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

Version 12.1

# Table of Contents

# BIG-IP APM Secure Web Gateway Overview

## About Secure Web Gateway for web access

BIG-IP® Access Policy Manager® (APM®) implements a Secure Web Gateway (SWG) by adding access control, based on URL categorization, to forward proxy. With SWG, 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 SWG, which can allow or block access to URL categories or indicate that the user should confirm the URL before access can be allowed.

## About the benefits APM provides 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.

## Additional resources and documentation for BIG-IP Access Policy Manager

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

| Document | Description |
|---|---|
| *BIG-IP® Access Policy Manager®: Application Access* | This guide contains information for an administrator to configure application tunnels for secure, application-level TCP/IP connections from the client to the network. |
| *BIG-IP® Access Policy Manager®: Authentication and Single-Sign On* | This guide contains information to help an administrator configure APM for single sign-on and for various types of authentication, such as AAA server, SAML, certificate inspection, local user database, and so on. |
| *BIG-IP® Access Policy Manager®: Customization* | This guide provides information about using the APM customization tool to provide users with a personalized experience for access policy screens, and errors. An administrator can apply your organization's brand images and colors, change messages and errors for local languages, and change the layout of user pages and screens. |
| *BIG-IP® Access Policy Manager®: Edge Client and Application Configuration* | This guide contains information for an administrator to configure the BIG-IP® system for browser-based access with the web client as well as for access using BIG-IP Edge Client® and BIG-IP Edge Apps. It also includes information about how to configure or obtain client packages and install them for BIG-IP Edge Client for Windows, Mac, and Linux, and Edge Client command-line interface for Linux. |
| *BIG-IP® Access Policy Manager®: Implementations* | This guide contains implementations for synchronizing access policies across BIG-IP systems, hosting content on a BIG-IP system, maintaining OPSWAT libraries, configuring dynamic ACLs, web access management, and configuring an access policy for routing. |
| *BIG-IP® Access Policy Manager®: Network Access* | This guide contains information for an administrator to configure APM Network Access to provide secure access to corporate applications and data using a standard web browser. |

| Document | Description |
|---|---|
| *BIG-IP® Access Policy Manager®: Portal Access* | This guide contains information about how to configure APM Portal Access. In Portal Access, APM communicates with back-end servers, rewrites links in application web pages, and directs additional requests from clients back to APM. |
| *BIG-IP® Access Policy Manager®: Secure Web Gateway* | This guide contains information to help an administrator configure Secure Web Gateway (SWG) explicit or transparent forward proxy and apply URL categorization and filtering to Internet traffic from your enterprise. |
| *BIG-IP® Access Policy Manager®: Third-Party Integration* | This guide contains information about integrating third-party products with Access Policy Manager (APM®). It includes implementations for integration with VMware Horizon View, Oracle Access Manager, Citrix Web Interface site, and so on. |
| *BIG-IP® Access Policy Manager®: Visual Policy Editor* | This guide contains information about how to use the visual policy editor to configure access policies. |
| Release notes | Release notes contain information about the current software release, including a list of associated documentation, a summary of new features, enhancements, fixes, known issues, and available workarounds. |
| Solutions and Tech Notes | Solutions are responses and resolutions to known issues. Tech Notes provide additional configuration instructions and how-to information. |

# URL Categorization

## About URL categorization

On a BIG-IP® system with an SWG subscription, URL categorization must be configured. The URL database must be downloaded and a download schedule must be set. Optionally, custom URL categories and filters can be created to extend the standard URL categories and URL filters that are provided.

On a BIG-IP system without an SWG subscription, URL categorization is an option. Standard URL categories and URL filters are not provided. URL filtering can be accomplished with user-defined URL categories and user-defined URL filters.

## Overview: Downloading the URL database and updating standard URL filters

Secure Web Gateway (SWG) 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.

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

SWG supplies default URL filters as a starting point for your configuration. For example, the URL filter named default blocks the majority of inappropriate web sites. You can use any default filter as a starting point from which to define your own URL filters to reflect your acceptable use policies.

Complete these tasks before you create a per-request policy to categorize and filter URL requests.

### Task summary

Use these tasks to download URL categories initially, to refresh them over time, and to specify URL filters that support your use and compliance policy. Before you begin, the BIG-IP® system must be licensed and provisioned to support URL categorization.

### Task list

*Downloading and updating URL categories*
*Adding custom URL categories to the URL database*
*Customizing standard categories from the URL database*
*Configuring URL filters*

### 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.

## Downloading and updating URL categories

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

For database downloads to work, you must have configured DNS for the BIG-IP device in the System area of the product. You must also must have configured a default route in the Network area of the product.

If URL database download is available on the BIG-IP system, you must download the URL categories for Secure Web Gateway (SWG) to work. In order 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.

***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. 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 for approximately 45 minutes.*
4. Click **Update Settings**.
5. 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.*

## 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) Select the **Glob Pattern Match** check box if you typed any globbing patterns in the URL field.
   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 that Secure Web Gateway (SWG) supplies by adding URLs to them. You might do this after you run SWG 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, SWG 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) Select the **Glob Pattern Match** check box if you typed any globbing patterns in the URL field.
   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.

## Configuring URL filters

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.

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.

   ***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.*

   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**.

   ***Note:*** *User-defined categories are subcategories of* ***Custom Category****.*

   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.
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. On a BIG-IP system with an SWG subscription, 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 URL request is made.

## 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.

## Implementation result

Now you have BIG-IP® Secure Web Gateway (SWG) configured to regularly download updates to URL categories. URL filters are configured and ready to be added to per-request policies.

## 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 Policy** > **Event Logs** > **Log Settings**.
   A log settings table displays.
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 Policy** > **Event Logs** > **Access System Logs**.

   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. |

# Overview: Configuring user-defined URL categories and filters

If you want to categorize and filter URL requests from your users, you need to use URL categories and URL filters. If URL categories and filters do not exist on a BIG-IP® system, you can create them.

Complete these tasks before you create a per-request policy that includes items to categorize (URL Category) and filter (URL Filter Assign) URL requests.

### Task summary

*Creating user-defined URL categories*
*Configuring URL filters*

## Creating user-defined URL categories

Create a 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 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) Select the **Glob Pattern Match** check box if you typed any globbing patterns in the URL field.
   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 or block) for the custom category.

## Configuring URL filters

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.

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.

   ***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.*

   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**.

   ***Note:*** *User-defined categories are subcategories of* ***Custom Category****.*

   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.
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. On a BIG-IP system with an SWG subscription, 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 URL request is made.

# Application Filter Configuration

## About application filtering and remote access forward proxy

Secure Web Gateway (SWG) does not support application filtering in a remote access forward proxy configuration.

## About application families

Access Policy Manager® (APM®) supports a predefined set of application families and applications. An *application family* name characterizes the type of applications associated with it. Users cannot add applications or application families to APM.

## About application filters

An *application filter* specifies the applications (and application families) that Access Policy Manager® (APM®) supports and a filtering action (allow or block) for each application. An application filter can be used in a per-request policy in a supported APM configuration to control access to supported applications.

APM provides predefined application filters: block-all, allow-all, and default. The default application filter allows access to some application families and blocks access to others. Users can define their own application filters and use those that APM provides.

## Overview: Configuring filters for application access

Access Policy Manager® (APM®) provides a few default application filters and you can configure additional filters. Application filtering is effected in a per-request policy.

**Task summary**

*Specifying the default filter action for an application*
*Configuring application filters*

### Specifying the default filter action for an application

You can change the default filter action (block or allow) for any application. When you create a new application filter, the applications in it specify the default filter action.

***Note:** A change to the default filter action for an application has no effect on existing application filters.*

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Applications**.
   The Applications screen displays.
2. To view applications, expand an application family.
3. To modify the default filter action for an application:
   a) Click the application name.
      An Application Properties screen displays.
   b) From the **Default Filter Action** list, retain the displayed setting or select another.

      The options are **Block** and **Allow**.
   c) Click **Update**.
      The Applications screen displays.

The default filtering action for the application is updated and is used when a new application filter is created.

## Configuring application filters

Configure an application filter to specify how to process requests for access to applications or application families. You can configure multiple application filters.

1. On the Main tab, click **Access Policy** > **Secure Web Gateway** > **Application Filters**.

   Click the name of any filter to view its settings.

   ***Note:** Default application filters, such as block-all, allow-all and default, are available. You cannot delete default application filters.*

   The Application Filters screen displays.
2. To configure a new application filter, click one of these:
   - **Create** button - Click to start with an application filter with the default filter action specified for each application.
   - **Copy** link - Click this link for an existing application filter in the table to start with its settings.

   Another screen opens.
3. In the **Name** field, type a unique name for the application filter.
4. In the **Description** field, type any descriptive text.
5. Click **Finished**.
   The properties screen displays with an Associated Applications table.
6. To block access to particular applications or entire application families, select them and click **Block**.

   ***Important:** When you select an application family, you also select the related applications. You can expand the application family and clear any applications that are selected.*

   ***Important:** To block any applications that Secure Web Gateway cannot categorize, select the application family **Unknown**.*
7. To allow access to particular applications or entire application families, select them and click **Allow**.

To use an application filter, you must assign it in a per-request policy. A per-request policy runs each time a request is made.

# User Identification

## About user identification

Access Policy Manager® (APM®) Secure Web Gateway (SWG) identifies users and maps them to IP addresses, or to sessions, without using cookies. The methods that are available for identifying users depend on access profile type.

### About session management cookies and Secure Web Gateway

Secure Web Gateway (SWG) does not use Access Policy Manager® (APM®) session management cookies. If presented with an APM session management cookie, SWG ignores it.

### About user identification with NTLM authentication

User identification by credentials is a method that is available for the SWG-Explicit access profile type. To support this option, an NTLM Auth Configuration object must be specified in the access profile and the result of NTLM authentication can be verified in the access policy.

For user identification by credentials, Secure Web Gateway (SWG) maintains an internal mapping of credentials to sessions.

### 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.

Secure Web Gateway (SWG) maintains an internal mapping of IP addresses to user names.

### About user identification with an 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 F5 DC Agent or the F5 Logon Agent must be downloaded, installed, and configured.

## Overview: Configuring 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.*

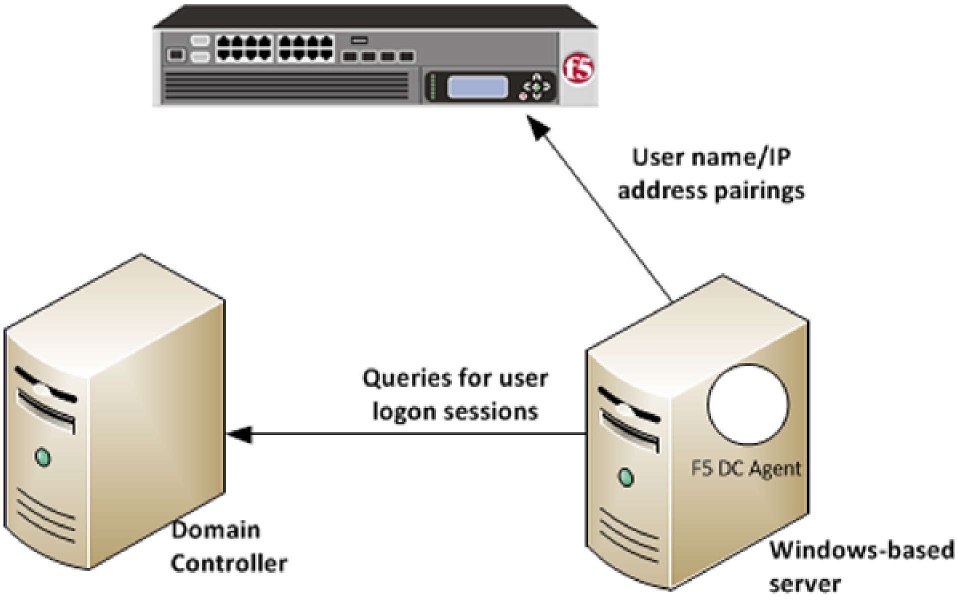


**Figure 1: How F5 DC Agent transparently identifies users**

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 users | Average amount of data transferred per day |
|---|---|
| 250 users | 30 KB |
| 2,000 users | 240 KB |
| 10,000 users | 1200 KB |

**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 domain controller polling in the dc_agent.txt file*
*Recovering from an unsuccessful installation*
*Enabling debug logging for the F5 DC Agent*
*Troubleshooting when a user is identified incorrectly*

## 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 IFMap 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) 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.)

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:<br>• 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:<br>• Windows Remote Registry Service is not running on the Windows server with the agent<br>• NetBIOS is not bound to the network adapter on the Windows server<br>• The Windows server and the domain controller use different network protocols for communication<br>• 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.<br>• 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 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.)

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 |

| Filename | File location | Additional information |
|---|---|---|
| | | 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 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.<br>**2.** If the NOPERSIST parameter is omitted, LogonApp.exe operates in persistent mode, located in the memory of the domain server and |

| Parameter | Description |
|---|---|
| | updates F5 Logon Agent with the usernames and IP addresses at predefined intervals. The default interval is 15 minutes.<br>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 logs out. `LogonApp.exe http://10.2.2.95:15880 /NOPERSIST /LOGOUT` |

# Explicit Forward Proxy Configuration

## Overview: Configuring SWG explicit forward proxy

A Secure Web Gateway (SWG) explicit forward proxy deployment provides an easy way to handle web requests from users. 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.

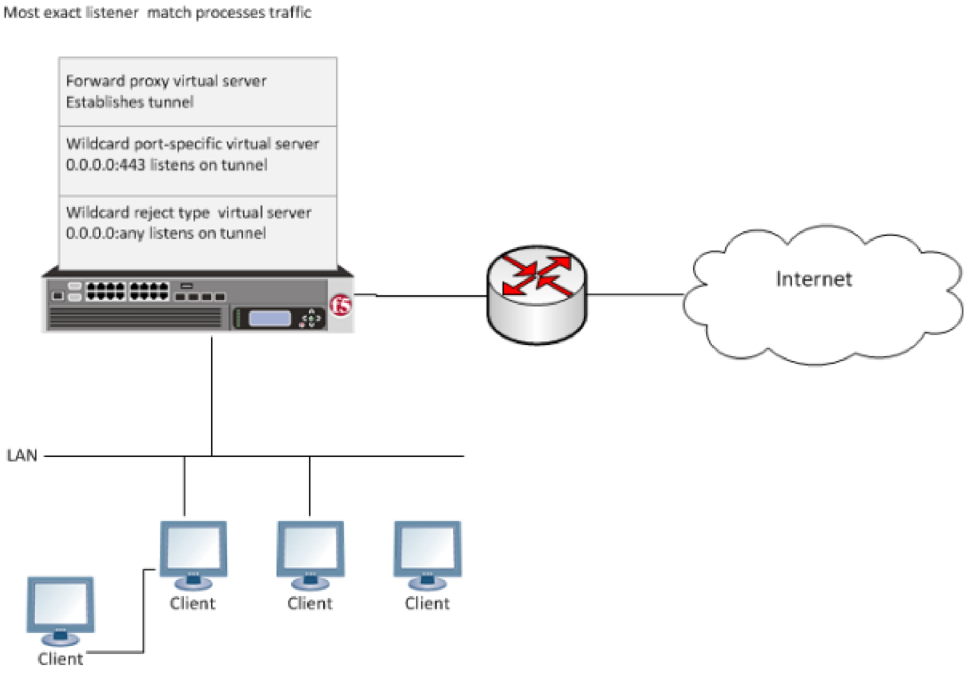

Most exact listener match processes traffic
Forward proxy virtual server
Establishes tunnel
Wildcard port-specific virtual server
0.0.0.0:443 listens on tunnel
Wildcard reject type virtual server
0.0.0.0:any listens on tunnel
Internet
LAN
Client
Client
Client
Client

**Figure 2: Explicit forward proxy configuration**

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. This implementation does not explain how to do these tasks. However, 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 Secure Web Gateway only. Note that possibly not all applications will work with a firewall configured this way. (Secure Web Gateway uses ports 80 and 443.) |

### Task summary

*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*
*Verifying log settings for the access profile*
*Configuring an access policy for SWG 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 iApps® template can set up either an explicit or a transparent forward proxy configuration. You can download the template from the F5® DevCentral™ iApp Codeshare wiki at (`http://devcentral.f5.com/wiki/iapp.Codeshare.ashx`).

## SWG explicit forward proxy configuration prerequisites

Ensure that prerequisites are complete before beginning the configuration.

### Per-request policy

A per-request policy is required in any Secure Web Gateway (SWG) forward proxy configuration. A per-request policy must specify the logic for processing URL requests.

### URL categorization

On a BIG-IP® system with an SWG subscription, you must download and install a URL database and schedule updates for it. On a system without an SWG subscription, you can configure user-defined URL categories and filters to control access by filtering URLs.

### Transparent user identification

On a system with an SWG subscription, if you plan to identify users transparently, you must first download, install, and configure an F5® user identification agent, either the F5 DC Agent or the F5 Logon Agent.

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

### Authentication

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 that you use NTLM or Kerberos authentication. If you plan to use authentication, ensure that you have what you need configured.

- For NTLM, you need an NTLM Auth Configuration in Access Policy Manager® (APM®).
- For Kerberos, you need a domain-joined Kerberos user account and a Kerberos AAA server configured in APM.

### SSL intercept

To intercept SSL connections that are passing through the proxy, ensure that you have imported a valid subordinate CA certificate and key that is trusted by the endpoints behind the proxy.

## About ACLs and SWG explicit forward proxy

Only L7 ACLs work with Secure Web Gateway (SWG) explicit forward proxy.

## 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**.

## 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; however, this requires that the virtual servers using the cache have a route to the Internet.*

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.
   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 Secure Web Gateway (SWG) explicit forward proxy configuration.

---

***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:*** *Secure Web Gateway (SWG) explicit forward proxy 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.

