

Athena FirePAC™ v5.2 Change Advisor

Installation and Deployment Guide

Athena FirePAC™ v5.2 Change Advisor is deployed in a multi-user, shared database environment. This deployment offers all of the standard FirePAC features, including the ability to share data between multiple users and to distribute the processing load among multiple hosts, plus the web-based forms for entering and reviewing Change Advisor requests. There are two components to the installation: the server component installation and one or more client components.

Server Component

The server component consists of the database server, which is shared amongst all the clients, the FirePAC License Manager server, and the FirePAC web server, which provides the web-based interface for Change Advisor. This should be installed on a designated server-class host.

Client Component

The client component consists of the FirePAC user interface and analysis software. Clients may be installed for different purposes. The most common use is to deploy one desktop client per network engineers. Another common use of the client component is to collect and update device configurations on a regularly scheduled basis. A client is automatically installed with the server component and is intended to be used for this purpose. If you intend to use the Impact Monitor feature, or to automatically generate scheduled analysis reports, it is recommended to also install a client exclusively for these activities.

Browser-Based Client

FirePAC Change Advisor provides a web-based interface for entering and reviewing Change Advisor requests. No installation is necessary, as this is provided as part of the server component. The supported browsers are MS Internet Explorer and Mozilla Firefox.

Installing FirePAC Change Advisor

To install the FirePAC server component, make sure you have the Installer program for the Shared Database edition. The distribution ZIP file should include the string "shareddb" in the filename. When you launch the Installer program, the splash image will say "Shared Database Edition" and you will be prompted to select between "Shared database installation" and "Client installation". Select the former to install the server component and the client component that runs on the same host. To install client components on other hosts, run the installer on each of the intended client hosts and select the "Client installation" option. The Installer will then provide step-by-step guidance through the installation process for that component.

When deploying FirePAC Change Advisor, it is helpful to keep the following points in mind:

1. It is recommended that the server component be installed on a high-end machine with ample memory and large disk capacity. Use the 32-bit install with 2 Gb of RAM if the firewalls are small to medium complexity. Use the 64-bit install, with at least 8 Gb of RAM if the firewalls are large and complex. FirePAC provides a complexity metric tool to measure complexity.
2. The web-based Change Advisor interface is provided by the server component. You will need to access the administrator pages of the web-based interface to finish configuring FirePAC Change Advisor. See the section on Configuring Change Advisor below for more details.
3. A FirePAC client will be automatically installed on the same machine as the server component, so a separate client installation is not necessary on the server host. To view this client, launch it from the desktop icon or the Start menu of the host on which the server is installed.
4. The FirePAC client may be installed on any number of hosts on your network. Use the "Client installation" branch in the Installer program to install these.
5. Each FirePAC client must have to have access to the shared database using port 3050 and to the License Manager using port 4568. This will be checked during installation of the client. These ports

