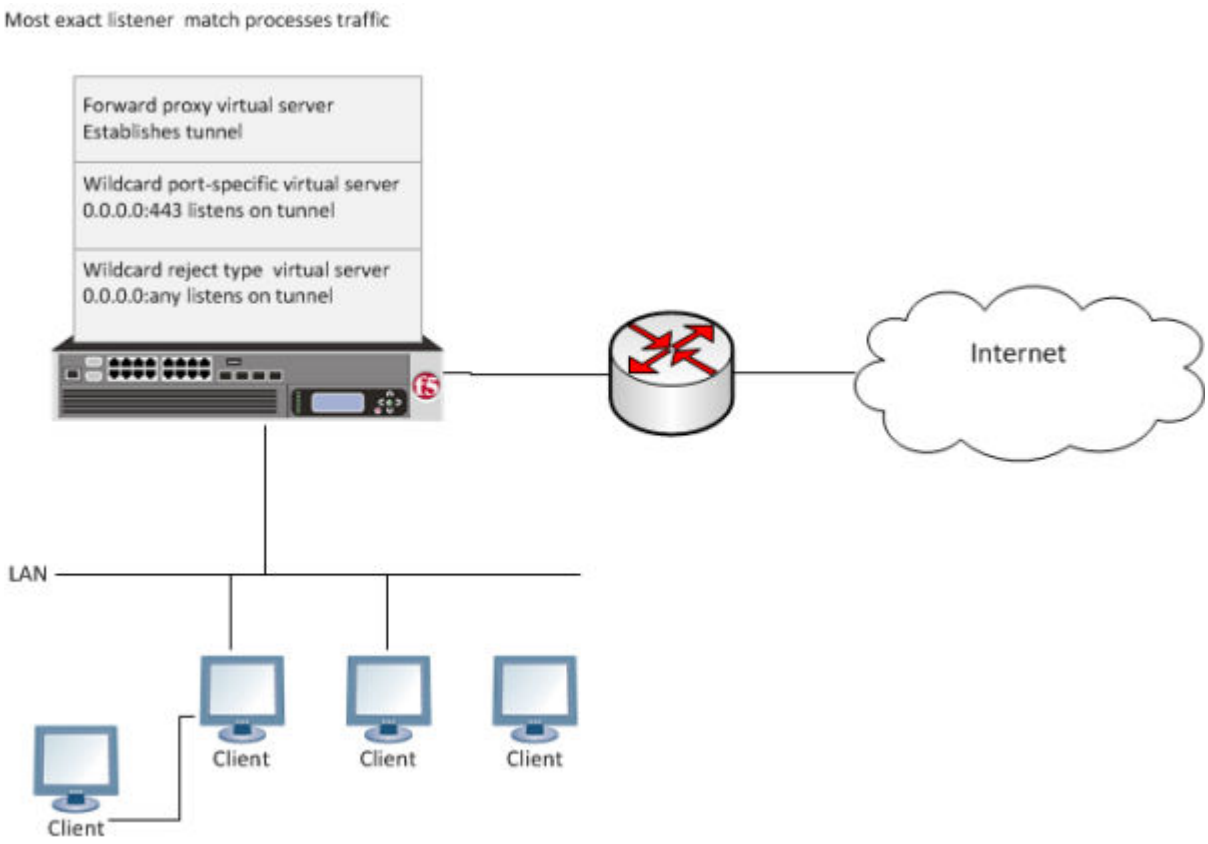


Figure 2: Explicit forward proxy configuration

Transparent Forward Proxy Configurations

Overview: Configuring transparent forward proxy

In transparent forward proxy, you configure your internal network to forward web traffic to the BIG-IP® system with Access Policy Manager® (APM®) configured to act as a forward proxy. Use this configuration when your topology includes a router on which you can configure policy-based routing or Web Cache Communication Protocol (WCCP) to send any traffic for ports 80 and 443 to the BIG-IP system.

This implementation describes only the configuration required on the BIG-IP system.

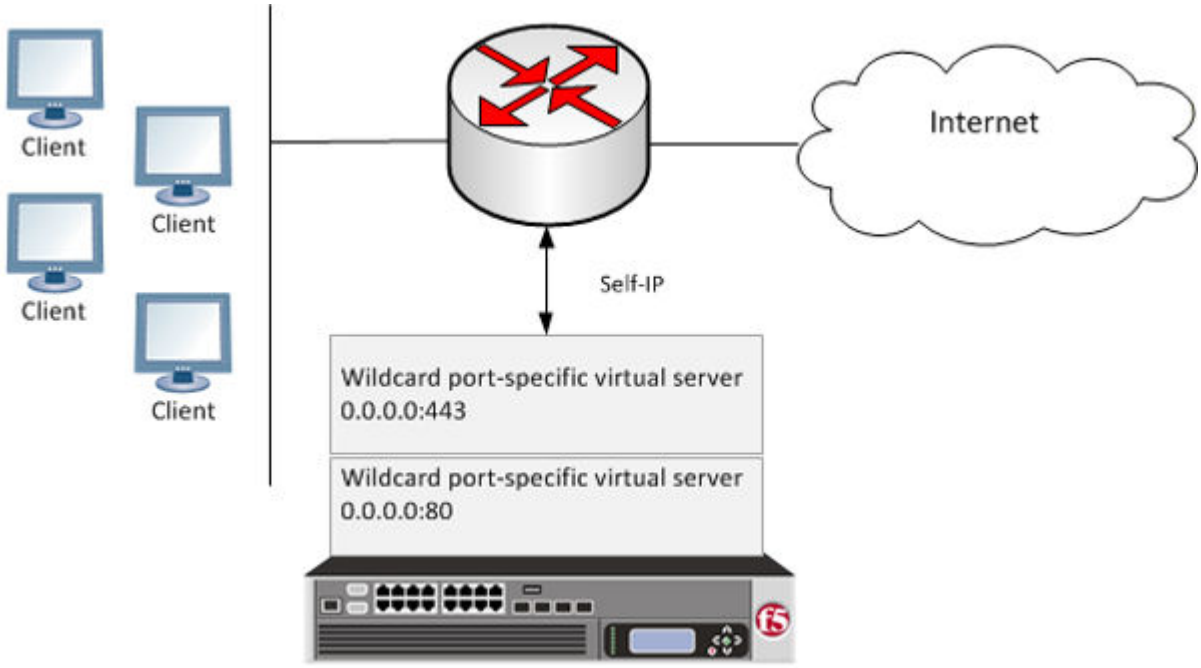


Figure 3: APM transparent forward proxy deployment

The router sends traffic to the self-ip address of a VLAN configured on the BIG-IP system. Virtual servers listen on the VLAN and process the traffic that most closely matches the virtual server address. APM identifies users without using session management cookies. A per-request policy, configured to use action items that determine the URL category and apply a URL filter, controls access.

Note: *Transparent forward proxy provides the option to use a captive portal. To use this option, you need an additional virtual server, not shown in the figure, for the captive portal primary authentication server.*

Task summary

Use these procedures to configure the virtual servers, SSL profiles, access profile, and VLAN that you need to support transparent forward proxy. When you are done, you must add an access policy and a per-request policy to this configuration to process traffic as you want.

Task list

Creating a VLAN for transparent forward proxy
Assigning a self IP address to a VLAN
Creating an access profile for transparent forward proxy

About the iApp for Secure Web Gateway configuration

When deployed as an application service, the Secure Web Gateway (SWG) iApps® template can set up either an explicit or a transparent forward proxy configuration. The template is designed for use on a system provisioned and licensed with SWG. To download a zipped file of iApp templates from the F5 Downloads site at (`downloads.f5.com`), you must register for an F5 support account. In the zipped file, a README and template for F5 Secure Web Gateway are located in the RELEASE_CANDIDATE folder.

About user identification with a logon page

User identification by IP address is a method that is available for these access profile types: SWG-Explicit, SWG-Transparent, and LTM-APM.

Note: *Identify users by IP address only when IP addresses are unique and can be trusted.*

To support this option, a logon page must be added to the access policy to explicitly identify users. The logon page requests user credentials and validates them to identify the users. For explicit forward proxy, a 407 response page is the appropriate logon page action. For transparent forward proxy, a 401 response page is the appropriate logon page action. For LTM-APM, the Logon Page action is appropriate.

F5® BIG-IP® Access Policy Manager® (APM®) maintains an internal mapping of IP addresses to user names.

About user identification with an SWG F5 agent

Transparent user identification makes a best effort to identify users without requesting credentials. It is not authentication. It should be used only when you are comfortable accepting a best effort at user identification.

Transparent user identification is supported in Secure Web Gateway (SWG) configurations for either explicit or transparent forward proxy. An agent obtains data and stores a mapping of IP addresses to user names in an IF-MAP server. An F5® DC Agent queries domain controllers. An F5 Logon Agent runs a script when a client logs in and can be configured to run a script when the client logs out.

Note: *Agents are available only on a BIG-IP® system with an SWG subscription.*

In an access policy, a Transparent Identity Import item obtains the IP-address-to-username-mapping from the IF-MAP server. This item can be used alone for determining whether to grant access or be paired with another query to look up the user or validate user information.

To support this option, either the Secure Web Gateway F5 DC Agent or F5 Logon Agent must be downloaded, installed, and configured.

Creating a VLAN for transparent forward proxy

You need a VLAN on which the forward proxy can listen. For increased security, the VLAN should directly face your clients.

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
   The New VLAN screen opens.
3. In the **Name** field, type a unique name for the VLAN.
4. For the **Interfaces** setting,
   a) From the **Interface** list, select an interface number.
   b) From the **Tagging** list, select **Untagged**.
   c) Click **Add**.
5. Click **Finished**.
   The screen refreshes, and displays the new VLAN in the list.

The new VLAN appears in the VLAN list.

Assigning a self IP address to a VLAN

Assign a self IP address to a VLAN on which the forward proxy listens.

1. On the Main tab, click **Network** > **Self IPs**.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP address.
4. In the **IP Address** field, type the IP address of the VLAN.
   The system accepts IPv4 and IPv6 addresses.
5. In the **Netmask** field, type the network mask for the specified IP address.
   For example, you can type `255.255.255.0`.
6. From the **VLAN/Tunnel** list, select the VLAN.
7. Click **Finished**.
   The screen refreshes, and displays the new self IP address.

Creating an access profile for transparent forward proxy

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.

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

4. From the **Profile Type** list, select **SWG-Transparent**.

Note: *After you complete this step, the* ***User Identification Method*** *is set to* ***IP Address*** *and cannot be changed.*

Additional settings display.

5. To use NTLM authentication before a session starts, from the **NTLM Auth Configuration** list select a configuration.

Important: *For NTLM authentication to work, you must also enable the* ***Captive Portals*** *setting and specify an IP address in the* ***Primary Authentication URI*** *field for the virtual server that you configure for the captive portal.*

In the case of a shared machine, an IP address might already be associated with a user or a session. Using NTLM authentication ensures that the system can associate the IP address with the correct session (new or existing) or with a new user each time a user logs on to the shared machine.

6. To direct users to a captive portal, for **Captive Portal** select **Enabled** and, in the **Primary Authentication URI** field, type the URI.

   You might specify the URI of your primary authentication server if you use single sign-on across multiple domains. Users can then access multiple back-end applications from multiple domains and hosts without needing to re-enter their credentials, because the user session is stored on the primary domain.

   For example, you might type `https://logon.siterequest.com` in the field.

7. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.

8. Click **Finished**.
   The Access Profiles list screen displays.

The access profile displays in the Access Profiles List. Default-log-setting is assigned to the access profile.

Creating a custom Client SSL forward proxy profile

Creating a Client SSL forward proxy profile makes it possible for client and server authentication, while still allowing the BIG-IP® system to perform data optimization, such as decryption and encryption. This profile applies to client-side SSL forward proxy traffic only.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client SSL profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **clientssl**.
5. To avoid issues with privacy concerns, you might need to enable SSL forward proxy bypass for URLs that expose personal user information, such as those for financial or government sites.
   a) Scroll down to the **SSL Forward Proxy** list, and select **Advanced**.
   b) Select the **Custom** check box for the SSL Forward Proxy area.
   c) From the **SSL Forward Proxy** list, select **Enabled**.

      You can update this setting later but only while the profile is not assigned to a virtual server.
   d) From the **CA Certificate** list, select a certificate.
   e) From the **CA Key** list, select a key.
   f) In the **CA Passphrase** field, type a passphrase.

g) In the **Confirm CA Passphrase** field, type the passphrase again.
h) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
i) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
j) (Optional) For the **Certificate Extensions List** setting, select the extensions that you want in the **Available extensions** field, and move them to the **Enabled Extensions** field using the **Enable** button.
k) From the **SSL Forward Proxy Bypass** list, select **Enabled**.

You can update this setting later but only while the profile is not assigned to a virtual server.

Additional settings display.

l) For **Default Bypass Action**, retain the default value **Intercept**.

You can override the value of this action on a case-by-case basis in the per-request policy for the virtual server.

Note: *Bypass and intercept lists do not work with per-request policies. Retain the setting* ***None*** *for the remainder of the fields.*

---

6. Click **Finished**.

The custom Client SSL forward proxy profile now appears in the Client SSL profile list screen.

Creating a custom Server SSL profile

Create a custom server SSL profile to support SSL forward proxy.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The Server SSL profile list screen opens.
2. Click **Create**.
   The New Server SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For **Parent Profile**, retain the default selection, **serverssl**.
5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. From the **SSL Forward Proxy** list, select **Enabled**.

   You can update this setting later, but only while the profile is not assigned to a virtual server.
8. From the **SSL Forward Proxy Bypass** list, select **Enabled** (or retain the default value **Disabled**).

   The values of the **SSL Forward Proxy Bypass** settings in the server SSL and the client SSL profiles specified in a virtual server must match. You can update this setting later but only while the profile is not assigned to a virtual server.
9. Scroll down to the **Secure Renegotiation** list and select **Request**.
10. Click **Finished**.

The custom Server SSL profile is now listed in the SSL Server profile list.

Creating a virtual server for forward proxy SSL traffic

You configure a virtual server to process the SSL web traffic in a transparent forward proxy configuration.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.

3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. If you plan to use this virtual server for proxy chaining from APM, from the **HTTP Proxy Connect Profile** list, select a profile that you configured previously or select **http-proxy-connect**.
9. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the Client SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.
10. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the Server SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

    Important: *To enable SSL forward proxy functionality, you can either:*

    - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
    - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

    Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.
11. For the **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
12. From the **Source Address Translation** list, select **Auto Map**.
13. For the **Address Translation** setting, clear the **Enabled** check box.
14. Click **Finished**.

The virtual server now appears in the Virtual Server List screen.

After you configure an access policy and a per-request policy, specify them in the Access Profile settings area of this virtual server.

Creating a virtual server for forward proxy traffic

You configure a virtual server to process web traffic going to port 80 in a transparent forward proxy configuration.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.

5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. For the **HTTP Connect Profile** setting, be sure to retain the default value **None**.
9. For the **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
10. From the **Source Address Translation** list, select **Auto Map**.
11. For the **Address Translation** setting, clear the **Enabled** check box.
12. Click **Finished**.

The virtual server now appears in the Virtual Server List screen.

After you configure an access policy and a per-request policy, specify them in the Access Profile settings area of this virtual server.

Creating a Client SSL profile for a captive portal

You create a Client SSL profile when you want the BIG-IP® system to authenticate and decrypt/encrypt client-side application traffic. You create this profile if you enabled Captive Portals in the access profile and if you want to use client-side SSL.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client SSL profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For the **Parent Profile** list, retain the default value, **clientssl**.
5. Select the **Custom** check box.
6. In the Certificate Key Chain area, select a certificate and key combination to use for SSL encryption for the captive portal.

   This certificate should match the FQDN configured in the access profile **SWG-Transparent** type to avoid security warnings, and should be generated by a certificate authority that your browser clients trust.

   Note: *If the key is encrypted, type a passphrase. Otherwise, leave the* ***Passphrase*** *field blank.*

   ---

7. Click **Finished**.

After creating the Client SSL profile and assigning the profile to a virtual server, the BIG-IP system can apply SSL security to the type of application traffic for which the virtual server is configured to listen.

Creating a virtual server for a captive portal

You configure a virtual server to use as a captive portal if you enabled the **Captive Portals** setting in the access profile.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.

Type a destination address in this format: `162.160.15.20`.

5. Specify a port in the **Service Port** field.

   If you plan to use client-side SSL, type `443` or select **HTTPS** from the list.
6. From the **HTTP Profile** list, be sure to retain the default value **http**.
7. For the **HTTP Connect Profile** setting, be sure to retain the default value **None**.

   Whether or not you plan to use client-side SSL, for a captive portal the value for this setting should be **None**.
8. If you plan to use client-side SSL, for the **SSL Profile (Client)** setting, move the profile you configured previously from the **Available** list to the **Selected** list.
9. Click **Finished**.

The virtual server appears in the Virtual Server List screen.

After you configure an access policy, specify it in the Access Profile settings area of this virtual server.

Implementation result

You now have the profiles, virtual servers, and other configuration objects that you need for transparent forward proxy.

Important: *Before you send traffic to this configuration, you need to configure an access policy and a per-request policy and specify them in the virtual servers.*

Access policy and per-request policy configuration depends on what you are trying to do. To locate examples, look for configurations that categorize and filter traffic, intercept or bypass SSL traffic, forward traffic to a third party proxy server, and so on.

Overview: Configuring transparent forward proxy
Creating a virtual server for a captive portal
Overview: Configuring transparent forward proxy in inline mode
Overview: Configuring transparent forward proxy in inline mode
Creating a virtual server for a captive portal
Overview: Configuring explicit forward proxy for Network Access

About redirects after access denied by captive portal

A tool that captures HTTP traffic can reveal what appears to be an extra redirect after a user attempts to gain access using a captive portal but fails. Instead of immediately redirecting the user to the logout page, the user is first redirected to the landing URI, and then a request to the landing URI is redirected to the logout page.

This sample output shows both redirects: the 302 to the landing page `http://berkeley.edu/index.html` and the 302 to the logout page `http://berkeley.edu/vdesk/hangup.php3`.

```
POST  https://bigip-master.com/my.policy?ORIG_URI=http://berkeley.edu/index.html
302   http://berkeley.edu/index.html

GET   http://berkeley.edu/index.html
302   http://berkeley.edu/vdesk/hangup.php3
```

Although the 302 to the landing page might seem to be an extra redirect, it is not. When a request is made, a subordinate virtual server transfers the request to the dominant virtual server to complete the access policy. When the dominant virtual server completes the access policy, it transfers the user back to the subordinate virtual server, on the same original request. The subordinate virtual server then enforces the result of the access policy.

Overview: Configuring transparent forward proxy in inline mode

In a configuration where Access Policy Manager® (APM®) acts as a transparent forward proxy, you configure your internal network to forward web traffic to the BIG-IP® system. This implementation describes an *inline deployment*. You place the BIG-IP system directly in the path of traffic, or inline, as the next hop after the gateway.

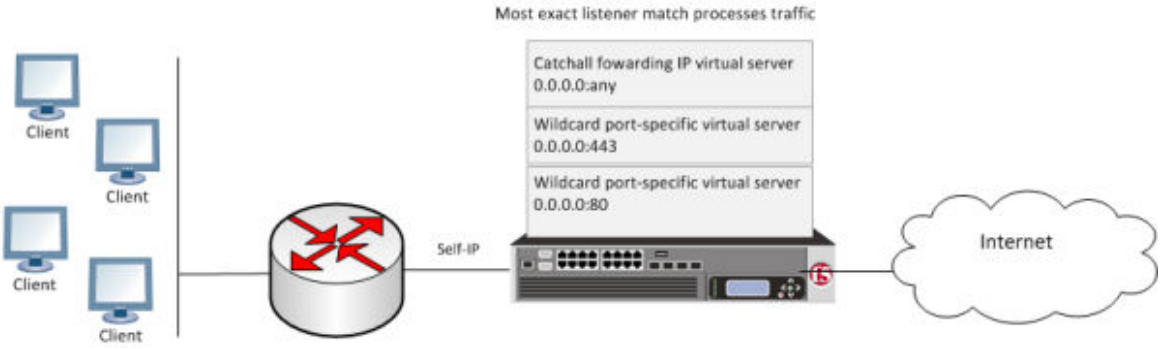


Figure 4: Transparent forward proxy inline deployment

The gateway sends traffic to the self IP address of a VLAN configured on the BIG-IP system. *Wildcard* virtual servers listen on the VLAN and process the traffic that most closely matches the virtual server address. A wildcard virtual server is a special type of network virtual server designed to manage network traffic that is targeted to transparent network devices.

Note: *Transparent forward proxy provides the option to use a captive portal. To use this option, you need an additional virtual server, not shown in the figure, for the captive portal primary authentication server.*

Task summary

Use these procedures to configure the virtual servers, SSL profiles, access profile, VLAN, and self-IP that you need to support inline transparent forward proxy. When you are done, you must add an access policy and a per-request policy to this configuration to process traffic as you want.

Task list

Creating a VLAN for transparent forward proxy
Assigning a self IP address to a VLAN
Creating an access profile for transparent forward proxy
Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
Creating a virtual server for forward proxy SSL traffic
Creating a virtual server for forward proxy traffic
Creating a forwarding virtual server
Creating a Client SSL profile for a captive portal
Creating a virtual server for a captive portal
Implementation result

About the iApp for Secure Web Gateway configuration

When deployed as an application service, the Secure Web Gateway (SWG) iApps® template can set up either an explicit or a transparent forward proxy configuration. The template is designed for use on a

system provisioned and licensed with SWG. To download a zipped file of iApp templates from the F5 Downloads site at (`downloads.f5.com`), you must register for an F5 support account. In the zipped file, a README and template for F5 Secure Web Gateway are located in the RELEASE_CANDIDATE folder.

Creating a VLAN for transparent forward proxy

You need a VLAN on which the forward proxy can listen. For increased security, the VLAN should directly face your clients.

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
   The New VLAN screen opens.
3. In the **Name** field, type a unique name for the VLAN.
4. For the **Interfaces** setting,
   a) From the **Interface** list, select an interface number.
   b) From the **Tagging** list, select **Untagged**.
   c) Click **Add**.
5. Click **Finished**.
   The screen refreshes, and displays the new VLAN in the list.

The new VLAN appears in the VLAN list.

Assigning a self IP address to a VLAN

Assign a self IP address to a VLAN on which the forward proxy listens.

1. On the Main tab, click **Network** > **Self IPs**.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP address.
4. In the **IP Address** field, type the IP address of the VLAN.
   The system accepts IPv4 and IPv6 addresses.
5. In the **Netmask** field, type the network mask for the specified IP address.
   For example, you can type `255.255.255.0`.
6. From the **VLAN/Tunnel** list, select the VLAN.
7. Click **Finished**.
   The screen refreshes, and displays the new self IP address.

Creating an access profile for transparent forward proxy

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.

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

4. From the **Profile Type** list, select **SWG-Transparent**.

Note: *After you complete this step, the* ***User Identification Method*** *is set to* ***IP Address*** *and cannot be changed.*

Additional settings display.

5. To use NTLM authentication before a session starts, from the **NTLM Auth Configuration** list select a configuration.

Important: *For NTLM authentication to work, you must also enable the* ***Captive Portals*** *setting and specify an IP address in the* ***Primary Authentication URI*** *field for the virtual server that you configure for the captive portal.*

In the case of a shared machine, an IP address might already be associated with a user or a session. Using NTLM authentication ensures that the system can associate the IP address with the correct session (new or existing) or with a new user each time a user logs on to the shared machine.

6. To direct users to a captive portal, for **Captive Portal** select **Enabled** and, in the **Primary Authentication URI** field, type the URI.

   You might specify the URI of your primary authentication server if you use single sign-on across multiple domains. Users can then access multiple back-end applications from multiple domains and hosts without needing to re-enter their credentials, because the user session is stored on the primary domain.

   For example, you might type `https://logon.siterequest.com` in the field.

7. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.

8. Click **Finished**.
   The Access Profiles list screen displays.

The access profile displays in the Access Profiles List. Default-log-setting is assigned to the access profile.

Creating a custom Client SSL forward proxy profile

Creating a Client SSL forward proxy profile makes it possible for client and server authentication, while still allowing the BIG-IP® system to perform data optimization, such as decryption and encryption. This profile applies to client-side SSL forward proxy traffic only.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client SSL profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **clientssl**.
5. To avoid issues with privacy concerns, you might need to enable SSL forward proxy bypass for URLs that expose personal user information, such as those for financial or government sites.
   a) Scroll down to the **SSL Forward Proxy** list, and select **Advanced**.
   b) Select the **Custom** check box for the SSL Forward Proxy area.
   c) From the **SSL Forward Proxy** list, select **Enabled**.

You can update this setting later but only while the profile is not assigned to a virtual server.

d) From the **CA Certificate** list, select a certificate.
e) From the **CA Key** list, select a key.
f) In the **CA Passphrase** field, type a passphrase.
g) In the **Confirm CA Passphrase** field, type the passphrase again.
h) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
i) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
j) (Optional) For the **Certificate Extensions List** setting, select the extensions that you want in the **Available extensions** field, and move them to the **Enabled Extensions** field using the **Enable** button.
k) From the **SSL Forward Proxy Bypass** list, select **Enabled**.

You can update this setting later but only while the profile is not assigned to a virtual server.

Additional settings display.

l) For **Default Bypass Action**, retain the default value **Intercept**.

You can override the value of this action on a case-by-case basis in the per-request policy for the virtual server.

Note: *Bypass and intercept lists do not work with per-request policies. Retain the setting* ***None*** *for the remainder of the fields.*

---

6. Click **Finished**.

The custom Client SSL forward proxy profile now appears in the Client SSL profile list screen.

Creating a custom Server SSL profile

Create a custom server SSL profile to support SSL forward proxy.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The Server SSL profile list screen opens.
2. Click **Create**.
   The New Server SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For **Parent Profile**, retain the default selection, **serverssl**.
5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. From the **SSL Forward Proxy** list, select **Enabled**.

   You can update this setting later, but only while the profile is not assigned to a virtual server.
8. From the **SSL Forward Proxy Bypass** list, select **Enabled** (or retain the default value **Disabled**).

   The values of the **SSL Forward Proxy Bypass** settings in the server SSL and the client SSL profiles specified in a virtual server must match. You can update this setting later but only while the profile is not assigned to a virtual server.
9. Scroll down to the **Secure Renegotiation** list and select **Request**.
10. Click **Finished**.

The custom Server SSL profile is now listed in the SSL Server profile list.

Creating a virtual server for forward proxy SSL traffic

You configure a virtual server to process the SSL web traffic in a transparent forward proxy configuration.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. If you plan to use this virtual server for proxy chaining from APM, from the **HTTP Proxy Connect Profile** list, select a profile that you configured previously or select **http-proxy-connect**.
9. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the Client SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.
10. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the Server SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

    Important: *To enable SSL forward proxy functionality, you can either:*

    - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
    - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

    Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.
11. For the **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
12. From the **Source Address Translation** list, select **Auto Map**.
13. For the **Address Translation** setting, clear the **Enabled** check box.
14. Click **Finished**.

The virtual server now appears in the Virtual Server List screen.

After you configure an access policy and a per-request policy, specify them in the Access Profile settings area of this virtual server.

Creating a virtual server for forward proxy traffic

You configure a virtual server to process web traffic going to port 80 in a transparent forward proxy configuration.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.

2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. For the **HTTP Connect Profile** setting, be sure to retain the default value **None**.
9. For the **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
10. From the **Source Address Translation** list, select **Auto Map**.
11. For the **Address Translation** setting, clear the **Enabled** check box.
12. Click **Finished**.

The virtual server now appears in the Virtual Server List screen.

After you configure an access policy and a per-request policy, specify them in the Access Profile settings area of this virtual server.

Creating a forwarding virtual server

For Secure Web Gateway transparent forward proxy in inline mode, you create a forwarding virtual server to intercept IP traffic that is not going to ports 80 or 443.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. From the **Type** list, select **Forwarding (IP)**.
5. In the **Source Address** field, type `0.0.0.0/0`.
6. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
7. In the **Service Port** field, type `*` or select *** All Ports** from the list.
8. From the **Protocol** list, select *** All Protocols**.
9. From the **VLAN and Tunnel Traffic** list, retain the default selection, **All VLANs and Tunnels**.
10. From the **Source Address Translation** list, select **Auto Map**.
11. Click **Finished**.

Creating a Client SSL profile for a captive portal

You create a Client SSL profile when you want the BIG-IP® system to authenticate and decrypt/encrypt client-side application traffic. You create this profile if you enabled Captive Portals in the access profile and if you want to use client-side SSL.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client SSL profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For the **Parent Profile** list, retain the default value, **clientssl**.
5. Select the **Custom** check box.

6. In the Certificate Key Chain area, select a certificate and key combination to use for SSL encryption for the captive portal.

   This certificate should match the FQDN configured in the access profile **SWG-Transparent** type to avoid security warnings, and should be generated by a certificate authority that your browser clients trust.

   Note: *If the key is encrypted, type a passphrase. Otherwise, leave the* ***Passphrase*** *field blank.*

7. Click **Finished**.

After creating the Client SSL profile and assigning the profile to a virtual server, the BIG-IP system can apply SSL security to the type of application traffic for which the virtual server is configured to listen.

Creating a virtual server for a captive portal

You configure a virtual server to use as a captive portal if you enabled the **Captive Portals** setting in the access profile.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.

   Type a destination address in this format: `162.160.15.20`.
5. Specify a port in the **Service Port** field.

