

Authentication with the Barracuda Web Security Gateway and the Barracuda WSA

<https://campus.barracuda.com/doc/53674098/>

This article applies to:

- Macintosh machines with OS 10.9 or higher, running version 2.0 and higher of the Barracuda Web Security Agent (WSA) with version 11.x and above of the Barracuda Web Security Gateway.
- Windows laptops and desktops running version 5.0 and higher of the Barracuda Web Security Agent with version 12.x and above of the Barracuda Web Security Gateway.

The Barracuda Web Security Agent (WSA) works as an extension of the Barracuda Web Security Gateway to enforce browsing policy on the client computer. For security, it is important that the Barracuda WSA verify the identity of the Barracuda Web Security Gateway before it downloads a new configuration or shares sensitive user details. This means configuring the Barracuda Web Security Gateway with a valid certificate, and requiring the Barracuda WSA to use HTTPS for its configuration and proxied traffic. If your network supports multiple Barracuda Web Security Gateways, such as for load-balancing, each of them should be configured with the same certificate.

This article describes how to create self-signed or upload trusted certificates on the Barracuda Web Security Gateway, or to use the existing current certificate, and configure the Barracuda WSA on each client machine with the certificate hash. The Barracuda WSA uses the certificate hash to verify the identity of the Barracuda Web Security Gateway and ensure that administrative traffic is encrypted and secure, even over insecure or hostile networks, such as an unencrypted conference room or public WiFi. This feature includes the ability to store and manage multiple certificates on the Barracuda Web Security Gateway to provide for seamless transition from an expiring certificate to a new one.

Why Using a Certificate for Encryption is Important

The Barracuda Web Security Gateway uses a security certificate to encrypt administrative traffic with clients and browsers, and this certificate can be used as a "fingerprint" to securely identify the Barracuda Web Security Gateway when connecting to it. The connection between Barracuda WSA and the Barracuda Web Security Gateway is critical to user security because the Barracuda WSA:

- Downloads its configuration from the service host (Barracuda Web Security Gateway).
- Redirects some or all user traffic to the service host.
- Sends user-identifiable information to the service host.
- May log user requests to the service host.

If the Barracuda Web Security Gateway is performing (server-side) SSL Inspection, it uses a separate (root) certificate that it uses to scan encrypted traffic that passes through. That certificate is configured on the **ADVANCED > SSL Inspection** page and is separate from the certificate type described in this article.

How to Configure an Authentication Certificate for Use With the Barracuda WSA

For security, Barracuda Networks recommends that the Barracuda Web Security Gateway administrator replace the default certificate that ships with the Barracuda Web Security Gateway, either by uploading one signed by a reputable CA or generating a new self-signed one directly on the device from the **ADVANCED > Remote Filtering** page. If you have already configured a secure certificate on the **ADVANCED > Secure Administration** page and are upgrading to version 11.0 or higher, that certificate information will show on the **ADVANCED > Remote Filtering** page. If you decide to use that certificate if it is trusted and current, skip to **Step 2** below. If you decide to replace the certificate with a new one, continue with **Step 1**.

Step 1. Configure a certificate on the Barracuda Web Security Gateway for use with the Barracuda WSA.

1. Log into the Barracuda Web Security Gateway web interface as *admin*.
2. Go to the **ADVANCED > Remote Filtering** page.
3. In the **Saved Certificates** section, click **Help** and follow instructions to either create a private (self-signed) certificate, or to upload a certificate purchased from a trusted CA.
4. After you create or upload the certificate, it will appear in the **Saved Certificates** table. Click **Activate** in the **Actions** column.

The certificate hash can now be shared with the Barracuda WSA on each client machine.






Step 2. Get the certificate hash to share with the client machine.