   SWG 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 Policy** > **Access Profiles**.
   The Access Profiles List 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 access 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 Secure Web Gateway (SWG) 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.

## Verifying log settings for the access profile

Confirm that the correct log settings are selected for the access profile to ensure that events are logged as you intend.

***Note:** Log settings are configured in the Access Policy Event Logs area of the product. They enable and disable logging for access system and URL request filtering events. Log settings also specify log publishers that send log messages to specified destinations.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit.
   The properties screen opens.
3. On the menu bar, click **Logs**.
   The access profile log settings display.
4. Move log settings between the **Available** and **Selected** lists.

   You can assign up to three log settings that enable access system logging to an access profile. You can assign additional log settings to an access profile provided that they enable logging for URl request logging only.

   ***Note:** Logging is disabled when the **Selected** list is empty.*
5. Click **Update**.

An access profile is in effect when it is assigned to a virtual server.

## Configuring an access policy for SWG explicit forward proxy

You configure an access policy for Secure Web Gateway (SWG) explicit forward proxy to populate session variables with group or class attribute information for use in the per-request policy. 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 Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the **(+)** icon anywhere in the access policy to add a new action 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.
3. If you specified an NTLM Auth configuration in the access profile, verify that authentication succeeded.
   a) Type `NTLM` in the search field.
   b) Select **NTLM Auth Result** from the results list.
   c) Click **Add Item**.
      A properties popup screen opens.
   d) Click **Save**.
      The properties screen closes. The visual policy editor displays.
4. To add Kerberos authentication to the access policy, add these actions in order: **HTTP 407 Response**, **Variable Assign**, and **Kerberos Auth** using these substeps:

a) On an access policy branch, click the plus symbol **(+)** to add an item to the access 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 SWG explicit forward proxy, you must assign the domain name for the forward 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 forward proxy virtual server.
j) Click **Finished**.

The popup screen closes.

k) Click **Save**.
The properties screen closes. The visual policy editor displays.
l) On an access policy branch, click the plus symbol **(+)** to add an item to the access policy.
m) Type `ker` in the search field, select **Kerberos Auth** from the results, 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 visual policy editor displays.

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

**5.** To identify a user transparently using information provided by a BIG-IP® user identification agent, perform these substeps:

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 an access policy branch, click the plus symbol **(+)** to add an item to the access 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 displays.
d) Add any additional access policy items to the fallback or associated branches.
You might add Kerberos authentication on the fallback branch.

6. To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the access 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.
7. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the access 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**.
8. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the access 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.
9. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

To apply this access policy to network traffic, add the access profile to a virtual server.

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

## Creating a virtual server to use as the forward proxy server

You specify a virtual server to handle forward proxy traffic with Secure Web Gateway (SWG). 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. From the **VLAN and Tunnel Traffic** list, select **Enabled on**.
9. For the **VLANs and Tunnels** setting, move the VLAN on the BIG-IP® system that connects to the internal networks to the **Selected** list.
10. From the **Source Address Translation** list, select **Auto Map**.
11. If the per-request policy that you configured earlier includes application filtering, perform these substeps:
    a) From the **Classification** list, select **Enabled**.
    b) Scroll down to the Resources area.
    c) For **Policies**, make sure that **sys_CEC_video_policy** is enabled.

    ***Note:*** *The per-request policy uses application filtering when it runs an Application Lookup action.*
12. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
13. From the **Per-Request Policy** list, select the per-request 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 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 SSL Server 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 using the Move button, 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. If the per-request policy that you configured earlier includes application filtering, perform these substeps:
    a) From the **Classification** list, select **Enabled**.
    b) Scroll down to the Resources area.
    c) For **Policies**, make sure that **sys_CEC_video_policy** is enabled.

    ***Note:*** *The per-request policy uses application filtering when it runs an Application Lookup action.*

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

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

## 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

Web traffic that originates from your enterprise networks is now inspected and controlled by F5® Secure Web Gateway forward proxy.

## 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`<br>***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: Processing RDP traffic on a device with SWG

If you configure Access Policy Manager® APM® as a gateway for RDP clients and configure Secure Web Gateway (SWG) 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 recommended SWG configuration 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.*

## 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.

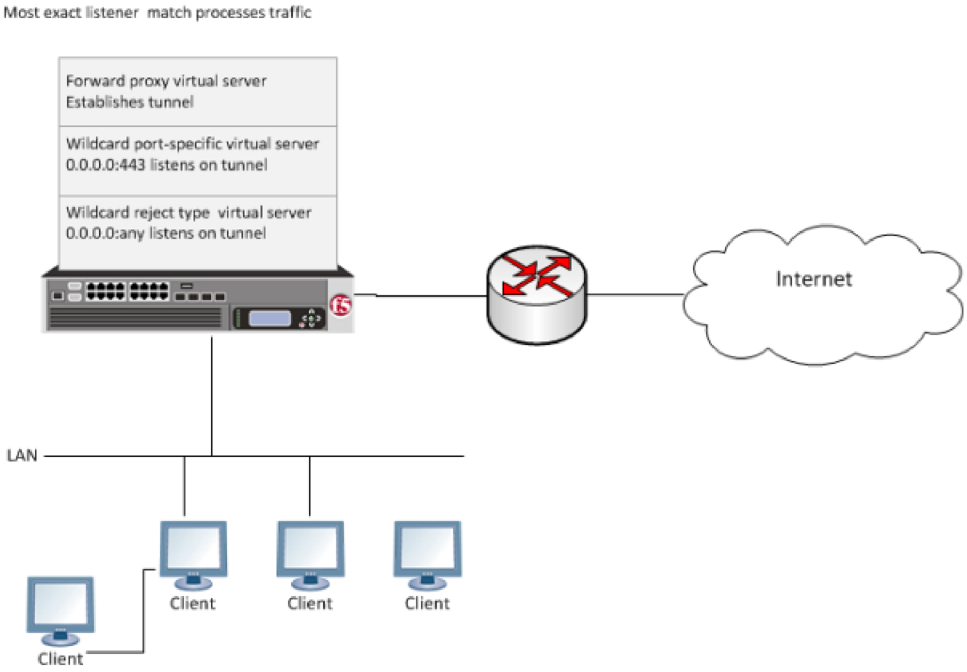

Most exact listener match processes traffic
Forward proxy virtual server
Establishes tunnel
Wildcard port-specific virtual server
0.0.0.0:443 listens on tunnel
Wildcard reject type virtual server
0.0.0.0:any listens on tunnel
Internet
LAN
Client
Client
Client
Client

**Figure 3: Explicit forward proxy configuration**

## 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.

# Transparent Forward Proxy Configurations

## Overview: Configuring transparent forward proxy in inline mode

In transparent forward proxy, you configure your internal network to forward web traffic to the BIG-IP® system with Secure Web Gateway (SWG). 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.

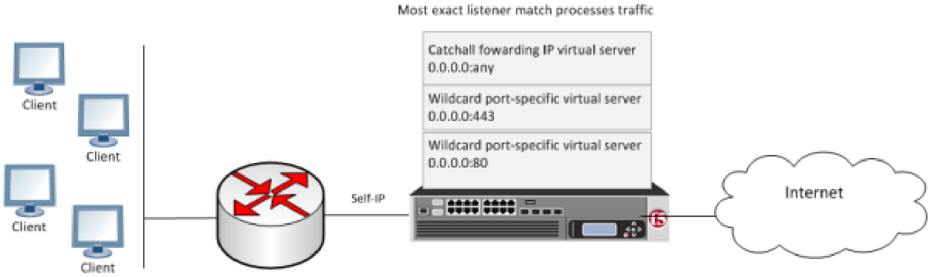

Most exact listener match processes traffic
Catchall fowarding IP virtual server
0.0.0.0:any
Wildcard port-specific virtual server
0.0.0.0:443
Wildcard port-specific virtual server
0.0.0.0:80
Client
Client
Client
Client
Self-IP
Internet

**Figure 4: Secure Web Gateway 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**

*Creating a VLAN for transparent forward proxy*
*Assigning a self IP address to a VLAN*
*Creating an access profile for SWG transparent forward proxy*
*Verifying log settings for the access profile*
*Configuring an access policy 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*

## About the iApp for Secure Web Gateway configuration

When deployed as an application service, the Secure Web Gateway iApps® template can set up either an explicit or a transparent forward proxy configuration. You can download the template from the F5® DevCentral™ iApp Codeshare wiki at (`http://devcentral.f5.com/wiki/iapp.Codeshare.ashx`).

## SWG transparent forward proxy configuration prerequisites

Ensure that prerequisites are complete before beginning the configuration.

#### Per-request policy

A per-request policy is required in any Secure Web Gateway (SWG) forward proxy configuration. A per-request policy must specify the logic for processing URL requests.

#### URL categorization

On a BIG-IP® system with an SWG subscription, you must download and install a URL database and schedule updates for it. On a system without an SWG subscription, you can configure user-defined URL categories and filters to control access by filtering URLs.

#### Transparent user identification

On a system with an SWG subscription, if you plan to identify users transparently, you must first download, install, and configure an F5® user identification agent, either the F5 DC Agent or the F5 Logon Agent.

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

#### Authentication

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 that you use NTLM or Kerberos authentication. If you plan to use authentication, ensure that you have what you need configured.

- For NTLM, you need an NTLM Auth Configuration in Access Policy Manager® (APM®).
- For Kerberos, you need a domain-joined Kerberos user account and a Kerberos AAA server configured in APM.

#### SSL intercept

To intercept SSL connections that are passing through the proxy, ensure that you have imported a valid subordinate CA certificate and key that is trusted by the endpoints behind the proxy.

#### Captive portal

If you plan to use the captive portal feature, make sure that a certificate and key with the proper common name is imported for use.

### SWG transparent forward proxy example: Clear text password

F5® recommends using NTLM or Kerberos authentication in a Secure Web Gateway (SWG) forward proxy configuration to prevent passwords from being exposed in clear text. With **Captive Portals** disabled in an SWG transparent type access profile, other types of authentication (AD Auth, LDAP Auth, or RADIUS Auth) in the access policy will work. However, the configuration is not secure because passwords can be exposed in clear text.

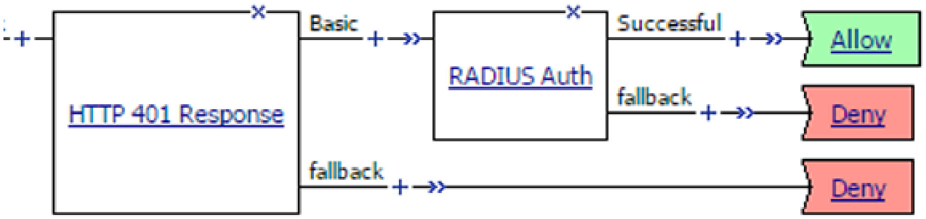


Figure 5: Access policy that can expose passwords in clear text (with captive portal disabled)

### SWG transparent forward proxy example: Encrypted password

F5® recommends using NTLM or Kerberos authentication in a Secure Web Gateway (SWG) forward proxy configuration to prevent passwords from being exposed in clear text. With **Captive Portals** enabled in an SWG transparent type access profile, using a Logon Page with other types of authentication (AD Auth, LDAP Auth, or RADIUS Auth) in the access policy will also work to keep passwords secure.

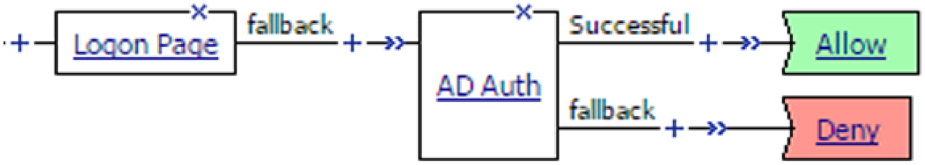


Figure 6: Access policy that keeps passwords secure (with captive portals enabled)

## 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 SWG 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 Policy** > **Access Profiles**.
   The Access Profiles List 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 access 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.

## Verifying log settings for the access profile

Confirm that the correct log settings are selected for the access profile to ensure that events are logged as you intend.

***Note:*** *Log settings are configured in the Access Policy Event Logs area of the product. They enable and disable logging for access system and URL request filtering events. Log settings also specify log publishers that send log messages to specified destinations.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit.
   The properties screen opens.
3. On the menu bar, click **Logs**.
   The access profile log settings display.
4. Move log settings between the **Available** and **Selected** lists.

   You can assign up to three log settings that enable access system logging to an access profile. You can assign additional log settings to an access profile provided that they enable logging for URl request logging only.

   ***Note:*** *Logging is disabled when the* ***Selected*** *list is empty.*
5. Click **Update**.

An access profile is in effect when it is assigned to a virtual server.

## Configuring an access policy for transparent forward proxy

You configure an access policy for Secure Web Gateway (SWG) transparent forward proxy to populate session variables with group or class attribute information for use in the per-request policy. You can also add access policy items to collect credentials and to authenticate a user, or you can add items to transparently identify the user without requesting credentials.

***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 Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the **(+)** icon anywhere in the access policy to add a new action 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.
3. If you specified an NTLM Auth configuration in the access profile, verify that authentication succeeded.
   a) Type `NTLM` in the search field.
   b) Select **NTLM Auth Result** from the results list.
   c) Click **Add Item**.
   A properties popup screen opens.
   d) Click **Save**.
   The properties screen closes. The visual policy editor displays.
4. To add Kerberos authentication to the access policy, add these actions in order: **HTTP 401 Response**, **Variable Assign**, and **Kerberos Auth** using these substeps:
   a) On an access policy branch, click the plus symbol **(+)** to add an item to the access policy.
   b) On the Logon tab, select **HTTP 401 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 SWG transparent forward proxy, you must assign the virtual server proxy domain name 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 visual policy editor displays.
   l) On an access policy branch, click the plus symbol **(+)** to add an item to the access policy.
   m) Type `ker` in the search field, select **Kerberos Auth** from the results, 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 visual policy editor displays.

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

**5.** To identify a user transparently using information provided by a BIG-IP® user identification agent, perform these substeps:

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 an access policy branch, click the plus symbol **(+)** to add an item to the access 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 displays.

d) Add any additional access policy items to the fallback or associated branches.
You might add Kerberos authentication on the fallback branch.

**6.** To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the access 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.

**7.** To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the access 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**.

**8.** To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the access 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.

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

To apply this access policy to network traffic, add the access profile to a virtual server.

> ***Note:** To ensure that logging is configured to meet your requirements, verify the log settings for 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 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 SSL Server 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 handle SSL web traffic.

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. For the **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
11. From the **Source Address Translation** list, select **Auto Map**.
12. For the **Address Translation** setting, clear the **Enabled** check box.
13. If you are using a captive portal, in the Access Policy area from the **Access Profile** list, select the access profile that you configured for transparent forward proxy, and from the **Per-Request Policy** list, select the per-request policy you configured earlier.
14. If you are using a captive portal and the per-request policy that you configured earlier includes application filtering, perform these substeps:
    a) From the **Classification** list, select **Enabled**.
    b) Scroll down to the Resources area.
    c) For **Policies**, make sure that **sys_CEC_video_policy** is enabled.

***Note:*** *The per-request policy uses application filtering when it runs an Application Lookup action.*

15. Click **Finished**.

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

## Creating a virtual server for forward proxy traffic

You configure a virtual server to handle web traffic going to port 80.

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 **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
9. From the **Source Address Translation** list, select **Auto Map**.
10. For the **Address Translation** setting, clear the **Enabled** check box.
11. If the per-request policy that you configured earlier includes application filtering, perform these substeps:
    a) From the **Classification** list, select **Enabled**.
    b) Scroll down to the Resources area.
    c) For **Policies**, make sure that **sys_CEC_video_policy** is enabled.

***Note:*** *The per-request policy uses application filtering when it runs an Application Lookup action.*

12. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.

13. From the **Per-Request Policy** list, select the per-request policy that you configured earlier.
14. Click **Finished**.

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

## 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 SSL.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client 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 SWG-Transparent access profile 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.

***Note:*** *If you do not plan to use client-side SSL, select a service port other than 443 and do not select an SSL client 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. 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, move the profile you configured previously from the **Available** list to the **Selected** list.
9. Scroll down to the Access Policy area.
10. From the **Access Profile** list, select the access profile you configured previously.
11. Click **Finished**.

The virtual server appears in the Virtual Server List screen.

## Implementation result

Web traffic that originates from your enterprise networks is now inspected and controlled by F5® Secure Web Gateway forward proxy.

## 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`<br>***Note:*** *This session variable is a default in the expression for LocalDB Group Lookup; any session variable in the expression must* | Local Database |

| Per-request policy item | Session variable | Access policy item |
|---|---|---|
| | *match the session variable used in the Local Database action in the access policy.* | |
| RADIUS Class Lookup | `session.radius.last.attr.class` | RADIUS Auth |

### 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 transparent forward proxy, you configure your internal network to forward web traffic to the BIG-IP® system with Secure Web Gateway (SWG). Use this implementation 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.