   If you plan to use client-side SSL, type `443` or select **HTTPS** from the list.
6. From the **HTTP Profile** list, be sure to retain the default value **http**.
7. For the **HTTP Connect Profile** setting, be sure to retain the default value **None**.

   Whether or not you plan to use client-side SSL, for a captive portal the value for this setting should be **None**.
8. If you plan to use client-side SSL, for the **SSL Profile (Client)** setting, move the profile you configured previously from the **Available** list to the **Selected** list.
9. Click **Finished**.

The virtual server appears in the Virtual Server List screen.

After you configure an access policy, specify it in the Access Profile settings area of this virtual server.

Implementation result

You now have the profiles, virtual servers, and other configuration objects that you need for transparent forward proxy.

Important: *Before you send traffic to this configuration, you need to configure an access policy and a per-request policy and specify them in the virtual servers.*

Access policy and per-request policy configuration depends on what you are trying to do. To locate examples, look for configurations that categorize and filter traffic, intercept or bypass SSL traffic, forward traffic to a third party proxy server, and so on.

Overview: Configuring transparent forward proxy
Creating a virtual server for a captive portal

Overview: Configuring transparent forward proxy in inline mode
Overview: Configuring transparent forward proxy in inline mode
Creating a virtual server for a captive portal
Overview: Configuring explicit forward proxy for Network Access

Remote Access Forward Proxy Configurations

Overview: Configuring explicit forward proxy for Network Access

You can configure Access Policy Manager® (APM®) to act as an explicit forward proxy so that APM processes the Internet traffic from a Network Access client in the same way that it processes such traffic from a client in the enterprise.

Note: *Using a distinct explicit forward proxy configuration to process traffic from remote clients separately from a configuration used for processing traffic from internal clients provides an important measure of network security.*

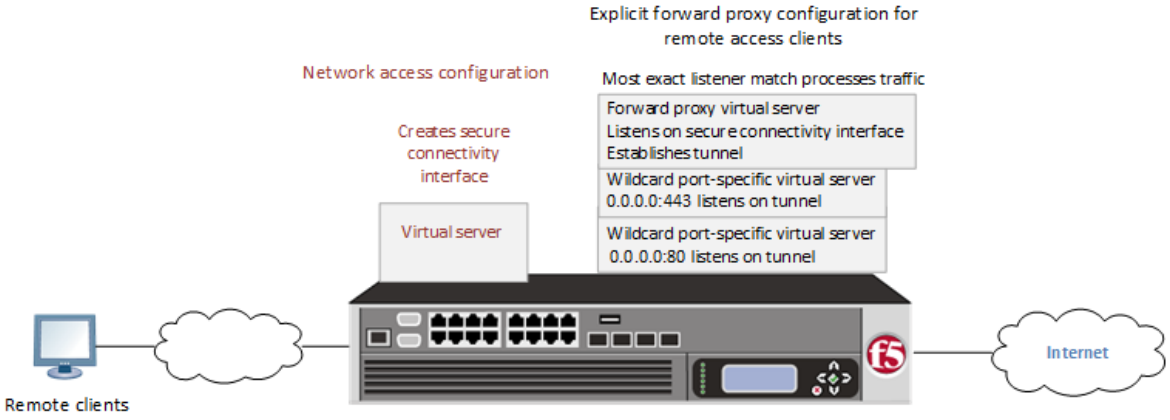


Figure 5: Explicit forward proxy for Network Access

Task summary

Creating a connectivity profile
Adding a connectivity profile to a virtual server
Creating a DNS resolver
Adding forward zones to a DNS resolver
Creating a custom HTTP profile for explicit forward proxy
Creating a virtual server as the forward proxy for Network Access traffic
Creating a wildcard virtual server for HTTP tunnel traffic
Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
Creating a wildcard virtual server for SSL traffic on the HTTP tunnel
Updating the access policy in the remote access configuration
Configuring a Network Access resource to forward traffic

Prerequisites for an explicit forward proxy configuration for Network Access

Before you start to create a configuration in which Access Policy Manager® (APM®) acts as an explicit forward proxy to support Network Access clients, you must have completed these tasks.

- You need to have configured a working a Network Access configuration.

- You need a per-request policy configured for forward proxy.
- On a BIG-IP® system with an SWG subscription, you must ensure that the URL database is downloaded. You can also configure any URL filters that you want to use in addition to, or instead of, the default URL filters.
- On a BIG-IP® system without an SWG subscription, if you want to designate only a few URLs for specific handling, you probably do not need to configure user-defined URL categories and filters. However, if you need to control access to many URLs, for better performance and ease-of-use you should configure user-defined URL categories and filters.

Configuration outline: Explicit forward proxy for Network Access

Tasks for integrating a Network Access configuration with a configuration in which Access Policy Manager® (APM)®acts as an explicit forward proxy follow this order.

- First, if your Network Access configuration does not include a connectivity profile, create one and add it to the virtual server.
- Next, create a configuration in which APM acts as an explicit forward proxy. This configuration includes the per-request policy.
- Finally, in the Network Access configuration, update the access policy (so that it populates any session variables required for successful execution of the per-request policy) and update the Network Access resource for client proxy.

Creating a connectivity profile

You create a connectivity profile to configure client connections.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.
   APM® provides a default profile, **connectivity**.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

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.

Adding a connectivity profile to a virtual server

Update a virtual server that is part of an Access Policy Manager® application access, network access, or portal access configuration to enable a secure connectivity interface for traffic from the client.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. Scroll down to the Access Policy area.
4. From the **Connectivity Profile** list, select the connectivity profile.
5. Click **Update** to save the changes.

Creating a DNS resolver

You configure a DNS resolver on the BIG-IP® system to resolve DNS queries and cache the responses. The next time the system receives a query for a response that exists in the cache, the system returns the response from the cache.

1. On the Main tab, click **Network** > **DNS Resolvers** > **DNS Resolver List**.
   The DNS Resolver List screen opens.
2. Click **Create**.
   The New DNS Resolver screen opens.
3. In the **Name** field, type a name for the resolver.
4. Click **Finished**.

Note: *When you create an OAuth Server, creating a DNS Resolver with a forward zone named . (period) is mandatory to forward all requests.*

Adding forward zones to a DNS resolver

Before you begin, gather the IP addresses of the nameservers that you want to associate with a forward zone.

Add a forward zone to a DNS resolver when you want the BIG-IP® system to forward queries for particular zones to specific nameservers for resolution in case the resolver does not contain a response to the query.

Note: *Creating a forward zone is optional. Without one, a DNS resolver can still make recursive name queries to the root DNS servers; the virtual servers using the cache must have a route to the Internet.*

When you create an OAuth Server, creating a DNS Resolver with a forward zone named . (period) is mandatory.

---

1. On the Main tab, click **Network** > **DNS Resolvers** > **DNS Resolver List**.
   The DNS Resolver List screen opens.
2. Click the name of the resolver you want to modify.
   The properties screen opens.
3. On the menu bar, click **Forward Zones**.
   The Forward Zones screen displays.
4. Click the **Add** button.

   Note: *You add more than one zone to forward based on the needs of your organization.*

   ---

5. In the **Name** field, type the name of a subdomain or type the fully qualified domain name (FQDN) of a forward zone.

   Note: *To forward all requests (such as when creating an OAuth server), specify . (period) as the name.*

   For example, either `example` or `site.example.com` would be valid zone names.
6. Add one or more nameservers:
   a) In the **Address** field, type the IP address of a DNS nameserver that is considered authoritative for this zone.

      Based on your network configuration, add IPv4 or IPv6 addresses, or both.

b) Click **Add**.
The address is added to the list.

Note: *The order of nameservers in the configuration does not impact which nameserver the system selects to forward a query to.*

7. Click **Finished**.

Creating a custom HTTP profile for explicit forward proxy

An HTTP profile defines the way that you want the BIG-IP® system to manage HTTP traffic.

Note: *To act an explicit forward proxy, Access Policy Manager® (APM®) requires a DNS resolver that you select in the HTTP profile.*

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **HTTP**.
The HTTP profile list screen opens.
2. Click **Create**.
The New HTTP Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Proxy Mode** list, select **Explicit**.
5. For **Parent Profile**, retain the **http-explicit** setting.
6. Select the **Custom** check box.
7. Scroll down to the Explicit Proxy area.
8. From the **DNS Resolver** list, select the DNS resolver you configured previously.
9. In the **Tunnel Name** field, you can retain the default value, **http-tunnel**, or type the name of a tunnel if you created one.

   APM requires a tunnel with tcp-forward encapsulation to support SSL traffic for explicit forward proxy.
10. From the **Default Connect Handling** list, retain the default setting **Deny**.

    Any CONNECT traffic goes through the tunnel to the virtual server that most closely matches the traffic; if there is no match, the traffic is blocked.
11. Click **Finished**.

The custom HTTP profile now appears in the HTTP profile list screen.

Creating a virtual server as the forward proxy for Network Access traffic

Before you begin, you need to know the name of the connectivity profile specified in the virtual server for the Network Access configuration that you want to protect with Access Policy Manager® (APM®) acting as an explicit forward proxy.

You specify a virtual server to process forward proxy traffic. This virtual server must listen on the secure connectivity interface that is specified on the virtual server through which network access clients connect. This virtual server is also the one that network access resources must specify as the client proxy server.

Note: *Use this virtual server for forward proxy traffic only. You should not try to use it for reverse proxy, or add a pool to it.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
The Virtual Server List screen opens.
2. Click the **Create** button.
The New Virtual Server screen opens.

3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type the IP address for a host virtual server.

   This field accepts an address in CIDR format (IP address/prefix). However, when you type the complete IP address for a host, you do not need to type a prefix after the address.

   Type a destination address in this format: `162.160.15.20`.
5. In the **Service Port** field, type the port number to use for forward proxy traffic.

   Typically, the port number is `3128` or `8080`.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select the HTTP profile you configured earlier.
8. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
9. For the **VLANs and Tunnels** setting, move the secure connectivity interface to the **Selected** list.
10. From the **Source Address Translation** list, select **Auto Map**.
11. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
12. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
13. Click **Finished**.

Creating a wildcard virtual server for HTTP tunnel traffic

You configure a virtual server to process web traffic coming in on the HTTP tunnel from the explicit forward-proxy virtual server.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
9. For the **VLANs and Tunnels** setting, move the tunnel to the **Selected** list.

   The tunnel name must match the tunnel specified in the HTTP profile for the forward proxy virtual server. The default tunnel is **http-tunnel**.
10. From the **Source Address Translation** list, select **Auto Map**.
11. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
12. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
13. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
14. Click **Finished**.

Creating a custom Client SSL forward proxy profile

Creating a Client SSL forward proxy profile makes it possible for client and server authentication, while still allowing the BIG-IP® system to perform data optimization, such as decryption and encryption. This profile applies to client-side SSL forward proxy traffic only.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client SSL profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **clientssl**.
5. To avoid issues with privacy concerns, you might need to enable SSL forward proxy bypass for URLs that expose personal user information, such as those for financial or government sites.
   a) Scroll down to the **SSL Forward Proxy** list, and select **Advanced**.
   b) Select the **Custom** check box for the SSL Forward Proxy area.
   c) From the **SSL Forward Proxy** list, select **Enabled**.
      You can update this setting later but only while the profile is not assigned to a virtual server.
   d) From the **CA Certificate** list, select a certificate.
   e) From the **CA Key** list, select a key.
   f) In the **CA Passphrase** field, type a passphrase.
   g) In the **Confirm CA Passphrase** field, type the passphrase again.
   h) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
   i) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
   j) (Optional) For the **Certificate Extensions List** setting, select the extensions that you want in the **Available extensions** field, and move them to the **Enabled Extensions** field using the **Enable** button.
   k) From the **SSL Forward Proxy Bypass** list, select **Enabled**.
      You can update this setting later but only while the profile is not assigned to a virtual server.
      Additional settings display.
   l) For **Default Bypass Action**, retain the default value **Intercept**.
      You can override the value of this action on a case-by-case basis in the per-request policy for the virtual server.

   Note: *Bypass and intercept lists do not work with per-request policies. Retain the setting* ***None*** *for the remainder of the fields.*
6. Click **Finished**.

The custom Client SSL forward proxy profile now appears in the Client SSL profile list screen.

Creating a custom Server SSL profile

Create a custom server SSL profile to support SSL forward proxy.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The Server SSL profile list screen opens.
2. Click **Create**.
   The New Server SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For **Parent Profile**, retain the default selection, **serverssl**.
5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. From the **SSL Forward Proxy** list, select **Enabled**.
   You can update this setting later, but only while the profile is not assigned to a virtual server.

8. From the **SSL Forward Proxy Bypass** list, select **Enabled** (or retain the default value **Disabled**).

   The values of the **SSL Forward Proxy Bypass** settings in the server SSL and the client SSL profiles specified in a virtual server must match. You can update this setting later but only while the profile is not assigned to a virtual server.
9. Scroll down to the **Secure Renegotiation** list and select **Request**.
10. Click **Finished**.

The custom Server SSL profile is now listed in the SSL Server profile list.

Creating a wildcard virtual server for SSL traffic on the HTTP tunnel

If you do not have existing client SSL and server SSL profiles that you want to use, configure them before you start.

You configure a virtual server to process SSL web traffic coming in on the HTTP tunnel from the forward proxy virtual server.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the Client SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

   ---
9. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the Server SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

   ---
10. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
11. For the **VLANs and Tunnels** setting, move the tunnel to the **Selected** list.

The tunnel name must match the tunnel specified in the HTTP profile for the forward proxy virtual server. The default tunnel is **http-tunnel**.

12. From the **Source Address Translation** list, select **Auto Map**.
13. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
14. For the **Address Translation** setting, clear the **Enabled** check box.
15. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
16. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
17. Click **Finished**.

Updating the access policy in the remote access configuration

Add queries to the access policy to populate any session variables that are required for successful execution of the per-request policy.

Note: *Class lookup or group lookup items in a per-request policy rely on session variables that can only be populated in this access policy.*

---

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. Click the name of the access profile that you want to edit.
   The properties screen opens.
3. In the General Properties area, click the **Edit Access Policy for Profile** ***profile_name*** link.
   The visual policy editor opens the access policy in a separate screen.
4. Click the **(+)** icon anywhere in the access policy to add a new item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
5. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the policy and configure its properties:
   a) From the **Server** list, select an AAA LDAP server.

      An LDAP Query uses SSL connections when you select an LDAP AAA server that is configured for LDAPS.
   b) Specify the **SearchDN**, and **SearchFilter** settings.

      SearchDN is the base DN from which the search is done.
   c) Click **Save**.

   This item populates the `session.ldap.last.attr.memberOf` session variable.
6. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the policy and configure its properties:
   a) From the **Server** list, select an AAA AD server.
   b) Select the **Fetch Primary Group** check box.

      The value of the primary user group populates the `session.ad.last.attr.primaryGroupID` session variable.
   c) Click **Save**.
7. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the policy and configure its properties:

a) From the **Server** list, select an AAA RADIUS server.
b) Click **Save**.

This item populates the `session.radius.last.attr.class` session variable.

8. To supply local database groups for use in the per-request policy, add a Local Database item anywhere in the policy and configure its properties:
   a) From the **LocalDB Instance** list, select a local user database.
   b) In the **User Name** field, retain the default session variable.
   c) Click **Add new entry**
      A new line is added to the list of entries with the Action set to **Read** and other default settings.
   d) In the Destination column **Session Variable** field, type `session.localdb.groups`.
      If you type a name other than `session.localdb.groups`, note it. You will need it when you configure the per-request access policy.
   e) In the Source column from the **DB Property** list, select **groups**.
   f) Click **Save**.

   This item populates the `session.localdb.groups` session variable.

The access policy is configured to support the per-request policy.

Click the **Apply Access Policy** link to apply and activate your changes to this access policy.

Note: *To ensure that logging is configured to meet your requirements, verify the log settings for the access profile.*

Configuring a Network Access resource to forward traffic

You must create a Network Access resource, or open an existing resource, before you can perform this task.

Configure a Network Access resource to forward traffic to the virtual server you configured for explicit forward proxy traffic so that Access Policy Manager® (APM®) can act as the explicit forward proxy.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Network Access (VPN)** > **Network Access Lists**.
   The Network Access Lists screen opens.
2. In the Name column, click the name of the network access resource you want to edit.
3. On the menu bar, click **Network Settings**.
4. For **Client Settings**, select **Advanced**.
5. Scroll down and select **Client Proxy Settings**.
   Additional settings display.
6. If the **Traffic Options** setting specifies **Force all traffic through tunnel**, configure these additional settings:
   a) In the **Client Proxy Address** field, type the IP address of the explicit forward proxy virtual server.
   b) In the **Client Proxy Port** field, type the port number of the explicit forward proxy virtual server.
      Typically, the port number is `3128` or `8080`; it might be different in your configuration.
7. If the **Traffic Options** setting specifies **Use split tunneling for traffic**, in the **Client Proxy Autoconfig Script** field, type the URL for a proxy auto-configuration script.
8. Click the **Update** button.
   Your changes are saved and the page refreshes.

The Network Access resource is configured to forward traffic to the explicit forward proxy server.

Implementation result

The configuration in which Access Policy Manager® (APM®) acts as an explicit forward proxy is ready to process web traffic from network access clients.

About configuration elements for explicit forward proxy (remote access)

When you configure Access Policy Manager® (APM®) to act as an explicit forward proxy for use by Network Access clients, you might want to understand how these objects fit into the overall configuration.

Secure connectivity interface

In a Network Access configuration, a connectivity profile on the virtual server specifies a secure connectivity interface for traffic from the client. The virtual server configured as the explicit forward proxy server must listen on the secure connectivity interface for traffic from Network Access clients.

Tunnel

The virtual server configured as the explicit forward proxy server must specify an HTTP profile that specifies the name of a tunnel of tcp-forward encapsulation type. You can use the default tunnel, http-tunnel, or create another tunnel and use it.

Per-request policy

In any APM forward proxy configuration, the determination of whether a user can access a URL must be made in a per-request policy. A per-request policy determines whether to block or allow access to a request based on time or date or group membership or other criteria that you configure.

Access policies

The access policy in the Network Access configuration continues to authenticate users, assign resources, and evaluate ACLs, if any. In addition, this access policy must populate any session variables used in the per-request policy. An access profile of the **SWG-Explicit** type is required in the forward proxy configuration; however, it is not necessary to include any items in the access policy.

Per-request policy items that read session variables

This table lists per-request policy items that read session variables and lists the access policy items that populate the variables.

Per-request policy item	Session variable	Access policy item
AD Group Lookup	`session.ad.last.attr.primaryGroupID`	AD Query
LDAP Group Lookup	`session.ldap.last.attr.memberOf`	LDAP Query
LocalDB Group Lookup	`session.localdb.groups` ***Note:*** *This session variable is a default in the expression for LocalDB Group Lookup; any session variable in the expression must match the session variable used in the Local Database action in the access policy.*	Local Database
RADIUS Class Lookup	`session.radius.last.attr.class`	RADIUS Auth

Overview: Configuring transparent forward proxy for remote access

Access Policy Manager® (APM®) can be configured to act as a transparent forward proxy to support remote clients that connect using application access, network access, or portal access.

Note: *Using a distinct APM transparent forward proxy configuration to process traffic from remote clients separately from a forward proxy configuration used for processing traffic from internal clients provides an important measure of network security.*

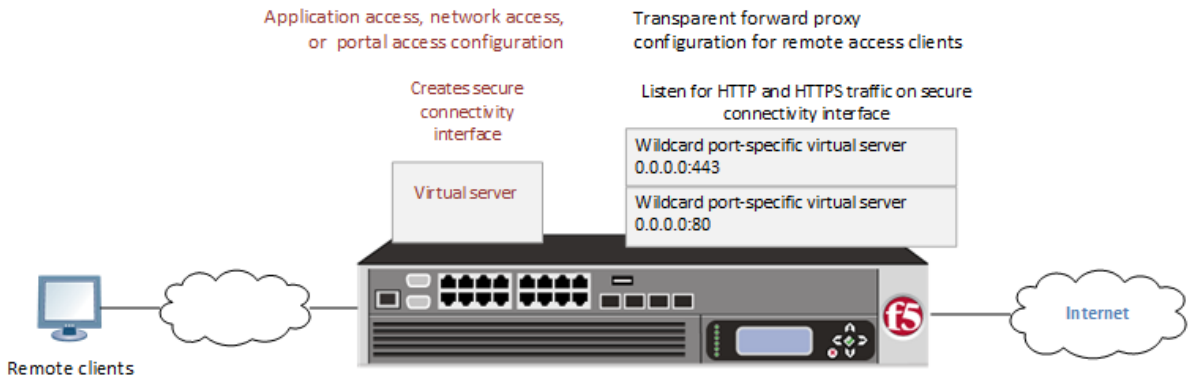


Figure 6: Transparent forward proxy for remote access

Task summary

Creating a connectivity profile
Adding a connectivity profile to a virtual server
Creating an access profile for transparent forward proxy
Creating a wildcard virtual server for HTTP traffic on the connectivity interface
Creating a custom Client SSL forward proxy profile
Creating a custom Server SSL profile
Creating a wildcard virtual server for SSL traffic on the connectivity interface
Updating the access policy in the remote access configuration

Prerequisites for APM transparent forward proxy for remote access

Before you start to create an Access Policy Manager® (APM®) transparent forward proxy configuration to support remote access clients, you must have completed these tasks.

- You must have a working Network Access, Portal Access, or Application Access configuration.
- You need a per-request policy configured for forward proxy.
- On a BIG-IP® system with an SWG subscription, you must ensure that the URL database is downloaded. You can also configure any URL filters that you want to use in addition to, or instead of, the default URL filters.
- On a BIG-IP® system without an SWG subscription, if you want to designate only a few URLs for specific handling, you probably do not need to configure user-defined URL categories and filters. However, if you need to control access to many URLs, for better performance and ease-of-use you should configure user-defined URL categories and filters.

Configuration outline for APM transparent forward proxy for remote access

Tasks for integrating an Access Policy Manager® (APM®) remote access configuration with a transparent forward proxy configuration for APM follow this order.

- First, update the existing application access, network access, or portal access configuration to add a secure connectivity profile to the virtual server if one is not already specified.
- Next, create a transparent forward proxy configuration for APM. The per-request policy is part of this configuration.
- Finally, update the access policy in the existing application access, network access, or portal access configuration if needed. If the per-request policy uses group or class lookup items, add queries to the access policy to populate the session variables on which the lookup items rely.

Creating a connectivity profile

You create a connectivity profile to configure client connections.

1. On the Main tab, click **Access** > **Connectivity / VPN** > **Connectivity** > **Profiles**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.
   APM® provides a default profile, **connectivity**.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

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.

Adding a connectivity profile to a virtual server

Update a virtual server that is part of an Access Policy Manager® application access, network access, or portal access configuration to enable a secure connectivity interface for traffic from the client.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. Scroll down to the Access Policy area.
4. From the **Connectivity Profile** list, select the connectivity profile.
5. Click **Update** to save the changes.

Creating an access profile for transparent forward proxy

You create an access profile to supply an access policy.

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.

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

4. From the **Profile Type** list, select **SWG-Transparent**.
   Additional fields display set to default values.
5. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
6. Click **Finished**.
   The Access Profiles list screen displays.

The access profile displays in the Access Profiles List. Default-log-setting is assigned to the access profile.

You do not need to add any actions or make any changes to the access policy.

Creating a wildcard virtual server for HTTP traffic on the connectivity interface

Before you begin, you need to know the name of the connectivity profile specified in the virtual server for the remote access configuration that you want Access Policy Manager® (APM®) to protect.

You configure a virtual server to process web traffic on the secure connectivity interface for a remote access client.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `80`, or select **HTTP** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
9. For the **VLANs and Tunnels** setting, move the secure connectivity interface to the **Selected** list.
10. From the **Source Address Translation** list, select **Auto Map**.
11. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
12. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
13. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
14. Click **Finished**.

Creating a custom Client SSL forward proxy profile

Creating a Client SSL forward proxy profile makes it possible for client and server authentication, while still allowing the BIG-IP® system to perform data optimization, such as decryption and encryption. This profile applies to client-side SSL forward proxy traffic only.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client SSL profile list screen opens.
2. Click **Create**.
   The New Client SSL Profile screen opens.

3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **clientssl**.
5. To avoid issues with privacy concerns, you might need to enable SSL forward proxy bypass for URLs that expose personal user information, such as those for financial or government sites.
   a) Scroll down to the **SSL Forward Proxy** list, and select **Advanced**.
   b) Select the **Custom** check box for the SSL Forward Proxy area.
   c) From the **SSL Forward Proxy** list, select **Enabled**.

      You can update this setting later but only while the profile is not assigned to a virtual server.
   d) From the **CA Certificate** list, select a certificate.
   e) From the **CA Key** list, select a key.
   f) In the **CA Passphrase** field, type a passphrase.
   g) In the **Confirm CA Passphrase** field, type the passphrase again.
   h) In the **Certificate Lifespan** field, type a lifespan for the SSL forward proxy certificate in days.
   i) (Optional) From the **Certificate Extensions** list, select **Extensions List**.
   j) (Optional) For the **Certificate Extensions List** setting, select the extensions that you want in the **Available extensions** field, and move them to the **Enabled Extensions** field using the **Enable** button.
   k) From the **SSL Forward Proxy Bypass** list, select **Enabled**.

      You can update this setting later but only while the profile is not assigned to a virtual server.

      Additional settings display.
   l) For **Default Bypass Action**, retain the default value **Intercept**.

      You can override the value of this action on a case-by-case basis in the per-request policy for the virtual server.

      Note: *Bypass and intercept lists do not work with per-request policies. Retain the setting* ***None*** *for the remainder of the fields.*
6. Click **Finished**.

The custom Client SSL forward proxy profile now appears in the Client SSL profile list screen.

Creating a custom Server SSL profile

Create a custom server SSL profile to support SSL forward proxy.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The Server SSL profile list screen opens.
2. Click **Create**.
   The New Server SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. For **Parent Profile**, retain the default selection, **serverssl**.
5. From the **Configuration** list, select **Advanced**.
6. Select the **Custom** check box.
   The settings become available for change.
7. From the **SSL Forward Proxy** list, select **Enabled**.

   You can update this setting later, but only while the profile is not assigned to a virtual server.
8. From the **SSL Forward Proxy Bypass** list, select **Enabled** (or retain the default value **Disabled**).

   The values of the **SSL Forward Proxy Bypass** settings in the server SSL and the client SSL profiles specified in a virtual server must match. You can update this setting later but only while the profile is not assigned to a virtual server.
9. Scroll down to the **Secure Renegotiation** list and select **Request**.

10. Click **Finished**.

The custom Server SSL profile is now listed in the SSL Server profile list.

Creating a wildcard virtual server for SSL traffic on the connectivity interface

Before you begin, you need to know the name of the connectivity profile specified in the virtual server for the remote access configuration that you want Secure Web Gateway (SWG) to protect. Also, if you do not have existing client SSL and server SSL profiles that you want to use, configure them before you start.

You configure a virtual server to process SSL web traffic coming in on the secure connectivity interface for a remote access client.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. In the **Destination Address** field, type `0.0.0.0/0` to accept any IPv4 traffic.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **HTTP Profile** list, select **http**.
8. For the **SSL Profile (Client)** setting, from the **Available** list, select the name of the Client SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

   ---

9. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the Server SSL forward proxy profile you previously created, and using the Move button, move the name to the **Selected** list.

   Important: *To enable SSL forward proxy functionality, you can either:*

   - Disassociate existing Client SSL and Server SSL profiles from a virtual server and configure the SSL Forward Proxy settings.
   - Create new Client SSL and Server SSL profiles and configure the SSL Forward Proxy settings.

   Then with either option, select the Client SSL and Server SSL profiles on a virtual server. You cannot modify existing Client SSL and Server SSL profiles while they are selected on a virtual server to enable SSL forward proxy functionality.

   ---

10. Scroll down to the **VLAN and Tunnel Traffic** setting and select **Enabled on**.
11. For the **VLANs and Tunnels** setting, move the secure connectivity interface to the **Selected** list.
12. From the **Source Address Translation** list, select **Auto Map**.
13. Scroll down to the **Port Translation** setting and clear the **Enabled** check box.
14. For the **Address Translation** setting, clear the **Enabled** check box.

15. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
16. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
17. Click **Finished**.

Updating the access policy in the remote access configuration

Add queries to the access policy to populate any session variables that are required for successful execution of the per-request policy.

Note: *Class lookup or group lookup items in a per-request policy rely on session variables that can only be populated in this access policy.*

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. Click the name of the access profile that you want to edit.
   The properties screen opens.
3. In the General Properties area, click the **Edit Access Policy for Profile** ***profile_name*** link.
   The visual policy editor opens the access policy in a separate screen.
4. Click the **(+)** icon anywhere in the access policy to add a new item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
5. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the policy and configure its properties:
   a) From the **Server** list, select an AAA LDAP server.

      An LDAP Query uses SSL connections when you select an LDAP AAA server that is configured for LDAPS.
   b) Specify the **SearchDN**, and **SearchFilter** settings.

      SearchDN is the base DN from which the search is done.
   c) Click **Save**.

   This item populates the `session.ldap.last.attr.memberOf` session variable.
6. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the policy and configure its properties:
   a) From the **Server** list, select an AAA AD server.
   b) Select the **Fetch Primary Group** check box.

      The value of the primary user group populates the `session.ad.last.attr.primaryGroupID` session variable.
   c) Click **Save**.
7. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the policy and configure its properties:
   a) From the **Server** list, select an AAA RADIUS server.
   b) Click **Save**.