The Barracuda Web Security Gateway certificate hash is the SHA-256 of the admin certificate and, with version 11.0 and higher, can be copied to the clipboard from the **Saved Certificates** table on the **ADVANCED > Remote Filtering** page. It is 64 hexadecimal characters long, and may be colon or space separated:

B082873E0F4F3622835033D8C16EA3314876393ED4EAD4922B73E2F9E559CFCE

B0:82:87:3E:0F:4F:36:22:83:50:33:D8:C1:6E:A3:31:48:76:39:3E:D4:EA:D4:92:2B:73:E2:F9:E5:59:CF:CE

B0 82 87 3E 0F 4F 36 22 83 50 33 D8 C1 6E A3 31 48 76 39 3E D4 EA D4 92 2B 73 E2 F9 E5 59 CF CE

Saved Certificates					Help
Certificates	Common Name	Expiry	Active	Actions	
<div>Created Certificates</div> <div> <div>21:65:7F:F1:66:8C:76:72:5E:93:42:B5:E4:A0:D6:1C:A2:F0:0B:D4</div> <div>3C:C5:A9:F2:43:B4:F3:EB:AF:FE:92:3B:79:65:AC:91:08:44:F2:55</div> <div>A5:24:E0:DF:21:1F:C2:CF:50:47:DE:8E:24:95:5C:EB:0E:C8:55:D3</div> <div>D6:E1:48:14:5B:10:B6:DB:98:E4:2B:B7:8B:1C:A3:DA:54:8F:AF:35</div> </div> <div>Uploaded Certificates</div> <div> <div>E0:6E:4D:D7:88:70:1C:5E:63:84:DD:13:7B:2C:1A:6C:F3:C9:80:D6</div> </div>	198.74.1.1	✓ Sep 6 22:28:59 2018 GMT	Yes	Activate 	
	198.74.1.1	✓ Sep 6 22:28:25 2017 GMT	No	Activate 	
	198.74.1.1	✓ Sep 6 22:29:38 2019 GMT	No	Activate 	
	198.74.1.1	✓ Sep 4 22:30:02 2026 GMT	No	Activate 	
	barracuda.com	✓ Feb 16 19:58:50 2018 GMT	No	Activate 	

If your Barracuda Web Security Gateway is running an earlier version than 11.0, the certificate hash can be retrieved using one of these methods:

- **From the command line on a Mac machine, and from Windows if *openssl* is installed:**

```
openssl s_client -connect webfilter.acme.com:443 </dev/null 2>/dev/null | openssl x509 -noout -fingerprint -sha256
```

- **Using Firefox to view the admin certificate for the Barracuda Web Security Gateway** (this is not currently supported with Safari or Chrome):

Launch Firefox and connect to the Barracuda Web Security Gateway admin page, eg: <https://webfilter.acme.com>. If the Barracuda Web Security Gateway certificate is self-signed, you may see a warning message such as "Your connection is not secure".

1. Click the **Advanced** button for more information.
2. Click the **Add Exception** button.
3. Click the **View...** button to view the certificate.
4. Select and copy the SHA-256 hash to the clipboard.

If the Barracuda Web Security Gateway certificate was issued by a trusted CA, you should see a Lock icon in the address bar.