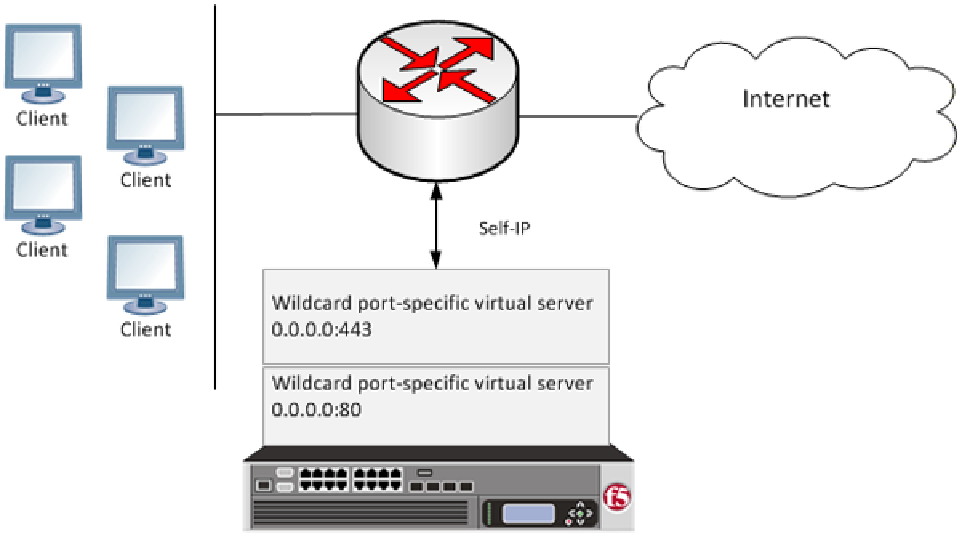

Client
Client
Client
Client
Internet
Self-IP
Wildcard port-specific virtual server
0.0.0.0:443
Wildcard port-specific virtual server
0.0.0.0:80

**Figure 7: Secure Web Gateway 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. Secure Web Gateway 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

*Creating a VLAN for transparent forward proxy*
*Assigning a self IP address to a VLAN*
*Creating an access profile for SWG transparent forward proxy*
*Verifying log settings for the access profile*
*Configuring an access policy 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 Client SSL profile for a captive portal*
*Creating a virtual server for a captive portal*

## SWG transparent forward proxy configuration prerequisites

Ensure that prerequisites are complete before beginning the configuration.

### Per-request policy

A per-request policy is required in any Secure Web Gateway (SWG) forward proxy configuration. A per-request policy must specify the logic for processing URL requests.

### URL categorization

On a BIG-IP® system with an SWG subscription, you must download and install a URL database and schedule updates for it. On a system without an SWG subscription, you can configure user-defined URL categories and filters to control access by filtering URLs.

### Transparent user identification

On a system with an SWG subscription, if you plan to identify users transparently, you must first download, install, and configure an F5® user identification agent, either the F5 DC Agent or the F5 Logon Agent.

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

### Authentication

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 that you use NTLM or Kerberos authentication. If you plan to use authentication, ensure that you have what you need configured.

- For NTLM, you need an NTLM Auth Configuration in Access Policy Manager® (APM®).
- For Kerberos, you need a domain-joined Kerberos user account and a Kerberos AAA server configured in APM.

### SSL intercept

To intercept SSL connections that are passing through the proxy, ensure that you have imported a valid subordinate CA certificate and key that is trusted by the endpoints behind the proxy.

### Captive portal

If you plan to use the captive portal feature, make sure that a certificate and key with the proper common name is imported for use.

## SWG transparent forward proxy example: Clear text password

F5® recommends using NTLM or Kerberos authentication in a Secure Web Gateway (SWG) forward proxy configuration to prevent passwords from being exposed in clear text. With **Captive Portals** disabled in an SWG transparent type access profile, other types of authentication (AD Auth, LDAP Auth, or RADIUS Auth) in the access policy will work. However, the configuration is not secure because passwords can be exposed in clear text.

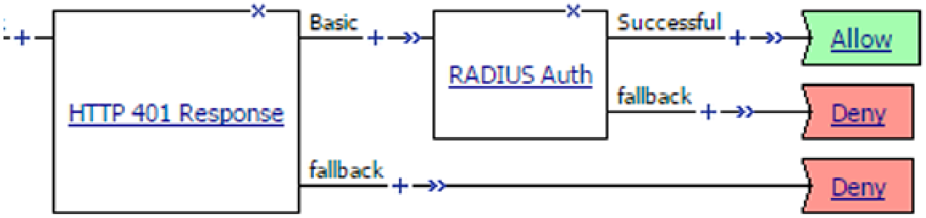


**Figure 8: Access policy that can expose passwords in clear text (with captive portal disabled)**

### SWG transparent forward proxy example: Encrypted password

F5® recommends using NTLM or Kerberos authentication in a Secure Web Gateway (SWG) forward proxy configuration to prevent passwords from being exposed in clear text. With **Captive Portals** enabled in an SWG transparent type access profile, using a Logon Page with other types of authentication (AD Auth, LDAP Auth, or RADIUS Auth) in the access policy will also work to keep passwords secure.

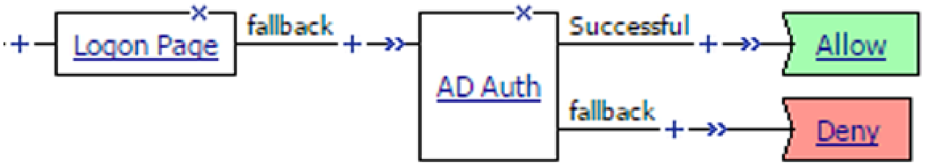


**Figure 9: Access policy that keeps passwords secure (with captive portals enabled)**

## About the iApp for Secure Web Gateway configuration

When deployed as an application service, the Secure Web Gateway iApps® template can set up either an explicit or a transparent forward proxy configuration. You can download the template from the F5® DevCentral™ iApp Codeshare wiki at (`http://devcentral.f5.com/wiki/iapp.Codeshare.ashx`).

## 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.

Secure Web Gateway (SWG) maintains an internal mapping of IP addresses to user names.

## About user identification with an 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 F5 DC Agent or the 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 SWG 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 Policy** > **Access Profiles**.
   The Access Profiles List 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 access 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.

## Verifying log settings for the access profile

Confirm that the correct log settings are selected for the access profile to ensure that events are logged as you intend.

***Note:** Log settings are configured in the Access Policy Event Logs area of the product. They enable and disable logging for access system and URL request filtering events. Log settings also specify log publishers that send log messages to specified destinations.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit.
   The properties screen opens.

3. On the menu bar, click **Logs**.
   The access profile log settings display.
4. Move log settings between the **Available** and **Selected** lists.

   You can assign up to three log settings that enable access system logging to an access profile. You can assign additional log settings to an access profile provided that they enable logging for URl request logging only.

   ***Note:*** *Logging is disabled when the* ***Selected*** *list is empty.*
5. Click **Update**.

An access profile is in effect when it is assigned to a virtual server.

## Configuring an access policy for transparent forward proxy

You configure an access policy for Secure Web Gateway (SWG) transparent forward proxy to populate session variables with group or class attribute information for use in the per-request policy. You can also add access policy items to collect credentials and to authenticate a user, or you can add items to transparently identify the user without requesting credentials.

***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 Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the **(+)** icon anywhere in the access policy to add a new action 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.
3. If you specified an NTLM Auth configuration in the access profile, verify that authentication succeeded.
   a) Type `NTLM` in the search field.
   b) Select **NTLM Auth Result** from the results list.
   c) Click **Add Item**.
   A properties popup screen opens.
   d) Click **Save**.
   The properties screen closes. The visual policy editor displays.
4. To add Kerberos authentication to the access policy, add these actions in order: **HTTP 401 Response**, **Variable Assign**, and **Kerberos Auth** using these substeps:
   a) On an access policy branch, click the plus symbol **(+)** to add an item to the access policy.
   b) On the Logon tab, select **HTTP 401 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 SWG transparent forward proxy, you must assign the virtual server proxy domain name 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 visual policy editor displays.

l) On an access policy branch, click the plus symbol **(+)** to add an item to the access policy.

m) Type `ker` in the search field, select **Kerberos Auth** from the results, 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 visual policy editor displays.

---

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

---

**5.** To identify a user transparently using information provided by a BIG-IP® user identification agent, perform these substeps:

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 an access policy branch, click the plus symbol **(+)** to add an item to the access 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 displays.

d) Add any additional access policy items to the fallback or associated branches.
   You might add Kerberos authentication on the fallback branch.

**6.** To supply LDAP group information for use in the per-request policy, add an LDAP Query item anywhere in the access 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.

7. To supply Active Directory groups for use in the per-request policy, add an AD Query item anywhere in the access 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**.
8. To supply RADIUS class attributes for use in the per-request policy, add a RADIUS Auth item anywhere in the access 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.
9. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

To apply this access policy to network traffic, add the access profile to a virtual server.

***Note:** To ensure that logging is configured to meet your requirements, verify the log settings for 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 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 SSL Server 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 handle SSL web traffic.

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. For the **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
11. From the **Source Address Translation** list, select **Auto Map**.
12. For the **Address Translation** setting, clear the **Enabled** check box.
13. If you are using a captive portal, in the Access Policy area from the **Access Profile** list, select the access profile that you configured for transparent forward proxy, and from the **Per-Request Policy** list, select the per-request policy you configured earlier.
14. If you are using a captive portal and the per-request policy that you configured earlier includes application filtering, perform these substeps:
    a) From the **Classification** list, select **Enabled**.
    b) Scroll down to the Resources area.
    c) For **Policies**, make sure that **sys_CEC_video_policy** is enabled.

    ***Note:*** *The per-request policy uses application filtering when it runs an Application Lookup action.*

15. Click **Finished**.

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

## Creating a virtual server for forward proxy traffic

You configure a virtual server to handle web traffic going to port 80.

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 **VLAN and Tunnel Traffic** setting, retain the default value **All VLANs and Tunnels** list.
9. From the **Source Address Translation** list, select **Auto Map**.
10. For the **Address Translation** setting, clear the **Enabled** check box.
11. If the per-request policy that you configured earlier includes application filtering, perform these substeps:
    a) From the **Classification** list, select **Enabled**.
    b) Scroll down to the Resources area.
    c) For **Policies**, make sure that **sys_CEC_video_policy** is enabled.

    ***Note:*** *The per-request policy uses application filtering when it runs an Application Lookup action.*
12. In the Access Policy area, from the **Access Profile** list, select the access profile that you configured earlier.
13. From the **Per-Request Policy** list, select the per-request policy that you configured earlier.
14. Click **Finished**.

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

## 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 SSL.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Client**.
   The Client 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 SWG-Transparent access profile 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.

***Note:** If you do not plan to use client-side SSL, select a service port other than 443 and do not select an SSL client 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. 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, move the profile you configured previously from the **Available** list to the **Selected** list.
9. Scroll down to the Access Policy area.
10. From the **Access Profile** list, select the access profile you configured previously.
11. Click **Finished**.

The virtual server appears in the Virtual Server List screen.

## Implementation result

Web traffic that originates from your enterprise networks is now inspected and controlled by F5® Secure Web Gateway forward proxy.

## 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`<br>***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 |

## 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.

# Remote Access Forward Proxy Configurations

## Overview: Configuring SWG explicit forward proxy for network access

You can configure Secure Web Gateway (SWG) explicit forward proxy and Network Access configurations so that SWG 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 SWG explicit forward proxy configuration to process traffic from remote clients separately from an SWG configuration used for processing traffic from internal clients provides an important measure of network security.*

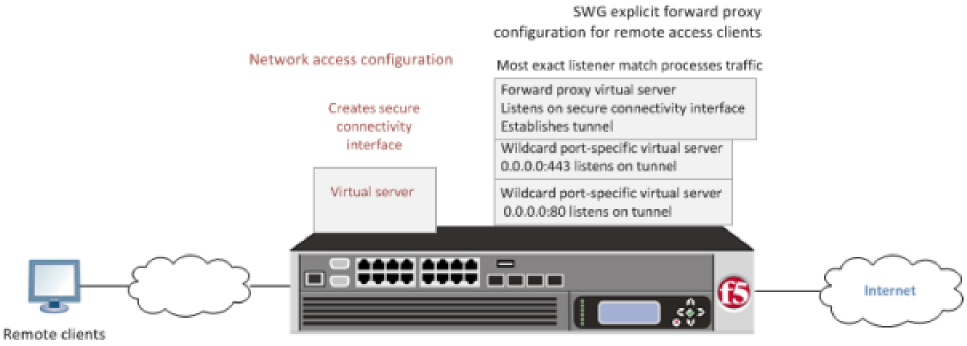

SWG explicit forward proxy configuration for remote access clients
Network access configuration
Most exact listener match processes traffic
Forward proxy virtual server
Listens on secure connectivity interface
Establishes tunnel
Creates secure connectivity interface
Wildcard port-specific virtual server
0.0.0.0:443 listens on tunnel
Virtual server
Wildcard port-specific virtual server
0.0.0.0:80 listens on tunnel
Internet
Remote clients

**Figure 10: 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 for network access client forward proxy server*
*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 SWG explicit forward proxy for network access

Before you start to create a Secure Web Gateway (SWG) explicit forward proxy configuration to support network access clients, you must have completed these tasks.

- You need to have configured a working 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 and you need to have configured 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 to use URL categories and filters, you must have created user-defined URL categories and URL filters.

## Configuration outline: SWG explicit forward proxy for Network Access

Tasks for integrating an Access Policy Manager® (APM®) Network Access configuration with a Secure Web Gateway (SWG) explicit forward proxy configuration 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 an SWG explicit forward proxy configuration. 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 Policy** > **Secure Connectivity**.
   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**.

## 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; however, this requires that the virtual servers using the cache have a route to the Internet.*

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.
   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:*** *Secure Web Gateway (SWG) explicit forward proxy 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.

   SWG 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 for network access client forward proxy server

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 using Secure Web Gateway (SWG).

You specify a virtual server to process forward proxy traffic with Secure Web Gateway (SWG). 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 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 SSL Server 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 Policy** > **Access Profiles**.
   The Access Profiles List 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 action 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 access 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 access 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 access 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 access 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 Secure Web Gateway (SWG) explicit forward proxy virtual server so that SWG can filter Internet traffic and analyze content, protecting the client from malware.

1. On the Main tab, click **Access Policy** > **Network Access** > **Network Access List**.
   The Network Access List 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 SWG explicit forward proxy virtual server.
   b) In the **Client Proxy Port** field, type the port number of the SWG 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 forwards traffic to the SWG explicit forward proxy server.

## Implementation result

The Secure Web Gateway (SWG) explicit forward proxy configuration is ready to process web traffic from network access clients.

## About configuration elements for explicit forward proxy (remote access)

When you configure Secure Web Gateway (SWG) 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. In the SWG configuration, an SWG explicit forward proxy server must listen on the secure connectivity interface for traffic from Network Access clients.

### Tunnel

In the SWG configuration, an HTTP profile on the explicit forward proxy server 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 SWG 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 SWG 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`<br>**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 SWG transparent forward proxy for remote access

Secure Web Gateway (SWG) can be configured to support remote clients that connect using application access, network access, or portal access.

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

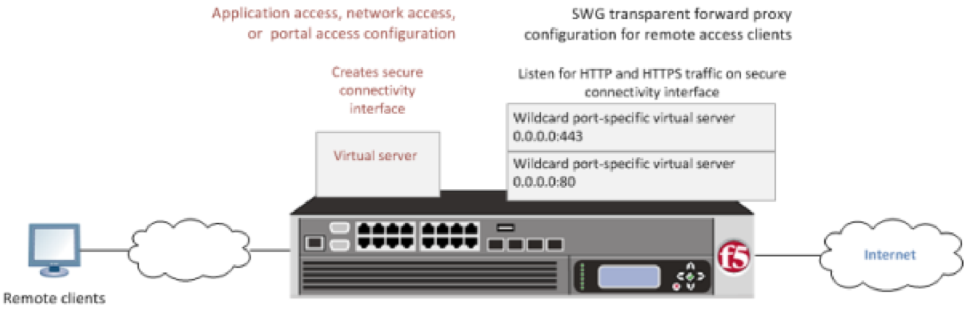

Application access, network access, or portal access configuration
SWG transparent forward proxy configuration for remote access clients
Creates secure connectivity interface
Listen for HTTP and HTTPS traffic on secure connectivity interface
Virtual server
Wildcard port-specific virtual server 0.0.0.0:443
Wildcard port-specific virtual server 0.0.0.0:80
Remote clients
Internet

**Figure 11: SWG 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 SWG transparent forward proxy*
*Verifying log settings for the access profile*
*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 SWG transparent forward proxy for remote access

Before you start to create a Secure Web Gateway (SWG) 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 and you need to have configured 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 to use URL categories and filters, you must have created user-defined URL categories and URL filters.

## Configuration outline for SWG transparent forward proxy for remote access

Tasks for integrating an Access Policy Manager® (APM®) remote access configuration with a Secure Web Gateway (SWG) transparent forward proxy configuration 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 an SWG transparent forward proxy configuration. 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 Policy** > **Secure Connectivity**.
   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 SWG transparent forward proxy

You create an access profile to supply an access policy.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List 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 access 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.

## Verifying log settings for the access profile

Confirm that the correct log settings are selected for the access profile to ensure that events are logged as you intend.

***Note:*** *Log settings are configured in the Access Policy Event Logs area of the product. They enable and disable logging for access system and URL request filtering events. Log settings also specify log publishers that send log messages to specified destinations.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click the name of the access profile that you want to edit.

The properties screen opens.

3. On the menu bar, click **Logs**.
   The access profile log settings display.
4. Move log settings between the **Available** and **Selected** lists.

   You can assign up to three log settings that enable access system logging to an access profile. You can assign additional log settings to an access profile provided that they enable logging for URl request logging only.

   ***Note:*** *Logging is disabled when the* ***Selected*** *list is empty.*

5. Click **Update**.

An access profile is in effect when it is assigned to a virtual server.

## 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 Secure Web Gateway (SWG) 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 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 SSL Server 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 Policy** > **Access Profiles**.
   The Access Profiles List 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 action 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 access 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 access 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 access 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 access 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

The Secure Web Gateway (SWG) transparent proxy configuration is ready to process web traffic from remote access clients.

## About configuration elements for transparent forward proxy (remote access)

When you configure Secure Web Gateway (SWG) 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 SWG configuration, SWG wildcard virtual servers must listen on the secure connectivity interface for traffic from remote access clients.

### Per-request policy

In any SWG 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 in the SWG 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`<br>***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 |

# Per-Request Policy Examples for SWG

## SSL bypass example

This example is for use in an SSL forward proxy configuration. In it, a per-request policy bypasses all SSL traffic from users in the Directors group. For other users, the policy bypasses SSL traffic only if it falls into a category that raises privacy concerns, such as one in which financial data might be accessed. After a determination about whether to bypass or intercept SSL traffic is complete, the policy can then move from processing HTTPS data to processing the HTTP data in the SSL payload.