   This item populates the `session.radius.last.attr.class` session variable.
8. To supply local database groups for use in the per-request policy, add a Local Database item anywhere in the policy and configure its properties:

a) From the **LocalDB Instance** list, select a local user database.
b) In the **User Name** field, retain the default session variable.
c) Click **Add new entry**
   A new line is added to the list of entries with the Action set to **Read** and other default settings.
d) In the Destination column **Session Variable** field, type `session.localdb.groups`.
   If you type a name other than `session.localdb.groups`, note it. You will need it when you configure the per-request access policy.
e) In the Source column from the **DB Property** list, select **groups**.
f) Click **Save**.

This item populates the `session.localdb.groups` session variable.

The access policy is configured to support the per-request policy.

Click the **Apply Access Policy** link to apply and activate your changes to this access policy.

Note: *To ensure that logging is configured to meet your requirements, verify the log settings for the access profile.*

Implementation result

A transparent forward proxy configuration is ready to process web traffic from remote access clients.

About configuration elements for transparent forward proxy (remote access)

When you configure the BIG-IP® system so that Access Policy Manager® (APM®) can act as a transparent forward proxy for use by remote access clients, you might want to understand how these objects fit into the overall configuration.

Secure connectivity interface

In a remote access configuration, a connectivity profile is required on the virtual server to specify a secure connectivity interface for traffic from the client. In the APM configuration, wildcard virtual servers must listen on the secure connectivity interface for traffic from remote access clients.

Per-request policy

In any APM forward proxy configuration, the determination of whether a user can access a URL must be made in a per-request access policy. A per-request access policy determines whether to block or allow access to a request based on time or date or group membership or other criteria that you configure.

Access policies

The access policy in the remote access configuration continues to authenticate users, assign resources, and evaluate ACLs, if any. In addition, this access policy must populate any session variables used in the per-request policy. An access profile of the **SWG-Transparent** type is required; however, it is not necessary to include any items in the access policy.

Per-request policy items that read session variables

This table lists per-request policy items that read session variables and lists the access policy items that populate the variables.

Per-request policy item	Session variable	Access policy item
AD Group Lookup	`session.ad.last.attr.primaryGroupID`	AD Query

Per-request policy item	Session variable	Access policy item
LDAP Group Lookup	`session.ldap.last.attr.memberOf`	LDAP Query
LocalDB Group Lookup	`session.localdb.groups` ***Note:*** *This session variable is a default in the expression for LocalDB Group Lookup; any session variable in the expression must match the session variable used in the Local Database action in the access policy.*	Local Database
RADIUS Class Lookup	`session.radius.last.attr.class`	RADIUS Auth

Policies for APM (with SWG) as a Secure Web Gateway

Overview: Controlling forward proxy traffic with SWG

With an SWG subscription, when you configure a per-request policy to control forward proxy access using URL categories, the Category Lookup agent can use standard categories (from the URL database) or any custom URL categories that you might have created or both. For non-encrypted traffic, Category Lookup can also be configured to return safe search results to your users. Additional analytics agents are available to scan URL responses for malware and scan URL requests for further filtering.

Task summary

Configuring an access policy for forward proxy with SWG
Creating a per-request policy
Configuring a policy to scan for malware and provide safe search
Blocking outgoing social media requests
Adding a per-request policy to the virtual server

Example policy: Categorize and scan traffic for malware

In this example per-request policy, a Category Lookup item obtains a list of categories and a response web page. If Category Lookup returns a value that specifies the response needs to be scanned to determine the appropriate category, Response Analytics runs.

Note: *Response Analytics is available only with an SWG subscription.*

Response Analytics scans the response for malicious embedded content and passes an analysis to the URL Filter Assign item. URL Filter Assign uses the analysis, if provided, and the specified filter to determine whether to allow the request.

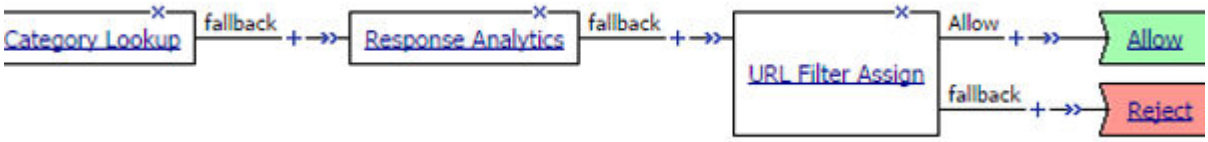


Figure 7: Process of Response Analytics contributing analysis results to URL filter assign

Example policy: URL database category-specific access control

This example uses two standard URL categories, Entertainment and Jobsearch, that are available on a BIG-IP system with an SWG subscription. In this per-request policy example, only recruiters are allowed to access URLs in the job search category. The policy also restricts access to entertainment sites during business hours.

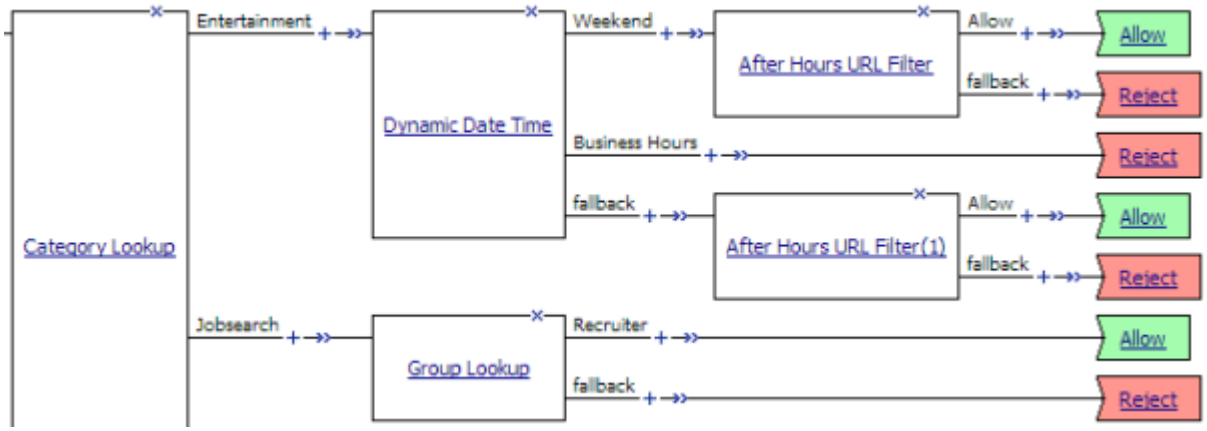


Figure 8: Category-specific access restrictions

Configuring an access policy for forward proxy with SWG

You configure an access policy to support explicit forward proxy or transparent forward proxy. If you plan to use branching by group or class attribute in your per-request policy, you add items to the access policy to populate that information. You can also add access policy items to collect credentials and to authenticate a user or add access policy items to identify the user transparently.

Note: *If you include authentication in your access policy and the first site that a user accesses uses HTTP instead of secure HTTP, passwords are passed as clear text. To prevent this from happening, F5 recommends using Kerberos or NTLM authentication.*

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. In the Per-Session Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. If you specified an NTLM Auth configuration in the access profile, verify that authentication succeeded.
   a) On the Authentication tab, select **NTLM Auth Result**.
   b) Click **Add Item**.
      A properties popup screen opens.
   c) Click **Save**.
      The properties screen closes. The policy displays.
5. To add Kerberos authentication to an access policy for forward proxy, add **HTTP 407 Response** (for explicit forward proxy) or **HTTP 401 Response** (for transparent forward proxy); then follow it with these actions in order: **Variable Assign**, and **Kerberos Auth**.

   Note: *This example uses **HTTP 407 Response**. You can replace it with **HTTP 401 Response**.*

   In a transparent forward proxy configuration, APM does not support Kerberos request-based authentication

a) On a policy branch, click the plus symbol **(+)** to add an item to the policy.
b) On the Logon tab, select **HTTP 407 Response** and click **Add Item**.
A properties screen opens.
c) From the **HTTP Auth Level** list, select **negotiate** and click **Save**.
The properties screen closes.
d) Click the **(+)** icon on the **negotiate** branch.
A popup screen opens.
e) On the Assignment tab, select **Variable Assign** and click **Add Item**.

For Kerberos authentication to work correctly with forward proxy, you must assign the domain name for the proxy virtual server to a session variable.

f) Click **Add new entry**.
An **empty** entry appears in the Assignment table.
g) Click the **change** link in the new entry.
A popup screen opens.
h) In the left pane, retain the selection of **Custom Variable** and type this variable name: `session.server.network.name`.
i) In the right pane, in place of **Custom Variable**, select **Text** and type the domain name for the proxy virtual server.
j) Click **Finished**.

The popup screen closes.

k) Click **Save**.
The properties screen closes. The policy displays.
l) On a policy branch, click the plus symbol **(+)** to add an item to the policy.
m) On the Authentication tab, select **Kerberos Auth** and click **Add Item**.
A properties screen opens.
n) From the **AAA Server** list, select an existing server.
o) From the **Request Based Auth** list, select **Disabled**.
p) Click **Save**.
The properties screen closes and the policy displays.

Note: *The* ***Max Logon Attempts Allowed*** *setting specifies attempts by an external client without a Kerberos ticket to authenticate on forward proxy.*

---

6. To identify a user transparently using information provided by a Secure Web Gateway (SWG) user identification agent, perform these steps:

For this step of the access policy to succeed, you must have installed and configured either the F5® DC Agent or the F5 Logon Agent. Either agent is supported on a BIG-IP system with an SWG subscription only.

a) On a policy branch, click the plus symbol **(+)** to add an item to the policy.
b) From the Authentication tab, select **Transparent Identity Import** and click **Add Item**.

The transparent identity import access policy item searches the database in the IF-MAP server for the client source IP address. By default, this access policy item has two branches: associated and fallback.

A properties screen opens.

c) Click **Save**.
The visual policy editor opens.
d) Add any additional access policy items to the fallback or associated branches.
For example, you might add Kerberos authentication on the fallback branch.

7. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the policy and configure its properties:

a) From the **Server** list, select an AAA LDAP server.

An LDAP Query uses SSL connections when you select an LDAP AAA server that is configured for LDAPS.

b) Specify the **SearchDN**, and **SearchFilter** settings.

SearchDN is the base DN from which the search is done.

c) Click **Save**.

This item populates the `session.ldap.last.attr.memberOf` session variable.

8. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the policy and configure its properties:
   a) From the **Server** list, select an AAA AD server.
   b) Select the **Fetch Primary Group** check box.

      The value of the primary user group populates the `session.ad.last.attr.primaryGroupID` session variable.
   c) Click **Save**.
9. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the policy and configure its properties:
   a) From the **Server** list, select an AAA RADIUS server.
   b) Click **Save**.

   This item populates the `session.radius.last.attr.class` session variable.
10. Click the **Apply Access Policy** link to apply and activate the changes to the policy.

Creating a per-request policy

You must create a per-request policy before you can configure it in the visual policy editor.

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. Click **Create**.
   The General Properties screen opens.
3. In the **Name** field, type a name for the policy and click **Finished**.

   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 screen.

Configuring a policy to scan for malware and provide safe search

Important: *This task specifies elements and options that are supported only on a BIG-IP® system with an SWG subscription.*

You configure per-request policy to control access to forward proxy with these agents: Category Lookup to categorize requests and to provide safe search results to your users; Response Analytics (after Category Lookup) to scan the output response web page for malware, if indicated, and to provide a result to the next agent; and, URL Filter Assign to determine whether to allow or block a request.

Note: *This task does not specify a complete per-request policy.*

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. In the **Name** field, locate the policy that you want to update, then in the **Per-Request Policy** field, click the **Edit** link.
   The visual policy editor opens in another tab.
3. On a policy branch, click the **(+)** icon to add an item to the policy.

A small set of actions are provided for building a per-request policy.

A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.

4. On the General Purpose tab, select **Category Lookup** item and click **Add Item**.
   A popup Properties screen opens.
5. For **Categorization Input**, select an option based on the type of traffic to process:
   - For HTTP traffic, select **Use HTTP URI (cannot be used for SSL Bypass decisions)**. If selected, the **SafeSearch Mode** field displays set to **Enabled**.
   - For SSL-encrypted traffic, select **Use SNI in Client Hello (if SNI is not available, use Subject.CN)** or **Use Subject.CN in Server Cert**.

   Tip: *Early in the per-request policy, you can insert a Protocol Lookup agent to provide separate branches for HTTPS and HTTP traffic.*
6. For **Category Lookup Type**, select the types of categories to look through for the URL.
   - **Custom categories first, then standard categories if not found** - Select to look through custom categories; then, if the URL is not found, look through the standard categories that the URL database maintains.
   - **Always process full list of both custom and standard categories** - Select to look through custom categories and standard categories.
   - **Process standard categories only** - Select to look through standard categories only.

   Category Lookup compiles a list of one or more categories for the URL.
7. Click **Save**.
   The properties screen closes. The visual policy editor displays.
8. On a branch after a Category Lookup item, add a **URL Filter Assign** agent and, in its properties, select a URL filter.
9. To trigger inspection of response web page contents, on a branch after a Category Lookup item and before a URL Filter Assign item, insert a **Response Analytics** agent and specify its properties:
   a) In the **Max Buffer Size** field, type the number of bytes to buffer.
   b) In the **Max Buffer time** field, type the number of seconds to retain response data in the buffer.
   c) For the **Reset on Failure** field, retain the default value **Enabled** to send a TCP reset if the server fails.
   d) For each type of content that you want to exclude from analysis, click **Add new entry** and then select a type from the list.

      The **All-Images** type is on the list by default because images are not scanned.
   e) Click **Finished**.
      The popup screen closes.
   f) Click **Save**.
      The popup screen closes. The visual policy editor displays.

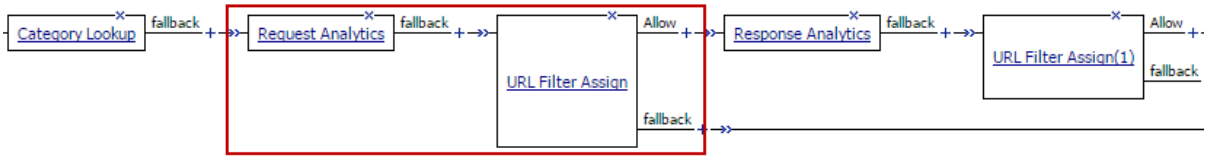
A per-request policy goes into effect when you add it to a virtual server. Depending on the forward proxy configuration, you might need to add the per-request policy to more than one virtual server.

Blocking outgoing social media requests

This configuration is specific to a BIG-IP® system with an SWG subscription. To use this procedure, you must already have a per-request policy configured that contains Category Lookup.

You might want to block outgoing requests to social media, particularly chat requests. To do this, you must insert two items after Category Lookup in the per-request policy: Request Analytics followed by

URL Filter Assign.



1. Open a per-request policy for editing.
2. Click the **(+)** icon after the **Category Lookup** item to add a new item.
   A popup screen opens, displaying tabs such as General Purpose and Logon.
3. On the General Purpose tab, select **Request Analytics** and click **Add Item**.
   The popup screen closes. A new popup screen displays the properties for the newly added item.
4. Click **Save**.
   The popup screen closes. The newly added item displays in the per-request policy.
5. After the newly added **Request Analytics** item, click the **(+)** icon.
6. On the General Purpose tab, select **URL Filter Assign** and click **Add Item**.
7. From the **URL Filter** list, select a URL filter and click **Save**.

Note: *A URL Filter Assign must follow the Request Analytics agent in addition to following the Response Analytics agent.*

The resulting per-request policy might include these items on a branch: Category Lookup, Request Analytics, URL Filter Assign, Response Analytics, and URL Filter Assign.

Adding a per-request policy to the virtual server

To add per-request processing to a configuration, associate the per-request policy with the virtual server.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server.
3. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
4. Click **Update**.

The per-request policy is now associated with the virtual server.

Virtual server Access Policy settings for forward proxy

F5 recommends multiple virtual servers for configurations where Access Policy Manager® (APM®) acts as an explicit or transparent forward proxy. This table lists forward proxy configurations, the virtual servers recommended for each, and whether an access profile and per-request policy should be specified on the virtual server.

Forward proxy	Recommended virtual servers (by purpose)	Specify access profile?	Specify per-request policy?
Explicit	Process HTTP traffic	Yes	Yes
	Process HTTPS traffic	Yes	Yes
	Reject traffic other than HTTP and HTTPS	N/A	N/A
Transparent Inline	Process HTTP traffic	Yes	Yes

Forward proxy	Recommended virtual servers (by purpose)	Specify access profile?	Specify per-request policy?
	Process HTTPS traffic	Only when a captive portal is also included in the configuration	Only when a captive portal is also included in the configuration
	Forward traffic other than HTTP and HTTPS	N/A	N/A
	Captive portal	Yes	No
Transparent	Process HTTP traffic	Yes	Yes
	Process HTTPS traffic	Only when a captive portal is also included in the configuration	Only when a captive portal is also included in the configuration
	Captive portal	Yes	No

About Response Analytics and the order of policy items

Note: *The Response Analytics per-request policy item is for use only on a BIG-IP® system with an SWG subscription.*

The Response Analytics per-request policy item makes an HTTP request and waits for the HTTP response before it completes. As a result to function properly, any policy items that rely on the information in the HTTP request or that attempt to modify the HTTP request must always precede the Response Analytics item. Specifically, the Category Lookup and HTTP Headers items must not follow a Response Analytics item.

Important: *You must enforce this ordering to ensure that your per-request policy functions as you intend.*

About Safe Search and supported search engines

Note: *Safe Search is supported only on a BIG-IP® system with an SWG subscription.*

Safe Search is a search engine feature that can prevent offensive content and images from showing up in search results. Safe Search can also protect video searches on Google, Bing, and Yahoo search engines.

Safe Search can be enabled in a per-request policy using the Category Lookup item. Secure Web Gateway (SWG) with Safe Search enabled supports these search engines: Ask, Bing, DuckDuckGo, Google, Lycos, and Yahoo. Some search engines, such as Google and Yahoo, use SSL by default; in this case, Safe Search works only when SWG is configured with SSL forward proxy.

Note: *For Safe Search filtering to work correctly, URLs for the supported search engine sites must not be added to a custom category. The search engine's domain must remain categorized in the Search Engines and Portals URL category.*

Policies for APM as a Secure Web Gateway

Overview: Controlling forward proxy traffic with APM

On a BIG-IP® system with Access Policy Manager® (APM®), you can configure per-request policies to control forward proxy access with user-defined URL categories and filters that you have configured.

Task summary

You must have created an explicit or a transparent forward proxy configuration.

Task list

Configuring an access policy for forward proxy with SWG
Creating a per-request policy
Applying user-defined URL categories and filters in a per-request policy
Adding a per-request policy to the virtual server

Configuring an access policy for forward proxy with SWG

You configure an access policy to support explicit forward proxy or transparent forward proxy. If you plan to use branching by group or class attribute in your per-request policy, you add items to the access policy to populate that information. You can also add access policy items to collect credentials and to authenticate a user or add access policy items to identify the user transparently.

Note: *If you include authentication in your access policy and the first site that a user accesses uses HTTP instead of secure HTTP, passwords are passed as clear text. To prevent this from happening, F5 recommends using Kerberos or NTLM authentication.*

---

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. In the Per-Session Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. If you specified an NTLM Auth configuration in the access profile, verify that authentication succeeded.
   a) On the Authentication tab, select **NTLM Auth Result**.
   b) Click **Add Item**.
      A properties popup screen opens.
   c) Click **Save**.
      The properties screen closes. The policy displays.
5. To add Kerberos authentication to an access policy for forward proxy, add **HTTP 407 Response** (for explicit forward proxy) or **HTTP 401 Response** (for transparent forward proxy); then follow it with these actions in order: **Variable Assign**, and **Kerberos Auth**.

Note: *This example uses* ***HTTP 407 Response****. You can replace it with* ***HTTP 401 Response****.*

In a transparent forward proxy configuration, APM does not support Kerberos request-based authentication

a) On a policy branch, click the plus symbol **(+)** to add an item to the policy.
b) On the Logon tab, select **HTTP 407 Response** and click **Add Item**.
A properties screen opens.
c) From the **HTTP Auth Level** list, select **negotiate** and click **Save**.
The properties screen closes.
d) Click the **(+)** icon on the **negotiate** branch.
A popup screen opens.
e) On the Assignment tab, select **Variable Assign** and click **Add Item**.

For Kerberos authentication to work correctly with forward proxy, you must assign the domain name for the proxy virtual server to a session variable.

f) Click **Add new entry**.
An **empty** entry appears in the Assignment table.
g) Click the **change** link in the new entry.
A popup screen opens.
h) In the left pane, retain the selection of **Custom Variable** and type this variable name: `session.server.network.name`.
i) In the right pane, in place of **Custom Variable**, select **Text** and type the domain name for the proxy virtual server.
j) Click **Finished**.

The popup screen closes.

k) Click **Save**.
The properties screen closes. The policy displays.
l) On a policy branch, click the plus symbol **(+)** to add an item to the policy.
m) On the Authentication tab, select **Kerberos Auth** and click **Add Item**.
A properties screen opens.
n) From the **AAA Server** list, select an existing server.
o) From the **Request Based Auth** list, select **Disabled**.
p) Click **Save**.
The properties screen closes and the policy displays.

Note: *The* ***Max Logon Attempts Allowed*** *setting specifies attempts by an external client without a Kerberos ticket to authenticate on forward proxy.*

6. To identify a user transparently using information provided by a Secure Web Gateway (SWG) user identification agent, perform these steps:

For this step of the access policy to succeed, you must have installed and configured either the F5® DC Agent or the F5 Logon Agent. Either agent is supported on a BIG-IP system with an SWG subscription only.

a) On a policy branch, click the plus symbol **(+)** to add an item to the policy.
b) From the Authentication tab, select **Transparent Identity Import** and click **Add Item**.

The transparent identity import access policy item searches the database in the IF-MAP server for the client source IP address. By default, this access policy item has two branches: associated and fallback.

A properties screen opens.

c) Click **Save**.
The visual policy editor opens.
d) Add any additional access policy items to the fallback or associated branches.

For example, you might add Kerberos authentication on the fallback branch.

7. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the policy and configure its properties:
   a) From the **Server** list, select an AAA LDAP server.
      An LDAP Query uses SSL connections when you select an LDAP AAA server that is configured for LDAPS.
   b) Specify the **SearchDN**, and **SearchFilter** settings.
      SearchDN is the base DN from which the search is done.
   c) Click **Save**.

   This item populates the `session.ldap.last.attr.memberOf` session variable.
8. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the policy and configure its properties:
   a) From the **Server** list, select an AAA AD server.
   b) Select the **Fetch Primary Group** check box.
      The value of the primary user group populates the `session.ad.last.attr.primaryGroupID` session variable.
   c) Click **Save**.
9. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the policy and configure its properties:
   a) From the **Server** list, select an AAA RADIUS server.
   b) Click **Save**.

   This item populates the `session.radius.last.attr.class` session variable.
10. Click the **Apply Access Policy** link to apply and activate the changes to the policy.

Example policy: User-defined category-specific access control

In this per-request policy example, only recruiters are allowed to access URLs in the user-defined category Employment. The policy also restricts access to entertaining videos during business hours.

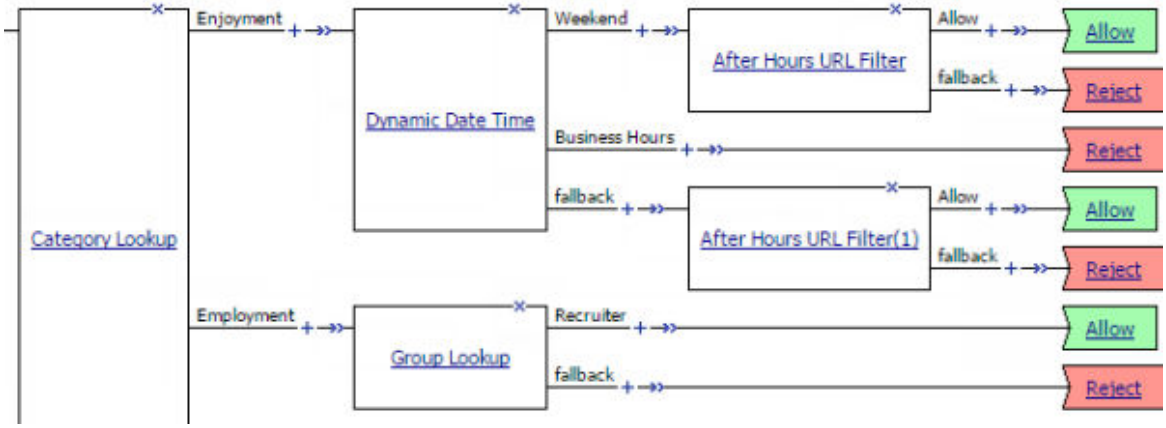


Figure 9: Category-specific access restrictions (using user-defined categories)

Example policy: URL filter per user group

Each URL Filter Assign item in this per-request policy example should specify a filter that is applicable to the user group.

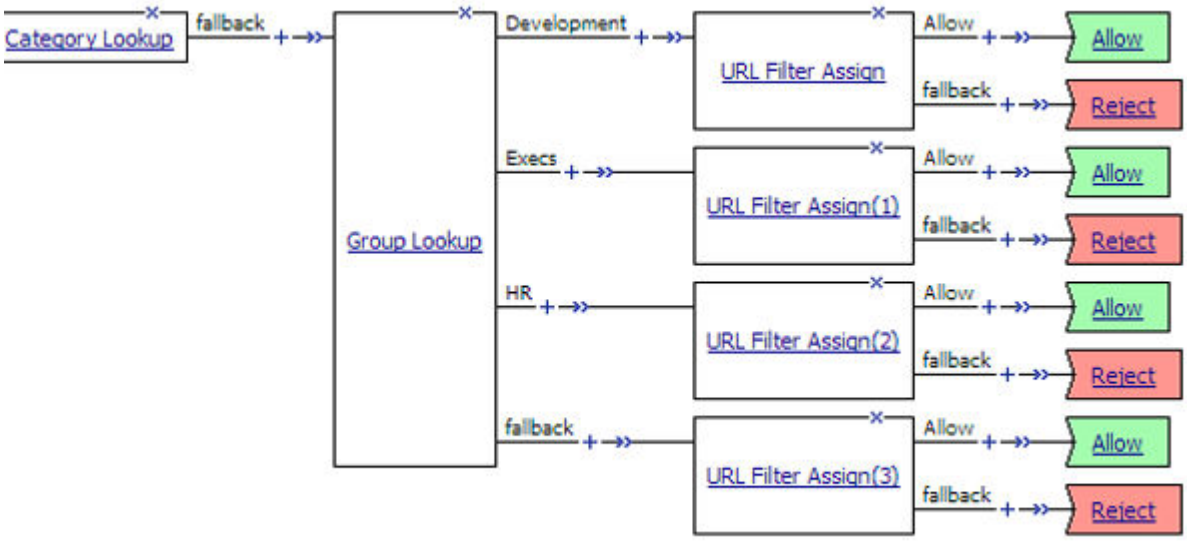


Figure 10: URL filter based on group membership

Creating a per-request policy

You must create a per-request policy before you can configure it in the visual policy editor.

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. Click **Create**.
   The General Properties screen opens.
3. In the **Name** field, type a name for the policy and click **Finished**.
   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 screen.

Applying user-defined URL categories and filters in a per-request policy

Important: *This task is for use on a BIG-IP® system without an SWG subscription.*

Look up the category for a URL request and assign a URL filter that blocks or allows access to control access to the web, based on the category of the URL request.

Note: *This task provides the steps for adding items to control web traffic based on the URL category. It does not specify a complete per-request policy.*

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. In the **Name** field, locate the policy that you want to update, then in the **Per-Request Policy** field, click the **Edit** link.
   The visual policy editor opens in another tab.
3. On the General Purpose tab, select **Category Lookup** item and click **Add Item**.
   A popup Properties screen opens.
4. For **Categorization Input**, select an option based on the type of traffic to process:

- For HTTP traffic, select **Use HTTP URI (cannot be used for SSL Bypass decisions)**. If selected, the **SafeSearch Mode** field displays set to **Enabled**.
- For SSL-encrypted traffic, select **Use SNI in Client Hello (if SNI is not available, use Subject.CN)** or **Use Subject.CN in Server Cert**.

Tip: *Early in the per-request policy, you can insert a Protocol Lookup agent to provide separate branches for HTTPS and HTTP traffic.*

5. For **Category Lookup Type**, you can only retain the default value **Process custom categories only**.
   Category Lookup looks through the user-defined categories to compile a list of categories for the URL.
6. Click **Save**.
   The properties screen closes. The visual policy editor displays.
7. On a branch after a Category Lookup item, add a **URL Filter Assign** agent and, in its properties, select a URL filter.

A per-request policy goes into effect when you add it to a virtual server. Depending on the forward proxy configuration, you might need to add the per-request policy to more than one virtual server.

Adding a per-request policy to the virtual server

To add per-request processing to a configuration, associate the per-request policy with the virtual server.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server.
3. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
4. Click **Update**.

The per-request policy is now associated with the virtual server.

Virtual server Access Policy settings for forward proxy

F5 recommends multiple virtual servers for configurations where Access Policy Manager® (APM®) acts as an explicit or transparent forward proxy. This table lists forward proxy configurations, the virtual servers recommended for each, and whether an access profile and per-request policy should be specified on the virtual server.