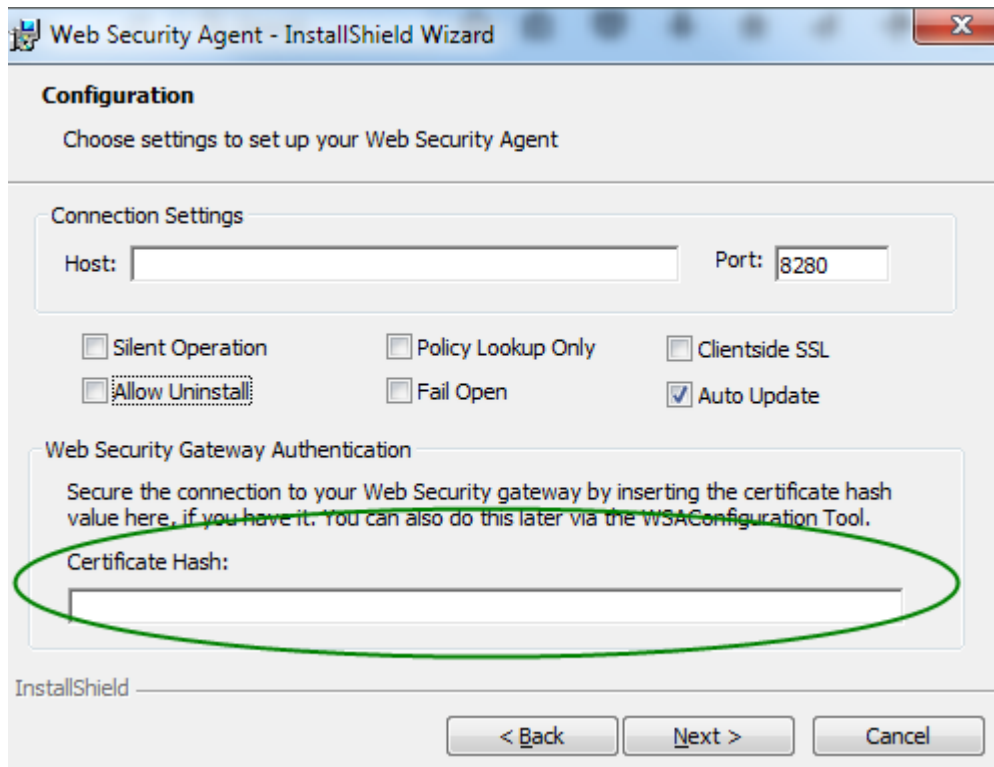
1. Click the Lock icon to check the page security.
2. Click the right arrow to check the connection security.
3. Click the **More Information** button.
4. Click the **View Certificate** button.
5. Select and copy the SHA-256 hash to the clipboard.

Step 3. Share the certificate hash with the client machine.

You can now share the certificate hash you copied to the clipboard with each client running the Barracuda WSA by doing **one** of the following:

On Windows:

- Run the latest WSA installer and paste the Certificate Hash from the clipboard when prompted. Click **Next** to proceed with the installation.

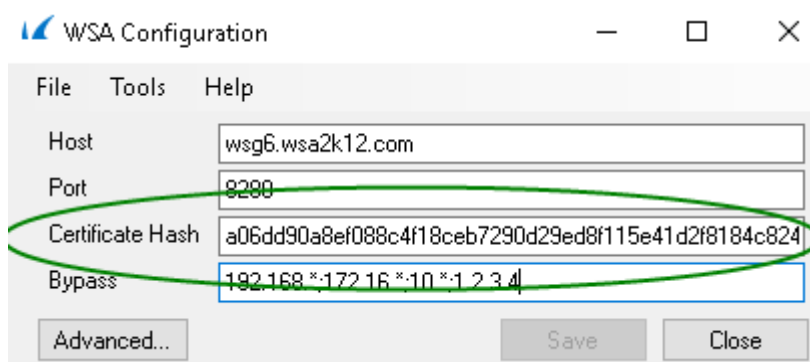


- OR -

- After the Barracuda WSA installation, run the Barracuda WSA [Configuration tool](#) and paste the Certificate Hash from the clipboard and click **Save**.

Important

If you leave the Certificate Hash field empty, then authentication trust will be disabled. Barracuda Networks recommends NOT leaving this field empty and using the authentication mechanism.