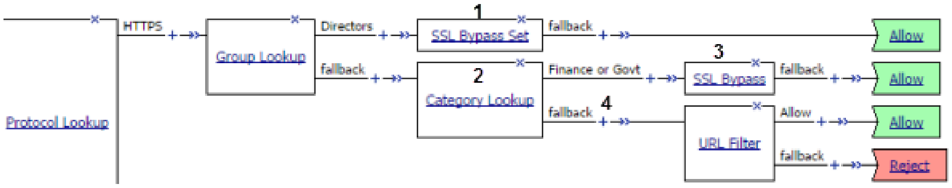


**Figure 12: SSL bypass decision based on group membership and URL category**

| | |
|---|---|
| 1 | For directors, do not intercept and inspect any SSL request. To bypass the traffic, use the SSL Bypass Set item. |
| 2 | To use Category Lookup to process HTTPS traffic, you must configure it to use SNI or Subject.CN input. |
| 3 | For users that are not in the Directors group, do not intercept and inspect SSL requests that contain private information. Bypass the traffic by inserting the SSL Bypass Set item. |
| 4 | After the policy completes HTTPS processing, you can start to process HTTP data. Continue with actions, such as URL Filter Assign or Application Lookup, that inspect the SSL payload. The URL Filter Assign item determines whether to allow, block, or confirm 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**.)

## URL filter per user group example

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

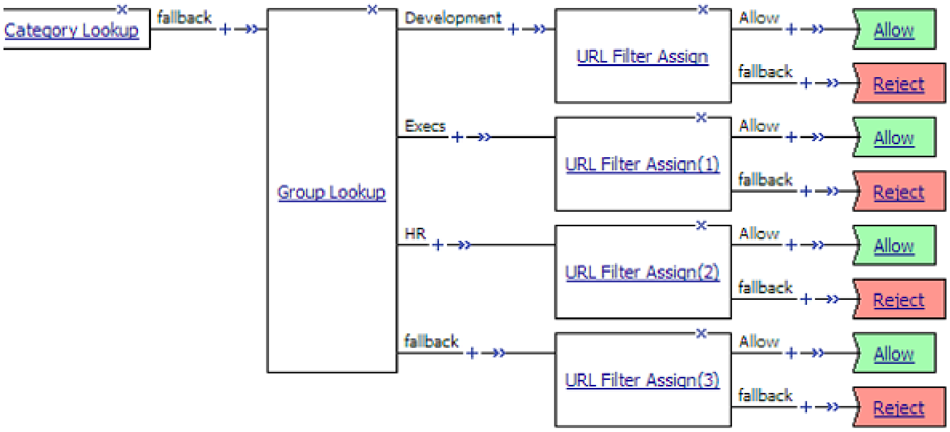


**Figure 13: URL filter based on group membership**

## Access control by date, time, and user group example

This per-request policy example applies specific URL filters for weekends and weeknights, and restricts access during work hours based on user group.

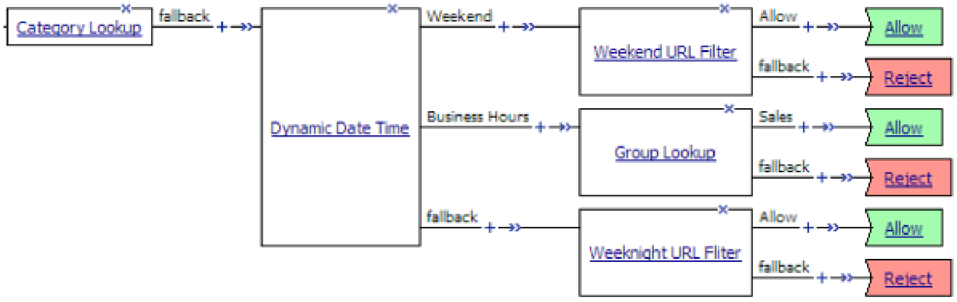


**Figure 14: Deny or allow access based on date and time and group membership**

## Response Analytics example

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.

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.

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

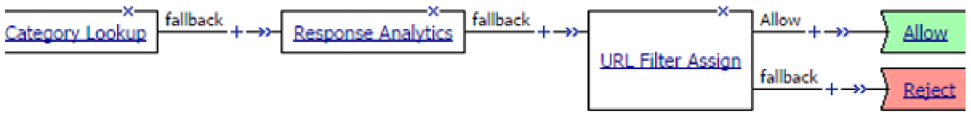


**Figure 15: Process of Response Analytics contributing analysis results to URL filter assign**

## Category-specific access control example

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.

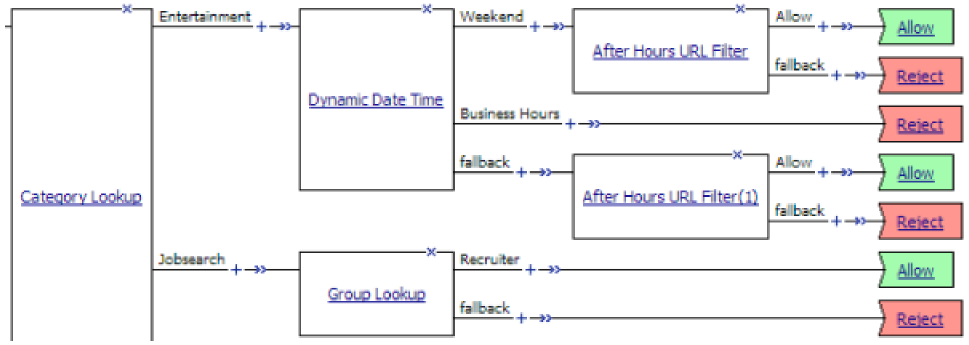


**Figure 16: Category-specific access restrictions**

## Application lookup and filter example

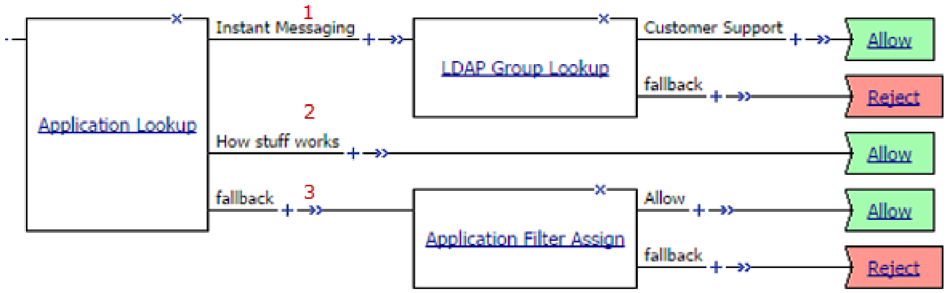


**Figure 17: Application access control by application family, application name, and application filter**

| | |
|---|---|
| 1 | A user-defined branch for the instant messaging application family. |
| 2 | A user-defined branch for a specific application. |
| 3 | The default fallback branch, on which an application filter is applied. Application Filter Assign needs the information provided by Application Lookup. |

## Confirm request subroutine example

In this per-request policy example, a subroutine that displays a **Confirm Box** follows the Confirm branch after the **URL Filter Assign** item.

***Note:*** *A subroutine starts a subsession in which the user must respond interactively.*

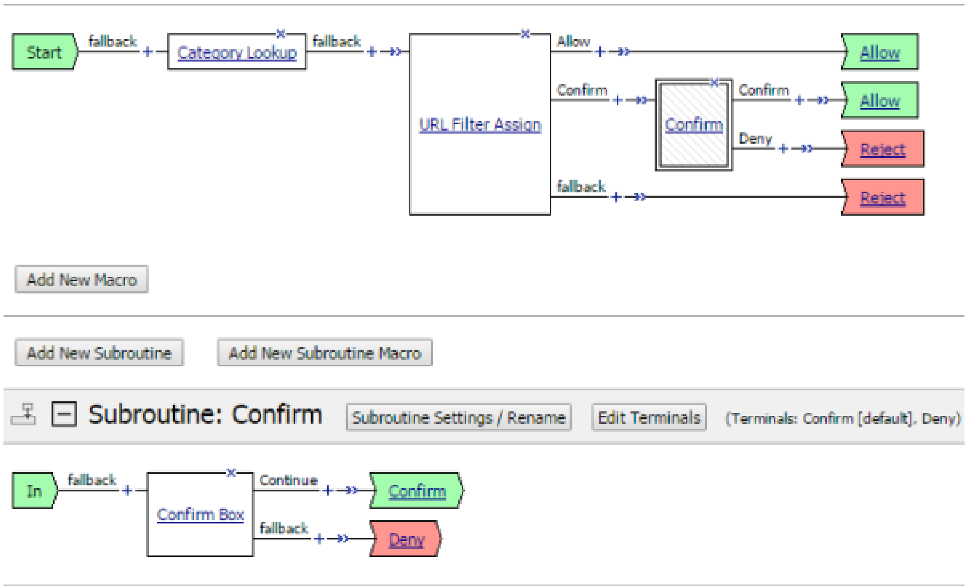


Figure 18: Per-request policy with subroutine to present Confirm Box

## Additional authentication subroutine example

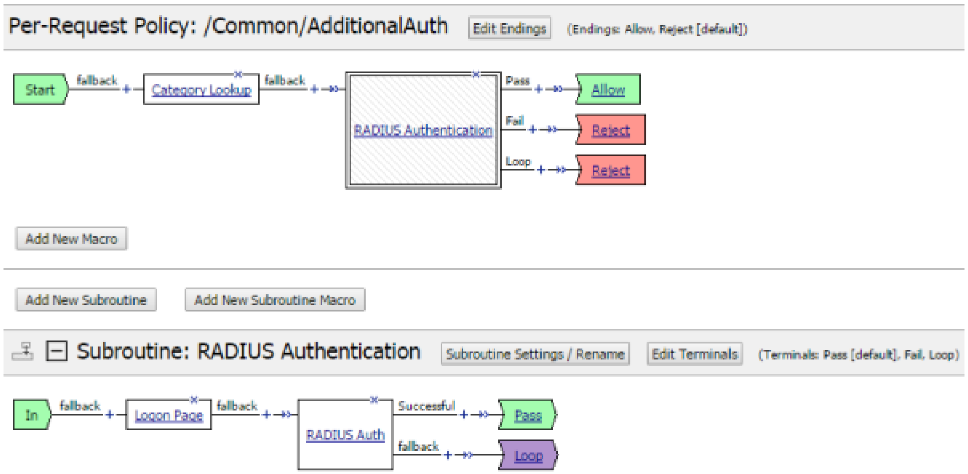


Figure 19: Per-request policy with subroutine for additional authentication

***Note:*** *A **Loop** terminal provides the user with multiple logon attempts. The subroutine exits on the **Loop** terminal only if no authentication attempt succeeds.*

# Per-Request Policy Configuration for SWG

## Overview: Configuring a per-request policy for SWG

A per-request policy must specify the logic that determines how to process URL requests whether they are requests for web access. How to make that determination is largely up to you.

To put SSL forward proxy bypass (specified in client and server SSL profiles) into effect, the per-request policy must ultimately determine whether to intercept or bypass the SSL traffic. If you plan to process SSL traffic, configure the policy to complete that processing first.

To put URL categorization into effect, the per-request policy must be configured to look up the URL category and assign the URL filter that allows or blocks URL requests.

To base processing of URL requests on a user group or user class, per-request policy items that look up a user group or user class read values stored in session variables. To ensure that the values are available, the access policy that creates the session must be configured with actions that populate the session variables.

### Task summary

After you create the per-request policy, use any of the remaining tasks to add items to it to build the per-request policy that you need.

### Task list

*Creating a per-request policy*
*Processing SSL traffic in a per-request policy*
*Configuring policies to branch by local database user group*
*Specifying URL categorization in a per-request policy*
*Requiring a user to confirm a request before obtaining access*
*Configuring a per-request policy to control access to applications*
*Configuring a per-request policy to branch by group or class*
*Blocking outgoing social media requests*

## 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 Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. Click **Create**.
   The General Properties screen displays.
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 Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. In the Access Policy column for the per-request policy that you want to update, 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 visual policy editor 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 process SSL traffic:
   - 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.

## Configuring policies to branch by local database user group

If you plan to look up local database groups from the per-request policy, you must configure local database-related items in the access policy and the per-request policy to use the same session variable.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access 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. On an access policy branch, click the **(+)** icon to add an item to the access policy.
   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
4. In the search field, type `local`, select **Local Database**, and click **Add Item**.
   A popup properties screen opens.
5. Configure properties for the Local Database action:
   a) From the **LocalDB Instance** list, select a local user database.
   b) Click **Add new entry**
      A new line is added to the list of entries with the Action set to **Read** and other default settings.
   c) In the **Destination** column in the **Session Variable** field, type the name of the variable in which to store the user groups retrieved from the local database.

      In the per-request policy, the default value that the LocalDB Group Lookup item uses is `session.localdb.groups`. If you enter a differentvalue, note it. You will need it to update the advanced expression in the LocalDB Group Lookup item in the per-request policy.
   d) In the **Source** column from the **DB Property** list, select **groups**.
   e) Click **Save**.
      The properties screen closes. The visual policy editor displays.

   This is not a complete access policy, but you can return to it and complete it later. You can close the visual policy editor or leave it open.

   The access policy includes a Local Database action that can read groups into a session variable.
6. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
7. In the Access Policy column for the per-request policy that you want to update, click the **Edit** link.
   The visual policy editor opens in another tab.
8. Click the **(+)** icon anywhere in the per-request policy to add a new item.
9. In the search field, type `local`, select **LocalDB Group Lookup**, and click **Add Item**.
   A popup properties screen opens.
10. Click the Branch Rules tab.
11. Click the **change** link in the entry for the default expression.
    A popup screen opens.
12. If the session variable you typed in the access policy Local Database action was `session.localdb.groups`, perform these substeps.
    a) In the **User is a member of** field, remove `MY_GROUP` and type the name of a group.
    b) Click **Finished**.
       The popup screen closes.
    c) Click **Save**.
       The properties screen closes and the visual policy editor displays.

13. If you typed a session variable other than `session.localdb.groups` in the access policy Local Database action, perform these substeps.
    a) Click the Advanced tab.
    In the field, this expression displays. `expression is expr { [mcget {session.localdb.groups}] contains "`*`MY_GROUP`*`" }`

    a) In the expression, replace `session.localdb.groups` with the name of the session variable you typed into the Local Database action.
    b) In the expression, replace `MY_GROUP` with the name of a group that should match a local database group.
    c) Click **Finished**.
    The popup screen closes.
    d) Click **Save**.
    The properties screen closes and the visual policy editor displays.

    This is not a complete per-request access policy, but you can return to it and complete it later.

The access and per-request policies are configured to use the same session variable. The access policy is configured to support the use of LocalDB Group Lookup in the per-request policy.

Complete the configuration of the access and per-request policies.

## Specifying URL categorization in a per-request policy

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.

***Important:*** *This task includes some references to category lookup options and policy items that are supported only on a BIG-IP® system with an SWG subscription. They are: standard categories, SafeSearch support, and content scanning (Response Analytics).*

***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 Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. In the Access Policy column for the per-request policy that you want to update, click the **Edit** link.
   The visual policy editor opens in another tab.
3. Add a **Category Lookup** item.

   ***Important:*** *A Category Lookup item triggers event logging for SWG, provides a response web page for the Response Analytics item (on systems that support it), and provides categories for the URL Filter Assign item.*

   a) Select an entry from the **Categorization Input** list based on the type of traffic to be processed. For HTTP traffic, select **Use HTTP URI (cannot be used for SSL Bypass decisions)**. For SSL-encrypted traffic, select either **Use SNI in Client Hello (if SNI is not available, use Subject.CN)** or **Use Subject.CN in Server Cert**.
   On a BIG-IP® system with an SWG subscription, if you select **Use HTTP URI (cannot be used for SSL Bypass decisions)**, the **SafeSearch Mode** list displays and **Enabled** is selected.
   b) From the **Category Lookup Type** list, select the category types in which to search for the requested URL. On a system with user-defined categories only, the **Process custom categories only** item is

the only choice. Otherwise, select one from **Custom categories first, then standard categories if not found**, **Always process full list of both custom and standard categories**, or **Process standard categories only**.

Depending on the selection, the item looks through custom categories or standard categories or both, and compiles a list of one or more categories from them. The list is available for subsequent processing by the URL Filter Assign item.

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

**4.** Add a **URL Filter Assign** item anywhere on a branch after a Category Lookup item.

In this item, you must specify a URL filter to apply to the URL categories that the Category Lookup item returned. If the filter specifies the Block action for any URL category, URL Filter Assign blocks the request. If URL Filter Assign does not block the request and the filter specifies the Confirm action for any URL category, URL Filter Assign takes the Confirm per-request policy branch.

**5.** To enable Safe Search for SSL-encrypted traffic on a BIG-IP® system with an SWG subscription, add an additional Category Lookup item with these settings:

a) Specify **Use HTTP URI (cannot be used for SSL Bypass decisions)** as the **Category Lookup Type**.
b) Retain the default setting (**Enabled**) for **SafeSearch Mode**.

**6.** To trigger inspection of the response web page contents on a BIG-IP® system with an SWG subscription, insert a **Response Analytics** item on a branch after a Category Lookup item and before a URL Filter Assign item.

The Category Lookup item supplies a response web page. The URL Filter Assign item blocks the URL request if the Response Analytics item identifies malicious content.

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.

Now the per-request policy might include items that look up the URL category and assign a URL filter. You can 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.

*Overview: Configuring a per-request policy for SWG*
*Configuring policies to branch by local database user group*
*Requiring a user to confirm a request before obtaining access*

## Requiring a user to confirm a request before obtaining access

You might want to postpone allowing access for some URL requests and disallow access unless a user confirms that the request is work-related or otherwise justified.