Forward proxy	Recommended virtual servers (by purpose)	Specify access profile?	Specify per-request policy?
Explicit	Process HTTP traffic	Yes	Yes
	Process HTTPS traffic	Yes	Yes
	Reject traffic other than HTTP and HTTPS	N/A	N/A
Transparent Inline	Process HTTP traffic	Yes	Yes
	Process HTTPS traffic	Only when a captive portal is also included in the configuration	Only when a captive portal is also included in the configuration
	Forward traffic other than HTTP and HTTPS	N/A	N/A

Forward proxy	Recommended virtual servers (by purpose)	Specify access profile?	Specify per-request policy?
	Captive portal	Yes	No
Transparent	Process HTTP traffic	Yes	Yes
	Process HTTPS traffic	Only when a captive portal is also included in the configuration	Only when a captive portal is also included in the configuration
	Captive portal	Yes	No

SSL Bypass and Intercept with APM

Overview: Bypassing SSL forward proxy traffic with APM

On a BIG-IP® system that supports SSL forward proxy, you can create an explicit or transparent forward proxy configuration that supports bypassing SSL forward proxy traffic. The key points of the configuration are that, on the virtual server that processes SSL traffic, the server and client SSL profiles must enable SSL forward proxy and SSL forward proxy bypass; the client SSL profile must set the default bypass action to **Intercept**.

An Access Policy Manager® (APM®) per-request policy can be configured to determine whether to intercept or bypass the SSL traffic.

Task summary

Before you start, you must have configured an explicit or transparent forward proxy configuration that supports bypassing SSL forward proxy traffic.

Task list

Creating a per-request policy
Processing SSL traffic in a per-request policy
Adding a per-request policy to the virtual server

Example policy: SSL forward proxy bypass

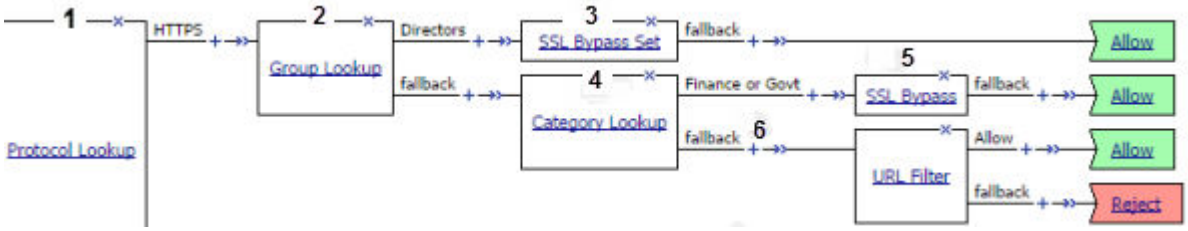


Figure 11: SSL bypass decision based on group membership and URL category

1	SSL traffic exits on the HTTPS branch of Protocol Lookup.
2	A lookup type item, such as LocalDB Group Lookup, identifies users in a group, Directors.
3	With SSL Bypass Set, any SSL request on the Directors branch is not intercepted or inspected.
4	Category Lookup processes HTTPS traffic when configured to use SNI or Subject.CN input. ***Note:*** *Finance or Govt is a standard URL category that SWG maintains on a system with an SWG subscription. User-defined URL categories can provide an alternative on systems without an SWG subscription.*
5	For users in a group other than Directors, bypass only requests that contain private information (determined through Category Lookup).
6	SSL traffic processing is complete. Now is the time to start processing HTTP data with actions that inspect the SSL payload. Using data provided by Category Lookup, URL Filter Assign item determines whether to allow or block traffic.

(For this example to be valid, both the server and client SSL profiles on the virtual server must enable SSL forward proxy and SSL forward proxy bypass; the client SSL profile must set the default bypass action to **Intercept**.)

Creating a per-request policy

You must create a per-request policy before you can configure it in the visual policy editor.

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. Click **Create**.
   The General Properties screen opens.
3. In the **Name** field, type a name for the policy and click **Finished**.

   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 screen.

Processing SSL traffic in a per-request policy

To use SSL forward proxy bypass in a per-request policy, both the server and client SSL profile must enable SSL forward proxy and SSL forward proxy bypass; and, in the client SSL profile, the default bypass action must be set to **Intercept**.

Important: *Configure a per-request policy so that it completes processing of HTTPS requests before it starts the processing of HTTP requests.*

Note: *These steps describe how to add items for controlling SSL web traffic to a per-request policy; the steps do not specify a complete per-request policy.*

---

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. In the **Name** field, locate the policy that you want to update, then in the **Per-Request Policy** field, click the **Edit** link.
   The visual policy editor opens in another tab.
3. To process the HTTPS traffic first, configure a branch for it by adding a **Protocol Lookup** item at the start of the per-request policy.
   a) Click the **(+)** icon anywhere in the per-request policy to add a new item.
      A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
   b) In the Search field, type `prot`, select **Protocol Lookup**, and click **Add Item**.
      A properties popup screen opens.
   c) Click **Save**.
      The properties screen closes. The policy displays.

   The Protocol Lookup item provides two default branches: HTTPS for SSL traffic and fallback.
4. Before you add an SSL Bypass Set, or an SSL Intercept Set, item to the per-request policy, you can insert any of the following policy items to do logging or to base how you process the SSL traffic on group membership, class attribute, day of the week, time of day, or URL category:

   - AD Group Lookup
   - LDAP Group Lookup
   - LocalDB Group Lookup
   - RADIUS Class Lookup

- Dynamic Date Time
- Logging
- Category Lookup

Important: *Category Lookup is valid for processing SSL traffic only when configured for SNI or Subject.CN categorization input and only before any HTTP traffic is processed.*

If you insert other policy items that inspect the SSL payload (HTTP data) before an SSL Bypass Set item, the SSL bypass cannot work as expected.

5. At any point on the HTTPS branch where you decide to bypass SSL traffic, add an **SSL Bypass Set** item.

The per-request policy includes items that you can use to complete the processing of SSL traffic. Add other items to the policy to control access according to your requirements.

A per-request policy goes into effect when you add it to a virtual server. Depending on the forward proxy configuration, you might need to add the per-request policy to more than one virtual server.

Adding a per-request policy to the virtual server

To add per-request processing to a configuration, associate the per-request policy with the virtual server.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server.
3. In the Access Policy area, from the **Per-Request Policy** list, select the policy that you configured earlier.
4. Click **Update**.

The per-request policy is now associated with the virtual server.

Virtual server Access Policy settings for forward proxy

F5 recommends multiple virtual servers for configurations where Access Policy Manager® (APM®) acts as an explicit or transparent forward proxy. This table lists forward proxy configurations, the virtual servers recommended for each, and whether an access profile and per-request policy should be specified on the virtual server.

Forward proxy	Recommended virtual servers (by purpose)	Specify access profile?	Specify per-request policy?
Explicit	Process HTTP traffic	Yes	Yes
	Process HTTPS traffic	Yes	Yes
	Reject traffic other than HTTP and HTTPS	N/A	N/A
Transparent Inline	Process HTTP traffic	Yes	Yes
	Process HTTPS traffic	Only when a captive portal is also included in the configuration	Only when a captive portal is also included in the configuration
	Forward traffic other than HTTP and HTTPS	N/A	N/A
	Captive portal	Yes	No

Forward proxy	Recommended virtual servers (by purpose)	Specify access profile?	Specify per-request policy?
Transparent	Process HTTP traffic	Yes	Yes
	Process HTTPS traffic	Only when a captive portal is also included in the configuration	Only when a captive portal is also included in the configuration
	Captive portal	Yes	No

About the SSL Bypass Set and SSL Intercept Set process

For SSL bypass or SSL intercept actions, Access Policy Manager® (APM®) forwards the client hello directly to the server. The client and server then negotiate SSL parameters. This must occur before any per-request policy item inspects the SSL payload (HTTP data). Everything that the policy does before an SSL Bypass Set or SSL Intercept Set policy item must operate either on SSL data (certificate or client hello) or on session data (which is not part of SSL payload).

About SSL Bypass Set and SSL Intercept Set and the order of policy items

To ensure that SSL Bypass Set and SSL Intercept Set work correctly, do not place them in a per-request policy after any of these items:

- Application Lookup
- Application Filter Assign
- Category Lookup, if configured to use HTTP URI for input
- HTTP Headers
- Proxy Select
- Select SSO Configuration
- URL Filter Assign

Forward Proxy Chaining with APM

BIG-IP system forward proxy chaining and APM benefits

The BIG-IP® system supports forward proxy chaining which enables connection to a next hop proxy server. Access Policy Manager® (APM®) brings these abilities to forward proxy chaining:

- Offload authentication from and support authentication to the next hop on the client's behalf.
- Support single sign-on to the next hop and to resources at the next hop.
- Select different proxy servers for different requests.
- Select different SSO configurations for different requests.

Interoperability characteristics for forward proxy chaining

In a forward proxy chain, Access Policy Manager® (APM®) selects the next hop proxy server, and interacts with it and resource servers behind it.

Note: *A proxy server can be located in the cloud. It can be located in another department of an enterprise.*

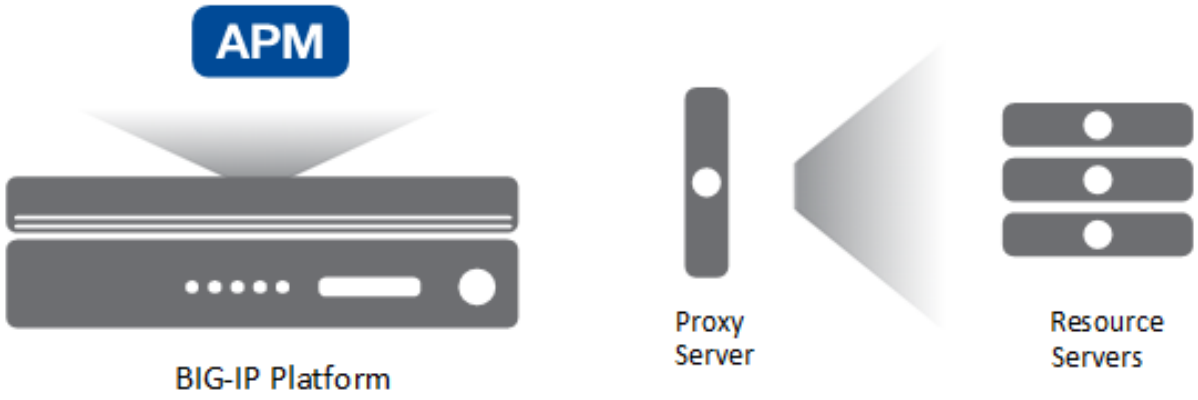


Figure 12: Forward proxy chaining: server types

For the BIG-IP® system, proxy server, and resource servers behind the proxy server, let's focus on these configuration characteristics.

Forward proxy mode

APM can be configured to act as an explicit or as a transparent forward proxy. The proxy server can be configured to act as explicit or transparent forward proxy. APM supports any combination of forward proxy modes.

SSL bypass mode

APM can be configured for SSL bypass or SSL intercept. The proxy server can be configured for SSL bypass or SSL intercept. APM supports all combinations of SSL bypass mode.

Authentication

Authentication might be configured on one or more servers:

- On APM, you can configure no authentication or any type of authentication that APM supports for an SWG-Explicit or SWG-Transparent access profile.

- On a proxy server, if you have HTTP Basic, NTLM, or Kerberos authentication configured, APM should authenticate to the proxy server. You can also have no authentication configured on the proxy server.
- On a resource server, if you have HTTP Basic, NTLM, or Kerberos authentication configured, APM should authenticate to the resource server. You can also have no authentication configured on the resource server.

Single sign-on

APM supports these types of SSO configuration to the proxy server or to a resource server: HTTP Basic, NTLMv1, NTLMv2, or Kerberos.

To a large extent, APM supports combinations of these configuration characteristics. However, given the number of possible configuration combinations and the varying capabilities of proxy servers, some configuration constraints can exist. Refer to *BIG-IP® Access Policy Manager®: Secure Web Gateway* and to Release Note: BIG-IP APM (for the product version you are using) on the AskF5™ web site located at `support.f5.com`.

Configuration essentials for forward proxy chaining

When configured to act as an explicit or transparent forward proxy, Access Policy Manager® (APM®) supports forward proxy chaining, with or without an SWG subscription. These configuration elements are key to forward proxy chaining:

- One or more pools of proxy servers. All servers in a pool must support the same forward proxy mode: explicit or transparent.
- A per-request policy that includes a Proxy Select agent, which specifies a pool of proxy servers.

Note: *Only the Proxy Select agent signals that a connection must be made to a next hop. A Pool Assign agent does not.*

- An HTTP Proxy Connect profile configured with its state disabled.
- The virtual server that processes HTTPS traffic for the forward proxy configuration with the disabled HTTP Proxy Connect profile specified.

Overview: Offloading authentication from the next hop

In this example, Access Policy Manager® (APM®) performs authentication on behalf of the proxy server and the resource servers.

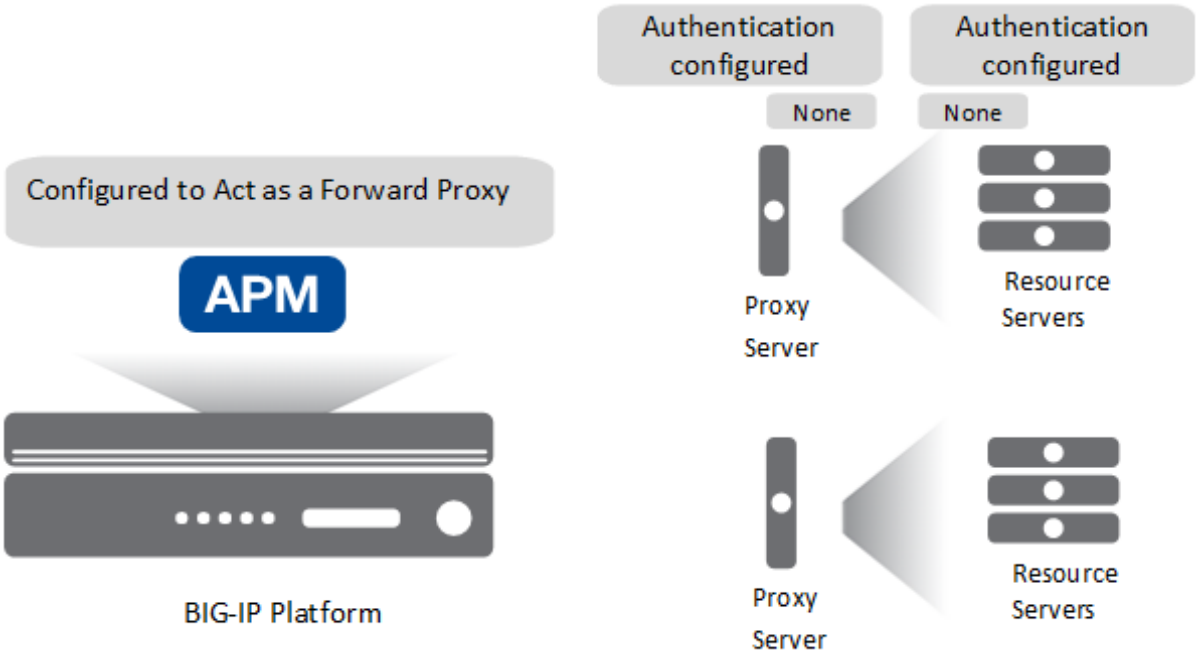


Figure 13: Expected initial configuration

Task summary

You need an access policy configured with any type of authentication that APM supports for an SWG-Explicit or SWG-Transparent access profile type, and a per-request policy that selects the next hop.

Task list

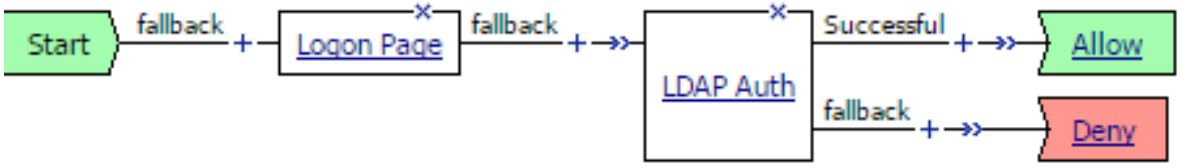
Configuring an access policy for authentication
Configuring a per-request policy to select the next hop

Configuring an access policy for authentication

You configure an access policy to authenticate users on behalf of a proxy server.

Note: *You can configure any type of authentication that Access Policy Manager® (APM®) supports for the access profile type (SWG-Explicit or SWG-Transparent) that is used in your forward proxy configuration.*

This example uses LDAP.



1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. Locate the access profile for the forward proxy configuration you are updating.
   Look in the **Profile Type** field for **SWG-Explicit** or **SWG-Transparent**.

3. In the Per-Session Policy column, click the **Edit** link
   The visual policy editor opens the access policy in a separate screen.
4. Click the **(+)** icon anywhere in the access policy to add a new item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
5. On the Logon tab, select **Logon Page** and click the **Add Item** button.
   The Logon Page Agent properties screen opens.
6. Click **Save**.
   The properties screen closes and the policy displays.
7. On a policy branch, click the **(+)** icon to add an item to the policy.
8. On the Authentication tab, select **LDAP Auth** and click **Add Item**.
   A Properties screen opens.
9. For **Server**, select the LDAP server you want to use from the list.

   Servers are defined in the **Access > Authentication** area of the Configuration utility.
10. For **SearchDN**, type the base node of the LDAP server search tree where you want to start the search.
11. For **SearchFilter**, type the search criteria to use when querying the LDAP server for the user's information.

    Session variables are supported as part of the search query string.

    When you type a string, enclose it in parentheses.

    For example, type `(sAmAccountName=%{session.logon.last.username})` or `(sAmAccountName=%{subsession.logon.last.username})`.
12. For **UserDN**, specify the Distinguished Name (DN) of the user.
13. Click **Save**.
    The properties screen closes and the policy displays.
14. Click the **Apply Access Policy** link to apply and activate the changes to the policy.

Configuring a per-request policy to select the next hop

Before you start, you must have configured a pool of proxy servers that are all configured to support the same forward proxy mode: explicit or transparent. (Pools are configured in the **Local TrafficPools** area of the product.)

You configure a per-request policy with a Proxy Select agent to select the next hop in a forward proxy chain.

Note: *If you include **SSL Intercept** or **SSL Bypass** agents in the policy, be sure to place them before other agents. If an SSL Bypass agent is included in the policy with a proxy select agent, the policy must contain a Category lookup agent before the bypass agent.*

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. If you are not going to update an existing policy, all you need to do to create a new one is click **Create**, type a name that is unique among all access profile and per-request policy names, and click **Finished**.
3. In the **Name** field, locate the policy that you want to update, then in the **Per-Request Policy** field, click the **Edit** link.
   The visual policy editor opens in another tab.

4. On a policy branch, click the **(+)** icon to add an item to the policy.

   A small set of actions are provided for building a per-request policy.

   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
5. On the General Purpose tab, select **Proxy Select** and click **Add Item**.
   A Properties popup screen opens.
6. From the **Pool** list, select a pool of one or more proxy servers from which to select the next hop.

   Important: *All proxy servers in the pool that you select must support the forward proxy mode that you specify in the* ***Upstream Proxy Mode*** *setting.*
7. From **Upstream Proxy Mode**, select **Explicit** or **Transparent**.
8. For **Username** and **Password**, most of the time you can retain the default values (blank).

   These fields support the use of static credentials to authenticate the user at the next hop using HTTP Basic authentication.
9. Click **Save**.
   The properties screen closes. The visual policy editor displays.

Be sure to add a disabled HTTP Connect Profile to the virtual server that processes SSL traffic for the forward proxy configuration.

Note: *A per-request policy is not in effect unless it and an access profile are specified in virtual servers in the forward proxy configuration.*

Overview: Using NTLM pass-through to the next hop

NTLM pass-through describes a configuration where authentication is not specified on Access Policy Manager® (APM®), but where NTLM authentication is configured at the next hop or at a resource server behind the next hop.

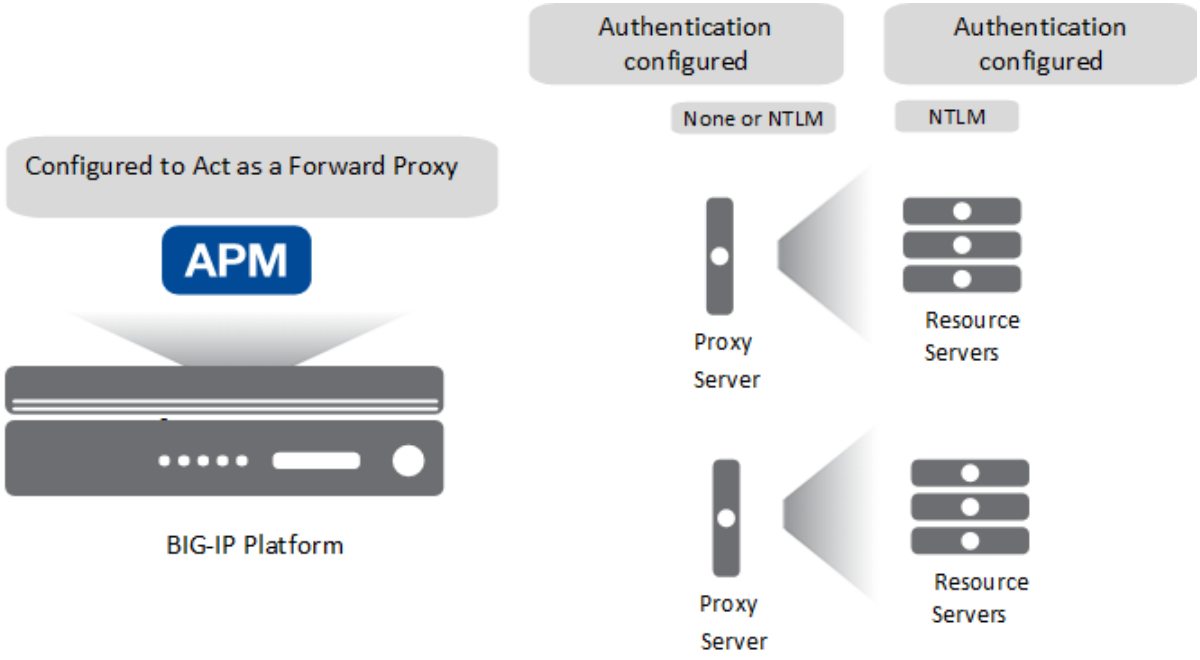


Figure 14: Expected initial configuration

Note: *APM supports NTLM pass-through only for HTTP traffic, and only when both APM and the proxy server are configured for explicit forward proxy.*

To support this configuration, you need an access policy, but no specific configuration is required in it. You also need a per-request policy configured to select the next hop.

Configuring a per-request policy to select the next hop

Before you start, you must have configured a pool of proxy servers that are all configured to support the same forward proxy mode: explicit or transparent. (Pools are configured in the **Local TrafficPools** area of the product.)

You configure a per-request policy with a Proxy Select agent to select the next hop in a forward proxy chain.

Note: *If you include **SSL Intercept** or **SSL Bypass** agents in the policy, be sure to place them before other agents. If an SSL Bypass agent is included in the policy with a proxy select agent, the policy must contain a Category lookup agent before the bypass agent.*

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. If you are not going to update an existing policy, all you need to do to create a new one is click **Create**, type a name that is unique among all access profile and per-request policy names, and click **Finished**.
3. In the **Name** field, locate the policy that you want to update, then in the **Per-Request Policy** field, click the **Edit** link.
   The visual policy editor opens in another tab.
4. On a policy branch, click the **(+)** icon to add an item to the policy.

   A small set of actions are provided for building a per-request policy.

   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
5. On the General Purpose tab, select **Proxy Select** and click **Add Item**.
   A Properties popup screen opens.
6. From the **Pool** list, select a pool of one or more proxy servers from which to select the next hop.

   Important: *All proxy servers in the pool that you select must support the forward proxy mode that you specify in the **Upstream Proxy Mode** setting.*
7. From **Upstream Proxy Mode**, select **Explicit** or **Transparent**.
8. For **Username** and **Password**, most of the time you can retain the default values (blank).

   These fields support the use of static credentials to authenticate the user at the next hop using HTTP Basic authentication.
9. Click **Save**.
   The properties screen closes. The visual policy editor displays.

Be sure to add a disabled HTTP Connect Profile to the virtual server that processes SSL traffic for the forward proxy configuration.

Note: *A per-request policy is not in effect unless it and an access profile are specified in virtual servers in the forward proxy configuration.*

Overview: Inserting HTTP headers for authentication to the next hop

Access Policy Manager® (APM®) supports inserting the X-Authenticated-User HTTP header and, optionally, the X-Forwarded-For HTTP header to authenticate on the user's behalf to a next hop proxy server or to a resource server behind the proxy. In this example, you can configure either HTTP Basic or NTLM authentication on the proxy server or on the resource server.

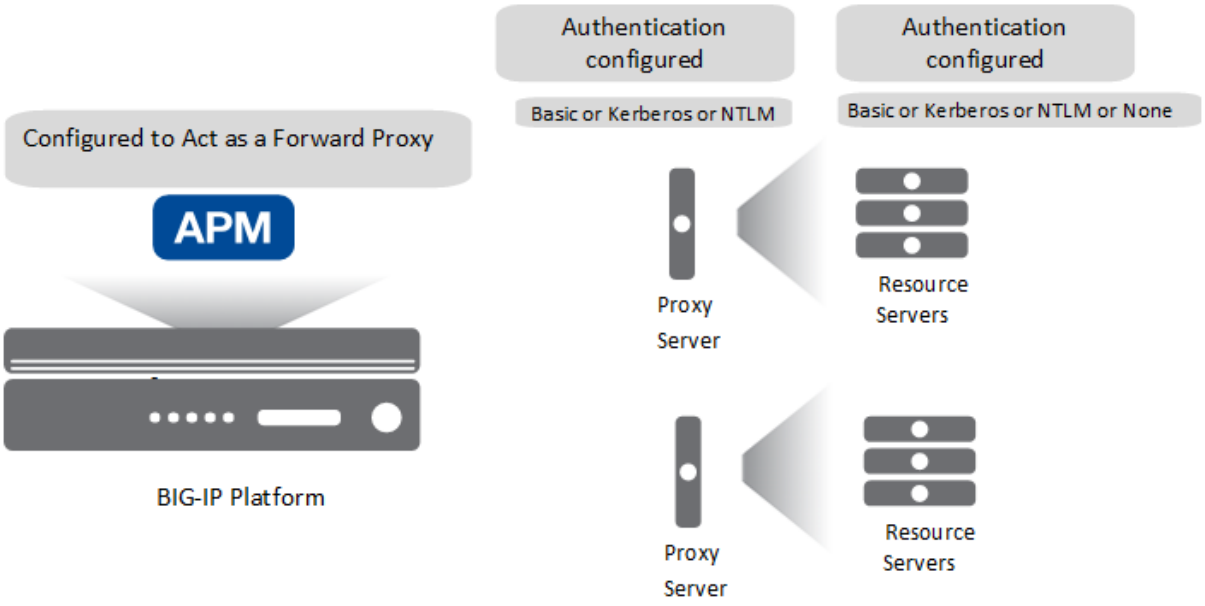


Figure 15: Expected initial configuration

Task summary

You need an access policy configured with any type of authentication that APM supports for an SWG-Explicit or SWG-Transparent access profile type and a per-request policy that inserts the header and selects the next hop.

Task list

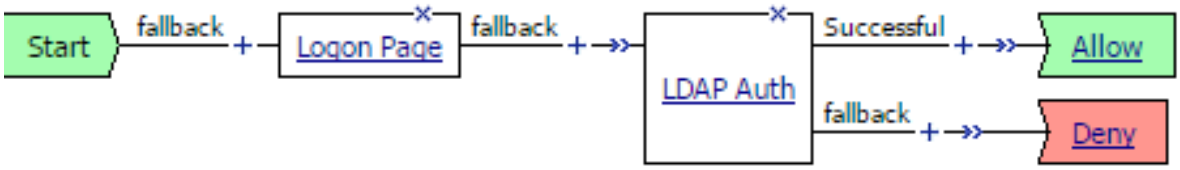
Configuring an access policy for authentication
Inserting the HTTP header and selecting the next hop

Configuring an access policy for authentication

You configure an access policy to authenticate users on behalf of a proxy server.

Note: *You can configure any type of authentication that Access Policy Manager® (APM®) supports for the access profile type (SWG-Explicit or SWG-Transparent) that is used in your forward proxy configuration.*

This example uses LDAP.



1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. Locate the access profile for the forward proxy configuration you are updating.
   Look in the **Profile Type** field for **SWG-Explicit** or **SWG-Transparent**.
3. In the Per-Session Policy column, click the **Edit** link
   The visual policy editor opens the access policy in a separate screen.
4. Click the **(+)** icon anywhere in the access policy to add a new item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
5. On the Logon tab, select **Logon Page** and click the **Add Item** button.
   The Logon Page Agent properties screen opens.
6. Click **Save**.
   The properties screen closes and the policy displays.
7. On a policy branch, click the **(+)** icon to add an item to the policy.
8. On the Authentication tab, select **LDAP Auth** and click **Add Item**.
   A Properties screen opens.
9. For **Server**, select the LDAP server you want to use from the list.
   Servers are defined in the **Access > Authentication** area of the Configuration utility.
10. For **SearchDN**, type the base node of the LDAP server search tree where you want to start the search.
11. For **SearchFilter**, type the search criteria to use when querying the LDAP server for the user's information.
    Session variables are supported as part of the search query string.
    When you type a string, enclose it in parentheses.
    For example, type `(sAmAccountName=%{session.logon.last.username})` or `(sAmAccountName=%{subsession.logon.last.username}).`
12. For **UserDN**, specify the Distinguished Name (DN) of the user.
13. Click **Save**.
    The properties screen closes and the policy displays.
14. Click the **Apply Access Policy** link to apply and activate the changes to the policy.

