

---

## Configuring Access to the Barracuda Web Application Firewall

<https://campus.barracuda.com/doc/55312412/>

The Barracuda Web Application Firewall is a critical component of an organization's security infrastructure, and any access to the Barracuda Web Application Firewall should be strictly controlled.

### Resetting the Factory Admin Password

---

The Barracuda Web Application Firewall is shipped with an "Admin" user account that has full administrative privileges and cannot be deleted from the system.

Barracuda Networks strongly recommends that administrators change the default admin password to a strong password.

The Barracuda Web Application Firewall does not enforce any rules on passwords, but general best practice guidelines recommend the following:

- Password lengths of more than 12 characters
- Use randomly generated passwords when possible
- Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relatives, or pet names
- Avoid romantic links and biographical information
- Include numbers and symbols in passwords
- If the system recognizes case, use both capital and lower-case letters

### Securing Network Access

---

Network access to the Barracuda Web Application Firewall should be controlled and limited. Recommended best practices include the following:

#### Use a Separate Management Network

Setting up a separate management network separates administrative traffic from WAN and LAN traffic. This physically ensures that only users with access to the management network can access the administrative interface on the Web Application Firewall.

To set up a separate management network, perform the following:

1. Use the Management (MGMT) port on the Barracuda Web Application Firewall to connect to the management domain.
2. Log into the Barracuda Web Application Firewall web interface
3. Go to the **BASIC > IP Configuration** page
4. In the **Management IP Configuration** section:
  1. Configure the IPv4/IPv6 address, IPv4 Subnet Mask/IPv6 CIDR Mask, IPv4/IPv6 Default Gateway and VLAN ID.
  2. Set **Allow Administration Access** to "Yes".
5. Save the configuration.

Test to see if you can reach the console using the management network. After you have confirmed you can reach the Web Application Firewall, log back into the Barracuda Web Application Firewall.

1. Go to the **BASIC > IP Configuration** page
2. Set **Allow Administration Access** to "No" in the **WAN IP Configuration** section.
3. Set **Allow Administration Access** to "No" in the **LAN IP Configuration** section.
4. Save the changes

## Use HTTPS-Only for Management Access

Log into the Barracuda Web Application Firewall web interface using HTTPS.

1. Go to the **ADVANCED > Secure Administration** page.
2. In the **Web Interface HTTPS/SSL Configuration** section, do the following:
  1. **HTTPS/SSL Access Only** - Select Yes to use HTTPS to access the web interface.
  2. **Web Interface HTTPS/SSL Port** - Specify the HTTPS port to access the web interface. The default value is 443.
  3. **Supported SSL Protocols** - Select the SSL protocols to be enabled for the web interface.
3. Save the changes.

## Controlling and Restricting Access

### Defining and Assigning Roles

Access to the Barracuda Networks management interface should be guided by the principle of least privilege. User roles ideally should be well-defined and should be limited to the minimal amount required to perform their job.

The Barracuda Web Application Firewall is shipped with eight predefined roles representing the most common user roles used to administer the Barracuda Web Application Firewall:

Role	Description
------	-------------

<b>Admin</b>	This is the super administrator role. The default 'admin' user is assigned this role. This role has the privilege to perform all system operations. An admin is responsible for creating and assigning roles.
<b>Audit-Manager</b>	User assigned to this role can perform auditing tasks. This role has the privilege to view logs, but is exempted from exporting logs. The role's responsibility is as follows: <ul style="list-style-type: none"> <li>• View logs</li> <li>• Generate reports</li> </ul>
<b>Certificate-Manager</b>	User assigned to this role can perform certificate management tasks. The role's responsibility includes: <ul style="list-style-type: none"> <li>• Uploading certificates</li> <li>• Creating certificates</li> <li>• Uploading trusted certificates</li> </ul>
<b>Guest</b>	User assigned to this role can view all configurations, but is exempted from modifying the configuration.
<b>Monitoring-Manager</b>	User assigned to this role can monitor system activities. The role's responsibility includes: <ul style="list-style-type: none"> <li>• Viewing logs</li> <li>• Configuring email notifications</li> <li>• Exporting System logs, Application Logs and FTP Access Logs</li> <li>• Generating and scheduling reports</li> </ul>
<b>Network-Manager</b>	User assigned to this role can perform network-related operations. The role's responsibility includes: <ul style="list-style-type: none"> <li>• Advanced IP configuration</li> <li>• Configuring SNAT and ACL's</li> <li>• Network troubleshooting</li> </ul>
<b>Policy-Manager</b>	User assigned to this role can manage security policies on the Barracuda Web Application Firewall.
<b>Service-Manager</b>	User assigned to this role can manage services on the Barracuda Web Application Firewall.

In addition to the predefined roles, the Barracuda Web Application Firewall gives administrators fine-grained access control capabilities to create custom roles that best represent what is needed for their teams. Administrators can create their own custom role in the **ADVANCED > Admin Access Control** page. For more information, see [Role-Based Administration \(RBA\)](#).

### Restrict IP Access

In addition to creating a management network and fine-grained user roles for access control, it is recommended that administrators restrict IP access on the management network to a limited subnet. This ensures that only a small set of users utilizing designated devices can access the management console of the Barracuda Web Application Firewall. You can configure the IP addresses/networks in the **BASIC > Administration** page, **Allowed API IP/Range** section. The configured IP addresses will be allowed to change configuration information on the Barracuda Web Application Firewall through the Barracuda Networks API.

Be careful when setting up the IP subnet of the management network. Incorrect configurations can lock out access to the Barracuda Web Application Firewall. If locked out, administrators will need to access the Barracuda Web Application Firewall via the serial console.

© 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.