***Note:** Typically, a subroutine to confirm a request is placed on the Confirm branch of the **URL Filter Assign** item.*

1. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. In the Access Policy column for the per-request policy that you want to update, click the **Edit** link.
   The visual policy editor opens in another tab.
3. Click the **Add New Subroutine** button.
   A popup screen displays.
4. From the **Subroutine from template** list, select **Confirm**.
   A description of the selected template and the actions in it display.
5. Click **Save**.
   The popup screen closes. The heading (**[+] Subroutine: `Name`**) for the subroutine, displays below the main editor.
6. Expand the subroutine for editing by clicking the (+) icon in the subroutine heading.
7. Click **Subroutine Settings/Rename**.
   A popup screen displays.
8. In the **Gating Criteria** field, type the name of a per-flow variable that contains a resource or resources.

   ***Important:** If the **Gating Criteria** field remains blank, the subroutine runs once and applies the same ending to all requests for resources for the duration of the subsession.*

   ***Important:** If you specify a per-flow variable as the gating criteria for a subroutine and the per-request policy does not populate it, the subroutine is invalidated and does not run.*

   A **Category Lookup** item that runs before a subroutine populates the `perflow.category_lookup.`*`name`* variables and an **Application Lookup** item that runs before a subroutine populates the `perflow.application_lookup.`*`name`* variables.

   For example, type `perflow.category_lookup.result.url` or `perflow.application_lookup.result.families`, or the name of any documented per-flow variable that returns resources instead of a Boolean result.
9. Click **Save**.
   The popup screen closes.
10. To add a subroutine to the per-request policy, in the main editor click the (+) icon.
    A popup screen opens, displaying tabs such as General Purpose and Logon.
11. Select the Subroutines tab.
12. Select a subroutine and click **Add Item**.
    The popup screen closes. The per-request policy displays the newly added subroutine.

A per-request policy goes into effect when you add it to a virtual server.

## Configuring a per-request policy to control access to applications

Access Policy Manager® (APM®) supports a preset group of application families and applications. You can configure your own application filters or use one of the filters that APM provides: block-all, allow-all, and default.

Configure a per-request policy to specify the logic that determines whether to allow access to the applications or application families.

***Note:*** *This task provides the steps for adding items to control requests based on the application name or application family or based on an application filter. It does not specify a complete per-request policy.*

1. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. In the Access Policy column for the per-request policy that you want to update, click the **Edit** link.
   The visual policy editor opens in another tab.
3. Add an **Application Lookup** item to the 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) From the General Purpose tab, select **Application Lookup**, and click **Add Item**.
   A Properties popup screen opens.
   c) Click **Save**.
   The Properties screen closes. The visual policy editor displays. A single branch, fallback, follows the **Application Lookup** item.

4. To branch by application family or application name, add branch rules to the **Application Lookup** item.
   a) Click the name of the application lookup item.
   A Properties popup screen displays.
   b) Click the Branch Rule tab.
   c) Click **Add Branch Rule**.
   A new entry with **Name** and **Expression** settings displays.
   d) Click the **change** link in the new entry.
   A popup screen opens.
   e) Click the **Add Expression** button.
   Settings are displayed.
   f) For **Agent Sel**, select **Application Lookup**.
   g) For **Condition** select **Application Family** or **Application Name**.

   a) From the list, **Application Family is** or **Application Name is**, select a family or name.

   a) Click **Add Expression**.
   The expression displays.
   b) Continue adding branches and when you are done, click **Finished**.
   The popup screen closes. The Branch Rules popup screen displays.
   c) Click **Save**.
   The visual policy editor displays.

   Newly created branches follow the **Application Lookup** item.
5. To apply an application filter to the request, add an **Application Filter Assign** item on a branch somewhere after the Application Lookup item.
   A Properties popup screen displays.
6. From the **Application Filter** list, select an application filter and click **Save**.
   The popup screen closes.

To put the per-request policy into effect, add it to the virtual server.

***Important:*** *To support application filtering, classification must be enabled on the virtual server.*

## Configuring a per-request policy to branch by group or class

Add a group or class lookup to a per-request policy when you want to branch by user group or class.

***Note:*** *The access policy must be configured to populate session variables for a group or class lookup to succeed. This task provides the steps for adding items to branch by group or class. It does not specify a complete per-request policy.*

1. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. In the Access Policy column for the per-request policy that you want to update, 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 Authentication tab, select an option: **AD Group Lookup**, **LDAP Group Lookup**, or **RADIUS Class Lookup** to the per-request policy.
5. Click **Add Item**.
   A properties popup screen opens.
6. Click the Branch Rules tab.
7. To edit an expression, click the **change** link.
   An additional popup screen opens, displaying the Simple tab.
8. Edit the default simple expression to specify a group or class that is used in your environment.
   In an LDAP Group Lookup item, the default simple expression is **User is a member of** `CN=MY_GROUP, CN=USERS, CN=MY_DOMAIN`. You can use the simple expression editor to replace the default values.
9. Click **Finished**.
   The popup screen closes.
10. Click **Save**.
    The popup screen closes. The visual policy editor displays.

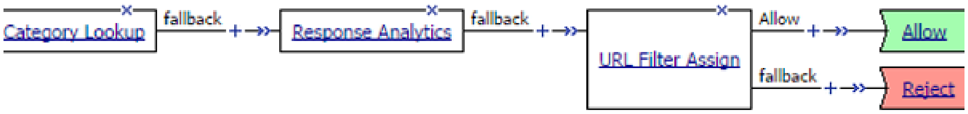
A per-request policy goes into effect when you add it to a virtual server.

## Blocking outgoing social media requests

This configuration is specific to a BIG-IP® system with an SWG subscription only.

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

1. Open a per-request policy for editing.
   For example, open a policy that already includes Response Analytics and URL Filter Assign items.



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. Click the **(+)** icon on the branch after the newly added **Request Analytics** item.
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.

*Overview: Configuring a per-request policy for SWG*

*Configuring a per-request policy to branch by group or class*

*Overview: Requiring additional authentication for sensitive resources*

## 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 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:

- Category Lookup, if configured to use HTTP URI for input
- Response Analytics
- URL Filter Assign
- HTTP Headers
- Application Lookup
- Application Filter Assign

## 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 how to trigger URL request event logging

Unless a per-request policy includes and executes a Category Lookup item, URL request event logging does not occur.

## 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.*

# Overview: Requiring additional authentication for sensitive resources

Typically, an access policy verifies endpoint security and authenticates a user before starting an access session. If the user requests access to a sensitive resource after the session is established, you can require additional authentication or revalidation of the credentials for that resource by configuring a per-request policy subroutine.

### Task summary

*Configuring a per-request policy subroutine*
*Specifying resources for the subroutine to validate and protect*
*Configuring multiple logon attempts for a subroutine*
*Adding a subroutine to a per-request policy*

## Configuring a per-request policy subroutine

Configure a per-request policy subroutine to prepare it for use in the per-request policy.

1. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. In the Access Policy column for the per-request policy that you want to update, click the **Edit** link.
   The visual policy editor opens in another tab.

3. Click the **Add New Subroutine** button.
   A popup screen displays.
4. To preview the available templates, select them one at a time from the **Subroutine from template** list.
   A description of the selected template and the items in it display.
5. Select a template and click **Save**.
   The popup screen closes. The subroutine, with the heading **[+] Subroutine: `Name`**, displays below the main editor.
6. Expand the subroutine by clicking the [+] icon.

   A red asterisk displays by the name of any item that needs some configuration.
7. Edit the properties of any item as needed.

   If the subroutine includes an AAA authentication item, you must specify an AAA server in the item properties.

Configure any additional items that you require in the subroutine.

## Specifying resources for the subroutine to validate and protect

Configure the gating criteria for a per-request policy subroutine to specify the resources associated with the subroutine.

***Note:*** *When a subsession for matching resources exists, Access Policy Manager® does not run the subroutine again, but takes the same branch that the subroutine took the last time that it ran.*

1. With the per-request policy open in the visual policy editor, expand the subroutine for editing by clicking the (+) icon in the subroutine heading.

   The heading ([+] Subroutine: `Name`) for the subroutine, displays below the main editor.
2. Click **Subroutine Settings/Rename**.
   A popup screen displays.
3. In the **Gating Criteria** field, type the name of a per-flow variable that contains a resource or resources.

   ***Important:*** *If the **Gating Criteria** field remains blank, the subroutine runs once and applies the same ending to all requests for resources for the duration of the subsession.*

   ***Important:*** *If you specify a per-flow variable as the gating criteria for a subroutine and the per-request policy does not populate it, the subroutine is invalidated and does not run.*

   A **Category Lookup** item that runs before a subroutine populates the `perflow.category_lookup.`*`name`* variables and an **Application Lookup** item that runs before a subroutine populates the `perflow.application_lookup.`*`name`* variables.

   For example, type `perflow.category_lookup.result.url` or `perflow.application_lookup.result.families`, or the name of any documented per-flow variable that returns resources instead of a Boolean result.
4. Click **Save**.
   The popup screen closes.

The subroutine is ready to be added to the per-request policy.

## Configuring multiple logon attempts for a subroutine

If you are configuring a per-request policy subroutine to obtain additional authentication and you want to provide users with more than one chance to supply credentials, you must configure and assign a **Loop** terminal.

***Note:*** *When you configure the properties for an authentication item in a subroutine, a property to enable multiple logon attempts is not available.*

1. With the per-request policy open in the visual policy editor, expand the subroutine for editing by clicking the (+) icon in the subroutine heading.

   The heading ([+] Subroutine: `Name`) for the subroutine, displays below the main editor.
2. If **Loop** does not display in the list of terminals in the heading, add a **Loop** terminal:
   a) Click **Subroutine Settings/Rename**.
   A popup screen displays.
   b) From the **Maximum Macro Loop Count** list, select a value greater than **1**.

   The maximum value is **5**.

   c) Click **Save**.
   The popup screen closes. **Loop** displays in the subroutine heading on the list of terminals.
3. To create a loop on a branch in the subroutine:
   a) Click the name of an existing terminal.
   A popup screen displays.
   b) Select **Loop**.
4. Click **Save**.

   ***Note:*** *When you specify **Loop** as a terminal, it enables repetition of the actions on the branch for up to the specified count. An action that does not complete successfully after the maximum count exits through the **Loop** terminal onto a **Loop** branch.*

   The popup screen closes.

## Adding a subroutine to a per-request policy

Put the subroutine that you configured to use by adding it to the per-request policy.

1. With the per-request policy open in the visual policy editor, click the (+) icon on a per-request policy branch.
   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
2. Select the Subroutines tab.
3. Select a subroutine and click **Add Item**.
   The popup screen closes and the per-request policy displays in the visual policy editor.

Ensure that the per-request policy includes an action that populates the gating criteria specified in the subroutine properties.

## Requesting authentication periodically throughout a session

Check the value of the **Maximum Session Timeout** setting in the access profile. If it is zero (0), this procedure cannot work.

Configure the subroutine so that it runs periodically during a session, forcing the user to reauthenticate to gain access to resources.

1. With the per-request policy open in the visual policy editor, expand the subroutine for editing by clicking the (+) icon in the subroutine heading.

   The heading ([+] Subroutine: `Name`) for the subroutine, displays below the main editor.
2. Click **Subroutine Settings/Rename**.
   A popup screen displays.
3. In the **Max Subsession Life (sec)** field, type a number that is less than the maximum session timeout specified in the access profile.

   The default maximum timeout for a session is one week, 604800 seconds.

   For example, if the session times out after a week and you want users to authenticate every day, type `86400`.
4. In the **Gating Criteria** field, type the name of a per-flow variable that contains a resource or resources.

   ***Important:*** *If the **Gating Criteria** field remains blank, the subroutine runs once and applies the same ending to all requests for resources for the duration of the subsession.*

   ***Important:*** *If you specify a per-flow variable as the gating criteria for a subroutine and the per-request policy does not populate it, the subroutine is invalidated and does not run.*

   A **Category Lookup** item that runs before a subroutine populates the `perflow.category_lookup.name` variables and an **Application Lookup** item that runs before a subroutine populates the `perflow.application_lookup.name` variables.

   For example, type `perflow.category_lookup.result.url` or `perflow.application_lookup.result.families`, or the name of any documented per-flow variable that returns resources instead of a Boolean result.
5. Click **Save**.
   The popup screen closes.

The subroutine is ready to be added to the per-request policy.

# Per-Request Policy Reference

## About access and per-request policies

Access Policy Manager® (APM®) provides two types of policies.

**Access policy**

The access policy runs when a client initiates a session. Depending on the actions you include in the access policy, it can authenticate the user and perform group or class queries to populate session variables with data for use throughout the session.

**Per-request policy**

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

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

### About per-request policies and the Apply Access Policy link

The Apply Access Policy link has no effect on a per-request policy. Conversely, updates made to a per-request policy do not affect the state of the Apply Access Policy link.

### About per-request policies and nested macros

Access Policy Manager® (APM®) supports calling a macro from a per-request policy and calling a subroutine macro from a per-request policy subroutine. However, APM does not support calling any type of macro from a per-request policy macro or from a per-request policy subroutine macro.

## About per-request policy subroutines

A per-request policy *subroutine* is a collection of actions. What distinguishes a subroutine from other collections of actions (such as macros), is that a subroutine starts a subsession that, for its duration, controls user access to specified resources. Subroutine properties not only specify resources but also specify subsession timeout values and maximum subsession duration.

### About subsessions

A *subsession* starts when a subroutine runs and continues until reaching the maximum lifetime specified in the subroutine properties, or until the session terminates. A subsession does not count against license limits. A subsession populates subsession variables that are available for the duration of the subsession. Subsession variables and events that occur during a subsession are logged. Multiple subsessions can exist at the same time.

### About typical per-request policy subroutine uses

A typical use for a per-request subroutine is to request additional authentication from a user after a period of time or before granting access to sensitive resources. Another typical use is to request confirmation from a user before granting access to URLs in a Secure Web Gateway (SWG) forward proxy configuration.

## About per-request policy items

When configuring a per-request policy, a few access policy items are available for inclusion in the policy. Most per-request policy items are unique to a per-request policy.

### About Protocol Lookup

A Protocol Lookup item determines whether the protocol of the request is HTTP or HTTPS. It provides two default branches: HTTPS and fallback. Use the Protocol Lookup item early in a per-request policy to process HTTPS traffic before processing HTTP traffic.

### About SSL Bypass Set

The SSL Bypass Set item provides a read-only element, **Action**, that specifies the **Bypass** option.

***Note:*** *For an SSL Bypass Set item to be effective, the client and server 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****; and the SSL Bypass Set item must occur in the policy before any items that process HTTP traffic.*

### About AD Group Lookup

An AD Group Lookup item can branch based on Active Directory group. The item provides one default advanced branch rule expression, `expr { [mcget {session.ad.last.attr.primaryGroupID}] == 100 }`, as an example.

A branch rule expression can include any populated session variable, such as `session.ad.last.attr.primaryGroupID`, `session.ad.last.attrmemberOf`, `session.ad.last.attr.lastLogon`, `session.ad.last.attr.groupType`, `session.ad.last.attr.member`, and so on. As an example, `expr { [mcget {session.ad.last.attr.memberOf}] contains "CN=Administrators"` is a valid expression.

***Note:*** *An AD Query action in the access policy can populate the session variables.*

## About LDAP Group Lookup

An LDAP Group Lookup item compares a specified string against the `session.ldap.last.attr.memberOf` session variable. The specified string is configurable in a branch rule. The default simple branch rule expression is `User is a member of CN=MY_GROUP, CN=USERS, CN=MY_DOMAIN` ; the values *`MY_GROUP`*, *`USERS`*, *`MY_DOMAIN`*, must be replaced with values used in the LDAP group configuration at the user site.

***Note:*** *An LDAP Query action is required in the access policy to populate the session variable.*

## About LocalDB Group Lookup

A per-request policy LocalDB Group Lookup item compares a specified string against a specified session variable.

The string is specified in a branch rule of the LocalDB Group Lookup item. The default simple branch rule expression is **User is a member of** `MY_GROUP`. The default advanced rule expression is `expression is expr { [mcget {session.localdb.groups}] contains "`*`MY_GROUP`*`" }`. In either the simple or the advanced rule, the variable, *`MY_GROUP`*, must be replaced with a valid group name.

The session variable must initially be specified and populated by a Local Database action in the access policy. A Local Database action reads groups from a local database instance into a user-specified session variable. It can be `session.localdb.groups` (used by default in the LocalDB Group Lookup advanced rule expression) or any other name. The same session variable name must be used in the Local Database action and the LocalDB Group Lookup advanced rule expression.

## About RADIUS Class Lookup

The RADIUS Class Lookup access policy item compares a user-specified class name against the `session.radius.last.attr.class` session variable. The specified class name is configurable in a branch rule.

The default simple branch rule expression is **RADIUS Class attribute contains** `MY_CLASS` . The variable *`MY_CLASS`* must be replaced with the name of an actual class.

***Note:*** *A RADIUS Acct or RADIUS Auth action is required in the access policy to populate the session variable.*

## About Dynamic Date Time

The Dynamic Date Time action enables branching based on the day, date, or time on the server. It provides two default branch rules:

**Weekend**
Defined as Saturday and Sunday.

**Business Hours**
Defined as 8:00am to 5:00pm.

The Dynamic Date Time action provides these conditions for defining branch rules.

### Time From

Specifies a time of day. The condition is true at or after the specified time.

### Time To

Specifies a time of day. This condition is true before or at the specified time.

### Date From

Specifies a date. This condition is true at or after the specified date.

### Date To

Specifies a date. This condition is true before or at the specified date

### Day of Week

Specifies a day. The condition is true for the entire day (local time zone).

### Day of Month

Specifies the numeric day of month. This condition is true for this day every month (local time zone).

## About SSL Intercept Set

The SSL Intercept Set item provides a read-only element, **Action**, that specifies the **Intercept** option.