Inserting the HTTP header and selecting the next hop

Before you start, make sure that the proxy servers at the next hop are capable of processing the HTTP header you insert.

You configure a per-request policy to insert an X-Authenticated-User HTTP header with the value of a successfully authenticated user name to authenticate to the next hop proxy server or to resource servers behind it.

*Note: If you include **SSL Intercept** or **SSL Bypass** agents in the policy, be sure to place them before other agents.*

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. If you are not going to update an existing policy, all you need to do to create a new one is click **Create**, type a name that is unique among all access profile and per-request policy names, and click **Finished**.
3. In the **Name** field, locate the policy that you want to update, then in the **Per-Request Policy** field, click the **Edit** link.
   The visual policy editor opens in another tab.
4. On a policy branch, click the **(+)** icon to add an item to the policy.

   A small set of actions are provided for building a per-request policy.

   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
5. On the General Purpose tab, select **HTTP Headers** and click **Add Item**.
   A Properties screen opens.
6. In the **HTTP Header Modify** area, click **Add new entry**.
7. For **Header Operation**, retain the default value **insert**.
8. In the **Header Name** field, type `X-Authenticated-User`.
9. In the **Header Value** field, type the value of a successfully authenticated username.
   For example, type `%{session.logon.last.userrname}`.
10. To also add an X-Forwarded-For HTTP header, perform these substeps:
    a) In the **HTTP Header Modify** area, click **Add new entry**.
    b) In the **Header Name** field, type `X-Forwarded-For`.
    c) In the **Header Value** field, type the value of the client IP address.
       For example, type `%{session.user.clientip}`.
11. Click **Save**.
    The properties screen closes. The visual policy editor displays.
12. Add any additional items you want to the policy.
13. Click the **(+)** icon anywhere in the per-request policy to add a new item.
14. On the General Purpose tab, select **Proxy Select** and click **Add Item**.
    A Properties popup screen opens.
15. From the **Pool** list, select a pool of one or more proxy servers from which to select the next hop.

    ***Important:** All proxy servers in the pool that you select must support the forward proxy mode that you specify in the **Upstream Proxy Mode** setting.*
16. From **Upstream Proxy Mode**, select **Explicit** or **Transparent**.
17. For **Username** and **Password**, most of the time you can retain the default values (blank).

    These fields support the use of static credentials to authenticate the user at the next hop using HTTP Basic authentication.
18. Click **Save**.
    The properties screen closes. The visual policy editor displays.

Be sure to add a disabled HTTP Connect Profile to the virtual server that processes SSL traffic for the forward proxy configuration.

Note: A per-request policy is not in effect unless it and an access profile are specified in virtual servers in the forward proxy configuration.

Configuration constraints for X-Authenticated-User header

Before configuring Access Policy Manager® (APM®) to forward X-Authenticated-User and X-Forwarded-For headers to a third-party proxy server, consider the capabilities of the specific proxy server. How a proxy server responds to X-Authenticated-User and X-Forwarded-For headers is completely dependent on the proxy server capabilities, and on the settings that a proxy server might provide for resource protection. Not all proxy servers can process the headers. Others might process and trust the headers but, based on configuration settings, require authentication regardless.

Overview: Authenticating with HTTP Basic to the next hop

With no authentication configured on Access Policy Manager® (APM®), you can still use HTTP Basic to authenticate to a next hop proxy server.

You don't need any particular configuration in the access policy. You do need to select the next hop proxy, and specify static credentials in the Proxy Select agent in the per-request policy.

Configuring a policy for HTTP Basic at the next hop

Before you start, you must have configured a pool of proxy servers that are all configured to support the same forward proxy mode: explicit or transparent. (Pools are configured in the **Local TrafficPools** area of the product.)

You configure a per-request policy to select the next hop in a forward proxy chain and provide static credentials for HTTP Basic authentication.

Note: *If you include* ***SSL Intercept*** *or* ***SSL Bypass*** *agents in the policy, be sure to place them before other agents.*

---

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. If you are not going to update an existing policy, all you need to do to create a new one is click **Create**, type a name that is unique among all access profile and per-request policy names, and click **Finished**.
3. In the **Name** field, locate the policy that you want to update, then in the **Per-Request Policy** field, click the **Edit** link.
   The visual policy editor opens in another tab.
4. On a policy branch, click the **(+)** icon to add an item to the policy.

   A small set of actions are provided for building a per-request policy.

   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
5. On the General Purpose tab, select **Proxy Select** and click **Add Item**.
   A Properties popup screen opens.
6. From the **Pool** list, select a pool of one or more proxy servers from which to select the next hop.

   Important: *All proxy servers in the pool that you select must support the forward proxy mode that you specify in the* ***Upstream Proxy Mode*** *setting.*

   ---
7. From **Upstream Proxy Mode**, select **Explicit** or **Transparent**.
8. For **Username** and **Password**, type the user name and password that APM can use to authenticate to the proxy server.

9. Click **Save**.
   The properties screen closes. The visual policy editor displays.

Be sure to add a disabled HTTP Connect Profile to the virtual server that processes SSL traffic for the forward proxy configuration.

Note: *A per-request policy is not in effect unless it and an access profile are specified in virtual servers in the forward proxy configuration.*

Troubleshooting Basic authentication at the next hop proxy server

The table lists some activities that you might observe with forward proxy chaining between Access Policy Manager® (APM®) and a third-party proxy server that uses Basic authentication. The table provides additional explanation.

Activity	Description
A client achieves single sign-on to a next hop proxy server that uses Basic authentication. However, the configuration on Access Policy Manager® (APM®) configuration does not include SSO.	The initial client request includes one these HTTP headers: `Proxy Authorization` or `Authorization`. This can happen when, for example, the user logged on as a domain user. Some third-party proxy servers accept these credentials at the initial request.
Packet captures show that a next hop proxy server rejected an initial client request with one of these HTTP headers: `Proxy Authorization` or `Authorization`.	Some third-party proxy servers deny such an initial request because the header is not expected. The proxy server then sends HTTP status code 407 (Proxy Authentication Required) or 401 (Authentication Required). APM responds to the HTTP code. If Basic SSO is configured, APM invokes it.

Overview: Configuring Basic or NTLM SSO to the next hop

Access Policy Manager® (APM®) supports the HTTP Basic, Kerberos, NTLMv1, and NTLMv2 types of SSO configuration to and behind a next hop proxy server. This example specifies the configuration for a Basic or NTLM type SSO. Authentication can be configured on the proxy server or on a resource server behind it.

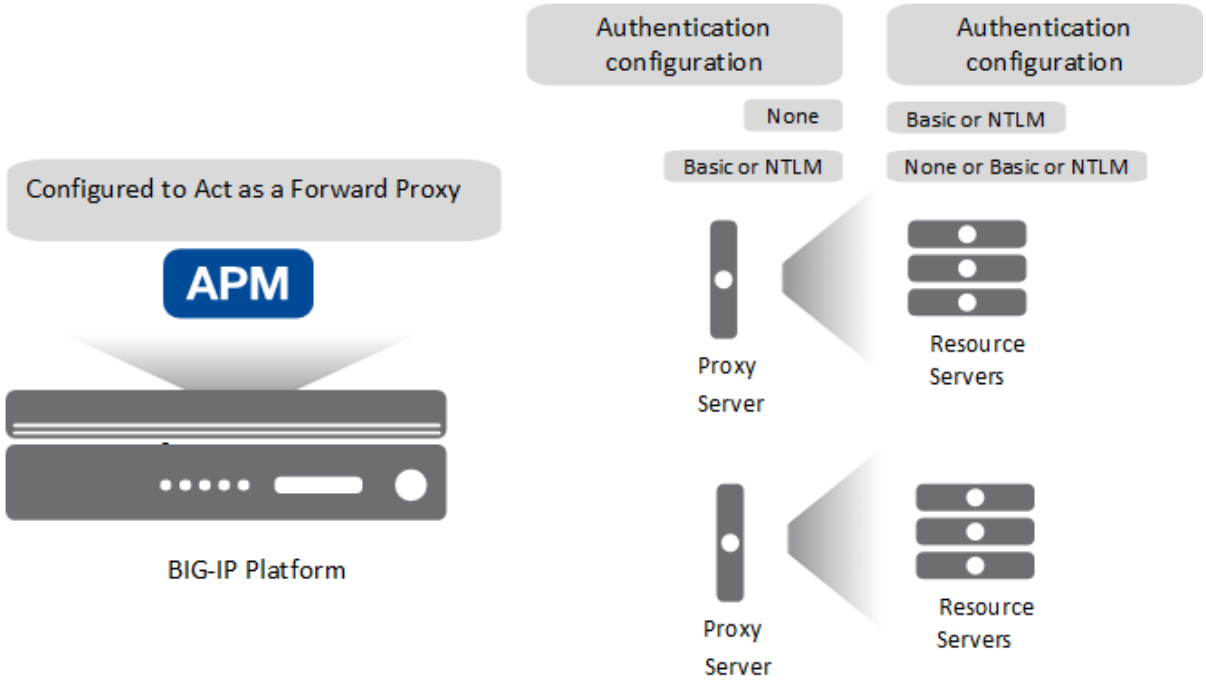


Figure 16: Expected initial configuration

Task summary

You need an access policy to gather and cache user credentials. You need a per-request policy to specify an SSO configuration and select the next hop proxy.

Task list

Configuring an access policy for SSO to the next hop
Configuring Basic or NTLM SSO to the next hop

Configuring an access policy for SSO to the next hop

To support SSO to the next hop proxy server in a forward proxy chain or to a resource server behind the next hop, you configure an access policy to collect credentials and cache them.

Note: *This example policy uses the Logon Page item to collect credentials; you can use other items.*

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. In the Per-Session Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. On the Logon tab, select **Logon Page** and click the **Add Item** button.
   The Logon Page Agent properties screen opens.
5. Click **Save**.

The properties screen closes and the policy displays.

6. On a policy branch, click the **(+)** icon to add an item to the policy.
7. On the Assignment tab, select **SSO Credential Mapping** and click **Add Item**.
   A properties screen opens.
8. Click **Save**.
   The properties screen closes and the policy displays.

Configuring Basic or NTLM SSO to the next hop

Before you start, you need to have configured:

- An HTTP Basic, NTLMv1, or NTLMv2 SSO configuration.

  Note: *SSO configurations are configured in the* ***Access*** > ***Single Sign-On*** *area of the product.*

- A pool of proxy servers, each of which is configured for the same forward proxy mode: explicit or transparent.

  Note: *Pools are configured in the* ***Local Traffic*** > ***Pools*** *area of the product.*

To support SSO from Access Policy Manager® (APM®) in a forward proxy chain, you configure a per-request policy to select an SSO configuration and later select the next hop.

Note: *If you include* ***SSL Intercept*** *or* ***SSL Bypass*** *agents in the policy, be sure to place them before other agents.*

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. If you are not going to update an existing policy, all you need to do to create a new one is click **Create**, type a name that is unique among all access profile and per-request policy names, and click **Finished**.
3. In the **Name** field, locate the policy that you want to update, then in the **Per-Request Policy** field, click the **Edit** link.
   The visual policy editor opens in another tab.
4. On a policy branch, click the **(+)** icon to add an item to the policy.

   A small set of actions are provided for building a per-request policy.

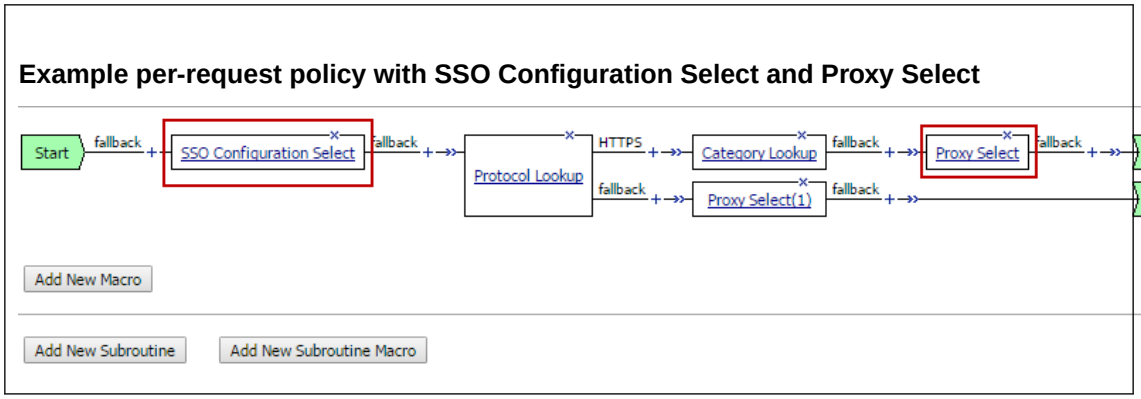
   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
5. On the General Purpose tab, select **SSO Configuration Select** and click **Add Item**.
   A Properties screen opens.
6. From **SSO Configuration Name**, select an SSO configuration, and click **Save**.
   The properties screen closes. The visual policy editor opens.
7. Add any additional items you want to the policy.
8. Click the **(+)** icon anywhere in the per-request policy to add a new item.
9. On the General Purpose tab, select **Proxy Select** and click **Add Item**.
   A Properties popup screen opens.
10. From the **Pool** list, select a pool of one or more proxy servers from which to select the next hop.

    Important: *All proxy servers in the pool that you select must support the forward proxy mode that you specify in the* ***Upstream Proxy Mode*** *setting.*

11. From **Upstream Proxy Mode**, select **Explicit** or **Transparent**.
12. For **Username** and **Password**, most of the time you can retain the default values (blank).

These fields support the use of static credentials to authenticate the user at the next hop using HTTP Basic authentication.

13. Click **Save**.
    The properties screen closes. The visual policy editor displays.



Be sure to add a disabled HTTP Connect Profile to the virtual server that processes SSL traffic for the forward proxy configuration.

Note: *A per-request policy is not in effect unless it and an access profile are specified in virtual servers in the forward proxy configuration.*

Configuration constraints for SSO to a resource server

Access Policy Manager® (APM®) does not support SSO to a resource server for SSL bypass traffic when the resource server performs authentication.

Overview: Configuring Kerberos SSO to the next hop

Access Policy Manager® (APM®) supports the HTTP Basic, Kerberos, NTLMv1, and NTLMv2 types of SSO configuration to and behind a next hop proxy server. This example specifies the configuration you need for Kerberos single sign-on to the next hop in a forward proxy chain.

Important: *APM does not support Kerberos SSO to a proxy server for HTTPS traffic.*

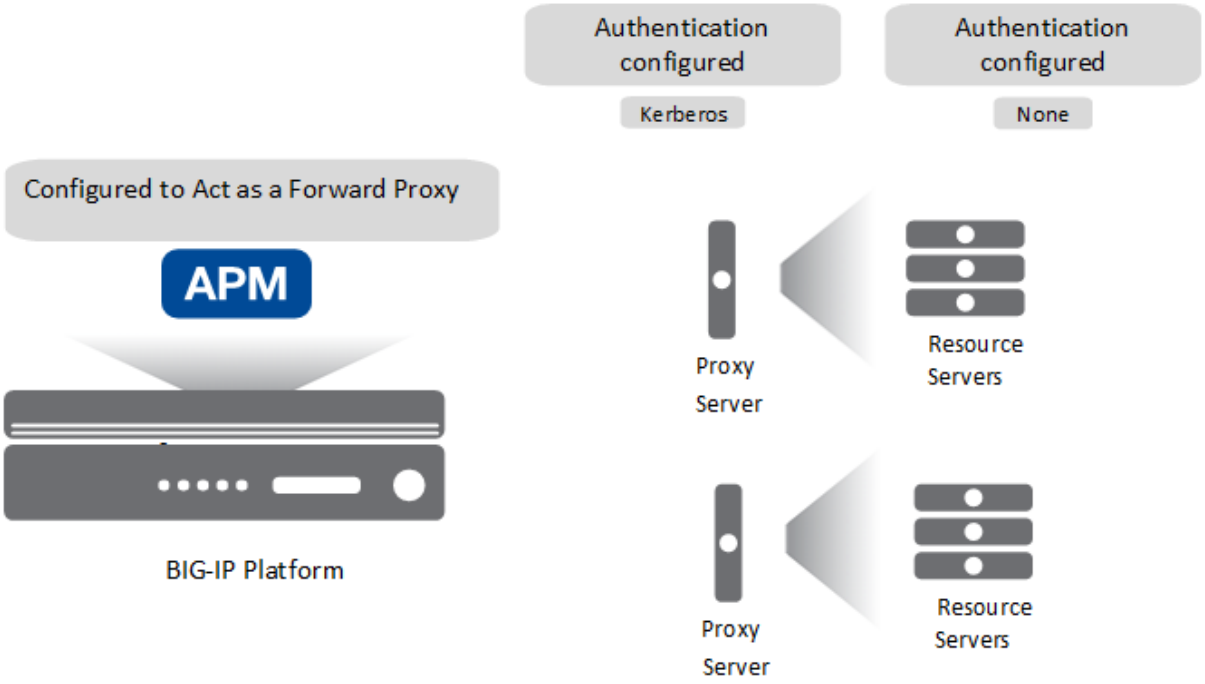


Figure 17: Expected initial configuration

Task summary

For Kerberos SSO, you need a delegation account in Active Directory for the next hop proxy server and a Kerberos SSO configuration in APM that references the delegation account.

For forward proxy chaining, you need an access policy to authenticate the user and cache credentials. You need a per-request policy to specify an SSO configuration and select the next hop proxy.

Task list

Configuring a delegation account for the next hop proxy server
Configuring APM Kerberos SSO for the next hop proxy server
Configuring an access policy for Kerberos SSO
Configuring a per-request policy for Kerberos SSO

Configuring a delegation account for the next hop proxy server

To support SSO to a next hop proxy server with Kerberos authentication configured on it, you need a delegation account in Active Directory for the next hop proxy server.

1. Open the Active Directory Users and Computers administrative tool, and create a new user account.

   The user account should be dedicated for delegation, and the **Password never expires** setting enabled.
2. Set the service principal name (SPN) on the Windows server for the user account.

   For the support tools that you can use and for the commands that you can use, such as `setspn` and `ktpass`, refer to Microsoft documentation.

   Note: *If you use the* `ktpass` *command, it sets the SPN on the Windows server and creates a keytab file. Access Policy Manager® (APM®) Kerberos SSO does not need or use a keytab file.*
3. Verify the result of setting the SPN.

This example is purely for illustration. Refer to Microsoft documentation for up-to-date commands and correct usage.

```
C:\Users\Administrator> setspn -L apm4
Registered ServicePrincipalNames for
CN=fproxy1,OU=users,DC=myhostname,DC=lab,DC=mynet,DC=com: HTTP/
fproxy1.myhostname.lab.mynet.com
```

where *fproxy1* is the name of the user account that you created.

4. Take note of the service principal name.

Important: *You will need to type the service principal name in the Kerberos SSO configuration that you create in APM.*

---

5. Return to the Active Directory Users and Computers screen to open your account again.

   A Delegation tab should appear.
6. Click the Delegation tab.
7. Select **Trust this user for delegation to specified services only**.
8. Select **Use any authentication protocol**, and add all your services to the list under **Services to which this account can present delegated credentials**.

   Every service should have Service Type HTTP (or http) and host name of the forward proxy server that you will use in your configuration.
9. Click **OK**.
   This creates the new delegation account.

Configuring APM Kerberos SSO for the next hop proxy server

Before you start, you must have configured a delegation account in Active Directory for the next hop proxy server.

To support Kerberos single sign-on to a next hop proxy server from Access Policy Manager® (APM®), you must create a Kerberos SSO configuration.

Note: *To complete this task, you need to know the service principal name (SPN) for the delegation account.*

---

1. On the Main tab, click **Access** > **Single Sign-On** > **Kerberos**.
   The Kerberos screen opens.
2. Click **Create**.
   The New SSO Configuration screen opens.
3. In the **Name** field, type a name for the SSO configuration.
4. From the **Log Setting** list, select one of the following options:
   - Select an existing APM log setting.
   - Click **Create** to create a new log setting.
5. In the Credentials Source area, specify the credentials that you want cached for Single Sign-On.
6. In the **Kerberos Realm** field, type the name of the realm in uppercase.

   For example, type `MYHOSTNAME.LAB.MYNET.COM`.
7. In the **Account Name** field, type the name of the Active Directory account configured for delegation.

   Type the account name in SPN format.

   In this example `HTTP/fproxy1.myhostname.lab.mynet.com@MYHOSTNAME.LAB.MYNET.COM`, `fproxy1` is the delegation account, `fproxy1.myhostname.lab.mynet.com` is its fully qualified domain name, and `MYHOSTNAME.LAB.MYNET.COM` is the realm.

8. In the **Account Password** and **Confirm Account Password** fields, type the delegation account password.
9. Click **Finished**.

Configuring an access policy for Kerberos SSO

You configure an access policy to support single sign-on to a next hop proxy server or to a resource server that has Kerberos authentication configured on it.

Note: *You need a logon item to collect credentials in this policy. You can use* ***HTTP 407 Response*** *(for explicit forward proxy), or* ***Logon Page****, or* ***HTTP 401 Response*** *(for transparent forward proxy). This example uses* ***HTTP 401 Response****.*

---

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. Locate the access profile for the forward proxy configuration you are updating.
   Look in the **Profile Type** field for **SWG-Explicit** or **SWG-Transparent**.
3. In the Per-Session Policy column, click the **Edit** link.
   The visual policy editor opens the access policy in a separate screen.
4. Click the **(+)** icon anywhere in the access policy to add a new item.

   Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
5. On the Logon tab, select **HTTP 401 Response** and click **Add Item**.
   A Properties screen opens.
6. From the **HTTP Auth Level** list, select **negotiate** and click **Save**.
   In a transparent forward proxy configuration, APM does not support Kerberos request-based authentication
   The properties screen closes.
7. Click the **(+)** icon on the **negotiate** branch.
   A popup screen opens.
8. For Kerberos authentication to work correctly with forward proxy, you must assign the domain name for the forward proxy virtual server to a session variable:
   a) On the Assignment tab, select **Variable Assign** and click **Add Item**.
   b) Click **Add new entry**.
      An **empty** entry appears in the Assignment table.
   c) Click the **change** link in the new entry.
      A popup screen opens.
   d) In the left pane, retain the selection of **Custom Variable** and type this variable name: `session.server.network.name`.
   e) In the right pane, in place of **Custom Variable**, select **Text** and type the domain name for the proxy virtual server.
   f) Click **Finished**.
      The popup screen closes.
   g) Click **Save**.
      The properties screen closes. The policy displays.
9. On a policy branch, click the **(+)** icon to add an item to the policy.
10. On the Assignment tab, select **SSO Credential Mapping** and click **Add Item**.

A properties screen opens.

11. Click **Save**.
    The properties screen closes and the policy displays.

Configuring a per-request policy for Kerberos SSO

Before you start, you need to have configured a pool of proxy servers, each of which is configured for the same forward proxy mode: explicit or transparent. (Pools are configured in the **Local Traffic** > **Pools** area of the product.)

To support SSO in a forward proxy chain, you configure a per-request policy that selects a supported SSO configuration and later selects the next hop.

Note: *If you include* ***SSL Intercept*** *or* ***SSL Bypass*** *agents in the policy, be sure to place them before other agents.*

---

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. If you are not going to update an existing policy, all you need to do to create a new one is click **Create**, type a name that is unique among all access profile and per-request policy names, and click **Finished**.
3. In the **Name** field, locate the policy that you want to update, then in the **Per-Request Policy** field, click the **Edit** link.
   The visual policy editor opens in another tab.
4. Click the **(+)** icon anywhere in the subroutine to add a new item.

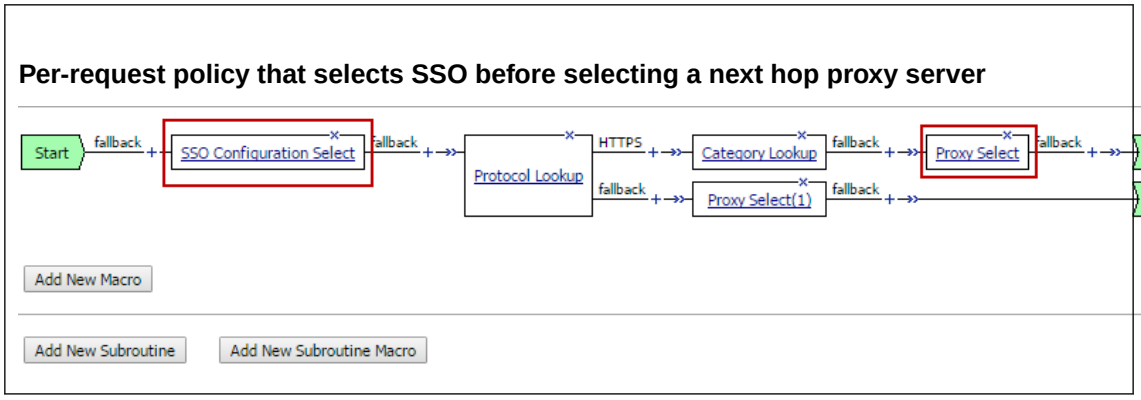
   A small set of actions are provided for building a subroutine.

   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
5. On the General Purpose tab, select **SSO Configuration Select** and click **Add Item**.
   A Properties screen displays.
6. From **SSO Configuration Name**, select a Kerberos SSO configuration.
7. Click the **(+)** icon anywhere in the per-request policy to add a new item.
8. Click **Save**.
   The properties screen closes. The visual policy editor displays.
9. Add any additional items you want to the policy.
10. Click the **(+)** icon anywhere in the per-request policy to add a new item.
11. On the General Purpose tab, select **Proxy Select** and click **Add Item**.
    A Properties popup screen opens.
12. From the **Pool** list, select a pool of one or more proxy servers from which to select the next hop.

    Important: *All proxy servers in the pool that you select must support the forward proxy mode that you specify in the* ***Upstream Proxy Mode*** *setting.*

    ---
13. From **Upstream Proxy Mode**, select **Explicit** or **Transparent**.
14. For **Username** and **Password**, most of the time you can retain the default values (blank).

    These fields support the use of static credentials to authenticate the user at the next hop using HTTP Basic authentication.
15. Click **Save**.
    The properties screen closes. The visual policy editor displays.



Be sure to add a disabled HTTP Connect Profile to the virtual server that processes SSL traffic for the forward proxy configuration.

Note: *A per-request policy is not in effect unless it and an access profile are specified in virtual servers in the forward proxy configuration.*

Overview: Configuring Kerberos SSO to a resource server

Access Policy Manager® (APM®) supports the HTTP Basic, Kerberos, NTLMv1, and NTLMv2 types of SSO configuration to and behind a next hop proxy server. This example specifies the configuration you need for Kerberos single sign-on to a resource server after the next hop in a forward proxy chain.

Important: *APM supports this configuration for HTTP traffic only.*

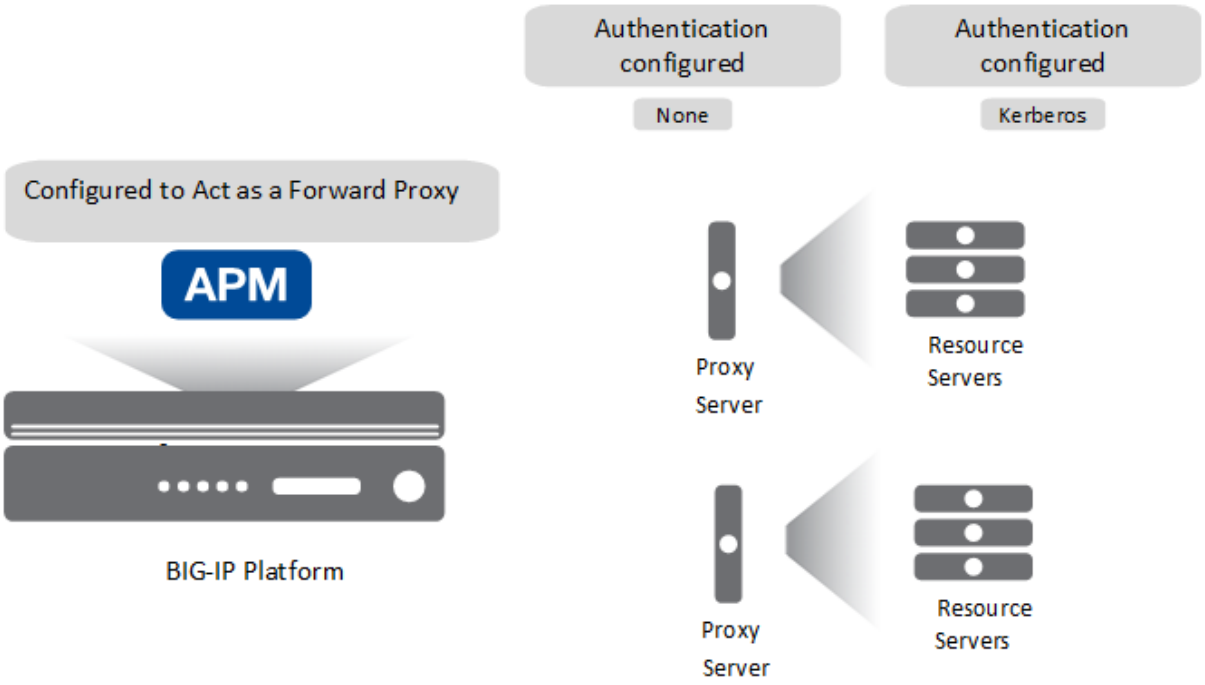


Figure 18: Expected initial configuration

Task summary

For Kerberos SSO, you need a delegation account in Active Directory for the next hop proxy server and a Kerberos SSO configuration in APM that references the delegation account and specifies **On 401 Status Code** as the value for the **Send Authentication** setting.

