Performance Management Advisors Deployment Guide

Deploy and Configure Apache

12/14/2025

Deploy and Configure Apache

Use the information on this page to install an Apache Web Server instance to direct http requests to the appropriate server. It is recommended to install Apache Web Server on a separate box.

You do not require a second Apache instance on the XML Generator server (local files are not produced). You can install a single Apache instance on a standalone server that points to the Advisors IP addresses and ports.

In a Frontline Advisor distributed mode configuration, the Apache HTTP configuration can be configured on any FA instance.

You can configure Apache to support HTTPs; to do so, you must:

- Generate the SSL security certificate and private key.
- Reconfigure Apache.

Both procedures are described on the *Configure Apache to Support HTTPS* tab below.

<tabber>

Deploy and Configure Apache for Advisors=

1. To enable Apache Web Server serving different modules in the Advisors interface (for example, Administration, Contact Center Advisor, Workforce Advisor), edit the `httpd.conf` file as described below. The `httpd.conf` file is located in the `conf` folder of the Apache Web Server installation.

a. Locate the following lines in the `httpd.conf` file:

   - `#LoadModule headers_module modules/mod_headers.so`
   - `#LoadModule proxy_module modules/mod_proxy.so`
   - `#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so`
   - `#LoadModule proxy_http_module modules/mod_proxy_http.so`

b. Remove the hash mark (#) from the beginning of each line, so that these four lines appear like this:

   - `LoadModule headers_module modules/mod_headers.so`
   - `LoadModule proxy_module modules/mod_proxy.so`
   - `LoadModule proxy_ajp_module modules/mod_proxy_ajp.so`
   - `LoadModule proxy_http_module modules/mod_proxy_http.so`

c. Locate the following entry and add a # to comment out `Deny from all` and to add `Allow from all`:

```
<Directory />
Options FollowSymLinks
AllowOverride None
```

```
Order deny,allow
#Deny from all
Allow from all
Satisfy all
</Directory>
```

d. Locate the following entry near line 133 and add a # to comment it out:
`#ServerAdmin`

e. Add the following line:
`ProxyRequests Off`

f. Add the lines shown below (see Platform and Advisors Modules below) to the bottom of the file and change the IP addresses or host names, as necessary. The format of this page might cause lines to wrap, but it is very important that each entry is on a single line in your `httpd.conf` file. You can comment out or exclude lines to proxy passes that are not installed.

The trailing slash must appear at the end of each line, as indicated below. If it is omitted, users might see a 404 or `Not  Found` error, get no response when clicking, or see empty white screens in the Advisors interface. Errors can typically be seen in the Geronimo log if DEBUG is enabled. For example, `ProxyPass /gc-admin/ ajp://server:8009/gc-admin` will generate an error. Should this happen, the solution is to fix the `httpd.conf` and restart Apache.

If you need to access external applications through the Advisors interface, you should have lines for each of those applications.
For example, `ProxyPass /APEX/ http://www.cra-arc.gc.ca/formspubs/menu-eng.html`.

```
# Platform and Advisors Modules
ProxyPass /am/ ajp://192.168.40.234:8009/am/
ProxyPass /admin/ ajp://192.168.40.234:8009/admin/
```

> **Important**
>
> Remove, or comment out, the `ProxyPass /admin/ ajp://192.168.40.234:8009/admin/` statement on FA presentation-only instances. If you use a load balancer, do not direct requests to the `/admin/` context to FA presentation-only instances.

```
ProxyPass /am-admin/ ajp://192.168.40.234:8009/am-admin/
ProxyPass /ca/ ajp://192.168.40.234:8009/ca/
ProxyPass /ca-ws/ ajp://192.168.40.234:8009/ca-ws/
ProxyPass /ea-ws/ ajp://192.168.40.234:8009/ea-ws/
ProxyPass /base-ws/ ajp://192.168.40.234:8009/base-ws/
ProxyPass /dashboard/ ajp://192.168.40.234:8009/dashboard/
ProxyPass /nav-service/ ajp://192.168.40.234:8009/nav-service/
ProxyPass /prefs-service/ ajp://192.168.40.234:8009/prefs-service/
ProxyPass /wu/ ajp://192.168.40.235:8009/wu/
ProxyPass /ca-xml/ ajp://192.168.40.234:8009/ca-xml/

# Genesys Resource Management Console Web Application
ProxyPass /rmc/ ajp://192.168.40.235:8009/rmc/

# FA
ProxyPass /fa/ ajp://192.168.40.234:8009/fa/

# Contact Center Advisor Mobile Edition
```

```
ProxyPass /ma/ ajp://HOSTNAME:8009/ma/
```

Important

If there is no Administration workbench module installed on the FA Platform server, add the following re-directs before `ProxyPass /fa/ ajp://192.168.40.234:8009/fa/` – this allows you to access the FA Administration module from the CCAdv/WA Platform server:

- `ProxyPass /fa/Admin ajp://192.168.40.234:8009/fa/Admin`
  Note that there is no slash at the end of the preceding statement; while this is different from most other ProxyPass statements, it is correct syntax for the `fa/Admin` statement.
- `ProxyPass /fa/com.informiam.fa.admin.gwt.AdminConsole/ ajp://192.168.40.234:8009/fa/com.informiam.fa.admin.gwt.AdminConsole/`

2. Copy the contents of the `baseweb-<version>-static-web.zip` from the Advisors Platform distribution (the directories within the `static-web-content`) into the Apache `htdocs` directory.

|-| Configure Apache to Support HTTPS=

Generating the SSL security certificate and private key

1. If not already installed, download and install the C++ redistributables from the official Microsoft downloads site.
2. If not already installed, download and install OpenSSL from an official SSL download site.
3. Add the `OpenSSL bin` directory (by default `C:\OpenSSL-Win32\bin`) to your Windows PATH.
4. From the `Start` menu, enter Run > `mmc`.
5. From the `File` menu, select `Add/Remove Snap-In`.
6. Execute the following:

```
Add > Certificates > Add > Computer Account > Local Computer
```

7. Expand `Console Root` > `Certificates` > `Personal` > `Certificates`.
8. Right-click and choose `All Tasks` > `Export`.
9. Select Yes to export the private key.
10. Deselect `Enable strong protection`.
11. Extract the certificate and key using the following command from the directory where the certificate was exported:

```
openssl pkcs12 -in inf-koi.pfx -out inf-koi.crt -nodes
```

Reconfiguring Apache to support HTTPS

1. Copy the certificate/key (`inf-koy.crt`) to the Apache `conf` directory (by default, `C:\Program Files\Apache Software Foundation\Apache2.2\conf`).
2. Edit `{Apache conf}\httpd.conf`.

a. Uncomment `LoadModule ssl_module modules/mod_ssl.so` (line 120).

b. Uncomment `Include conf/extra/httpd-ssl.conf` (line 474).

c. Comment out `Listen 80` (line 46).

3. Edit `{Apache conf}\extra\httpd-ssl.conf` and point `SSLCertificateFile` and `SSLCertificateKeyFile` to the certificate.

4. Restart Apache.

5. Verify the configuration by browsing to `https://inf-koi`. This will require accepting a certificate warning unless the client has added the server's certificate.