***Note:*** *For an SSL Intercept Set item to be effective, the client and server 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****; and the SSL Intercept Set item must occur in the policy before any items that process HTTP traffic.*

## About the Logging action

The Logging action can be used in an access policy or in a per-request policy. In an access policy, the Logging action adds logging for session variables to the access policy. In a per-request policy, the Logging action can add logging for both session variables and per flow variables to the per-request policy.

This action is useful for tracing the variables that are created for a specific category, or in a specific branch.

***Note:*** *A session variable might or might not exist at the time of logging; depending on the result of the access policy branch, or results of processing the access policy.*

The Logging action provides these configuration elements and options:

### Log Message

For an access policy, specifies text to add to the log file. For a per-request policy, specifies the message text and the session and per-flow variables to add to the message. Complete variable names must be typed. Wildcards are not supported for per-request policies. An example log message for a per-request policy follows.

```
The system found this URL %{perflow.category_lookup.result.url} in these
categories %{perflow.category_lookup.result.categories} and placed it into
 this category %{perflow.category_lookup.result.primarycategory}.
```

```
An HTTPS request was made to this host
%{perflow.category_lookup.result.hostname}; the per-request policy set SSL
 bypass to %{perflow.ssl_bypass_set}.
```

```
Requests from this platform %{session.client.platform} were made during
this session %{perflow.session.id}.
```

### Session Variables

Specifies a session variable from a list of predefined session variables or a custom session variable.

***Note:*** *This option is available only when adding the Logging action to an access policy.*

## About Category Lookup

A Category Lookup item looks up URL categories for a request and obtains a web response page.

The Category Lookup item provides these elements and options.

### Categorization Input

The list specifies these options:

- **Use HTTP URI (cannot be used for SSL Bypass decisions)**: For HTTP traffic, this option specifies performing a URL-based lookup. When selected, on a BIG-IP® system with an SWG subscription the **SafeSearch Mode** setting displays.
- **Use SNI in Client Hello (if SNI is not available, use Subject.CN)**: For HTTPS traffic, this option specifies performing a host-based lookup.
- **Use Subject.CN in Server Cert**: For HTTPS traffic, this option specifies performing a host-based lookup. (This option is not for use in a reverse proxy configuration.)

### SafeSearch Mode

The options are **Enabled** (default) and **Disabled**. When enabled, SWG enables Safe Search for supported search engines.

***Note:*** *SafeSearch is available only with an SWG subscription.*

### Category Lookup Type

Select the category types in which to search for the requested URL. On a BIG-IP® system with an SWG subscription, options are:

- **Select one from Custom categories first, then standard categories if not found**
- **Always process full list of both custom and standard categories**
- **Process standard categories only**

On a BIG-IP® system without an SWG subscription, the available option is **Process custom categories only**. Depending on the selection, the Category Lookup Type item looks through custom categories or standard categories or both, and compiles a list of one or more categories from them. The list is available for subsequent processing by the URL Filter Assign item.

### Reset on Failure

When enabled, specifies that SWG send a TCP reset to the client in the event of a server failure.

## About Response Analytics

A Response Analytics item inspects a web response page for malicious embedded contents. Response Analytics must be preceded by a Category Lookup item because it obtains a web response page.

***Note:*** *Response Analytics works only on a BIG-IP® system with an SWG subscription.*

Response Analytics provides these elements and options.

### Max Buffer Size

Specifies the maximum amount of response data (in bytes) to collect before sending it for content scanning. The system sends the content for analysis when the buffer reaches this size or when the buffer contains all of the response content. Otherwise, the system retains the response data in the buffer.

### Max Buffer Time

Specifies the maximum amount of time (in seconds) for buffering and analyzing response data. If the time elapses at any point in this process, the agent sets the `perflow.response_analytics.failure` variable to 1 (which indicates an ANTserver failure) and discards the response data.

### Reset on Failure

When enabled, specifies that SWG send a TCP reset to the client in the event of an ANTserver failure. If disabled and an ANTserver failure occurs, SWG logs all perflow variables and provides the SWG block page to the client.

### Exclude Types

Specifies one entry for each type of content to be excluded from content analysis. Images, the **All-Images** type, do not get analyzed.

## About Request Analytics

A Request Analytics item inspects an outgoing web request for malicious embedded contents. In a per-request policy, a Request Analytics item must be preceded by a Category Lookup item and followed by a URL Filter Assign item. To block outgoing traffic from chat applications, a Request Analytics item is required.

***Note:*** *Request Analytics works only on a BIG-IP® system with an SWG subscription.*

Request Analytics provides these elements and options.

### Max Buffer Size

Specifies the maximum amount of request data (in bytes) to collect before sending it for content scanning. The system sends the content for analysis when the buffer reaches this size or when the buffer contains all of the request content. Otherwise, the system retains the request data in the buffer.

### Max Buffer Time

Specifies the maximum amount of time (in seconds) for buffering and analyzing request data. If the time elapses at any point in this process, the agent sets the `perflow.request_analytics.failure` variable to 1 (which indicates an ANTserver failure) and discards the request data.

**Reset on Failure**

When enabled, specifies that SWG send a TCP reset to the client in the event of an ANTserver failure. If disabled and an ANTserver failure occurs, SWG logs all perflow variables and provides the SWG block page to the client.

## About URL Filter Assign

A URL Filter Assign item looks up the URL filter action for each category that the Category Lookup item found for a request. If any filter action is set to Block, the request is blocked. In a configuration with an SWG subscription, the URL Filter Assign item also uses the analysis from the Response Analytics item, if used, to determine whether to block the request.

By default, the URL Filter Assign item has three branches: Allow, Confirm, and fallback. If the request is not blocked and any filter action is set to Confirm, the per-request policy takes the Confirm branch.

A URL Filter Assign item provides the **URL Filter** element, with a list of filters from which to select.

***Note:*** *A Category Lookup item must precede the URL Filter Assign item.*

## About Application Lookup

An Application Lookup item obtains the name of the application that is being requested and looks up the application family that matches it. By default, this item has a fallback branch only.

Application Lookup can be used to branch by application family or by application name; branch rules are required to do this. If an Application Filter Assign item is included in the per-request policy, an Application Lookup must complete before it.

## About Application Filter Assign

An Application Filter Assign item matches an application or application family against an application filter. Application Filter Assign provides one configuration element. The **Application Filter** element specifies the application filter to use in determining whether to block access to an application or allow it. The Application Filter Assign item exits on the Allow branch if the filter action specifies allow. Otherwise, Application Filter Assign exits on the fallback branch.

***Important:*** *To supply input for the Application Filter Assign agent, an Application Lookup item must run in the per-request policy sometime prior to it.*

## About HTTP Headers

An HTTP Headers action supports modifying an outgoing HTTP request to a back-end server. The action supports manipulation of HTTP and cookie headers being sent to back-end servers.

***Important:*** *The HTTP Headers item cannot manipulate HTTP cookies in outgoing HTTP requests to any portal access application.*

The HTTP Headers item provides these configuration options and elements.

An entry in the HTTP Header Modify table includes these elements.

### Header Operation

Specifies **insert**, **append**, **replace**, or **remove**.

### Header Name

Specifies the header name on which to operate.

### Header Value

Specifies the value on which to operate.

***Note:*** *Any per-flow or session variable can be used as a header value, for example,* *%{`session.user.clientip`}* *or* *%{`perflow.session.id`}.*

### Header Delimiter

Specifies the separator to use when appending a header.

An entry in the HTTP Cookie Modify table includes these elements.

### Cookie Operation

Specifies **update** or **delete**.

***Note:*** *When* ***update*** *is selected and a cookie that matches the name and value does not exist, HTTP Header adds the specified cookie.*

### Cookie Name

Specifies the name to match.

### Cookie Value

Specifies the value to match when deleting a cookie or the new value to set when updating a cookie.

***Note:*** *Any per-flow or session variable can be used as a cookie value.*

## About per-request policy subroutine items

When configuring a per-request policy subroutine, a few access policy items are available for inclusion in the subroutine. A Confirm Box action (for use with Secure Web Gateway forward proxy configurations) is unique to a per-request policy subroutine.

## Access policy and subroutine agent differences

The agents in this table are available to access policies and to per-request policy subroutines. In a per-request policy subroutine, not all options for an agent are supported and support for some options is implemented differently.

### Table 2: Per-Request Policy Subroutine Agents with Differences

| Agent | Description |
|---|---|
| HTTP 401 Response | Supports no authentication or HTTP Basic authentication only. |
| Logon Page | A **Subsession Variable** field replaces the **Session Variable** field. **Split domain from full Username** |

| Agent | Description |
|---|---|
| | and **CAPTCHA Configuration** fields do not display because the functionalities are not supported. |
| AD Auth | Support for multiple logon attempts can be implemented using a macro loop. The **Max Logon Attempts Allowed** property does not display. The **Show Extended Error** property is not supported. |
| LDAP Auth | Support for multiple logon attempts can be implemented using a macro loop. The **Max Logon Attempts Allowed** property does not display. The **Show Extended Error** property is not supported. |
| RADIUS Auth | Support for multiple logon attempts can be implemented using a macro loop. The **Max Logon Attempts Allowed** property does not display. The **Show Extended Error** property is not supported. |

## About Confirm Box

A Confirm Box action presents links for these options: **Continue** and **Cancel**. The action is available for a per-request policy subroutine only and is for use in a Secure Web Gateway (SWG) configuration. Confirm Box offers these elements and options for customization.

**Language**
Specifies the language to use to customize the Confirm Box page. Selecting a language causes the content in the remaining fields display in the selected language.

***Note:*** *Languages on the list reflect those that are configured in the access profile.*

**Message**
Specifies the message to display.

**Field 1 image**
Specifies the icon (red, green, or none) to display with the **Continue** option.

**Continue**
Specifies the text to display for this option.

**Field 2 image**
Specifies the icon (red, green, or none) to display with the **Cancel** option.

**Cancel**
Specifies the text to display for this option.

## About AD Auth

An AD Auth action authenticates a user against an AAA Active Directory server. In an access policy, an authentication action typically follows a logon action that collects credentials.

***Note:*** *When configured in a per-request subroutine, some screen elements and options described here might not be available.*

### Type

Specifies Authentication, the type of this Active Directory action.

### Server

Specifies an Active Directory server; servers are defined in the Access Policy AAA servers area of the Configuration utility.

### Cross Domain Support

Specifies whether AD cross domain authentication support is enabled for this action.

### Complexity check for Password Reset

Specifies whether Access Policy Manager® (APM®) performs a password policy check. APM supports these Active Directory password policies:

- Maximum password age
- Minimum password age
- Minimum password length
- Password must meet complexity requirements

APM must retrieve all related password policies from the domain to make the appropriate checks on the new password.

***Note:*** *Because this option might require administrative privileges, the administrator name and password might be required on the AAA Active Directory server configuration page.*

***Note:*** *Enabling this option increases overall authentication traffic significantly because APM must retrieve password policies using LDAP protocol and must retrieve user information during the authentication process to properly check the new password.*

### Show Extended Error

When enabled, causes comprehensive error messages generated by the authentication server to display on the user's logon page. This setting is intended only for use in testing, in a production or debugging environment. If enabled in a live environment, your system might be vulnerable to malicious attacks. (When disabled, displays non-comprehensive error messages generated by the authentication server on the user's logon page.)

### Max Logon Attempts Allowed

Specifies the number of user authentication logon attempts to allow. A complete logon and password challenge and response is considered as one attempt.

### Max Password Reset Attempts Allowed

Specifies the number of times that APM allows the user to try to reset password.

## About HTTP 401 Response

The HTTP 401 Response action sends an HTTP 401 Authorization Required Response page to capture HTTP Basic or Negotiate authentication.

***Note:*** *For a per-request policy subroutine, HTTP 401 Response supports HTTP Basic authentication only.*

The HTTP 401 Response action provides up to three branches: Basic, Negotiate, and fallback. Typically, a basic type of authentication follows on the Basic branch and a Kerberos Auth action follows on the Negotiate branch.

An HTTP 401 Response action provides these configuration elements and options.

### Basic Auth Realm

Specifies the authentication realm for use with Basic authentication.

### HTTP Auth Level

Specifies the authentication required for the policy.

- **none** - specifies no authentication.
- **basic** - specifies Basic authentication only.
- **negotiate** - specifies Kerberos authentication only.

  ***Note:*** *This option is not available for a per-request policy subroutine.*
- **basic+negotiate** - specifies either Basic or Kerberos authentication.

  ***Note:*** *This option is not available for a per-request policy subroutine.*

The action provides customization options that specify the text to display on the screen.

### Language

Specifies the language to use to customize this HTTP 401 response page. Selecting a language causes the content in the remaining fields display in the selected language.

***Note:*** *Languages on the list reflect those that are configured in the access profile.*

### Logon Page Input Field #1

Specifies the text to display on the logon page to prompt for input for the first field. When **Language** is set to **en**, this defaults to `Username`.

### Logon Page Input Field #2

Specifies the text to display on the logon page to prompt for input for the second field. When **Language** is set to **en**, this defaults to `Password`.

### HTTP response message

Specifies the text that appears when the user receives the 401 response, requesting authentication.

## About iRule Event

An iRule Event action adds iRule processing to an access policy or to a per-request policy subroutine at a specific point. An iRule Event provides one configuration option: ID, which specifies an iRule event ID.

***Note:*** *iRule event access policy items must be processed and completed before the access policy can continue.*

An iRule Event action can occur anywhere in an access policy or a per-request policy subroutine.

## About LDAP Auth

An LDAP Auth action authenticates a user against an AAA LDAP server. An LDAP Auth action provides these configuration elements and options.

***Note:*** *When configured in a per-request subroutine, some screen elements and options described here might not be available.*

### Type

Specifies Authentication, the type of this LDAP action.

### Server

Specifies an LDAP server; servers are defined in the Access Policy AAA servers area of the Configuration utility.

### SearchDN

Specifies the base node of the LDAP server search tree to start the search with.

### SearchFilter

Specifies 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. Parentheses are required around search strings; (`sAmAccountName=%{session.logon.last.username}`)

### UserDN

Specifies the Distinguished Name (DN) of the user. The DN can be derived from session variables.

### Show Extended Error

When enabled, causes comprehensive error messages generated by the authentication server to display on the user's logon page. This setting is intended only for use in testing, in a production or debugging environment. If enabled in a live environment, your system might be vulnerable to malicious attacks. (When disabled, displays non-comprehensive error messages generated by the authentication server on the user's logon page.)

### Max Logon Attempts Allowed

Specifies the number of user authentication logon attempts to allow. A complete logon and password challenge and response is considered as one attempt.

## About Logon Page

A logon page action prompts for a user name and password, or other identifying information. The logon page action typically precedes the authentication action that checks the credentials provided on the logon page. The logon page action provides up to five customizable fields and enables localization.

The logon page action provides these configuration options and elements.

***Note:*** *When configured in a per-request subroutine, some screen elements and options described here might not be available.*

### Split domain from full username

Specifies **Yes** or **No**.

- **Yes** - specifies that when a username and domain combination is submitted (for example, `marketing\jsmith` or `jsmith@marketing.example.com`), only the username portion (in this example, `jsmith`) is stored in the session variable `session.logon.last.username`.
- **No** - specifies that the entire username string is stored in the session variable.

### CAPTCHA configuration

Specifies a CAPTCHA configuration to present for added CAPTCHA security on the logon page.

### Type

Specifies the type of logon page input field: **text**, **password**, **select**, **checkbox**, or **none**.

- **text** Displays a text field, and shows the text that is typed in that field.
- **password** Displays an input field, but displays the typed text input as asterisks.

- **select** Displays a list. The list is populated with values that are configured for this field.
- **checkbox** Displays a check box.
- **none** Specifies that the field is not displayed on the logon page.

### Post Variable Name

Specifies the variable name that is prepended to the data typed in the text field. For example, the POST variable **username** sends the user name input `omaas` as the POST string `username=omaas`.

### Session Variable Name (or Subsession Variable Name)

Specifies the session variable name that the server uses to store the data typed in the text field. For example, the session variable **username** stores the username input `omaas` as the session variable string `session.logon.last.username=omaas`.

***Note:*** *A per-request policy subroutine uses subsession variables in place of session variables.*

### Values

Specifies values for use on the list when the input field type is **select**.

### Read Only

Specifies whether the logon page agent is read-only, and always used in the logon process as specified. You can use **Read Only** to add logon POST variables or session variables that you want to submit from the logon page for every session that uses this access policy, or to populate a field with a value from a session variable. For example, you can use the On-Demand Certificate agent to extract the **CN** (typically the user name) field from a certificate, then you can assign that variable to **session.logon.last.username**. In the logon page action, you can specify `session.logon.last.username` as the session variable for a read only logon page field that you configure. When Access Policy Manager® displays the logon page, this field is populated with the information from the certificate **CN** field (typically the user name).

Additionally, customization options specify text and an image to display on the screen.

### Language

Specifies the language to use to customize this logon page. Selecting a language causes the content in the remaining fields to display in the selected language.

***Note:*** *Languages on the list reflect those that are configured in the access profile.*

### Form Header Text

Specifies the text that appears at the top of the logon box.

### Logon Page Input Field # *`number`*

Specifies the text to display for each input field (number 1 through 5) that is defined in the Logon Page Agent area with **Type** set to other than **none**.

### Logon Button

Specifies the text that appears on the logon button, which a user clicks to post the defined logon agents.

### Front Image

Specifies an image file to display on the logon page. The **Replace Image** link enables customization and the **Revert to Default Image** discards any customization and use the default logon page image.

### Save Password Check Box

Specifies the text that appears adjacent to the check box that allows users to save their passwords in the logon form. This field is used only in the secure access client, and not in the web client.

### New Password Prompt

Specifies the prompt displayed when a new Active Directory password is requested.

### Verify Password Prompt

Specifies the prompt displayed to confirm the new password when a new Active Directory password is requested.

### Password and Password Verification do not Match

Specifies the prompt displayed when a new Active Directory password and verification password do not match.

### Don't Change Password

Specifies the prompt displayed when a user should not change password.