For forward proxy chaining, you need an access policy to authenticate the user and cache credentials. You need a per-request policy to specify an SSO configuration and select the next hop proxy.

Task list

Setting up a delegation account to support Kerberos SSO

Before you can configure Kerberos SSO in Access Policy Manager®, you must create a delegation account in Active Directory.

Note: *For every server realm, you must create a delegation account in that realm.*

1. Open the Active Directory Users and Computers administrative tool and create a new user account.

   The user account should be dedicated for delegation, and the **Password never expires** setting enabled.
2. Set the service principal name (SPN) on the Windows server for the user account.

   For the support tools that you can use, and for the commands, such as `setspn` and `ktpass`, refer to Microsoft documentation.

   Note: *If you use the* `ktpass` *command, it sets the SPN on the Windows server and creates a keytab file. APM Kerberos SSO does not need or use a keytab file.*
3. Verify the result of setting the SPN.

   This example is purely for illustration. Refer to Microsoft documentation for up-to-date commands and correct usage.

   ```
   C:\Users\Administrator> setspn -L apm4
   Registered ServicePrincipalNames for
   CN=apm4,OU=users,DC=yosemite,DC=lab,DC=dnet,DC=com: HTTP/
   apm4.yosemite.lab.dnet.com
   ```

   where *apm4* is the name of the user account that you created.
4. Return to the Active Directory Users and Computers screen to open your account again.

   A Delegation tab should appear.
5. Click the Delegation tab.
6. Select **Trust this user for delegation to specified services only**.
7. Select **Use any authentication protocol**, and add all your services to the list under **Services to which this account can present delegated credentials**.

   Every service should have Service Type HTTP (or http) and host name of the pool member or web application resource host that you will use in your configuration.
8. Click **OK**.
   This creates the new delegation account.

Configuring APM Kerberos SSO for a resource server

Before you start, you must have configured a delegation account in Active Directory for Access Policy Manager® (APM®) .

To support Kerberos single sign-on authentication from Access Policy Manager® (APM®) to a resource server, you must create a Kerberos SSO configuration with the **Send Authentication** field set to **On 401 Status Code**.

Note: *To complete this task, you need to know the service principal name (SPN) for the delegation account.*

---

1. On the Main tab, click **Access** > **Single Sign-On** > **Kerberos**.
   The Kerberos screen opens.
2. Click **Create**.
   The New SSO Configuration screen opens.
3. In the **Name** field, type a name for the SSO configuration.
4. From the **Log Setting** list, select one of the following options:
   - Select an existing APM log setting.
   - Click **Create** to create a new log setting.
5. In the Credentials Source area, specify the credentials that you want cached for Single Sign-On.
6. In the **Kerberos Realm** field, type the name of the realm in uppercase.
   For example, type `MY.HOST.LAB.MYNET.COM`.
7. In the **Account Name** field, type the name of the Active Directory account configured for delegation.
   Type the account name in SPN format.
   In this example `HTTP/apm4.my.host.lab.mynet.com@MY.HOST.LAB.MYNET.COM`, `apm4` is the delegation account, `apm4.my.host.lab.mynet.com` is its fully qualified domain name, and `MY.HOST.LAB.MYNET.COM` is the realm.
8. In the **Account Password** and **Confirm Account Password** fields, type the delegation account password.
9. For **Send Authorization**, select **On 401 Status Code**.
10. Click **Finished**.

Configuring an access policy for Kerberos SSO

You configure an access policy to support single sign-on to a next hop proxy server or to a resource server that has Kerberos authentication configured on it.

Note: *You need a logon item to collect credentials in this policy. You can use* ***HTTP 407 Response*** *(for explicit forward proxy), or* ***Logon Page****, or* ***HTTP 401 Response*** *(for transparent forward proxy). This example uses* ***HTTP 401 Response****.*

---

1. On the Main tab, click **Access** > **Profiles / Policies**.
   The Access Profiles (Per-Session Policies) screen opens.
2. Locate the access profile for the forward proxy configuration you are updating.
   Look in the **Profile Type** field for **SWG-Explicit** or **SWG-Transparent**.
3. In the Per-Session Policy column, click the **Edit** link.
   The visual policy editor opens the access policy in a separate screen.
4. Click the **(+)** icon anywhere in the access policy to add a new item.

Note: *Only an applicable subset of access policy items is available for selection in the visual policy editor for any access profile type.*

A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.

5. On the Logon tab, select **HTTP 401 Response** and click **Add Item**.
   A Properties screen opens.
6. From the **HTTP Auth Level** list, select **negotiate** and click **Save**.

   In a transparent forward proxy configuration, APM does not support Kerberos request-based authentication

   The properties screen closes.
7. Click the **(+)** icon on the **negotiate** branch.
   A popup screen opens.
8. For Kerberos authentication to work correctly with forward proxy, you must assign the domain name for the forward proxy virtual server to a session variable:
   a) On the Assignment tab, select **Variable Assign** and click **Add Item**.
   b) Click **Add new entry**.
      An **empty** entry appears in the Assignment table.
   c) Click the **change** link in the new entry.
      A popup screen opens.
   d) In the left pane, retain the selection of **Custom Variable** and type this variable name: `session.server.network.name`.
   e) In the right pane, in place of **Custom Variable**, select **Text** and type the domain name for the proxy virtual server.
   f) Click **Finished**.

      The popup screen closes.
   g) Click **Save**.
      The properties screen closes. The policy displays.
9. On a policy branch, click the **(+)** icon to add an item to the policy.
10. On the Assignment tab, select **SSO Credential Mapping** and click **Add Item**.
    A properties screen opens.
11. Click **Save**.
    The properties screen closes and the policy displays.

Configuring a per-request policy for Kerberos SSO

Before you start, you need to have configured a pool of proxy servers, each of which is configured for the same forward proxy mode: explicit or transparent. (Pools are configured in the **Local Traffic** > **Pools** area of the product.)

To support SSO in a forward proxy chain, you configure a per-request policy that selects a supported SSO configuration and later selects the next hop.

Note: *If you include **SSL Intercept** or **SSL Bypass** agents in the policy, be sure to place them before other agents.*

1. On the Main tab, click **Access** > **Profiles / Policies** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. If you are not going to update an existing policy, all you need to do to create a new one is click **Create**, type a name that is unique among all access profile and per-request policy names, and click **Finished**.

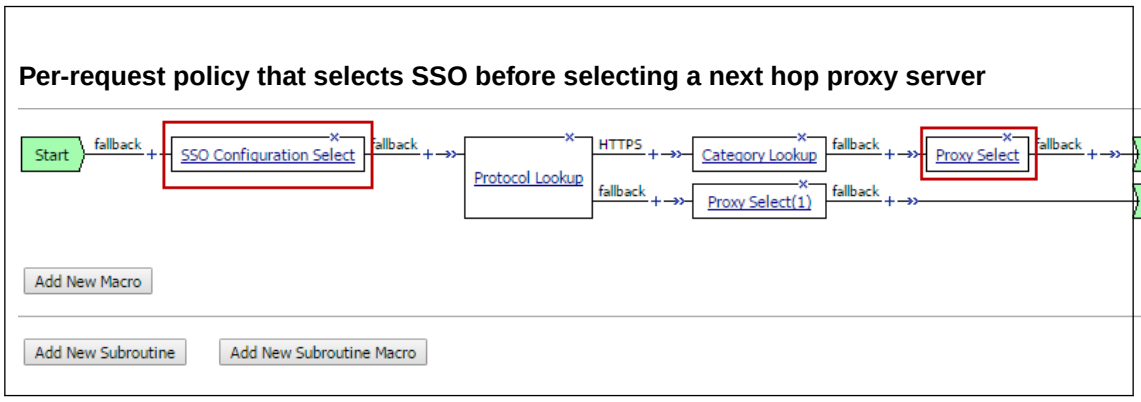
3. In the **Name** field, locate the policy that you want to update, then in the **Per-Request Policy** field, click the **Edit** link.
   The visual policy editor opens in another tab.
4. Click the **(+)** icon anywhere in the subroutine to add a new item.

   A small set of actions are provided for building a subroutine.

   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
5. On the General Purpose tab, select **SSO Configuration Select** and click **Add Item**.
   A Properties screen displays.
6. From **SSO Configuration Name**, select a Kerberos SSO configuration.
7. Click the **(+)** icon anywhere in the per-request policy to add a new item.
8. Click **Save**.
   The properties screen closes. The visual policy editor displays.
9. Add any additional items you want to the policy.
10. Click the **(+)** icon anywhere in the per-request policy to add a new item.
11. On the General Purpose tab, select **Proxy Select** and click **Add Item**.
    A Properties popup screen opens.
12. From the **Pool** list, select a pool of one or more proxy servers from which to select the next hop.

    Important: *All proxy servers in the pool that you select must support the forward proxy mode that you specify in the* ***Upstream Proxy Mode*** *setting.*
13. From **Upstream Proxy Mode**, select **Explicit** or **Transparent**.
14. For **Username** and **Password**, most of the time you can retain the default values (blank).

    These fields support the use of static credentials to authenticate the user at the next hop using HTTP Basic authentication.
15. Click **Save**.
    The properties screen closes. The visual policy editor displays.



Be sure to add a disabled HTTP Connect Profile to the virtual server that processes SSL traffic for the forward proxy configuration.

Note: *A per-request policy is not in effect unless it and an access profile are specified in virtual servers in the forward proxy configuration.*

Configuration constraints for Kerberos SSO to a resource server

Access Policy Manager® (APM®) does not support Kerberos SSO to a resource server for SSL traffic when: the resource server performs Kerberos authentication; and, the next hop proxy server simply passes the Kerberos credential to the resource server without performing Kerberos authentication.

Overview: Updating virtual servers for forward proxy chaining with APM

For forward proxy chaining, Access Policy Manager® (APM®) requires an HTTP proxy connect profile configured with its state disabled. The HTTP proxy connect profile must be specified in the virtual server that processes the HTTPS traffic for the explicit or transparent forward proxy configuration.

Task summary

Disabling HTTP proxy connect for forward proxy chaining
Updating a virtual server for forward proxy chaining with APM

Disabling HTTP proxy connect for forward proxy chaining

For Access Policy Manager® (APM®) to support forward proxy chaining, you need an HTTP proxy connect profile with its default state disabled.

1. On the Main tab, select **Local Traffic** > **Profiles** > **Other** > **HTTP Proxy Connect**.
2. Click **Create**.
3. Type a name for the profile and, for the **Parent Profile** setting, retain **http-proxy-connect**.
4. In the Settings area, for **Default State** clear the **Enabled** check box.
5. Click **Finished**.

Updating a virtual server for forward proxy chaining with APM

For Access Policy Manager® (APM®) to support forward proxy chaining, you must specify an HTTP proxy connect profile on the virtual server that processes SSL traffic in the forward proxy configuration.

Important: *If this virtual server functions as a captive portal or processes HTTP traffic, you must retain the default value of* ***None*** *for the* ***HTTP Proxy Connect Profile*** *setting.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. In the Configuration area from **HTTP Proxy Connect Profile**, select a profile that you know to be configured with the **Default State** setting disabled.
4. Click **Update** to save the changes.

Virtual server Access Policy settings for forward proxy

F5 recommends multiple virtual servers for configurations where Access Policy Manager® (APM®) acts as an explicit or transparent forward proxy. This table lists forward proxy configurations, the virtual servers recommended for each, and whether an access profile and per-request policy should be specified on the virtual server.

Forward proxy	Recommended virtual servers (by purpose)	Specify access profile?	Specify per-request policy?
Explicit	Process HTTP traffic	Yes	Yes
	Process HTTPS traffic	Yes	Yes

Forward proxy	Recommended virtual servers (by purpose)	Specify access profile?	Specify per-request policy?
	Reject traffic other than HTTP and HTTPS	N/A	N/A
Transparent Inline	Process HTTP traffic	Yes	Yes
	Process HTTPS traffic	Only when a captive portal is also included in the configuration	Only when a captive portal is also included in the configuration
	Forward traffic other than HTTP and HTTPS	N/A	N/A
	Captive portal	Yes	No
Transparent	Process HTTP traffic	Yes	Yes
	Process HTTPS traffic	Only when a captive portal is also included in the configuration	Only when a captive portal is also included in the configuration
	Captive portal	Yes	No

Configuring the URL Database for SWG

About initial configuration steps for SWG

On a BIG-IP® system with an SWG subscription, the first thing you must do is download the URL database. After that, if you want to use transparent user identification, you should install one of the Secure Web Gateway user identification agents: F5 DC Agent or F5 Logon Agent.

Overview: Downloading and updating the URL database for SWG

Note: *A URL database is available only on a BIG-IP® system with an SWG subscription.*

On a system where URL database download is available, you must complete the download before you start to configure per-request policies to categorize and filter URLs. You can download the URL database to the BIG-IP system or to an upstream proxy.

For SWG to best protect your network from new threats, schedule regular database downloads to update the existing URL categories with new URLs. Without these updates, SWG uses obsolete security intelligence and as a result, protection of your networks is less effective.

Task summary

Configuring an upstream proxy for the BIG-IP system
Downloading the URL database
Looking up a URL category in the master database
Configuring logging for the URL database
Viewing a URL database report

Configuring an upstream proxy for the BIG-IP system

If your network practices do not permit you to download data from the Internet to the BIG-IP® system, configure an upstream proxy to use for this type of access instead.

Note: *You can configure only one upstream proxy for the BIG-IP system.*

1. On the Main tab, select **System** > **Configuration** > **Device** > **Upstream Proxy** > **.**
2. In the **Name** field, type a name for the proxy server.
3. In the **IP Address** field, type the IP address for the proxy server.
4. In the **Port** field, type the port number for the proxy server.
5. In the **User Name** and **Password**fields, type credentials for an account on the proxy server if needed.
6. Click **Save**.

The upstream proxy is configured.

You can update the IP address, port, and credentials for the upstream proxy if needed. To change the name, you must delete the configuration and create it again.

Downloading the URL database

Note: *Database download is required and available only on a BIG-IP® system with an SWG subscription.*

To download the database to the BIG-IP system, before you start you must have configured:

- DNS for the BIG-IP device in the System area of the product.
- A default route in the Network area of the product.

To download the database to a proxy for the BIG-IP system, before you start you must have configured an upstream proxy in the **System** area of the product.

Download the URL database to supply URLs and URL categories.

Note: *Schedule database downloads to occur during off-peak hours (very little to no user activity), so that users are not impacted. Alternatively, you can initiate database downloads on-demand.*

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Database Settings** > **Database Download**.
2. In the Download Settings area from the **Downloads** list, select **Enabled**.
   Additional settings display. **Download Schedule** displays a default schedule for the download.
3. To download the database to an upstream proxy, select the **Use Proxy** check box.
4. In the **Download Schedule** settings, configure a two-hour period in which to start the download.
   Schedule the download to occur during off-peak hours. The default schedule is between one and three A.M.

   Warning: *After the download completes, database indexing occurs. It consumes a high amount of CPU.*

   The process of downloading the master database and the database indexing that follows can take 30 minutes to several hours depending on system capacity.
5. Click **Update Settings**.
6. To download the database immediately, click **Download Now**.
   A download occurs only when a newer version becomes available.

   Warning: *Database indexing occurs after the download and impacts system performance.*

   Warning: *The ANTserver service is not available on the BIG-IP system for approximately 300 milliseconds after the database download completes.*

Looking up a URL category in the master database

You can look up a URL to determine whether it already exists in the master database and, if it exists, to see which categories include it.

Note: *A URL database is available only on a BIG-IP® system with an SWG subscription.*

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Database Settings** > **URL Category Lookup**.
2. In the **URL** field, type the URL that you want to look up.
   Type the complete URL, including the URI scheme.
   Type `https://www.google.com`; not `www.google.com` or `https://www.google`.

3. Click **Search**.

   Note: *Custom categories are not searched.*

   Results display in the URL Category table.

If the URL is not found, you can add it to an existing or a custom category. If the URL is found, you do not need to do anything, but can recategorize it by adding it to another category.

Configuring logging for the URL database

Configure logging for the URL database so that log messages are published to the destinations, and at the minimum log level, that you specify. (Logging for the URL database occurs at the system level, not the session level, and is controlled using the default-log-setting log setting.)

Note: *A URL database is available only on a BIG-IP® system with an SWG subscription.*

1. On the Main tab, click **Access** > **Overview** > **Event Logs** > **Settings**.
   A log settings table screen opens.
2. From the table, select **default-log-setting** and click **Edit**.
   A log settings popup screen displays.
3. Verify that the **Enable access system logs** check box is selected.
4. To configure settings for access system logging, select **Access System Logs** from the left pane.
   Access System Logs settings display in the right panel.
5. From the **Log Publisher** list, select the log publisher of your choice.

   A log publisher specifies one or more logging destinations.

   Important: *The BIG-IP® system is not a logging server and has limited capacity for storing, archiving, and analyzing logs. For this reason a dedicated logging server is recommended.*
6. To change the minimum log level, from the **Secure Web Gateway** list, select a log level.

   Note: *Setting the log level to **Debug** can adversely impact system performance.*

   The default log level is **Notice**. At this level, logging occurs for messages of severity Notice and for messages at all incrementally greater levels of severity.
7. Click **OK**.
   The popup screen closes. The table displays.

Viewing a URL database report

You can view URL database log messages in an Access System Logs report if local logging is configured for the URL database.

Important: *The BIG-IP® system is not a logging server and has limited capacity for storing, archiving, and analyzing logs. For this reason a dedicated logging server is recommended.*

Create a report to view URL database event logs.

Note: *A URL database is available only on a BIG-IP® system with an SWG subscription.*

1. On the Main tab, click **Access** > **Overview** > **Access Reports**.

   The Reports Browser displays in the right pane. The Report Parameters popup screen opens and displays a description of the current default report and default time settings.

2. Click **Cancel**.
   The Report Parameters popup screen closes.
3. In the Reports Browser in the General Reports list, select **URL DB Messages** > **Run Report**.
   The Report Parameters popup screen displays.
4. Update the parameters, if necessary, and click **Run Report**.
   The popup screen closes. The report displays in the Report Browser.

Note: *The session ID for a URL database message is* ***00000000*** *because URL database downloads occur outside of a client session.*

Secure Web Gateway database download log messages

When you deploy Secure Web Gateway (SWG), the database downloads output messages to the log destinations specified in the default-log-setting. This table lists messages that are available only when you enable debug.

Note: *Database downloads are possible only on a BIG-IP® system with an SWG subscription.*

Debug message	Description
`Transfer Status 247`	The file is transferred successfully to the BIG-IP® system. If you see a Transfer Status other than 247, it might indicate an error.
`RTU Type`	The RTU Type is always 1. If you see an RTU Type other than 1, it might indicate an error.
`Expiration Date`	The BIG-IP system does not use the expiration date in this message. Instead, the BIG-IP system enforces the SWG license and the database download works accordingly.

Customizing URL Categories and Filters for SWG

Overview: Customizing URL categories and filters for SWG

On a BIG-IP® system with an SWG subscription, you can customize URL categories and URL filters any time after the initial download of the URL database has completed. Customizing URL categories and URL filters is completely optional.

With regularly scheduled downloads, URLs are added to the URL database on an ongoing basis. With predefined URL filters, if they completely serve your needs, you do not need to configure more.

About the Instant Messaging URL category

Note: *A predefined Instant Message URL category is available only on a BIG-IP® system with an SWG subscription.*

Secure Web Gateway (SWG) supports HTTP and HTTPS-based instant messaging protocols. As a result, when you use the Instant Messaging URL category to block messages, SWG can block messages to ICQ, for example, but cannot block messages from applications that use non-standard ports or tunneling over HTTP, such as, Yahoo Messenger, Skype, Google Talk, and so on.

Similarly, SWG cannot block messages from file-sharing and peer-to-peer protocols that do not use HTTP or HTTPS; most of these protocol types do not use either HTTP or HTTPS.

Adding custom URL categories to the URL database

Note: *A URL database is available only on a BIG-IP® system with a Secure Web Gateway (SWG) subscription.*

You can add a custom category to the standard Secure Web Gateway URL categories to specify a list of URLs that you want to block or allow, or for which you want to obtain confirmation from a user before blocking or allowing access.

Note: *The URL categories that you add become subcategories of Custom Categories. Custom Categories take precedence over standard categories.*

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **URL Categories**.
   The URL Categories table displays; **Custom Categories** displays as the first entry in the table.
2. Click **Create**.
   The Category Properties screen displays.
3. In the **Name** field, type a unique name for the URL category.
4. From the **Default Action** list, retain the default value **Block**; or, select an alternative: **Allow** or **Confirm**.

   If no action has been specified in a filter for this category, the URL Filter agent takes the branch for the default action.
5. Add, edit, or delete the URLs that are associated with the category by updating the **Associated URLs** list.
6. To add URLs to the **Associated URLs** list:
   a) In the **URL** field, type a URL.

You can type a well-formed URL that the system must match exactly or type a URL that includes globbing patterns (wildcards) for the system to match URLs.

b) If you typed globbing patterns in the **URL** field, select the **Glob Pattern Match** check box .

c) Click **Add**.
The URL displays in the **Associated URLs** list.

These are well-formed URLs:

- `https://www.siterequest.com/`
- `http://www.siterequest.com:8080/`
- `http://www.sitequest.com/docs/siterequest.pdf/`
- `http://www.sitequest.com/products/application-guides/`

This URL `*siterequest.[!comru]` includes globbing patterns that match any URL that includes `siterequest`, except for `siterequest.com` or `siterequest.ru`.
This URL `*://siterequest.com/education/*` includes globbing patterns that match any HTTP URL that includes `siterequest.com/education`, but that do not match any HTTPS URLs if Category Lookup specifies that the input is SNI or CN.Subject.

Important: *For SNI or CN.Subject input, Category Lookup uses* `scheme://host` *for matching, instead of matching the whole URL.*

---

7. Click **Finished**.
The URL Categories screen displays.
8. To view the newly created URL category, expand **Custom Categories**.
The custom URL category displays in the Sub-Category column.

Add or edit a URL filter to specify an action (allow, block, or confirm) for the custom category.

Customizing standard categories from the URL database

You can customize the standard URL categories supplied in the URL database by adding URLs to them. You might do this after you use APM as a forward proxy for a while, view logs and reports, and determine that you need to make changes.

Note: *A URL database is available only on a BIG-IP® system with an SWG subscription.*

Note: *If you add a URL to a URL category, APM gives precedence to that categorization and database downloads do not overwrite your changes.*

---

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **URL Categories**.
The URL Categories table displays.
2. Click the name of any category or subcategory to edit the properties for it.

   To view and select a subcategory, expand categories.

   The Category Properties screen displays. There are many URLs in a given category; however, any URLs that display on the **Associated URLs** list are entered by the user.
3. Edit or delete any URLs on the **Associated URLs** list.
4. To add URLs to the **Associated URLs** list:

   a) In the **URL** field, type a URL.

   You can type a well-formed URL that the system must match exactly or type a URL that includes globbing patterns (wildcards) for the system to match URLs.

   b) If you typed globbing patterns in the **URL** field, select the **Glob Pattern Match** check box .

   c) Click **Add**.

The URL displays in the **Associated URLs** list.

These are well-formed URLs:

- `https://www.siterequest.com/`
- `http://www.siterequest.com:8080/`
- `http://www.sitequest.com/docs/siterequest.pdf/`
- `http://www.sitequest.com/products/application-guides/`

This URL `*siterequest.[!comru]` includes globbing patterns that match any URL that includes `siterequest`, except for `siterequest.com` or `siterequest.ru`.
This URL `*://siterequest.com/education/*` includes globbing patterns that match any HTTP URL that includes `siterequest.com/education`, but that do not match any HTTPS URLs if Category Lookup specifies that the input is SNI or CN.Subject.

Important: *For SNI or CN.Subject input, Category Lookup uses* `scheme://host` *for matching, instead of matching the whole URL.*

---

5. Click **Add**.
   The URL displays in the **Associated URLs** list.
6. Click **Update**.
   The URL Properties screen refreshes.
7. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **URL Categories**.
   The URL Categories table displays. The screen displays **(recategorized)** next to the URL category that you customized.

URLs are added to the URL category that you selected.

Customizing URL filters for SWG

You configure a URL filter to specify whether to allow, block, or confirm requests for URLs in URL categories. You can configure multiple URL filters.

Note: *On a BIG-IP® system with an SWG subscription, default URL filters, such as* ***block-all*** *and* ***basic-security****, are available. You cannot delete default URL filters.*

---

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **URL Filters**.
   You can click the name of any filter to view its settings.
   The URL Filters screen displays.
2. To configure a new URL filter, click one of these options.
   - **Create** button: Click to start with a URL filter that allows all categories.
   - **Copy** link: Click for an existing URL filter in the table to start with its settings.
3. In the **Name** field, type a unique name for the URL filter.
4. Click **Finished**.
   The screen redisplays. An Associated Categories table displays. It includes each URL category and the filtering action that is currently assigned to it. The table includes a Sub-Category column. Any URL categories that were added by administrators are subcategories within **Custom Categories**
5. To block access to particular categories or subcategories, select them and click **Block**.

Important: *When you select a category, you also select the related subcategories. You can expand the category and clear any subcategory selections.*

---

6. Expand the category **Miscellaneous**, select **Uncategorized**, and then click **Block**.

Important: *It is important to block URLs that SWG cannot categorize.*

7. To allow access to particular categories or subcategories, select them and click **Allow**.
8. To indicate that you want a user to confirm that access is work-related or otherwise justified before obtaining access to the URLs in a category, select the categories or subcategories and click **Confirm**.

To put a URL filter into effect, you must assign it in a per-request policy. A per-request policy runs each time a user makes a URL request.

Creating User-Defined URL Categories and Filters for APM

Overview: Configuring user-defined URL categories and filters

On a BIG-IP® system without a URL database, if you want to control traffic based on the type of URL being requested, and you have many URLs to consider, you should configure user-defined URL categories and user-defined URL filters. This approach provides good performance, ease-of-use, and the ability to use the **URL Category** and the **URL Filter Assign** agents in a per-request policy.

If you have only a few URLs that you want to treat differently, you can probably skip creating user-defined URL categories and filters and use a simple **URL Branching** agent in a per-request policy. In this case, you specify the URLs that you want to match directly in the **URL Branching** agent.

To configure user-defined URL categories and URL filters, complete these tasks.

Task summary

Configuring user-defined URL categories
Configuring user-defined URL filters

Configuring user-defined URL categories

Configure a user-defined URL category to specify a group of URLs over which you want to control access.

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **URL Categories**.
   The URL Categories table displays. If you have not created any URL categories, the table is empty.
2. Click **Create**.
   The Category Properties screen displays.
3. In the **Name** field, type a unique name for the URL category.
4. From the **Default Action** list, retain the default value **Block**; or, select **Allow**.

   Note: *A Confirm Box action in a per-request policy subroutine serves the purpose of enabling appropriate choices in a forward proxy (outbound) configuration. Currently, Access Policy Manager® does not support a similar action for reverse proxy.*

   ---

5. Add, edit, or delete the URLs that are associated with the category by updating the **Associated URLs** list.
6. To add URLs to the **Associated URLs** list:
   a) In the **URL** field, type a URL.

      You can type a well-formed URL that the system must match exactly or type a URL that includes globbing patterns (wildcards) for the system to match URLs.
   b) If you typed globbing patterns in the **URL** field, select the **Glob Pattern Match** check box .
   c) Click **Add**.
      The URL displays in the **Associated URLs** list.

   These are well-formed URLs:

   - `https://www.siterequest.com/`
   - `http://www.siterequest.com:8080/`

- `http://www.sitequest.com/docs/siterequest.pdf/`
- `http://www.sitequest.com/products/application-guides/`

This URL `*siterequest.[!comru]` includes globbing patterns that match any URL that includes `siterequest`, except for `siterequest.com` or `siterequest.ru`.
This URL `*://siterequest.com/education/*` includes globbing patterns that match any HTTP URL that includes `siterequest.com/education`, but that do not match any HTTPS URLs if Category Lookup specifies that the input is SNI or CN.Subject.

Important: *For SNI or CN.Subject input, Category Lookup uses* `scheme://host` *for matching, instead of matching the whole URL.*

---

7. Click **Finished**.
   The URL Categories screen displays.
8. To view the newly created URL category, expand **Custom Categories**.
   The custom URL category displays in the Sub-Category column.

Add or edit a URL filter to specify an action (allow, block, or confirm) for the custom category.

Configuring user-defined URL filters

You configure a URL filter to specify how to process requests for content in URL categories: allow, block, or confirm access. You can configure multiple URL filters.

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **URL Filters**.
   You can click the name of any filter to view its settings.
   The URL Filters screen displays.
2. To configure a new URL filter, click one of these options.
   - **Create** button: Click to start with a URL filter that allows all categories.
   - **Copy** link: Click for an existing URL filter in the table to start with its settings.
3. In the **Name** field, type a unique name for the URL filter.
4. Click **Finished**.
   The screen redisplays. An Associated Categories table displays. It includes each URL category and the filtering action that is currently assigned to it. The table includes a Sub-Category column. Any URL categories that were added by administrators are subcategories within **Custom Categories**
5. To specify that you want to block access to particular categories or subcategories, select them and click **Block**.

