

How to Create and Apply Custom User Objects

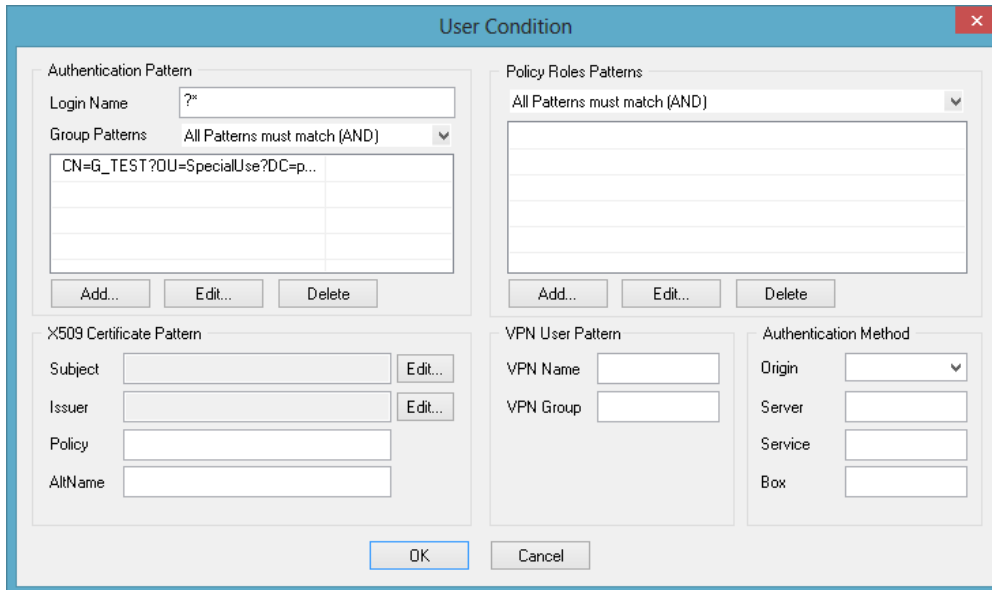
<https://campus.barracuda.com/doc/96026270/>

Create custom user objects to reference users and groups for implementation within the Barracuda CloudGen Firewall forwarding rule set. In a user object, you can enter conditions such as authentication patterns and policy roles, depending on your requirements, to define the users that you want to include in the user object. You can also reference other user objects that have already been configured.

Create a User Object

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. From the left menu, select **Users and Groups**.
4. Right-click the table and select **New**.
5. In the **Edit/Create User Object** window, enter a **Name** for the user object. E.g., Trusted LAN Users
6. Click **New** to add a user condition. The **User Condition** window opens.
7. Enter the **Login Name**. Question marks (?) and asterisks (*) are allowed. If you enter a question mark and asterisk (?*), you must also enter at least one character.
8. From the **Group Patterns** list, select the required group condition. You have the following options:
 - **One Pattern must match (OR)** - Users must match one of the patterns listed in the **Group Patterns** section.
 - **All Patterns must match (AND)** - Users must match all the patterns listed in the **Group Patterns** section.
9. Click **Add** to select your users. The **Edit Group Pattern** window opens.

This option lets you perform an **AD Lookup**. Select **Use current AD Connection** to check entries from your configured Active Directory domain controller or enter your search criteria in the provided fields.
10. Select the users and/or groups the user object applies to, and click **OK**.

The image shows a 'User Condition' dialog box with a blue title bar and a red close button. It contains several sections: 'Authentication Pattern' with a 'Login Name' field (containing '?*') and a 'Group Patterns' dropdown (set to 'All Patterns must match (AND)'); a table with one row containing 'CN=G_TEST?OU=SpecialUse?DC=p...'; 'Policy Roles Patterns' with a dropdown (set to 'All Patterns must match (AND)') and an empty table; 'X509 Certificate Pattern' with fields for 'Subject', 'Issuer', 'Policy', and 'AltName', each with an 'Edit...' button; 'VPN User Pattern' with 'VPN Name' and 'VPN Group' fields; and 'Authentication Method' with a dropdown for 'Origin' and text fields for 'Server', 'Service', and 'Box'. At the bottom are 'Add...', 'Edit...', and 'Delete' buttons for each section, and 'OK' and 'Cancel' buttons at the very bottom.

11. After you specify the conditions for all of the users that you want to include in this object, click **OK** to create the user object.
12. Click **Send Changes** and **Activate**.

If you are using Offline Authentication, ensure that user-specific rules are sequenced after the fwauth rule (see [How to Configure Offline Firewall Authentication](#)).

Apply a User Object to an Access Rule

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Edit the access rule that you want to apply the user object to.
4. From the **Authenticated User** list, select the user object.
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Figures

1. custom_user_object.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.