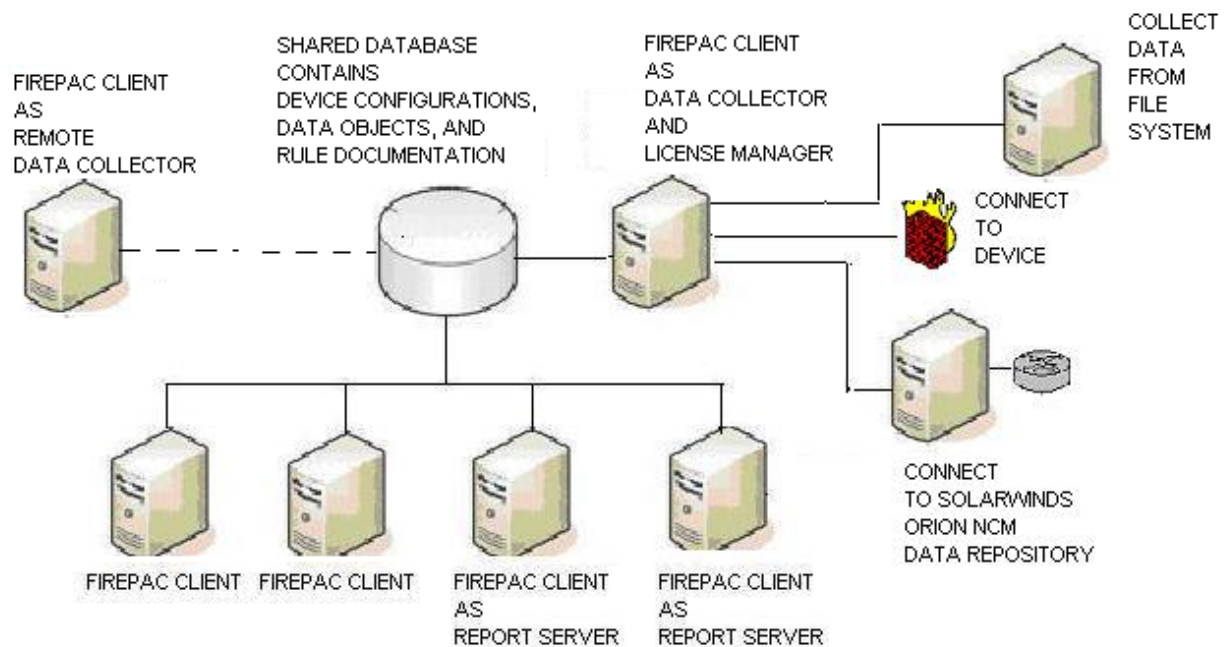
can be changed during the installation process, but they must be set to the same values for *all* FirePAC clients.

FirePAC Change Advisor allows for very flexible deployment arrangements. Each FirePAC client is exactly the same and is installed using the same steps in the Installer program. However, you may want to consider designating different clients for different purposes. The diagram on the next page depicts several different options for configuring the FirePAC clients.

FirePAC Clients For Individual Use

In general, each FirePAC user will want a copy of the FirePAC client installed on his or her workstation. The only requirement is that the host on which the FirePAC client is installed be able to communicate with the server host where the shared database and License Manager are installed. The Installer performs tests to check for connectivity.

Using the FirePAC client user interface, you can view firewall details, issue rule, object, and traffic flow queries, or generate security and rule clean up reports on an *ad hoc* basis. You can also perform change modeling by comparing the production version of a firewall configuration with local changes that you want to ultimately deploy to the production system.



Each FirePAC client may schedule its own reports to run locally. These scheduled tasks are only visible to the local client. For regularly repeating reports, it is recommended that a separate dedicated host be set up to generate reports automatically as this frees the user's host from the heavy processing involved in these tasks (see below).

FirePAC Client As Data Collector

One host supporting an installation of the FirePAC client should be designated as the *Data Collector Client*. This client will be used to schedule Update tasks to refresh the firewall configurations in the inventory on a regular and on-going basis.

If the number of devices is small (< 250) and the devices are locally situated, it is reasonable to install the FirePAC client on the same host as the server component and to designate this client as the Data Collector Client. For a larger number of devices, or if you have many devices with large configuration files that take longer to download, you will find it advantageous to designate a different host (other than the database server host) as the Data Collector Client.

FirePAC provides several methods for acquiring device configurations:

1. Directly connect to the device. The Data Collector Client will need to be able to connect to each device, typically using port 22 (SSH).
2. Download configurations from the Solarwinds Orion NCM repository. This requires having Orion NCM installed on a host in your network and configured for the FirePAC NCM integration.
3. Import configurations from the local file system. This requires that the firewall configurations be available on the local file system, typically through some other process.

You can mix and match the data collection methods to suit your environment. If your devices are located in multiple geographic locations, multiple FirePAC clients can act as local data collectors, one in each location on a host closer to the device. The data collector will directly upload the configurations into the shared database. You can set up a remote data collector connecting to the database server over a VPN connection.