   Important: *When you select a category, you also select the related subcategories. You can expand the category and clear any subcategory selections.*

   ---

6. To specify that you want to allow access to particular categories or subcategories, select them and click **Allow**.
7. To specify that you want the user to confirm access for particular categories or subcategories, select them and click **Confirm**.

To use a URL filter, you must include a URL Filter item in a per-request policy. A per-request policy runs each time a user makes a URL request.

Overview: Configuring user-defined URL categories and filters

Configuring user-defined URL categories

Overview: Configuring the SWG F5 DC Agent

Configuring an SWG Agent for User Identification

About user identification with an SWG F5 agent

Transparent user identification makes a best effort to identify users without requesting credentials. It is not authentication. It should be used only when you are comfortable accepting a best effort at user identification.

Transparent user identification is supported in Secure Web Gateway (SWG) configurations for either explicit or transparent forward proxy. An agent obtains data and stores a mapping of IP addresses to user names in an IF-MAP server. An F5® DC Agent queries domain controllers. An F5 Logon Agent runs a script when a client logs in and can be configured to run a script when the client logs out.

Note: *Agents are available only on a BIG-IP® system with an SWG subscription.*

In an access policy, a Transparent Identity Import item obtains the IP-address-to-username-mapping from the IF-MAP server. This item can be used alone for determining whether to grant access or be paired with another query to look up the user or validate user information.

To support this option, either the Secure Web Gateway F5 DC Agent or F5 Logon Agent must be downloaded, installed, and configured.

Overview: Configuring the SWG F5 DC Agent

The F5® DC Agent enables *transparent user identification*, a best effort to identify users without requesting credentials.

Note: *F5 DC Agent is available only on a BIG-IP® system with an SWG subscription.*

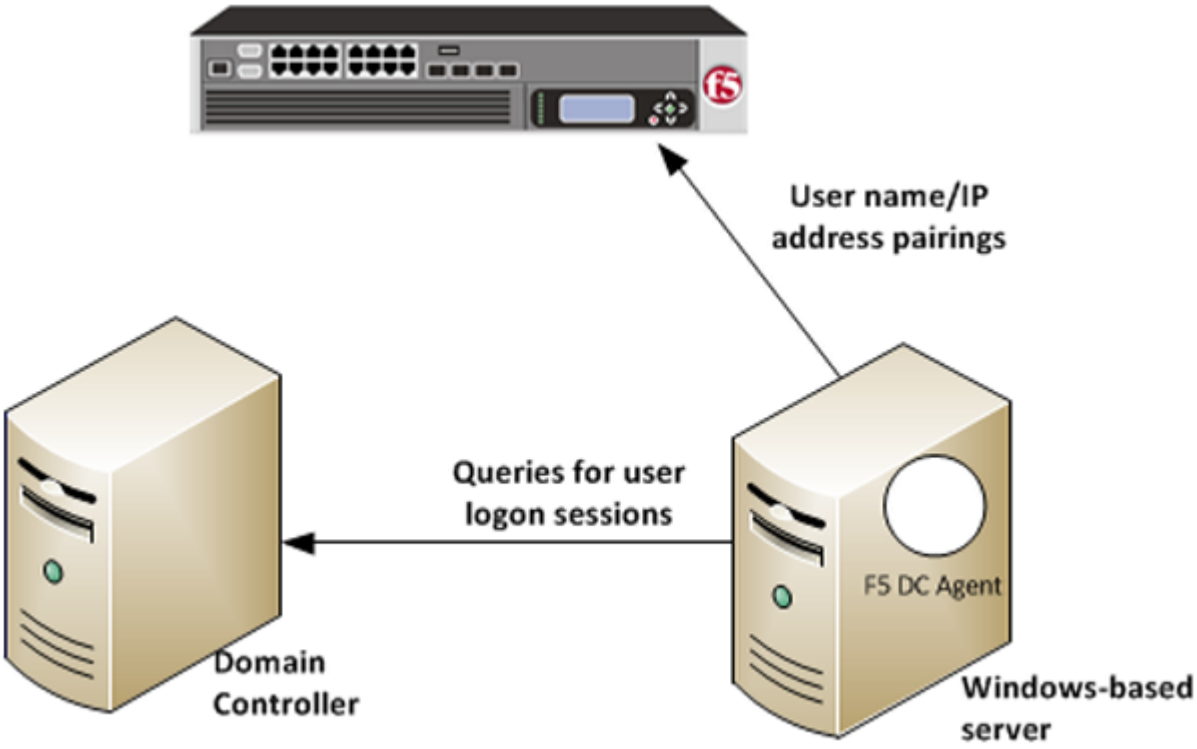


Figure 19: How F5 DC Agent transparently identifies users

You can install the F5® DC Agent on a Windows-based server in any domain in the network. The F5 DC Agent discovers domains and domain controllers, queries the domain controllers for logon sessions, and sends an IP-address-to-user-name mapping to the BIG-IP® system. F5 DC Agent sends only those new user name and IP address pairs recorded since the previous query. The BIG-IP system maintains user identity information in an IF-MAP server and stores only the most recently identified user name for a given IP address.

Note: *F5 DC Agent does not transmit passwords or any other confidential information.*

Considerations for installing multiple agents

You can install more than one F5 DC Agent in your network and configure F5 DC Agents to communicate with the same BIG-IP system.

NetBIOS port 139

F5 DC Agent uses NetBIOS port 139 for automatic domain detection. If NetBIOS port 139 is blocked in your network, you can deploy an F5 DC Agent instance for each virtually or physically remote domain.

Multiple subnets

As a best practice, install a separate F5 DC Agent in each subnet to avoid problems gathering logon information from domain controllers.

Network size, disk space, and RAM

If your network is very large (10,000+ users or 30+ domain controllers), you might benefit from installing F5 DC Agent on multiple machines to evenly distribute resource usage. F5 DC Agent uses TCP to transmit data, and transmits roughly 80 bytes per user name and IP address pair.

Number of data transferred per day	300 KB users	2,400 KB users

Number of users	Average amount of data transferred per day
1,000	1 GB
2,000	2 GB
5,000	5 GB
10,000	10 GB

Task summary

Configuring the BIG-IP system for the F5 DC Agent
Verifying network communication
Downloading and installing F5 DC Agent
Updating privileges for the F5 DC Agent service
Configuring the initialization file

Configuring the BIG-IP system for the F5 DC Agent

You use an iApps® template to deploy an application service that configures objects that the F5® DC Agent uses to communicate with the IF-MAP server on the BIG-IP® system.

Note: *You can configure the F5 DC Agent to authenticate with the BIG-IP system using certificate inspection or using clientless HTTP basic authentication against a local user database.*

1. To support certificate inspection:
   a) Obtain a trusted certificate and key that are valid for all fully qualified domain names (FQDNs) used to access the BIG-IP system.
   b) Import the certificate and key into the BIG-IP system.
      You can import SSL certificates from the System area of the product.
2. Obtain the iApps template file for IF-MAP Secure Web Gateway from F5® DevCentral™ at `http://devcentral.f5.com`:
   a) In the Search field, type `IF-MAP` and click the search icon.
   b) Download the zip file and extract all contents.
      Template file names end with `.tmpl`.
3. Import the template:
   a) On the Main tab, click **iApps** > **Templates**.
   b) Next, click **Import**.
   c) Select the **Overwrite Existing Templates** check box.
   d) Click **Choose File**, then browse to and choose the template file.
   e) Click **Upload**.
4. Deploy an application service:
   a) On the Main tab, click **iApps Application** > **Services**, and then click **Create**.
   b) In the **Name** field, type a name.

      Note: *The application service prefixes this name to the names of configuration objects it creates.*

   c) From the **Template** list, select **f5.ifmap**.

      Note: *This iApps template displays on the list only when APM is provisioned.*

   d) Follow the instructions on the screen to complete the deployment.
   A summary displays the configuration objects.
   e) Take note of the IP address of the virtual server created by the service. You need to type it into F5 DC Agent initialization file later.

      Note: *This virtual server must be accessible by the F5 DC Agent from a routing perspective.*

5. To enable clientless HTTP basic authentication, create a user and password in the local user database.
   The purpose of this user account is to authenticate communication between the F5 DC Agent and the BIG-IP system.
   a) On the Main tab, click **Access Policy** > **Local User DB** > **Manage Users**.
   The Manage Users screen displays.

b) Click **Create New User**.
The Create New Local User screen opens and displays User Information settings.
c) From the **Instance** list, select the instance created when you deployed the application service.
d) In the **User Name** field, type the user name.
Take note of the user name and password. You need to type them again later when you configure the initialization file for F5 DC Agent.
e) In the **Password** and **Confirm Password** fields, type the user's password.

Verifying network communication

You can verify that there are no DNS or NetBIOS or network communications issues on a Windows-based server before you install the F5® DC Agent on it. Alternatively, you can use these steps for troubleshooting if you observe a problem.

1. Open a command prompt on the Windows-based server that hosts, or will host, the F5 DC Agent.
2. To verify that the Windows-based server sees all required domains, use the `net view` command.
For example, type `net view /network`
3. To check for DNS issues, use the `nslookup` command.
For example, to verify that DNS resolves the host name, testmachine1, type this command: `nslookup testmachine1`. If the DNS lookup succeeds, the result is similar to: `Server: testdns.test.example.com Address: 10.56.1.4 Name: testmachine1.test.example.com Address: 10.56.100.15`
4. To verify that F5 DC Agent will be able to use NetBIOS, try to telnet to a domain controller on port `139`.
If the command is successful, the screen remains blank. If unsuccessful, then:
   - A router, firewall, or other device might be blocking NetBIOS traffic.
   - NetBIOS might not be enabled and the domain controller might not be listening on port `139`.
5. If you could not successfully telnet to a domain controller on port `139`, verify the status of the port using the `netstat` command.
For example, type: `netstat -na | find "139"`
6. To verify that the F5 DC Agent will be able to communicate with the virtual server on the BIG-IP® system, telnet to the IP address of the virtual server on port `8096` or on the port that you entered when creating the application service.
This virtual server was created using an application service based on the f5.ifmap iApps template.

Downloading and installing F5 DC Agent

F5® DC Agent is available when Access Policy Manager® (APM®) is licensed and provisioned on the BIG-IP® system. Before you perform these steps, make sure that the Windows Computer Browser service is running on the Windows server where you plan to install F5 DC Agent.

You perform this task to be able to identify clients transparently by IP address. (Do this only in an environment where IP addresses are trusted and unique.) You perform this task so that APM can gather information to support the user identity service.

1. Go to the BIG-IP® system Configuration utility Welcome screen.
If you are already logged in, click the F5® logo to open the Welcome screen.
2. In the BIG-IP User Identification Agents area, click the **User Identification Agents** link.
A `SWGUserIdentificationAgents.exe` file downloads.
3. Copy the downloaded file to a Windows-based server that is joined to a domain controller.

Important: *Do not install F5 DC Agent on a domain controller because the F5 DC Agent can put a load on the domain controller.*

4. From an account with both local and administrator privileges, click the `SWGUserIdentificationAgents.exe` file to start the installer.

   The installer displays instructions.
5. Follow the instructions to complete the installation.

Important: *F5® strongly recommends that you use the default destination folder. On the Destination Folder screen, click* ***Next*** *without making any changes.*

Important: *Install either F5 DC Agent or F5 Logon Agent, but not both. This overwrites the omapd user map every time an update is published.*

The program installs a Windows service, F5 DC Agent.

Updating privileges for the F5 DC Agent service

The F5® DC Agent service must run from a privileged account. You can create a new user account or use an existing account configured as specified in step 1.

1. On the Windows-based server, create a user account for F5 DC Agent:
   a) Assign the new account domain administrator privileges in all domains.
   b) Assign the same password to this account in all domains.

      Make a note of the password. You must type it again in step 2.
   c) Set the password to never expire.
2. Configure the F5 DC Agent service to log on as the user account you just configured:
   a) Open the Windows Services dialog box.
      From the Control Panel, select **Administrative Tools** > **Services**.
   b) Locate the F5 DC Agent service, right-click the service name, and select **Stop**.
   c) Double-click the service name, and then select the Log On tab.
   d) Select **This account** and type the account name and password for the account you created in step 1.

      Note: *Some domains require that you type the account name in the format domain\username.*
   e) Close the Services dialog box.

Start the F5 DC Agent service again after the initialization file configuration is complete.

Configuring the initialization file

Before you can configure the initialization file, you must have the F5® DC Agent installed on a domain-joined, Windows-based server. You must also have deployed an iApps® application service to configure objects that enable communication between the F5 DC Agent and the BIG-IP® system.

Note: *The following steps require you to enter some values that are available only as a result of completing the prerequisites.*

You configure an initialization file for the F5 DC Agent so that it can send IP address and user name pairs to the BIG-IP system.

1. Log on to the Windows-based server where you installed the F5® DC Agent.

2. Navigate to this directory: `C:\Program Files\F5 Networks\User Identity Agents \config`.
3. Using a text editor, open the `transid.ini` file.

   The file contains one section, [DC Agent].
4. For `IFMapServer`, type the protocol, host address, and port for the server.

   This is the virtual server that was created by the application service. Port `8096` is the default port. You might have specified another port number when you deployed the application service.

   For example, `IFMapServer=https://AA.BB.CC.DD:8096`, where *`AA.BB.CC.DD`* is the IP address of the virtual server created by the application service.
5. To authenticate to the BIG-IP system using clientless HTTP authentication, type values for these parameters.
   a) For `IFMapUsername`, type the name of the user that logs on to the IF-MAP server on behalf of the F5 DC Agent.

      This is the name of a user you created in the local user database on the BIG-IP system.
   b) For `IFMapPassword`, type the password for the user.

      This is the password you typed in the local user database.
6. (Optional) To authenticate using a certificate, for `IFMapCertClient`, type the path to the SSL certificate file to use for authenticating to the BIG-IP system.

   This must match the name of the certificate you specified in the application service on the BIG-IP system. Make sure that this certificate is imported into the certificate store on the BIG-IP system.
7. For the remainder of the parameters, you can retain the default values or change them.
   a) For `IFMapLifeTimeType`, retain the default value, *`forever`*.

      `IFMapLifeTimeType` specifies whether to keep or purge a user entry from the IF-MAP server when a session ends or times out. The alternative value is *`session`*.

      Note: *You can specify an absolute lifetime for a user entry in the* `IPCleanLifetime` *property.*

      ---
   b) For `PurgeOnStart`, retain the default value, *`true`*.

      `PurgeOnStart` specifies whether the IF-MAP server should purge user records after the F5 DC Agent restarts.
   c) For `IdleUpdate`, you can retain the default value of *`120`* seconds.

      `IdleUpdate` specifies the interval between keep-alive pings from the F5 DC Agent to the IF-MAP server.
   d) For `DiscoveryInterval`, retain the default value of *`84600`* seconds (24 hours).

      `DiscoveryInterval` specifies the interval at which the domain auto-discovery process runs.
   e) For `DC AgentEnable`, retain the default value of *`true`*.

      `DC AgentEnable` specifies whether domain auto-discovery is enabled (*`true`*) or disabled (*`false`*).
   f) For `QueryInterval`, you can retain the default value of *`10`* seconds.

      `QueryInterval` specifies the interval at which the F5 DC Agent queries domain controllers in seconds. Valid values are between 5 and 90 seconds.
   g) For `IPCleanLifetime`, you can retain the default value of *`7200`* seconds (2 hours).

      `IPCleanLifetime` specifies the amount of time a user entry remains in the IF-MAP server before it is removed, in seconds. Valid values are integers greater than 3600; specify 0 to disable.
8. Start or restart the F5 DC Agent service.

The F5 DC Agent discovers domain controllers and starts to send user identity information to the BIG-IP system.

Configuring domain controller polling in the dc_agent.txt file

After the F5® DC Agent starts for the first time, it might take a few minutes to complete domain discovery and to write the list of domains and domain controllers into the `dc_agent.txt` file. If the F5 DC Agent does not create a `dc_agent.txt` file, you can create one manually; refer to the examples in this task.

You configure the list of the domains and domain controllers that F5 DC Agent polls to ensure that the list is accurate and complete. If you installed more than one F5 DC Agent, you edit the `dc_agent.txt` file on each Windows-based server to ensure that each domain controller is queried by one F5 DC Agent only.

1. Log on to the Windows-based server where you installed the F5® DC Agent.
2. Navigate to this directory: `C:\Program Files\F5 Networks\User Identity Agents\`.
3. If the `dc_config.txt` file already exists, make a backup copy in another location.
4. Create or open the `dc_config.txt` file using a text editor.
5. Verify that all domains and controllers are on the list.
   This example shows two domain controller entries in each of two domains, WEST_DOMAIN and EAST_DOMAIN; polling is enabled on each domain controller. Note the blank line at the end of the file; it is required.

```
[WEST_DOMAIN]
dcWEST1=on
dcWEST2=on
[EAST_DOMAIN]
dcEAST1=on
dcEAST2=on

```

6. If domains or domain controllers are missing, add them.

   To make sure that F5 DC Agent can see a domain, run the `net view /domain` command before you add the domain.
7. If the list contains domain controllers that F5 DC Agent should not poll, change the entry value from *`on`* to *`off`*.

   If you configure F5 DC Agent to avoid polling an active domain controller, the agent cannot transparently identify the users that log on to it.

   Important: *Rather than deleting a domain controller, change the setting to `off`. Otherwise, F5 DC Agent adds it to the file again after it next discovers domain controllers.*

   In this example, polling is disabled for the `dcEAST2` domain controller.

```
dcEAST2=off
```

8. Make sure that the file includes a carriage return after the last entry, creating a blank line at the end of the file.

   If you do not include the hard return, the last entry in the file get truncated, and an error message is written.
9. Save the changes and close the file.
10. Use the Windows Services dialog box to restart the F5 DC Agent service.

Recovering from an unsuccessful installation

To install F5® DC Agent correctly, first remove any failed installations and then install.

1. Log on to the Windows-based server from a user account with local and domain administrator privilege.
2. From the Windows Programs and Features dialog box, uninstall the F5 Installer application.
3. From Windows Explorer, click the `SWGUserIdentificationAgents.exe` file and follow the instructions to install F5 DC Agent again.

Enabling debug logging for the F5 DC Agent

When you are troubleshooting, you might want debug errors to be logged.

1. Log on to the Windows-based server where you installed the F5® DC Agent.
2. Navigate to this directory: `C:\Program Files\F5 Networks\User Identity Agents \config`.
3. Using a text editor, open the `diagnostics.cfg` file.
4. Look for `log4j.threshold` in Global configuration.
5. Note the value for `log4j.threshold`; you will need it when you complete troubleshooting tasks.
6. Modify the value to `DEBUG`.
7. Restart the DC agent service.
   Debug errors start to be logged.
8. When you are done with troubleshooting, edit the `diagnostics.cfg` file, reset `log4j.threshold` to the previous value, and restart the DC agent service.

Troubleshooting when a user is identified incorrectly

Troubleshooting is critical if you suspect or determine that a user is not being correctly identified.

1. Log on to the client system that belongs to the user.
2. Open a browser and navigate to four or more distinctive web sites.
3. Log on to the Windows-based server where the F5® DC Agent is installed.
4. Look for error messages in the Windows Event Viewer.
5. Proceed based on any error messages that you discover.

F5 DC Agent error messages

Error messages from the F5® DC Agent display in the Event Viewer on the Windows-based server where DC Agent is installed.

Error code	Error message	Possible causes
3	`Could not configure DC Agent (Code 3)`	An attempt was made to install F5 DC Agent using an account that does not have domain and local administrator privileges. As a result, some required files are not installed properly, and F5 DC Agent service cannot run.
5	`ERROR_ACCESS_DENIED`	F5 DC Agent service does not have sufficient permissions to perform required tasks. This error can occur when: • A `NetSessionEnum` call from F5 DC Agent fails due to Local Security Policy or Trust Relationship configurations.

Error code	Error message	Possible causes
		• F5 DC Agent uses an anonymous account and the domain controller is configured to not give the list of user logon sessions to an anonymous user.
53	ERROR_BAD_NETPATH	A network problem prevents F5 DC Agent from contacting a domain controller. This error can occur when: • Windows Remote Registry Service is not running on the Windows server with the agent • NetBIOS is not bound to the network adapter on the Windows server • The Windows server and the domain controller use different network protocols for communication • The Windows-based server cannot communicate with the domain controller or with the BIG-IP® system possibly because of a problem with network connection or with placement within the network. • Remote administration is not enabled on the domain controller.
71	`System error while enumerating the domain controllers. domain: (****)ecode: 71 : message: No more connections can be made to this remote computer at this time because there are already as many connections as the computer can accept.`	The error results from F5 DC Agent automatic domain discovery process, used to identify new domains and domain controllers. It can also occur when F5 DC Agent tries to connect to a Windows XP-based computer that is broadcasting itself as the master browser for a non-company domain or workgroup. Although the issue might indicate a problem with connectivity to the domain controller, it is more likely that the domain is a workgroup with no domain controllers. This error can be ignored.
997	`Error Code 997`	An attempt was made to install F5 DC Agent using an account that does not have domain and local administrator privileges. As a result, some required files are not installed properly, and F5 DC Agent service cannot run.
1058	`Error Code 1058`	This error is seen on startup. A Local Security Policy on the Windows-based server might have disabled the F5 DC Agent service.

Overview: Configuring the SWG F5 Logon Agent

The F5® Logon Agent enables *transparent user identification*, a best effort to identify users without requesting credentials.

Note: *F5 Logon Agent is available only on a BIG-IP® system with an SWG subscription.*

You can install the F5 Logon Agent on a Windows-based server in any domain in the network. The F5 Logon Agent identifies users in real time when the users log on to domains, which prevents missing a

user logon because of a query timing issue. F5 Logon Agent sends up-to-date session information to the BIG-IP® system.

Note: *F5 Logon Agent does not transmit passwords or any other confidential information.*

F5 Logon Agent identification process

1. When users log on to the network, a network logon script invokes the logon application (`LogonApp.exe`).
2. The logon application contacts F5 Logon Agent using HTTP.
3. F5 Logon Agent sends an NTLM authentication challenge, and the logon application provides a user name, hashed password, and IP address to F5 Logon Agent.
4. F5 Logon Agent verifies the username and password combination from the logon application by establishing a session with the domain controller. (F5 Logon Agent contacts User Service to determine which domain controller is the logon source.)
5. After verifying the user name and IP address pair, F5 Logon Agent sends the information to the BIG-IP system and adds an entry to its user map in local memory. The user map is periodically saved to a backup file, `AuthServer.bak`.
6. The BIG-IP system records user name and IP address pairs to the BIG-IP system copy of the user map in local memory. Confidential information (such as user passwords) is not sent to the BIG-IP system.

Considerations for installing multiple agents

You can install more than one F5 Logon Agent in your network, and configure F5 Logon Agents to communicate with the same BIG-IP system. If you have multiple BIG-IP systems, each BIG-IP system must be able to communicate with every F5 Logon Agent in your network.

NetBIOS port 139

F5 Logon Agent uses NetBIOS port 139 for automatic domain detection. If NetBIOS port 139 is blocked in your network, you can deploy an F5 Logon Agent instance for each virtually or physically remote domain.

Multiple subnets

As a best practice, install a separate F5 Logon Agent in each subnet to avoid problems gathering logon information from domain controllers.

Network size, disk space, and RAM

If your network is very large (10,000+ users or 30+ domain controllers), you might benefit from installing F5 Logon Agent on multiple machines to evenly distribute resource usage.

Task summary

Configuring the BIG-IP system for the F5 Logon Agent
Verifying network communication
Downloading and installing F5 Logon Agent
Updating privileges for the F5 Logon Agent service
Configuring the initialization file
Recovering from an unsuccessful installation
Enabling debug logging for the F5 Logon Agent
Troubleshooting when a user is identified incorrectly

Configuring the BIG-IP system for the F5 Logon Agent

You use an iApps® template to deploy an application service that configures objects that the F5® Logon Agent uses to communicate with the IF-MAP server on the BIG-IP® system.

Note: *You can configure the F5 Logon Agent to authenticate with the BIG-IP system using certificate inspection or using clientless HTTP basic authentication against a local user database.*

1. Set up to support certificate inspection:
   a) Obtain a trusted certificate and key that are valid for all fully qualified domain names (FQDNs) used to access the BIG-IP system.
   b) Import the certificate and key into the BIG-IP system.
      You can import SSL certificates from the System area of the product.
2. Obtain the IF-Maps iApps template file from F5® DevCentral™at `http://devcentral.f5.com/wiki/iapp.Codeshare.ashx`.
3. Import the template:
   a) On the Main tab, click **iApps** > **Templates**.
   b) Click **Import**.
   c) Select the **Overwrite Existing Templates** check box.
   d) Click **Browse**, then browse to and select the template file.
   e) Click **Upload**.
4. Deploy an application service:
   a) On the Main tab, click **iApps** > **Application Services**, and then click **Create**.
   b) In the **Name** field, type a name.

      Note: *The application service prefixes this name to the names of configuration objects it creates.*

   c) From the **Template** list, select **f5.ifmap**.

      Note: *This iApps template displays on the list only when APM is provisioned.*

   d) Follow the instructions on the screen to complete the deployment.
      A summary displays the configuration objects.
   e) Take note of the IP address of the virtual server created by the service. You need to type it into F5 Logon Agent initialization file later.

      Note: *This virtual server must be accessible by the F5 Logon Agent from a routing perspective.*

5. To enable clientless HTTP basic authentication, create a user and password in the local user database.
   The purpose of this user account is to authenticate communication between the F5 Logon Agent and the BIG-IP system.
   a) On the Main tab, click **Access Policy** > **Local User DB** > **Manage Users**.
      The Manage Users screen displays.
   b) Click **Create New User**.
      The Create New Local User screen opens and displays User Information settings.
   c) From the **Instance** list, select the instance created when you deployed the application service.
   d) In the **User Name** field, type the user name.
      Take note of the user name and password. You need to type them again later when you configure the initialization file for F5 Logon Agent.
   e) In the **Password** and **Confirm Password** fields, type the user's password.

Verifying network communication

You can verify that there are no DNS or NetBIOS or network communications issues on a Windows-based server before you install the F5® Logon Agent on it. Alternatively, you can use these steps for troubleshooting if you observe a problem.

1. Open a command prompt on the Windows-based server that hosts, or will host, the F5 Logon Agent.

2. To verify that the Windows-based server sees all required domains, use the `net view` command.
   For example, type `net view /network`.
3. To check for DNS issues, use the `nslookup` command.
   For example, to verify that DNS resolves the host name, `testmachine1`, type this command: `nslookup testmachine1` . If the DNS lookup succeeds, the result is similar to: `Server: testdns.test.example.com Address: 10.56.1.4 Name: testmachine1.test.example.com Address: 10.56.100.15`
4. To verify that F5 Logon Agent will be able to use NetBIOS, try to open a Telnet session to a domain controller on port `139`.
   If the command is successful, the screen remains blank. If unsuccessful, then:
   - A a router, firewall, or other device might be blocking NetBIOS traffic.
   - NetBIOS might not be enabled and the domain controller might not be listening on port `139`.
5. If you could not successfully use a Telnet connection to a domain controller on port `139`, verify the status of the port using the `netstat` command.
   For example, type `netstat -na | find"139"` .)
6. To verify that the F5 Logon Agent will be able to communicate with the virtual server on the BIG-IP® system, use a Telnet connection to the IP address of the virtual server on port `8096` or on the port that you entered when creating the application service.
   This virtual server was created using an application service based on the `f5.ifmap` iApps® template.

Downloading and installing F5 Logon Agent

F5® Logon Agent is available when Access Policy Manager® (APM®) is licensed and provisioned on the BIG-IP® system. Before you perform these steps, make sure that the Windows Computer Browser service is running on the Windows server where you plan to install F5 Logon Agent.

You perform this task to be able to identify clients transparently by IP address. (Do this only in an environment where IP addresses are trusted and unique.) You perform this task so that APM can gather information to support the user identity service.

1. Go to the BIG-IP Configuration utility Welcome screen.
   If you are already logged in, click the F5® logo to open the Welcome screen.
2. In the Secure Web Gateway User Identification Agents area, click the **User Identification Agents** link.
   A `SWGUserIdentificationAgents.exe` file downloads.
3. Copy the downloaded file to a Windows-based server that is joined to a domain controller.

   Important: *Do not install F5 Logon Agent on a domain controller because the F5 Logon Agent can put a load on the domain controller.*

4. From an account with both local and administrator privileges, click the `SWGUserIdentificationAgents.exe` file to start the installer.
   The installer displays instructions.
5. Follow the instructions to complete the installation.

   Important: *F5® strongly recommends that you use the default destination folder. On the Destination Folder screen, click* ***Next*** *without making any changes.*

   Important: *Install either F5 DC Agent or F5 Logon Agent, but not both. This overwrites the omapd user map every time an update is published.*

   The program installs a Windows service, F5 Logon Agent.

Updating privileges for the F5 Logon Agent service

The F5® Logon Agent service must run from a privileged account. You can create a new user account or use an existing account configured as specified in step 1.

1. On the Windows-based server, create a user account for F5 Logon Agent:
   a) Assign the new account domain administrator privileges in all domains.
   b) Assign the same password to this account in all domains.
      Make a note of the password. You must type it again in step 2.
   c) Set the password to never expire.
2. Configure the F5 Logon Agent service to log on as the user account you just configured:
   a) Open the Windows Services dialog box.
      From the Control Panel, select **Administrative Tools** > **Services**.
   b) Locate the F5 Logon Agent service, right-click the service name, and select **Stop**.
   c) Double-click the service name, and then select the Log On tab.
   d) Select **This account** and type the account name and password for the account you created in step 1.

