

User Objects

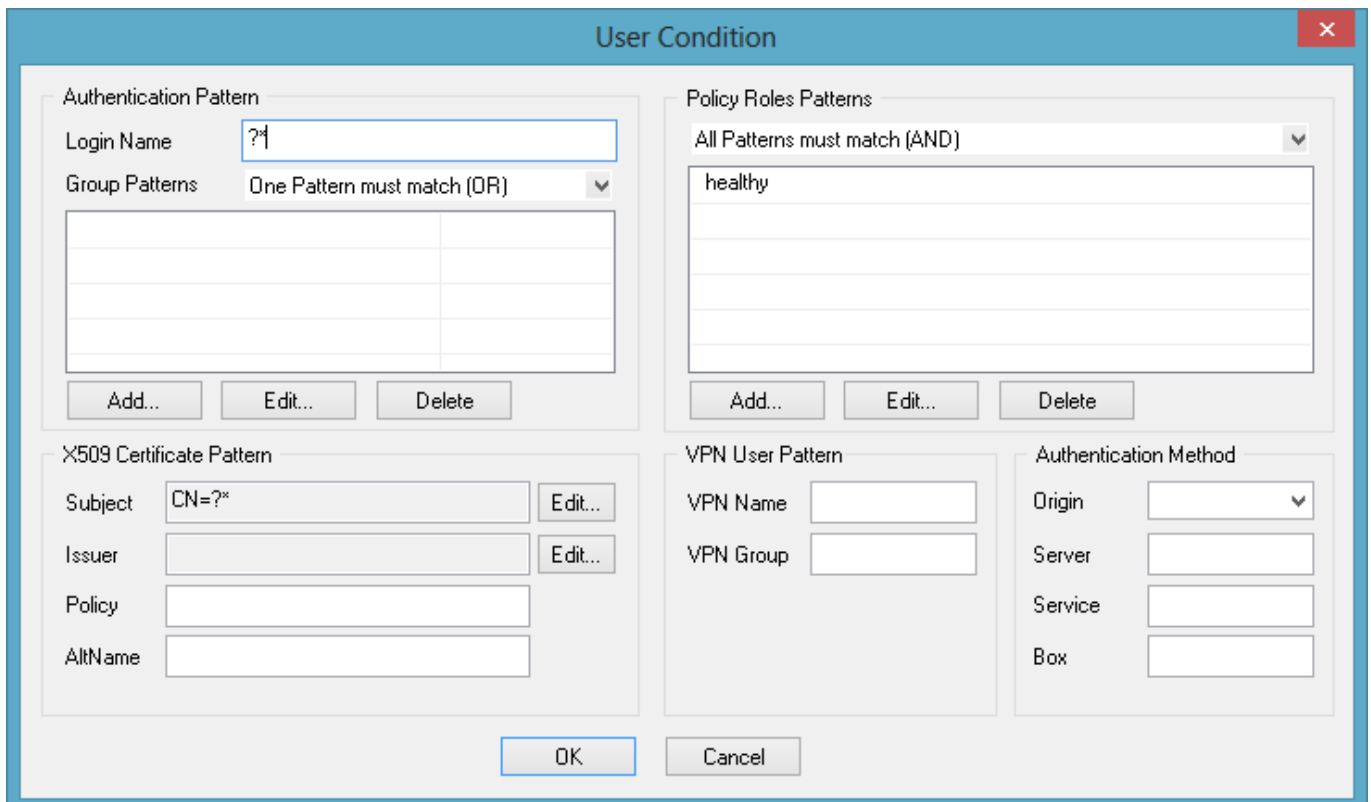
<https://campus.barracuda.com/doc/43846869/>

User objects restrict firewall rules to specific users and user groups. You can apply user objects to forwarding firewall rules and specify user conditions such as login names, groups, and policy role patterns. You also have the option to include VPN groups in the object configuration.

User objects are populated by querying the external authentication servers or the local authentication service on the Barracuda NG Firewall. For VPN, users objects can also query X.509 certificate patterns.

User Conditions

When you create a new user object, configure the following settings in the **User Condition** configuration window to define the users that the user object applies to:



The screenshot shows the 'User Condition' configuration window. It is divided into several sections:

- Authentication Pattern:** Includes a 'Login Name' text box containing '?*' and a 'Group Patterns' section with a dropdown menu set to 'One Pattern must match (OR)'. Below this is a table with three columns and three rows, and buttons for 'Add...', 'Edit...', and 'Delete'.
- Policy Roles Patterns:** Includes a dropdown menu set to 'All Patterns must match (AND)' and a list box containing the text 'healthy'. Below the list box are buttons for 'Add...', 'Edit...', and 'Delete'.
- X509 Certificate Pattern:** Includes fields for 'Subject' (containing 'CN=?*'), 'Issuer', 'Policy', and 'AltName', each with an 'Edit...' button.
- VPN User Pattern:** Includes fields for 'VPN Name' and 'VPN Group'.
- Authentication Method:** Includes fields for 'Origin', 'Server', 'Service', and 'Box', each with a dropdown menu.

At the bottom of the window are 'OK' and 'Cancel' buttons.

- **Authentication Pattern** - The group assignments of the users, according to the affected external authentication scheme (MSAD, LDAP, or RADIUS).
- **Policy Roles Patterns** - The policy role patterns for VPN users when using the [Barracuda Network Access Client](#). You can select:

- healthy
- unhealthy
- untrusted
- probation
- **X509 Certificate Pattern** - The certificate conditions for VPN users and groups:
 - **Subject/Issuer** - The subject/issuer of the affected X.509 certificate. If multiple subject parts (key value pairs) are required, separate them with a forward slash (/). For example, if OU=test1 and OU=test2 are required, select **OU** and enter test1/test2.
- **Policy/AltName** - The ISO number and the SubjectAltName according to the certificate.
- **VPN User Pattern** - The VPN login and VPN group policy that the object has to apply to in the **VPN Group** field.
- **Authentication Method** - In this section, you can specify the following settings:
 - **Origin** - Defines the type of originator. The following originators are available when configured:
 - **VPNP (PersonalVPN)**
 - **VPNG (GroupVPN)**
 - **VPNT (Tunnel)**
 - **HTTP (Browser login)**
 - **Proxy (Login via proxy)**
 - **Server/Service/Box** - Allows enforcing authentication on a certain server/service/box.

Create a User Object

- [How to Create and Apply Custom User Objects](#)
- [How to Create and Apply User Objects for VPN Users](#)

Figures

1. user_object_cn.png

© Barracuda Networks Inc., 2019 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.