## About On-Demand Cert Auth

Typically, when a client makes an HTTPS request, an SSL handshake request occurs at the start of an SSL session. If the client SSL profile skips the initial SSL handshake, an On-Demand Cert Auth action can re-negotiate the SSL connection from an access policy by sending a certificate request to the user. This prompts a certificate screen to open. After the user provides a valid certificate, the On-Demand Cert Auth action checks the result of certificate authentication. The agent verifies the value of the session variable `session.ssl.cert.valid` to determine whether authentication was a success.

The On-Demand Cert Auth action provides one configuration option, **Auth Mode**, with two supported modes:

### Request

With this mode, the system requests a valid certificate from the client, but the connection does not terminate if the client does not provide a valid certificate. Instead, this action takes the fallback route in the access policy. This is the default option.

### Require

With this mode, the system requires that a client provides a valid certificate. If the client does not provide a valid certificate, the connection terminates and the client browser stops responding.

***Note:*** *For an iPod or an iPhone, the **Require** setting must be used for On-Demand certificate authentication. To pass a certificate check using Safari, the user is asked to select the certificate multiple times. This is expected behavior.*

***Note:*** *On-demand certificate authentication does not work when added to a subroutine for a per-request policy that is part of a forward proxy configuration.*

## About RADIUS Auth

A RADIUS Auth action authenticates a client against an external RADIUS server. A RADIUS Auth action provides these configuration elements and options.

***Note:*** *When configured in a per-request subroutine, some screen elements and options described here might not be available.*

### AAA Server

Specifies the RADIUS accounting server; servers are defined in the Access Policy AAA servers area of the Configuration utility.

**Show Extended Error**

When enabled, causes comprehensive error messages generated by the authentication server to display on the user's logon page. This setting is intended only for use in testing, in a production or debugging environment. If enabled in a live environment, your system might be vulnerable to malicious attacks. (When disabled, displays non-comprehensive error messages generated by the authentication server on the user's logon page.)

**Max Logon Attempts Allowed**

Specifies the number of user authentication logon attempts to allow. A complete logon and password challenge and response is considered as one attempt.

## About per-request policy endings

An ending provides a result for a per-request policy branch. An ending for a per-request policy branch is one of two types.

**Allow**

Allows the user to continue to the requested URL.

**Reject**

Blocks the user from continuing and triggers the access profile Logout screen.

## Access policy and subroutine agent differences

The agents in this table are available to access policies and to per-request policy subroutines. In a per-request policy subroutine, not all options for an agent are supported and support for some options is implemented differently.

**Table 3: Per-Request Policy Subroutine Agents with Differences**

| Agent | Description |
|---|---|
| HTTP 401 Response | Supports no authentication or HTTP Basic authentication only. |
| Logon Page | A **Subsession Variable** field replaces the **Session Variable** field. **Split domain from full Username** and **CAPTCHA Configuration** fields do not display because the functionalities are not supported. |
| AD Auth | Support for multiple logon attempts can be implemented using a macro loop. The **Max Logon Attempts Allowed** property does not display. The **Show Extended Error** property is not supported. |
| LDAP Auth | Support for multiple logon attempts can be implemented using a macro loop. The **Max Logon Attempts Allowed** property does not display. The **Show Extended Error** property is not supported. |
| RADIUS Auth | Support for multiple logon attempts can be implemented using a macro loop. The **Max Logon** |

| Agent | Description |
|---|---|
|  | **Attempts Allowed** property does not display. The **Show Extended Error** property is not supported. |

## Per-flow and subsession variables

Per-flow variables exist only while a per-request policy runs. Per-flow variables for a per-request policy subroutine exist while the subsession exists. Multiple subsessions can run simultaneously. The table lists per-flow variables and their values.

| Name | Value |
|---|---|
| `perflow.agent_ending.result` | `0` (success) or `1` (failure). |
| `perflow.application_lookup.result.families` | Comma-separated list of application families. |
| `perflow.application_filter_lookup.result.action` | `0` (reject) or `1` (allow). |
| `perflow.application_lookup.result.effective_application` | Name of the application that is ultimately used. |
| `perflow.application_lookup.result.effective_family` | Name of the application family that is ultimately used. |
| `perflow.application_lookup.result.names` | Comma-separated list of application names. |
| `perflow.application_lookup.result.primary_application` | Name of the application that APM® determines is the primary one. |
| `perflow.application_lookup.result.primary_family` | Name of the application family that Access Policy Manager® (APM) determines is the primary one. (An application might fit into more than one application family.) |
| `perflow.bypass_lookup.result.ssl` | `0` (http) or `1` (https). |
| `perflow.category_lookup.failure` | `0` (success) or `1` (server failure). |
| `perflow.category_lookup.result.categories` | Comma-separated list of categories. |
| `perflow.category_lookup.result.customcategory` | Unique number that identifies a custom category; used internally. |
| `perflow.category_lookup.result.effective_category` | Name of the category that is ultimately used. |
| `perflow.category_lookup.result.filter_name` | Name of the URL filter. |
| `perflow.category_lookup.result.hostname` | Host name retrieved from SSL input. |
| `perflow.category_lookup.result.numcategories` | Integer. Total number of categories in the comma-separated list of categories. |
| `perflow.category_lookup.result.primarycategory` | Name of the category that APM determines is the primary one. (A URL might fit into more than one category, such as news and sports.) |
| `perflow.category_lookup.result.url` | Requested URL. |
| `perflow.protocol_lookup.result` | `http` or `https`. Defaults to https. |
| `perflow.response_analytics.failure` | `0` (success) or `1` (server failure). |
| `perflow.session.id` | Session ID. |
| `perflow.ssl_bypass_set` | `0` (bypass) or `1` (intercept). SSL Bypass Set and SSL Intercept Set items update this value. |

| Name | Value |
|---|---|
| `perflow.ssl.bypass_default` | `0` (bypass) or `1` (intercept). Specified in the client SSL profile, used when SSL Bypass Set and SSL Intercept Set items not included in per-request policy. |
| `perflow.urlfilter_lookup.result.action` | `0` (reject) or `1` (allow). |
| `perflow.username` | User name. |
| `perflow.on_demand_cert.result` | `0` (success) or `1` (failure) of On-Demand Certificate authentication in the subroutine. |
| `perflow.decision_box.result` | `0` (continue) or `1` (cancel) selected for the Confirm Box action in the subroutine. |
| `perflow.subroutine.out_terminal` | Name of the subroutine out terminal. |
| `perflow.subroutine.invalidated` | `0` (validated) or `1` (invalidated) subroutine. |
| `perflow.subroutine.loop_countdown` | Number of iterations remaining on a subroutine loop. |
| `subsession.logon.last.username` | User name for the last login. |
| `subsession.logon.last.authtype` | Last authentication type |
| `subsession.ad.last.actualdomain` | Domain name for the last login. |
| `subsession.ad.last.authresult` | `0` (success) or `1` (failure) of Active Directory authentication in the subroutine. |
| `subsession.ad.last.errmsg` | Displays the error message for the last login. |
| `subsession.ldap.last.authresult` | `0` (success) or `1` (failure) of LDAP authentication in the subroutine. |
| `subsession.ldap.last.errmsg` | Displays the error message for the last login. |
| `subsession.radius.last.attr.filter-id` | RADIUS attribute filter ID |
| `subsession.radius.last.attr.framed-compression` | RADIUS attribute framed compression |
| `subsession.radius.last.attr.framed-mtu` | RADIUS attribute framed MTU |
| `subsession.radius.last.attr.framed-protocol` | RADIUS attribute framed protocol |
| `subsession.radius.last.attr.service-type` | RADIUS attribute service type. |
| `subsession.radius.last.errmsg` | Displays the error message for the last login. |
| `subsession.radius.last.result` | `0` (success) or `1` (failure) of RADIUS authentication in the subroutine. |

## Customizing messages for the per-request policy Reject ending

You need an access profile configured.

Customize the messages to display when a per-request policy terminates on a Reject ending. When this happens, the per-request policy triggers the access profile Logout screen.

1. On the Main tab, click **Access Policy** > **Customization** > **General**.
   The Customization tool appears in General Customization view, displaying **Form Factor: Full/Mobile Browser** settings.
2. In the left pane, click the Text tab.

A navigation tree displays in the left pane.

3. Expand the **Access Profiles** folder.
   Folders for access profiles that are configured on the BIG-IP® system in the current partition display.
4. Expand the folder for access profile that you want to update.
   Folders for access profile objects display.
5. Expand the **Logout** folder for the access profile.
   The **General** setting displays in the folder.
6. Click **General**.
   Message settings display in the right pane.
7. In the right pane, update values.
8. On the menu bar, click **Save**.
9. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.
10. On the list of access profiles to apply, verify that the access profile that you updated is selected.
11. Click the **Apply Access Policy** button.

## Exporting and importing a per-request policy across BIG-IP systems

Export a per-request policy from one BIG-IP® system and import it on another (at the same product version level) to copy a policy across systems.

***Note:*** *Per-request policy import does not support the import of custom categories or the URLs defined for them. Before you import a per-request policy from one BIG-IP system to another BIG-IP system, you must first list any custom categories configured on the source system and make sure you have the same custom categories on the target system. Otherwise, import will fail.*

1. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
2. Click the link in the **Export** column for the policy that you want to export.
   A file downloads.
3. Note the list of custom categories:
   a) Click **Access Policy** > **Secure Web Gateway** > **URL Categories**.
   b) Expand the Custom Categories list.
4. Log in to the Configuration utility on the BIG-IP system where you want to import the per-request policy.
5. Verify that the custom categories that exist on the other BIG-IP system also exist on this BIG-IP system:
   a) Click **Access Policy** > **Secure Web Gateway** > **URL Categories**.
   b) Expand the Custom Categories list.
   c) Create any additional custom categories needed to match the list on the other BIG-IP system.

      The import process does not add URLs to custom categories. To include the URLs defined for a custom category on the source system, you can add them to the target system now or wait until after you import the per-request policy.
6. On the Main tab, click **Access Policy** > **Per-Request Policies**.
   The Per-Request Policies screen opens.
7. Click **Import**.
   An Import Policy screen displays.

8. In **New Policy Name**, type a name.
9. For **Config File Upload**, click **Browse**, locate and select the file downloaded from the other BIG-IP system.
10. To reuse objects already existing on this BIG-IP system, select the **Reuse Existing Objects** check box.
11. Click **Import**.

# Reports, Logs, and 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**

*About the Secure Web Gateway Overview*
*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.

*Overview: Monitoring Internet traffic for threats*
*Overview: Monitoring Internet traffic for threats*
*Configuring statistics collection for SWG reports*

## 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 Policy** > **Secure Web Gateway** > **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:*** *You can also export any single report widget from the Overview screen. Click the widget configuration icon for the report and select **Export**.*

   The Choose Export Options popup screen opens.
4. Choose the appropriate option.
   - To save the report as a PDF on your computer, select **Save the report file on your computer**.
   - To send this report to someone, select **Send the report file via E-Mail as an attachment**, select the **SMTP Server**, and **Target E-Mail Address(es)**.
5. Click **Export**.
   The system saves the report to a file, or emails the file to the specified recipients. If SMTP is not configured (when sending reports by email), you receive a message that SMTP must be set up before you can send the reports.

## 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.

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 the time period 12:35-13:35. 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.*

## 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. |

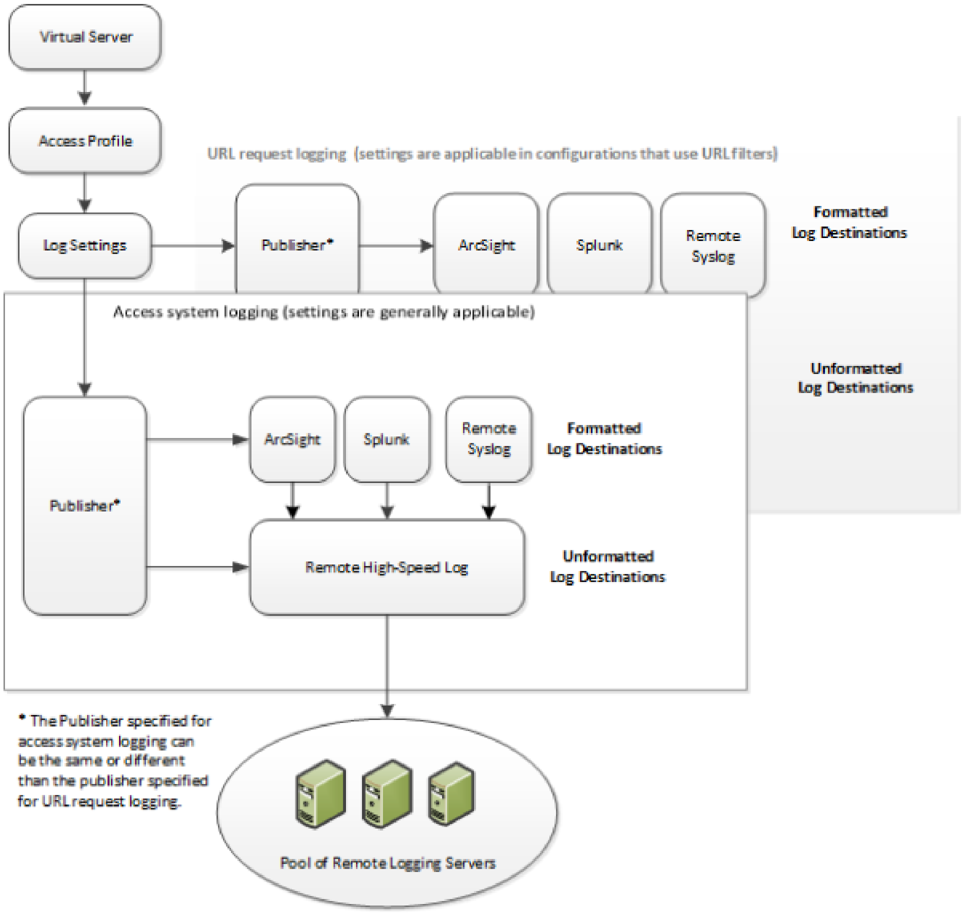

Virtual Server
Access Profile
Log Settings
URL request logging (settings are applicable in configurations that use URL filters)
Publisher*
ArcSight
Splunk
Remote Syslog
Formatted Log Destinations
Unformatted Log Destinations
Access system logging (settings are generally applicable)
Publisher*
ArcSight
Splunk
Remote Syslog
Formatted Log Destinations
Remote High-Speed Log
Unformatted Log Destinations
* The Publisher specified for access system logging can be the same or different than the publisher specified for URL request logging.
Pool of Remote Logging Servers

**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**, 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** 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 Policy** > **Event Logs** > **Log Settings**.
   A log settings table displays.
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. |

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 Policy** > **Access Profiles**.
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.*

# APM log example

The table breaks a typical Access Policy Manager® (APM®) log entry into its component parts.

### An example APM log entry

```
Feb  2 12:37:05 site1 notice tmm[26843]: 01490500:5: /Common/for_reports:Common:
 bab0ff52: New session from
client IP 10.0.0.1 (ST=/CC=/C=) at VIP 20.0.0.1 Listener /Common/site1_http
(Reputation=Unknown)
```

| Information Type | Example Value | Description |
|---|---|---|
| Timestamp | **Feb 2 12:37:05** | The time and date that the system logged the event message. |
| Host name | **site1** | The host name of the system that logged the event message. Because this is typically the host name of the local machine, the appearance of a remote host name could be of interest. |
| Log level | **notice** | The text value of the log level for the message. |
| Service | **tmm** | The process that generated the event. |
| PID | **[26843]** | The process ID. |
| Log ID | **01490500** | A code that signifies the product, a subset of the product, and a message number. |
| Level | **5** | The numeric value of the log level for the message. |
| Partition | **/Common/for_reports:Common** | The partition.to which configuration objects belong. |
| Session ID | **bab0ff52** | The ID associated with the user session. |

| Information Type | Example Value | Description |
|---|---|---|
| Log message | **New session from client IP 10.0.0.1 (ST=/CC=/C=) at VIP 20.0.0.1 Listener /Common/site1_http (Reputation=Unknown)** | The generated message text. |

## About local log destinations and publishers

The BIG-IP® system provides two local logging destinations:

**local-db**
Causes the system to store log messages in the local MySQL database. Log messages published to this destination can be displayed in the BIG-IP Configuration utility.

**local-syslog**
Causes the system to store log messages in the local Syslog database. Log messages published to this destination are not available for display in the BIG-IP Configuration utility.

***Note:*** *Users cannot define additional local logging destinations.*

The BIG-IP system provides a default log publisher for local logging, sys-db-access-publisher; initially, it is configured to publish to the local-db destination and the local-syslog destination. Users can create other log publishers for local logging.

### Configuring a log publisher to support local reports

APM® provides preconfigured reports that are based on log data. To view the reports and to display log data from the BIG-IP® Configuration utility, configure a publisher to log to the local-db destination.

***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.*

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Select the log publisher you want to update and click **Edit**.
3. For the **Destinations** setting, select **local-db** from the **Available** list, and move the destination to the **Selected** list.
4. Click **Finished**.

To use a log publisher, specify it in an access policy log setting, ensure that the access profile selects the log setting, and assign the access profile to a virtual server.

***Note:*** *Log settings are configured in the* ***Access Policy*** *>* ***Event Logs*** *area of the product.*

## Viewing an APM report

If Access Policy Manager® (APM®) events are written to the local database on the BIG-IP® system, they can be viewed in APM reports.

Create a report to view event log data.

1. On the Main tab, click **Access Policy** > **Event Logs** > **Access System Logs**.

   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. (Optional) Select the appropriate **Restrict by Time** settings.
3. Click **Run Report**.
   The popup screen closes. The report displays in the Reports Browser.

You can select and run various system-provided reports, change the default report, and create custom reports.

## Viewing URL request logs

To view URL request logs from the user interface, your access profile log setting must enable URL request logs. The log setting must also specify a log publisher that publishes to the local-db log destination.

