

Advanced Settings

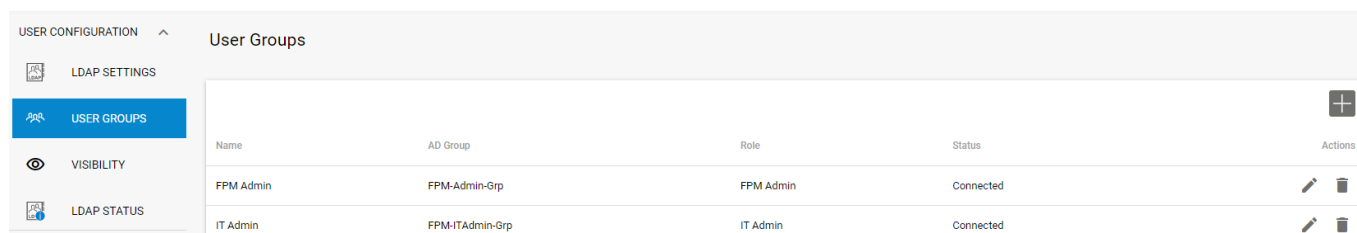
<https://campus.barracuda.com/doc/93199133/>





The Firewall Policy Manager **Advanced** tab lets users with administrative permissions configure authentication settings and manage user groups. From here, you can also link a database for assets that should be applied to your firewall rules, configure Intrusion Prevention System (IPS) policies, and add Control Centers and Firewalls to be used for rule assignment. A backup and export section allows the definition of an SMB server from where the Firewall Policy Manager configuration can be backed up or exported to an external destination. To access the advanced configuration page, click the **Advanced** tab.

Use the link menu on the left of the **Advanced** page to access the following settings:

User Configuration

The **User Configuration** menu lets users with administrative permissions manage user groups and configure authentication settings for the Firewall Policy Manager.



Name	AD Group	Role	Status	Actions
FPM Admin	FPM-Admin-Grp	FPM Admin	Connected	 
IT Admin	FPM-ITAdmin-Grp	IT Admin	Connected	 

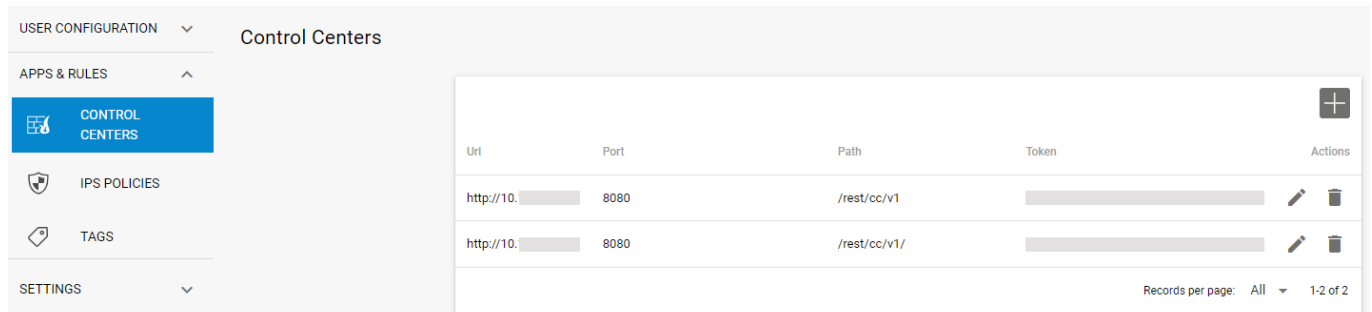
From the navigation pane on the left of this page, you can access the following sub-items:

- **LDAP Settings** – This page allows configuration of authentication and MSAD user filtering criteria.
- **User Groups** – On this page, administrators can add and manage user groups and configure role permissions.
- **Visibility** – Use the **Show all rules** check box to display or hide all rules on the **Rules** page.
- **LDAP Status** – This page provides detailed information on Firewall Policy Manager connection details, configured LDAP settings, and related group definitions.

For more information, see: [Get Started](#).

Apps & Rules

The **Apps & Rules** menu lets administrators add Firewall Control Centers and configure Intrusion Prevention System (IPS) policies. Here, you can also define operative categories for applications and rules.



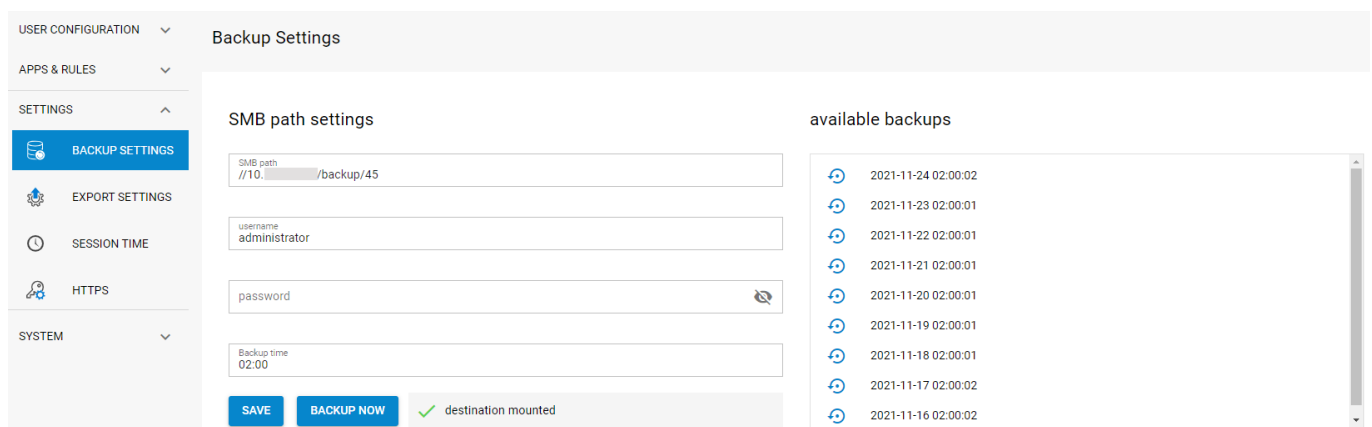
Uri	Port	Path	Token	Actions
http://10. [redacted]	8080	/rest/cc/v1	[redacted]	[edit] [delete]
http://10. [redacted]	8080	/rest/cc/v1/	[redacted]	[edit] [delete]