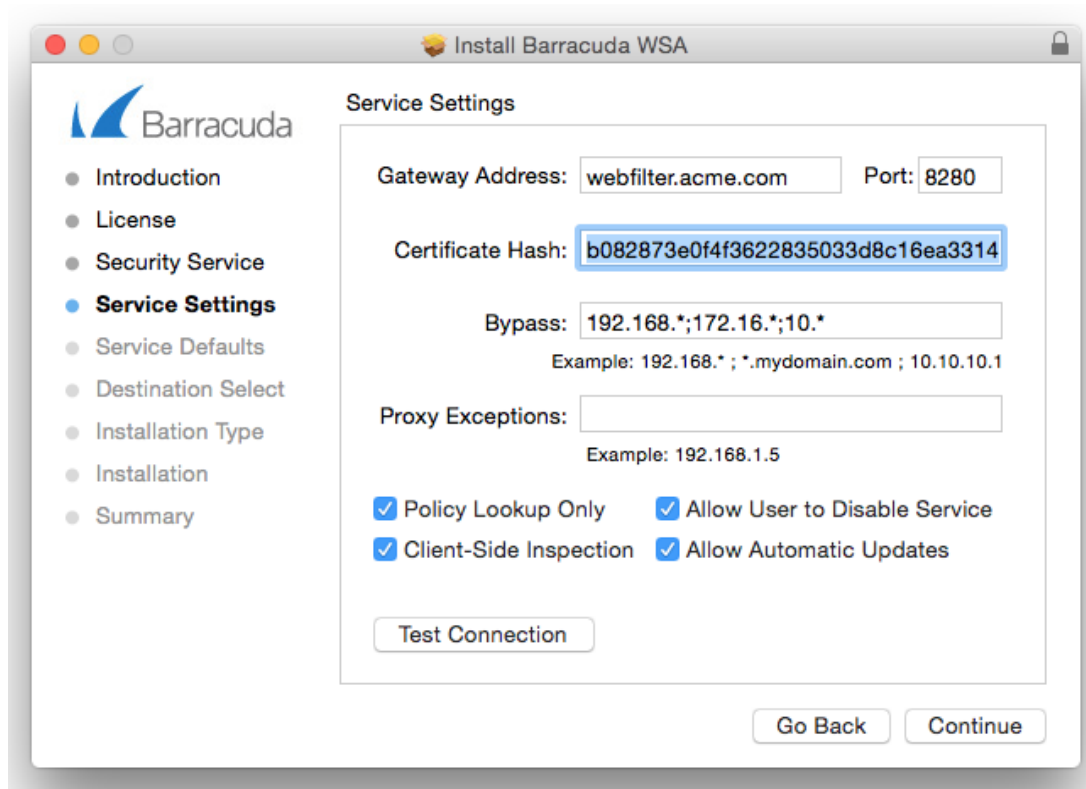
- OR -

- Under the **Tools** menu, click **Sync settings**.

After completing one of these tasks, the Barracuda Web Security Gateway shares the certificate hash with the Barracuda WSA.

On the Macintosh:

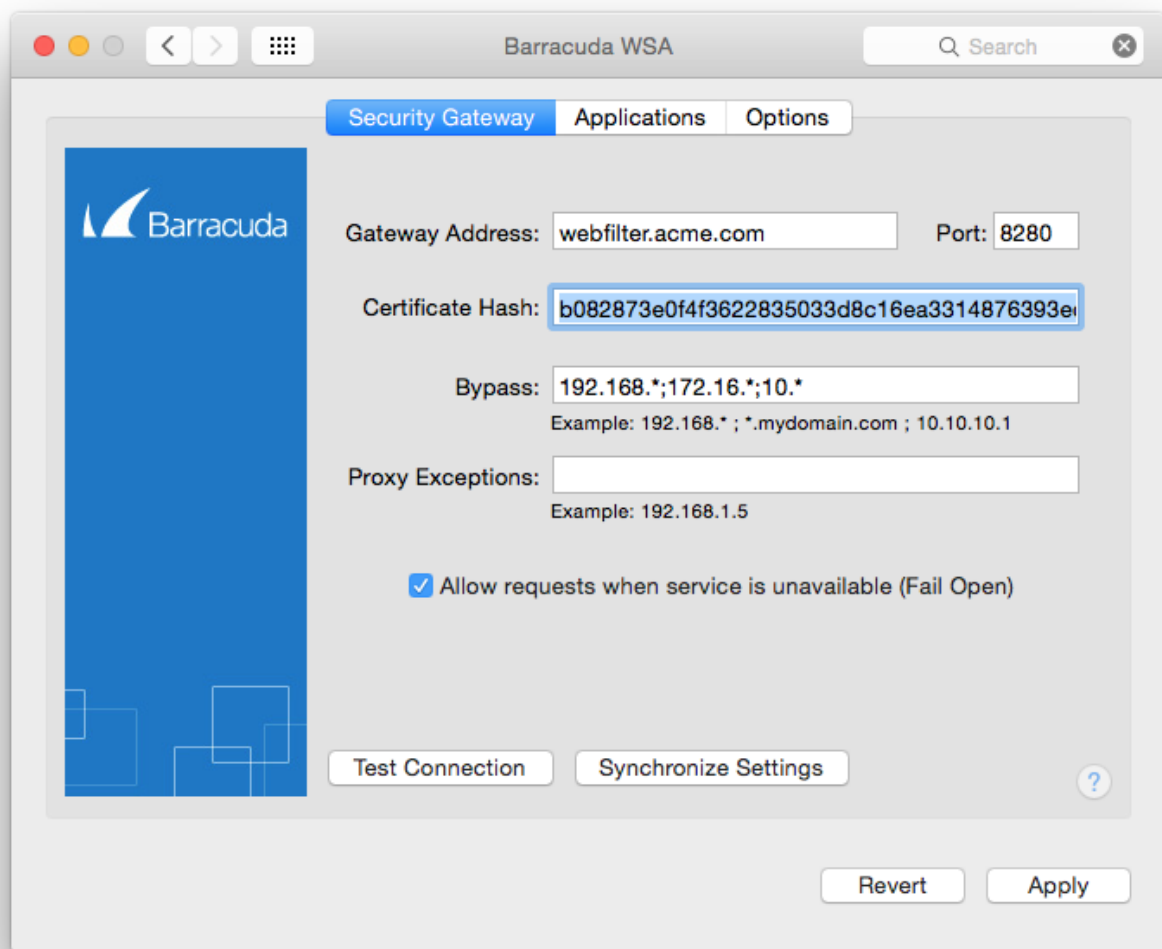
- Log into the Macintosh as administrator.
- Run the latest Barracuda WSA installer and paste the Certificate Hash from the clipboard when prompted. Click **Continue**.