Each FirePAC Data Collector Client can have data collection tasks independently scheduled, so that data collection takes place automatically on a regular basis. You can have several data collection tasks scheduled on the same FirePAC client.

FirePAC Client As Report Generator

Besides generating reports on an *ad hoc* basis, you may want to use the Impact Monitor feature to generate reports automatically on a periodic basis, using the Scheduler facility. Because of the intensive CPU and memory resources required for firewall analysis, it is recommended that you designate a FirePAC client as a dedicated *Report Client*.

Each report task can be run on its own independent schedule. The Report Client will generate reports by picking up the latest configurations available from the shared database at the start of report generation. When the report generation task is completed, the reports will be delivered to a location in the local file system, as designated when the task was created.

It is possible to use multiple hosts as Report Clients, one for each location in a distributed environment to deal with the firewalls in that location.

Configuring Change Advisor

Once the FirePAC server component has been installed, make sure that the server process has been started. If it has not started, you can start it using the FirePAC menu item in the Start menu of the installation host. The web-based interface will be immediately available. Before actually using Change Advisor, you will want to configure the connection to Active Directory services and to create user accounts.

In order to configure FirePAC Change Advisor, you will need to log into the web-based interface. Launch a web browser and point it at the following URL:

`http://<hostname or IP>:8080/firepac/login.jsp`

where *<hostname or IP>* is either the hostname or IP address of the host where the FirePAC server component is installed. You will see the FirePAC Change Advisor login page displayed in the browser.

Sign into the web interface using the built-in administrator account. The username is "admin" and the password is "admin". You will see the list of user accounts displayed. In a brand-new installation, only the built-in administrator account is listed. There are three options listed across the menu bar at the top of the page: List Accounts, New User Account, and Settings.

Adding User Accounts

You will need to create a user account for each person who will be accessing the Change Advisor web UI. Each account must have a role assigned to it. The roles control what information is visible to the user and what actions are available. The three roles are described below:

User	The user role can create new change requests and can view any change request created by the same user. This role should be
------	--

	assigned to any user account who will be submitting change requests.
Network Engineer	The engineer role can create new change requests and can view all change requests created by all users in the system. It can also interactively request a packet tracer report for any change request. This role should be assigned to any user account who will be reviewing change requests or making changes in the firewall configurations to fulfill change requests.
Change Advisor Administrator	The administrator role can create, view, and modify the profiles of all user accounts defined in the system. It can also specify the settings for Windows domains and Active Directory servers. There is one default account called "admin" that has this role, but others may be created.

To create a new user account, click on the **New User Account** option displayed in the menu bar at the top of the page. The New User Account page displays a form to enter the information required to create a new user account. The following fields are shown:

Username	Name of the user account. Must be unique to Change Advisor.
Password	Password for the account.
Account type	User role, as described above.
Full Name	Full name of the user who will have access to the account.
Email	Email address for the user
Department	A string describing what part of the organization the user is in.

All of these fields are required. When all the fields have all been filled in, click the **Update Account** button to create the account.

Connecting to Active Directory

FirePAC Change Advisor accesses the host definitions available from Active Directory to simplify the task of entering sources and destinations for change requests. FirePAC can use data from multiple Windows domains and can access multiple Active Directory servers.

To specify the Active Directory connection, click on the **Settings** option displayed in the menu bar at the top of the page. The Settings page shows a single tab called "Configure Windows Domains" and two tables, which should be empty. The left-most table displays the Windows domains known to FirePAC. Press the **Add Domain** button and enter the name of your domain in the pop-up dialog. When you click "OK" the domain should be added to the Windows Domain table.

Click the radio button next to the entry for the domain in the table to select it. Then press the **Add Server** button and enter the IP address of a domain server for the specified domain and the username and password of an account that has access to the domain server.

You can add multiple Windows domains and multiple Active Directory servers for each domain. FirePAC will merge all of the entries found in the list of known hosts.