You can display, search, and export URL request logs.

1. On the Main tab, click **Access Policy** > **Event Logs** > **URL Request Logs**.

   Any logs for the last hour are displayed.

   ***Note:*** *APM® writes logs for blocked requests, confirmed requests, allowed requests, or all three, depending on selections in the access profile log setting.*
2. To view logs for another time period, select it from the list.
3. To search the logs, type into the field and click **Search** or click **Custom Search** to open a screen where you can specify multiple search criteria.
4. To export the logs for the time period and filters, click **Export to CSV**.

## Configuring a log publisher to supply local syslogs

If you must have syslog files available on the local device, configure a publisher to log to the local-syslog destination.

***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.*

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Select the log publisher you want to update and click **Edit**.
3. For the **Destinations** setting, select **local-syslog** from the **Available** list, and move the destination to the **Selected** list.
4. Click **Finished**.

To use a log publisher, specify it in an access policy log setting, ensure that the access profile selects the log setting, and assign the access profile to a virtual server.

***Note:*** *Log settings are configured in the* ***Access Policy*** *>* ***Event Logs*** *area of the product.*

## Preventing logging to the /var/log/apm file

To stop logs from being written to the /var/log/apm file, remove the local-syslog destination from log publishers that are specified for access system logging in APM® log settings.

***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.*

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Select the log publisher you want to update and click **Edit**.
3. For the **Destinations** setting, if the **Selected** list contains **local-syslog**, move it to the **Available** list.
4. Click **Finished**.

To use a log publisher, specify it in an APM log setting, ensure that the log setting is assigned to an access profile, and assign the access profile to a virtual server.

***Note:*** *Log settings are configured in the Event Logs area of the product.*

## About local log storage locations

The BIG-IP® system publishes logs for portal access traffic and for connections to virtual desktops (VDI) to the `/var/log/rewrite*` files. APM® cannot publish these logs to remote destinations.

APM can publish URL request logs to remote or local destinations. Logs published to the local-db destination are stored in the local database and are available for display from the Configuration utility. Logs published to the local-syslog destination are stored in the `/var/log/urlfilter.log` file.

APM can publish access system logs to remote or local destinations. Logs published to the local-db destination are stored in the local database. Logs in the local database are available for display in APM reports. Logs published to the local-syslog destination are stored in the `/var/log/apm` file.

## Code expansion in Syslog log messages

The BIG-IP® system log messages contain codes that provide information about the system. You can run the Linux command `cat log |bigcodes |less` at the command prompt to expand the codes in log messages to provide more information. For example:

```
   Jun 14 14:28:03 sccp bcm56xxd [ 226 ] : 012c0012 : (Product=BIGIP
Subset=BCM565XXD) : 6: 4.1 rx [ OK 171009 Bad 0 ] tx [ OK 171014 Bad 0 ]
```

## About configurations that produce duplicate log messages

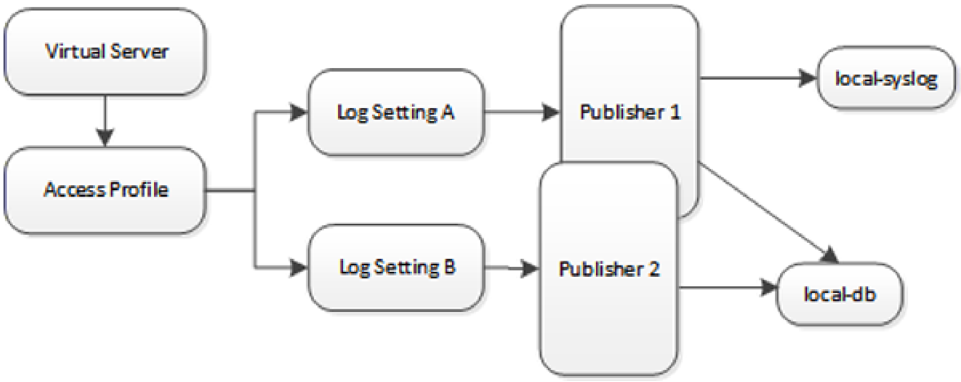


**Figure 21: Event log duplication**

The figure illustrates a configuration that writes duplicate logs. Two log publishers specify the same log destination, local-db. Each log publisher is specified in one of the log settings that are assigned to an access profile. Logs are written to the local-db destination twice.

## Methods to prevent or eliminate duplicate log messages

Duplicate log messages are written when the same log destination is specified by two or more log publishers and more than one of the log publishers is specified in the log settings that are assigned to an access profile.

One way to avoid or eliminate this problem is to specify only one log setting for each access profile. Another is to ensure that the log publishers you associate with log settings for an access profile do not contain duplication log destinations.

## About log level configuration

Log levels can be configured in various ways that depend on the specific functionality. Log levels for access portal traffic and for connections to virtual desktops are configured in the System area of the product. The log level for the URL database download is configured in the default-log-setting in the Access Policy Event Logs area of the product. The log level for NTLM authentication of Microsoft Exchange clients is configured using the ECA option in any log setting. Other access policy (and Secure Web Gateway) log levels are configured in any log setting.

### Updating the log level for NTLM for Exchange clients

Before you follow these steps, you should have a working configuration of NTLM authentication for Microsoft Exchange clients. The configuration should include a log setting that enables logging for Access Policy Manager® and is assigned to the access profile.

You can change the level of logging for NTLM authentication for Microsoft Exchange clients.

***Note:** Logging at the default level, **Notice**, is recommended.*

1. On the Main tab, click **Access Policy** > **Event Logs** > **Log Settings**.
   A log settings table displays.
2. Select the check box for the log setting that you want to update and click **Edit**.
   A popup screen displays.
3. To configure settings for access system logging, select **Access System Logs** from the left pane.
   Access System Logs settings display in the right panel.
4. For the **ECA** setting, select a log level.

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

5. Click **OK**.
   The popup screen closes.

## 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 Policy** > **Event Logs** > **Log Settings**.
   A log settings table displays.
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.

## Setting log levels for Portal Access and VDI events

Change the logging level for access policy events when you need to increase or decrease the minimum severity level at which Access Policy Manager® (APM®) logs that type of event. Follow these steps to change the log level for events that are related to portal access traffic or related to connections to virtual desktops (VDI).

***Note:*** *You can configure log levels for additional APM options in the Event Logs area.*

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Options**.
2. Scroll down to the Access Policy Logging area.

   The options **Portal Access** and **VDI** display; each displays a selected logging level.

   ***Note:*** *The log settings that you change on this page impact only the access policy events that are logged locally on the BIG-IP® system.*
3. For each option that you want to change, select a logging level from the list.

   ***Note:*** *Setting the log level to* ***Debug*** *affects the performance of the BIG-IP® system.*

   ***Warning:*** *F5® recommends that you do not set the log level for* ***Portal Access*** *to* ***Debug****. Portal Access can stop working. The BIG-IP system can become slow and unresponsive.*
4. Click **Update**.

APM starts to log events at the new minimum severity level.

# Kerberos Authentication for SWG Forward Proxy

## Overview: Authenticating SWG users with Kerberos

You can include authentication in the access policy in a Secure Web Gateway (SWG) explicit or transparent forward proxy configuration. However, if 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.

To use Kerberos authentication with SWG, if you do not already have Kerberos authentication configured and working with Access Policy Manager®, complete these tasks before you configure access policies for SWG.

**Task summary**

*Joining a Kerberos user account to a domain*
*Configuring an AAA server for Kerberos authentication*

### About basic authentication and Kerberos end-user logon

Access Policy Manager® (APM®) provides an alternative to the form-based login authentication method. Instead, an HTTP 401 (unauthorized) or HTTP 407 (proxy authentication required) response triggers a browser login screen to collect credentials.

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

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

The benefits of this feature include:

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

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

### How does end-user logon work?

To retrieve user credentials for end-user logon, you can use the basic authentication method, or the SPNEGO/Kerberos method (which is recommended), or both.

### Basic authentication

Use this method to retrieve user credentials (user name and password) from a browser. You can think of this method as a replacement for form-based authentication used by the standard login screen. If you use basic authentication, Access Policy Manager® (APM®) populates the user name and password session variables, which can then be used by any other authentication actions, such as Active Directory or RADIUS.

***Note:*** *When using basic authentication, passwords are passed as clear text.*

### SPNEGO/Kerberos

Use this method to retrieve user credentials through the SPNEGO/Kerberos authentication header. With the Kerberos method, the client system must first join a domain. A Kerberos action does not run immediately; it runs only when the server requests SPNEGO/Kerberos authentication. By default, Kerberos authentication runs not only on the first request, but also on subsequent requests where authentication is needed, such as for new connections. APM validates the request by confirming that a valid ticket is present.

***Note:*** *You can disable Kerberos per request-based authentication in the AAA Kerberos authentication access policy item configuration in APM. If you disable it, authentication occurs while the access policy runs and subsequent authentications do not occur.*

Both methods require that either an HTTP 401 Response (unauthorized) or an HTTP 407 Response (proxy authentication required) action item be configured in the access policy, and that the authentication method (basic, negotiate, or basic + negotiate) be specified in the action item.

In cases where both methods (basic + negotiate) are selected, the browser determines which method to perform based on whether the system has joined a domain. The HTTP 401 Response and HTTP 407 Response actions each have two default branches to indicate whether basic authentication or Kerberos method is performed.

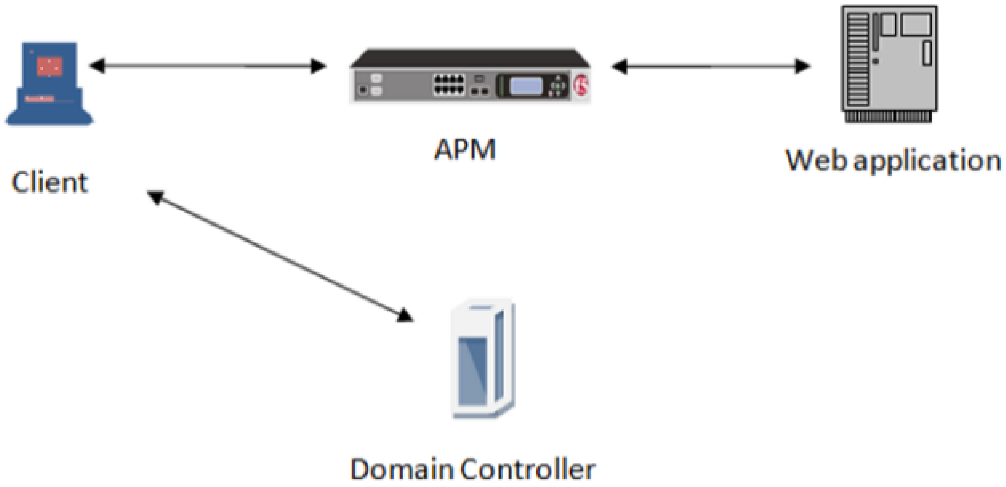


**Figure 22: How SPNEGO/Kerberos end-user login works**

The end-user logon works with events happening in this order:

- The client becomes a member and connects to the domain.
- The client connects to a virtual server on the BIG-IP® system.
- The access policy runs and issues a 401 or 407 HTTP response.
- If a Kerberos ticket is present or can be obtained, the browser forwards the Kerberos ticket along with the request when it receives the 401 or 407 response.
- APM validates the Kerberos ticket after the request is received, and determines whether or not to permit the request.

## About Kerberos authentication requirements

To configure Kerberos authentication, you must meet specific configuration requirements as described here.

**Virtual server**
The virtual server IP address and host name are necessary to configure DNS.

**DNS configuration**
Make sure you have the zone file and PTR record for the virtual server IP address. For example:

```
testbed.lab.companynet 10.10.4.100
```

**Browser configuration**
Configure the browser to use Kerberos. Typically, Internet Explorer is already configured for Kerberos; however, you might need to configure it for trusted sites. To use Firefox, you must configure it for negotiate authentication.

## Joining a Kerberos user account to a domain

To use Kerberos authentication, you need the client joined and connected to a domain and you need a keytab file.

1. Create a surrogate user in the domain.

   In this example, the hostname of the virtual server on the BIG-IP® system is testbed.lab.companynet.com and the user name is john.

   ```
   setspn -U -A HTTP/testbed.lab.companynet.com john
   ```
2. Map the user account to the service account and generate a keytab file for the service.

   You can use the ktpass utility to do this.

   In this example, `LAB.COMPANYNET.COM` specifies the Kerberos authentication realm, which is case-sensitive and must be specified in uppercase. The user name, which is specified in UPN format (`john@lab.companynet.com`), is not case-sensitive. (The user name can be specified in user name format, DN format, or UPN format).

   ```
   c:>ktpass -princ HTTP/testbed.lab.companynet.com@LAB.COMPANYNET.COM -mapuser
   john@lab.companynet.com -crypto rc4-hmac-nt -ptype KRB5_NT_SRV_HST -pass
   password -out c:\temp\john.keytab
   ```

## Configuring an AAA server for Kerberos authentication

Configure a Kerberos AAA server so that you can add it to a Kerberos authentication action in an access policy.

1. On the Main tab, click **Access Policy** > **AAA Servers** > **Kerberos**.
   The Kerberos Servers list screen opens.
2. Click **Create**.
   The New Server properties screen opens.
3. In the **Name** field, type a unique name for the authentication server.

4. In the **Auth Realm** field, type a Kerberos authentication realm name (administrative name), such as `LAB.COMANYNET`.

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

   A keytab file contains Kerberos encryption keys (these are derived from the Kerberos password).
7. Click **Finished**.
   The new server displays on the list.

## Kerberos authentication troubleshooting tips

You might choose to verify Kerberos authentication configurations in some instances. Use these troubleshooting tips to help resolve any issues you might encounter.

### Verify the keytab file

From the command line, use the `klist` command as shown in this example.

***Important:*** *The command must be typed on one line.*

```
klist -ke
WRFILE:/config/filestore/files_d/Common_d/kerberos_keytab_file_d/\:Common\:SUN-SPNEGO-APM106_key_file_2
```

The output for the example contains information like this.

```
Keytab name:
FILE:/config/filestore/files_d/Common_d/kerberos_keytab_file_d/:Common:SUN-SPNEGO-APM106_key_file_2
KVNO Principal
3    HTTP/apm106.labt.companynet.com@labt.companynet.com(arcfour-hmac)
```

### Verify Kerberos delegation

From the command line, use the `kinit` command, as shown in this example.

```
kinit HTTP/apm106.labt.companynet.com@labt.companynet.com
```

You are prompted for a password and should receive a ticket (no output, no error).

### Verify ticket

From the command line, type `klist`. Here is sample output: `/etc/krb5.conf`

### Capture a TCP dump

Make sure the client sends the ticket to the BIG-IP® system; this verifies that the client setup is successful.

## Implementation result

You should have a domain-joined user account for Kerberos and an AAA Kerberos server configured in Access Policy Manager®.

# NTLM Authentication for SWG Forward Proxy

## Overview: Authenticating SWG users with NTLM

You can include authentication in the access policy in a Secure Web Gateway (SWG) explicit or transparent forward proxy configuration. However, if 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.

To use NTLM authentication, you must specify an **NTLM Auth Configuration** when you configure the access profile for SWG explicit or SWG transparent forward proxy. If an **NTLM Auth Configuration** does not yet exist on the BIG-IP® system, use these steps to configure it.

### Task summary

*Configuring a machine account*
*Creating an NTLM Auth configuration*
*Maintaining a machine account*

## Configuring a machine account

You configure a machine account so that Access Policy Manager® (APM®) can establish a secure channel to a domain controller.

1. On the Main tab, click **Access Policy** > **Access Profiles** > **NTLM** > **Machine Account**.
   A new Machine Account screen opens.
2. In the Configuration area, in the **Machine Account Name** field, type a name.
3. In the **Domain FQDN** field, type the fully qualified domain name (FQDN) for the domain that you want the machine account to join.
4. (Optional) In the **Domain Controller FQDN** field, type the FQDN for a domain controller.
5. In the **Admin User** field, type the name of a user who has administrator privilege.
6. In the **Admin Password** field, type the password for the admin user.

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

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

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

## Creating an NTLM Auth configuration

Create an NTLM Auth configuration to specify the domain controllers that a machine account can use to log in.

1. On the Main tab, click **Access Policy** > **Access Profiles** > **NTLM** > **NTLM Auth Configuration**.
   A new NTLM Auth Configuration screen opens.
2. In the **Name** field, type a name.
3. From the **Machine Account Name** list, select the machine account configuration to which this NTLM Auth configuration applies.

   You can assign the same machine account to multiple NTLM authentication configurations.
4. For each domain controller, type a fully qualified domain name (FQDN) and click **Add**.

   ***Note:*** *You should add only domain controllers that belong to one domain.*

   By specifying more than one domain controller, you enable high availability. If the first domain controller on the list is not available, Access Policy Manager® tries the next domain controller on the list, successively.
5. Click **Finished**.

This specifies the domain controllers that a machine account can use to log in.

## Maintaining a machine account

In some networks, administrators run scripts to find and delete outdated machine accounts on the domain controllers. To keep the machine account up-to-date, you can renew the password periodically.

1. On the Main tab, click **Access Policy** > **Access Profiles** > **NTLM** > **Machine Account**.
   The Machine Account screen opens.
2. Click the name of a machine account.
   The properties screen opens and displays the date and time of the last update to the machine account password.
3. Click the **Renew Machine Password** button.
   The screen refreshes and displays the updated date and time.

This changes the machine account last modified time.

# Legal Notices

## Legal notices

### Publication Date

This document was published on May 9, 2016.

### Publication Number

MAN-0504-03

### Copyright

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

### Trademarks

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: *http://www.f5.com/about/guidelines-policies/patents*

### Export Regulation Notice

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

### RF Interference Warning

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

### FCC Compliance

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

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

### Canadian Regulatory Compliance

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

### Standards Compliance

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

# Index