From the navigation pane on the left of this page, you can access the following sub-items:

- **Control Centers** – This page lets administrators add Firewall Control Centers that should be used for rules assignment to CC-managed firewalls. A linked path to the CC REST API allows CC-specific commands to be used for role processing. For more information, see: [Application and Rules Assignment](#).
- **IPS Policies** – This page allows the definition of Intrusion Prevention System (IPS) policies that can be applied to firewall rules. For more information, see: [Get Started](#).
- **Tags** – This page lets administrators define operative environments that can be selected when creating applications. For more information, see: [Get Started](#).

Settings

The **Settings** menu provides backup and export functionalities for the Firewall Policy Manager configuration and lets administrators add certificates and keys.

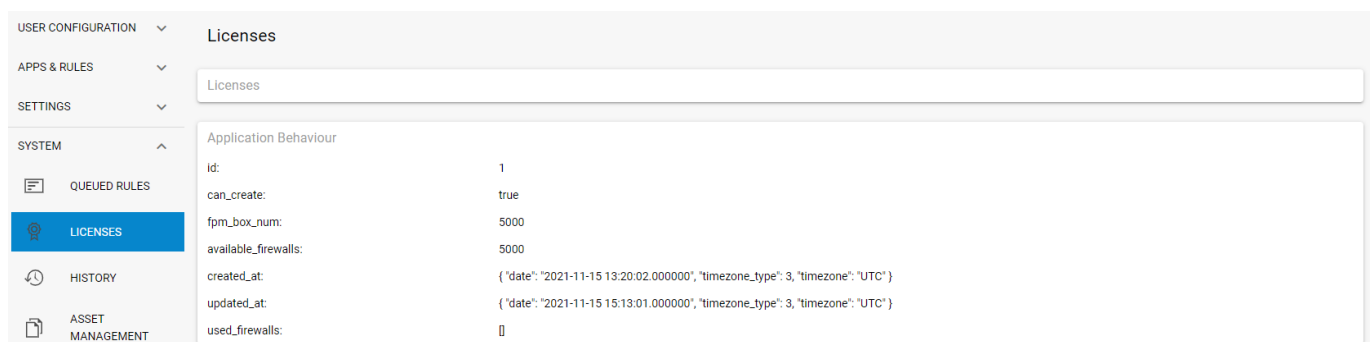


From the navigation pane on the left of this page, you can access the following sub-items:

- **Backup Settings** – Here, you can back up the configuration of the Firewall Policy Manager. For more information, see: [How to Backup the Firewall Policy Manager](#).
- **Export Settings** – This page allows you to export dedicated configuration entities to an external destination. For more information, see: [How to Backup the Firewall Policy Manager](#).
- **Session Time** – By entering a value here, you can configure the Firewall Policy Manager session idle time in seconds.
- **HTTPS** – This page lets administrators add HTTPS certificates and private key for the Firewall Policy Manager.

System

The **System** menu provides information on rules that have the status "Queued". Here, you can also access the configuration history, manage licenses, and configure an external MSSQL database from where asset data can be applied to rules.



The screenshot shows the 'System' menu in the Barracuda Firewall Policy Manager interface. The left navigation pane is expanded, showing 'SYSTEM' with sub-items: 'QUEUED RULES', 'LICENSES' (highlighted), 'HISTORY', and 'ASSET MANAGEMENT'. The main content area displays the 'Licenses' section, which includes a search bar and a table of application behavior details.

Application Behaviour	
id:	1
can_create:	true
fpm_box_num:	5000
available_firewalls:	5000
created_at:	{ "date": "2021-11-15 13:20:02.000000", "timezone_type": 3, "timezone": "UTC" }
updated_at:	{ "date": "2021-11-15 15:13:01.000000", "timezone_type": 3, "timezone": "UTC" }
used_firewalls:	[]

From the navigation pane on the left of this page, you can access the following sub-items:

- **Queued Rules** – This page shows all rules that have the status "Queued". Queued rules can be assigned to a Control Center. For more information, see: [Application and Rules Assignment](#).
- **Licenses** – Access this page to view details related to licenses used by firewalls.
- **History** – This page provides a detailed view on the Firewall Policy Manager configuration history.
- **Asset Management** – From here, you can configure an external MSSQL database from where asset data can be applied to firewall rules. For more information, see: [Get Started](#).
- **Firewall Filters** – On this page, you can filter for different firewall models.

Figures

1. user_conf.png
2. cc_conf.png
3. bu_settings.png
4. lic_settings.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.