      Note: *Some domains require that you type the account name in the format domain\username.*

   e) Close the Services dialog box.

Start the F5 Logon Agent service again after the initialization file configuration is complete.

Configuring the initialization file

Before you can configure the initialization file, you must have the F5® Logon Agent installed on a domain-joined, Windows-based server. You must also have deployed an iApps® application service to configure objects that enable communication between the F5 Logon Agent and the BIG-IP® system.

Note: *This task requires you to enter some values that are available as a result of completing the prerequisites.*

You configure an initialization file for the F5 Logon Agent so that it can send IP address and user name pairs to the BIG-IP system.

1. Log on to the Windows-based server where you installed the F5® DC Agent.
2. Navigate to this directory: `C:\Program Files\F5 Networks\User Identity Agents\config`.
3. Using a text editor, open the `authserver.ini` file.
   The file contains one section, [Logon Agent].
4. For `IFMapServer`, type the protocol, host address, and port for the server.
   This is the virtual server that was created by the application service. Port `8096` is the default port. You might have specified another port number when you deployed the application service.
   For example, `IFMapServer=https://AA.BB.CC.DD:8096`, where *`AA.BB.CC.DD`* is the IP address of the virtual server created by the application service.
5. To authenticate to the BIG-IP system using clientless HTTP authentication, type values for these parameters.
   a) For `IFMapUsername`, type the name of the user that logs on to the IF-MAP server on behalf of the F5 Logon Agent.
      This is the name of a user you created in the local user database on the BIG-IP system.

b) For `IFMapPassword`, type the password for the user.

This is the password you typed in the local user database.

6. (Optional) To authenticate using a certificate, for `IFMapCertClient`, type the path to the SSL certificate file to use for authenticating to the BIG-IP system.

This must match the name of the certificate you specified in the application service on the BIG-IP system. Make sure that this certificate is imported into the certificate store on the BIG-IP system.

7. For the remainder of the parameters, you can retain the default values or change them.

a) For `IFMapLifeTimeType`, retain the default value, *`forever`*.

`IFMapLifeTimeType` specifies whether to keep or purge a user entry from the IF-MAP server when a session ends or times out. The alternative value is *`session`*.

Note: *You can specify an absolute lifetime for a user entry in the* `IPCleanLifetime` *property.*

---

b) For `PurgeOnStart`, retain the default value, *`false`*.

`PurgeOnStart` specifies whether the IF-MAP server should purge user records after the F5 Logon Agent restarts.

c) For `IdleUpdate`, you can retain the default value of *`120`* seconds.

`IdleUpdate` specifies the interval between keep-alive pings from the F5 Logon Agent to the IF-MAP server.

d) For `QueryInterval`, you can retain the default value of *`900`* seconds.

`QueryInterval` specifies the interval at which the F5 Logon Agent queries domain controllers in seconds. Valid values are between 5 and 90 seconds.

e) For `EntryLifetime`, retain the default value of *`86400`* seconds.

`EntryLifetime` specifies the interval at which the domain auto-discovery process runs.

f) For `ReconfigPeriod`, you can retain the default value of *`60`* seconds.

`ReconfigPeriod` specifies the amount of time between agent reconfiguring during an initialization file update.

g) For `LogonAgentIP`, type the address.

`LogonAgentIP` specifies the address that the server should bind to.

h) For `LogonAgentPort`, you can retain the default value of *`15880`* seconds.

`LogonAgentPort` specifies the TCP/IP Port that the agent should listen on.

8. Start or restart the F5 Logon Agent service.

The F5 Logon Agent discovers domain controllers and starts to send user identity information to the BIG-IP system.

Recovering from an unsuccessful installation

You install F5® Logon Agent correctly by first removing any failed installations, and then installing.

1. Log on to the Windows-based server from a user account with local and domain administrator privilege.
2. From the Windows Programs and Features dialog box, uninstall the F5 Installer application.
3. From Windows Explorer, click the `SWGUserIdentificationAgents.exe` file and follow the instructions to install F5 Logon Agent again.

Enabling debug logging for the F5 Logon Agent

When you are troubleshooting, you might want debug errors to be logged.

1. Log on to the Windows-based server where you installed the F5® DC Agent.

2. Navigate to this directory: `C:\Program Files\F5 Networks\User Identity Agents\`.
3. Using a text editor, open the `diagnostics.cfg` file.
4. Look for `log4j.threshold` in Global configuration.
5. Note the value for `log4j.threshold`; you will need it when you complete troubleshooting tasks.
6. Modify the value to `DEBUG`.
7. Restart the Logon Agent service.
   Debug errors start to be logged.
8. When you are done with troubleshooting, edit the `diagnostics.cfg` file, reset `log4j.threshold` to the previous value, and restart the Logon Agent service.

Troubleshooting when a user is identified incorrectly

Troubleshooting is critical if you suspect or determine that a user is not being correctly identified.

1. Log on to the client system that belongs to the user.
2. Open a browser and navigate to four or more distinctive web sites.
3. Log on to the Windows-based server where the F5® Logon Agent is installed.
4. Look for error messages in the Windows Event Viewer.
5. Proceed based on any error messages that you discover.

Files used by Logon Agent

This table explains the relevant files used by F5® Logon Agent after you install the installation file from the BIG-IP® system Configuration utility Welcome screen.

Filename	File location	Additional information
`LogonApp.exe`	Stored in User Identity Agents > LogonApp > Windows folder.	Sends user information to F5 Logon Agent. Captures user logon sessions as they occur. Runs on Windows client machines.
`logon.bat`	Stored in User Identity Agents > LogonApp > Windows folder.	Invokes `LogonApp.exe`, which runs on client machines and captures logon sessions.
`AuthServer.ini`	Stored in User Identity Agents > config folder.	Contains one initialization parameter for Logon Agent.

Overview: Creating a script on a Windows system for SWG F5 Logon Agent

When you install the F5® Logon Agent, you must create a logon script for clients that identify the clients to the BIG-IP® system when they log on to a Windows domain. The application, LogonApp.exe, provides a username and IP address to F5 Logon Agent each time a Windows client connects to a Windows Active Directory or a Windows NT directory service.

When installing F5 Logon Agent, the following files are placed in the F5 Networks folder (by default, `C:\Program Files\F5 Networks\User Identity Agents\LogonApp`):

- LogonApp.exe
- logon.bat

Task summary

Creating a logon or logout script

Running a logon or logout script on Active Directory

Creating a logon or logout script

When you install F5® Logon Agent on a Windows system, the installation stores a batch file, logon.bat, in your local User Identity Agents directory. The batch file contains instructions for using scripting parameters and two sample scripts: a logon script that runs LogonApp.exe, and a logout script that removes user information from the BIG-IP® system when a user logs out. You can create a logon or logout script from the logon.bat examples.

1. On your Windows screen, click **Start** > **Accessories** > **Notepad**
2. In the untitled Notepad menu, click **File** > **Open**
3. Navigate to the directory with the logon.bat file. For example:`C:\Program Files\F5 Networks \User Identity Agents\LogonApp\Windows\logon.bat`.
   The .bat file displays logon script examples.
4. Open a new Notepad file.
5. Using the examples in logon.bat, create a script for either F5 Logon Agent logon or logout options.
6. Click **Save** and select .bat as the file extension.

You have created a logon or logout script

Running a logon or logout script on Active Directory

You must create a script before you can run it on Active Directory.

You can configure your logon or logout script to run with a group policy on Active Directory.

1. On the Active Directory machine, click **Control Panel**.
   The Control Panel window displays.
2. From the window, select **Administrative Tools** > **Active Directory Users and Computers**.
3. Right-click the domain and select **Properties**.
4. On the Group Policy tab, click **New**.
5. In the New Group Policy screen, create a new policy.
6. Click **Edit**.
   A window displaying a tree structure displays.
7. Expand **User Configuration**.
8. For Windows Settings option, click **Scripts (Logon/Logoff)**.
9. On the right screen, double-click **Logon**.
10. Click **Show Files**.
    The folder that contains the logon script opens in Windows Explorer.
11. Copy the files `logon.bat` and `LogonApp.exe` to the folder.
12. Close the Windows Explorer window.
13. In the Logon Properties dialog box, click **Add**.
14. For the **Script Name** field, type `logon.bat`.
15. Click **OK**.
16. In the domain Properties dialog box, click **OK**.

You have configured your logon or logout script to run with a group policy on Active Directory.

Logon and logout script parameters

This table explains the relevant parameters used by a logon or logout script for F5® Logon Agent.

Parameter	Description
<server>	The IP address of the BIG-IP® system F5 Logon Agent.
<port>	The port number used by F5 Logon Agent. The default value is 15880.
/NOPERSIST	1. Triggers the logon application to send user information to F5 Logon Agent only at logon. The username and IP address are communicated to the server during the logon process and remain in the F5 Logon Agent user map until the user data is automatically cleared at a predefined time interval. The default user entry expiration is 24 hours. 2. If the NOPERSIST parameter is omitted, LogonApp.exe operates in persistent mode, located in the memory of the domain server and updates F5 Logon Agent with the usernames and IP addresses at predefined intervals. The default interval is 15 minutes. The following example logon script sends user information to F5 logon Agent at the logon step only. The information is not updated during the user's session (NOPERSIST). The information is sent to port 15880 on the server identified by IP address 10.2.2.95. `LogonApp.exe http://10.2.2.95:15880 /NOPERSIST`
/COPY	Copies the logon application to the `%USERPROFILE%\Local Settings\Temp` directory on the user machine, where the logon script runs it from the local memory. This optional parameter helps prevent your logon script from hanging. COPY can be used only in persistent mode.
/VERBOSE	A debugging parameter that can be used only with help from technical support.
/LOGOUT	Used only in an optional logout script, this parameter removes the user's logon information from the F5 Logon Agent user map when the user logs off. If you use Active Directory, this parameter can clear the logon information from the user map before the interval that is defined for F5 Logon Agent has elapsed. Use this optional parameter in a logout script in a batch file that is different than the one containing the logon script. The following example logout script clears the logon information for each user as soon as the user

Parameter	Description
	logs out. `LogonApp.exe http://10.2.2.95:15880 /NOPERSIST /LOGOUT`

Secure Web Gateway Statistics

About SWG data for threat monitoring

After Secure Web Gateway (SWG) starts proxying web access, it provides information that you can use to monitor threats and to fine-tune URL filters.

On a BIG-IP® system with Access Policy Manager®, SWG can provide logs and reports.

On a BIG-IP system with an SWG subscription, SWG can provide overview statistics in addition to logs and reports.

Note: *If you configure high-speed remote event logging, you have data on a remote system from which you can create your own reports.*

Overview: Monitoring Internet traffic for threats

You can view Secure Web Gateway (SWG) statistics on the BIG-IP® system and adjust URL filters to handle new threats based on the information that you gather from logs and reports.

Before you begin, event logging should be configured. SWG reports and charts depend on event logging for URL filters. For event logging to occur, log settings must be configured and then specified in the access profile, and a Category Lookup item must be run in the per-request policy.

Task summary

Configuring statistics collection for SWG reports
Examining statistics on the SWG Overview
Focusing the Overview on security threats
Exporting or emailing SWG statistics
Creating an SMTP server configuration
About statistics aggregation for weekly and longer time ranges

About the Secure Web Gateway Overview

The Secure Web Gateway (SWG) overview provides multiple reports and charts that summarize the top requests, such as top URLs, top categories by blocked request count, top users by permitted request count or by blocked request count, and so on. The overview can be customized to show the specific type of data that you are interested in.

Note: *SWG overview is available only on a BIG-IP® system with an SWG subscription.*

In addition to the reports and charts on the overview, SWG provides the All Requests and Blocked Requests reports and charts. The reports can be filtered to show the information that you want to see.

Configuring statistics collection for SWG reports

Configure report settings to specify whether to gather statistics for Secure Web Gateway (SWG) reports and whether to use data sampling.

1. On the Main tab, click **Access** > **Overview** > **SWG Reports** > **Settings**.

The Report Settings screen displays.

2. To enable statistics gathering, select the **Collect Data** check box.

   If you clear the check box, data collection stops.

3. To enable dynamic data sampling, select the **Sample Data** check box.

   In exchange for a performance gain, data sampling might provide slightly inaccurate statistics. If statistics must be more accurate, then disable data sampling.

Examining statistics on the SWG Overview

Note: *Newer browsers (Internet Explorer 9 or later, Firefox 3.6 or later, or Chrome 14 or later) support viewing charts with no additional plug-in. If using older browsers (Internet Explorer 8 or earlier), Adobe® Flash® Player (version 8 or later) must be installed on the computer where you plan to view charts.*

You can review charts that show statistical information about traffic from your enterprise to the Internet. The charts provide visibility into the top requests for URL categories, blocked URL categories, top users, and so on.

Note: *The system updates the statistics every five minutes; you can refresh the charts periodically to see the updates.*

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Overview**.

   Note: *The Overview is available only on a BIG-IP® system with an SWG subscription.*

   The Overview screen displays.

2. From the **Override time range to** list, select a new time frame to apply to all of the widgets in the overview.

   Tip: *Within each widget you can override the default time range, as needed.*

3. For each widget, select the data format and the time range to display, as needed.
4. To focus on the specific details you want more information about, click the chart or the **View Details** link.
   The system refreshes the charts and displays information about the item.
5. From the **View By** list, select the specific network object type for which you want to display statistics.

   You can also click **Expand Advanced Filters** to filter the information that displays.
6. On the screen, the system displays the path you followed to reach the current display, including the items you clicked. For example, to review details for the top categories, follow these steps:
   a) In the Top categories by Request Count chart, click the category that interests you.
      Assume that your URL filters allow access to some news and media sites and that **News and Media** is among the top categories. Click **News and Media**.
      Charts display the request count per action over time and the request count per action. A details table lists the request count for allowed actions.
   b) In the **View By** list, select **URLs**.
      Charts update and a list of URLs displays in the details table. These are the top news and media URLs.
   c) To see which filter allowed this URL, from here you can continue to drill down successively by clicking a link in each details table that displays. As an alternative to drilling down, you can select any of the statistics displayed on the **View By** list; for example you can select **URL Filter** directly.

   The Overview charts display summarized data. You might notice as you drill down that details display on the Reports screen.

You can review the access policy to ensure that you use the optimal strategy for processing traffic. You can update URL filters to block, confirm, or allow particular URL categories. You can update URL categories to include new URLs that you have seen in statistics details, or to recategorize existing URLs to fit your policies. You can continue to review the collected metrics and troubleshoot the system as needed.

Focusing the Overview on security threats

You can display attempted access to sites that pose a security risk by adding the security category widget to the Secure Web Gateway (SWG) Overview screen and by filtering a Blocked Request report using the security categories filter.

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Overview**.

   Note: *The Overview is available only on a BIG-IP® system with an SWG subscription.*

   The Overview screen displays.
2. Click the **Add Widget** link near the bottom of the screen.
   The Add New Widget screen displays.
3. From the **Modules** list, select **Secure Web Gateway (Blocked)**.

   The security categories widget includes data requests that were blocked.
4. From the **View by** list, select **Security Categories**.

   Requests that were blocked for URLs because they are included in the Security category or any of its subcategories are included in the data.
5. Move a measurement from **Available measurements** to the **Select up to 6 measurements to display** list.
6. For **Data visualization**, select one of the options.

   Details Table is the default option.
7. Click **Done**.
   The Add New Widget screen closes.

The Overview screen displays the Security Categories chart.

You can also filter a Blocked Requests report to view this data by selecting **Security Categories** from the **View by** list.

Exporting or emailing SWG statistics

You can export or email charts that show Secure Web Gateway (SWG) statistics.

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Overview**.

   Note: *The Overview is available only on a BIG-IP® system with an SWG subscription.*

   The Overview screen displays.
2. Display the charts that show the information you want, clicking any of the options and adjusting the content as needed.
3. On the upper right of the charts screen, click **Export**.

   Tip: *To send the report to others by email, go to* ***Statistics*** > ***Analytics*** > ***Scheduled Reports****.*
4. Click **Export**.

Creating an SMTP server configuration

You specify the SMTP server configuration so that you can send emails through an SMTP server.

1. On the Main tab, click **System** > **Configuration** > **Device** > **SMTP**.
2. Click the **Create** button.
   The New SMTP Configuration screen opens.
3. In the **Name** field, type a name for the SMTP server that you are creating.
4. In the **SMTP Server Host Name** field, type the fully qualified domain name for the SMTP server host.
5. In the **SMTP Server Port Number** field, type a port number.

   For no encryption or TLS encryption, the default is `25`. For SSL encryption, the default is `465`.
6. In the **Local Host Name** field, type the host name used in the SMTP headers in the form of a fully qualified domain name.

   This host name is not the same as the BIG-IP® system's host name.
7. In the **From Address** field, type the email address that you want displayed as the reply-to address for the email.
8. From the **Encrypted Connection** list, select the encryption level required for the SMTP server.
9. To require that the SMTP server validates users before allowing them to send email, select the **Use Authentication** check box, and type the user name and password required to validate the user.
10. Click the **Finish** button.

You can now configure the system to use this SMTP server to send emails. For the SMTP mailer to work, you must make sure the SMTP server is on the DNS lookup server list, and configure the DNS server on the BIG-IP® system.

Implementation result

Secure Web Gateway (SWG) is configured to produce reports and charts.

About the reporting interval for charts and reports

The system updates the statistics for charts and reports at five minute intervals: at five minutes after the hour, ten minutes after the hour, and so on. Each five-minute mark includes data from the previous five minutes; so 12:45 includes data starting from 12:40:01 to 12:45:00.

Charts and data that you export from charts reflect the publishing interval of five minutes. For example, if you request data for the time period 12:40-13:40, the data in the chart or in the file that you export is for that time period. But if there is a request for data from 12:42-13:42, the data in the chart is from 12:45-13:45. By default, the BIG-IP® system displays one hour of data.

About statistics aggregation for weekly and longer time ranges

Secure Web Gateway (SWG) reports and charts for weekly, monthly, and yearly time ranges include statistics up through the previously completed hour. The system performs hourly updates to the aggregated statistics.

Overview: Monitoring Internet traffic for threats

Creating an SMTP server configuration

Overview: Configuring remote high-speed APM and SWG event logging

About Secure Web Gateway statistics

Secure Web Gateway (SWG) reports display statistical information about web traffic on your system. These details are available:

Actions
Action (allowed, blocked, or confirmed) taken on the URL request.

Client IP address
IP address from which the request for the URL originated.

Host Name
When available, host name from which the request for the URL originated.

Categories
Name of the preconfigured or custom URL category into which a requested URL falls.

URLs
Requested URL.

URL filters
Name of the URL filter SWG applied to the request based on the schedule in the scheme.

Security categories
The security category of the URL if it was blocked, because it matched a security category.

Note: *Security categories are available on a BIG-IP® system with an SWG subscription.*

Users
Name of the user that made the request, if available.

Note: *Configuring your system to identify users is optional.*

SSL bypass
Whether the request was bypassed (yes or no).

Note: *Configuring your system to omit certain SSL traffic from inspection is optional.*

Logging and Reporting

Overview: Configuring remote high-speed APM and SWG event logging

You can configure the BIG-IP® system to log information about Access Policy Manager® (APM®) and Secure Web Gateway events and send the log messages to remote high-speed log servers.

When configuring remote high-speed logging of events, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Log Setting	Add event logging for the APM system and configure log levels for it or add logging for URL filter events, or both. Settings include the specification of up to two log publishers: one for access system logging and one for URL request logging.
Access profile	Add log settings to the access profile. The log settings for the access profile control logging for the traffic that comes through the virtual server to which the access profile is assigned.

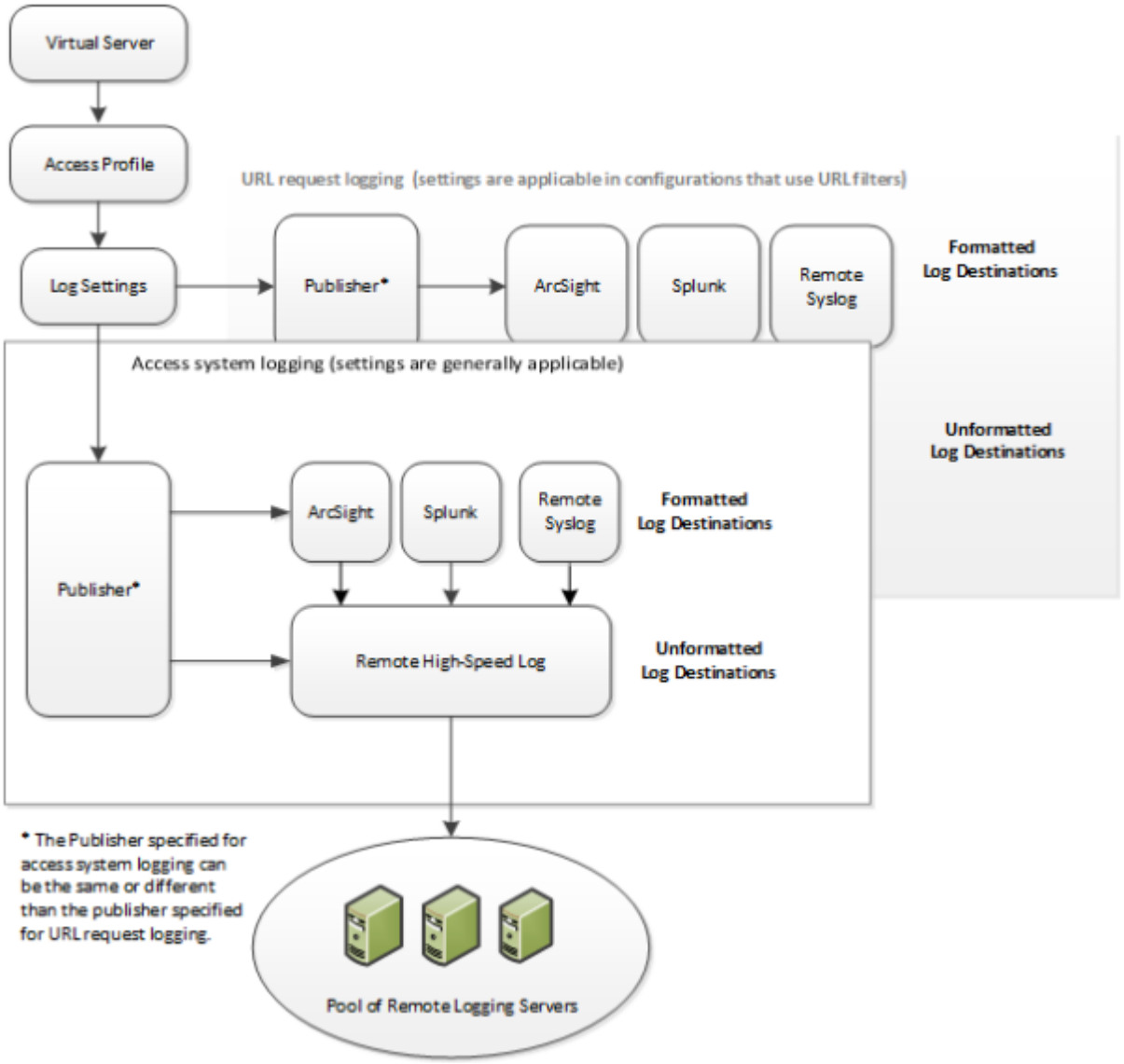


Figure 20: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure remote high-speed APM and SWG event logging on the BIG-IP system.

Note: *Enabling remote high-speed logging impacts BIG-IP system performance.*

Task list

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Configuring log settings for access system and URL request events
Disabling logging

About the default-log-setting

Access Policy Manager® (APM®) provides a default-log-setting. When you create an access profile, the default-log-setting is automatically assigned to it. The default-log-setting can be retained, removed, or replaced for the access profile. The default-log-setting is applied to user sessions only when it is assigned to an access profile.

Regardless of whether it is assigned to an access profile, the default-log-setting applies to APM processes that run outside of a user session. Specifically, on a BIG-IP® system with an SWG subscription, the default-log-setting applies to URL database updates.

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

   Note: *Typical remote logging servers require port* `514`*.*

   c) Click **Add**.
5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. With this configuration, the BIG-IP system can send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.

5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select a formatted logging destination, such as **Remote Syslog**, **Splunk**, or **ArcSight**.

   The Splunk format is a predefined format of key value pairs.

   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, then from the **Syslog Format** list select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*
6. If you selected **Splunk**, then from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.

   The Splunk format is a predefined format of key value pairs.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*
5. Click **Finished**.

Configuring log settings for access system and URL request events

Create log settings to enable event logging for access system events or URL filtering events or both. Log settings specify how to process event logs for the traffic that passes through a virtual server with a particular access profile.

1. On the Main tab, click **Access** > **Overview** > **Event Logs** > **Settings**.
   A log settings table screen opens.
2. Select a log setting and click **Edit** or click **Create** for a new APM® log setting.
   A popup screen opens with General Information selected in the left pane.
3. For a new log setting, in the **Name** field, type a name.
4. To specify logging, select one or both of these check box options:
   - **Enable access system logs** - This setting is generally applicable. It applies to access policies, per-request policies, Secure Web Gateway processes, and so on. When you select this check box, **Access System Logs** becomes available in the left pane.
   - **Enable URL request logs** - This setting is applicable for logging URL requests when you have set up a BIG-IP® system configuration to categorize and filter URLs. When you select this check box, **URL Request Logs** becomes available in the left pane.

   Important: *When you clear either of these check boxes and save your change, you are not only disabling that type of logging, but any changes you made to the settings are also removed.*
5. To configure settings for access system logging, select **Access System Logs** from the left pane.
   Access System Logs settings display in the right panel.
6. For access system logging, from the **Log Publisher** list select the log publisher of your choice.
   A log publisher specifies one or more logging destinations.

   Important: *The BIG-IP® system is not a logging server and has limited capacity for storing, archiving, and analyzing logs. For this reason a dedicated logging server is recommended.*
7. For access system logging, retain the default minimum log level, **Notice**, for each option.
   You can change the minimum log level, but **Notice** is recommended.

Option	Description
Access Policy	Events that occur while an access policy runs.
Per-Request Policy	Events that occur while a per-request policy runs.
ACL	Events that occur while applying APM access control lists.
SSO	Events that occur during single-sign on.
Secure Web Gateway	Events that occur during URL categorization on a BIG-IP® system with an SWG subscription.
ECA	Events that occur during NTLM authentication for Microsoft Exchange clients.
OAuth	Events that occur while APM, as an OAuth authorization server, processes requests.
PingAccess Profile	Events related to PingAccess authentication. ***Important:*** *For PingAccess authentication, only the log levels defined in default-log-settings apply.*

Option	Description
VDI	Events related to connections to virtual desktop resources.
Endpoint Management System	Events related to connections to an endpoint management system.

8. To configure settings for URL request logging, select **URl Request Logs** from the left pane.
   URL Request Settings settings display in the right panel.
9. For URL request logging, from the **Log Publisher** list, select the log publisher of your choice.
   A log publisher specifies one or more logging destinations.

   Important: *The BIG-IP® system is not a logging server and has limited capacity for storing, archiving, and analyzing logs. For this reason a dedicated logging server is recommended.*

10. To log URL requests, you must select at least one check box option:
    - **Log Allowed Events** - When selected, user requests for allowed URLs are logged.
    - **Log Blocked Events** - When selected, user requests for blocked URLs are logged.
    - **Log Confirmed Events** - When selected, user requests for confirmed URLs are logged.

    Whether a URL is allowed, blocked, or confirmed depends on both the URL category into which it falls, and the URL filter that is applied to the request in the per-request policy.
11. (Optional) To assign this log setting to multiple access profiles now, perform these substeps:

    Note: *Up to three log settings for access system logs can be assigned to an access profile. If you assign multiple log settings to an access profile, and this results in duplicate log destinations, logs are also duplicated.*

    a) Select **Access Profiles** from the left pane.
    b) Move access profiles between the **Available** and the **Selected** lists.

    Note: *You can delete (and add) log settings for an access profile on the Logs page for the access profile.*

    Note: *You can configure the log destinations for a log publisher from the Logs page in the System area of the product.*

12. Click **OK**.
    The popup screen closes. The table displays.

To put a log setting into effect, you must assign it to an access profile. Additionally, the access profile must be assigned to a virtual server.

Disabling logging

Disable event logging when you need to suspend logging for a period of time or you no longer want the BIG-IP® system to log specific events.

Note: *Logging is enabled by adding log settings to the access profile.*

1. To clear log settings from access profiles, on the Main tab, click **Access** > **Profiles / Policies**.
2. Click the name of the access profile.
   Access profile properties display.
3. On the menu bar, click **Logs**.
4. Move log settings from the **Selected** list to the **Available** list.

5. Click **Update**.

Logging is disabled for the access profile.

About event log levels

Event log levels are incremental, ranging from most severe (**Emergency**) to least severe (**Debug**). Setting an event log level to **Warning** for example, causes logging to occur for warning events, in addition to events for more severe log levels. The possible log levels, in order from highest to lowest severity are:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice** (the default log level)
- **Informational**
- **Debug**

Note: *Logging at the* ***Debug*** *level can increase the load on the BIG-IP® system.*

Legal Notices

Legal notices

Publication Date

This document was published on August 16, 2018.

Publication Number

MAN-0504-07

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

E

F

G

H

I

K

L

M

N

P

R

S

T

U

V

W

X