- OR -

- After the Barracuda WSA installation, open the Barracuda WSA Preferences, and, on the **Security Gateway** tab, paste the Certificate Hash from the clipboard and click **Apply**.

- OR -



- From the **Tools** menu, click **Synchronize Settings** and click **Apply**.
















After completing one of these tasks, the Barracuda Web Security Gateway shares the certificate hash with the Barracuda WSA.

NOTE

You must be logged into the Macintosh as an administrator to manage certificate authentication, synchronize settings and check for updates.

Seamless Renewal of Certificate for Authentication

You can create and/or upload and store multiple certificates for use with the Barracuda WSA, accessible from the **ADVANCED > Remote Filtering** page. In this example, there are four private (self-signed) certificates stored and one uploaded certificate.

Saved Certificates					Help
Certificates	Common Name	Expiry	Active	Actions	
Created Certificates					
 21:65:7F:F1:66:8C:76:72:5E:93:42:B5:E4:A0:D6:1C:A2:F0:0B:D4	198.74.1.1	 Sep 6 22:28:59 2018 GMT	Yes	Activate 	
 3C:C5:A9:F2:43:B4:F3:EB:AF:FE:92:3B:79:65:AC:91:08:44:F2:55	198.74.1.1	 Sep 6 22:28:25 2017 GMT	No	Activate 	
 A5:24:E0:DF:21:1F:C2:CF:50:47:DE:8E:24:95:5C:EB:0E:C8:55:D3	198.74.1.1	 Sep 6 22:29:38 2019 GMT	No	Activate 	
 D6:E1:48:14:5B:10:B6:DB:98:E4:2B:B7:8B:1C:A3:DA:54:8F:AF:35	198.74.1.1	 Sep 4 22:30:02 2026 GMT	No	Activate 	
Uploaded Certificates					
 E0:6E:4D:D7:88:70:1C:5E:63:84:DD:13:7B:2C:1A:6C:F3:C9:80:D6	barracuda.com	 Feb 16 19:58:50 2018 GMT	No	Activate 	

The benefits of storing multiple certificates is that the "current" certificate can be stored, as well as a newer certificate with a later expiration date that takes effect when the initial one expires. The administrator can update the certificate on each client machine to the newer one before the current certificate expires, creating a seamless transition to a new certificate.

Be sure to allow enough time (1-2 weeks) between installing a new certificate and activating it, to allow each client an opportunity to request and update its configuration so that it recognizes the new fingerprint.

In case of Barracuda WSA trust failure If the Barracuda WSA was configured with a certificate hash, but does not recognize the certificate returned by the Barracuda Web Security Gateway, it will refuse to connect to the service host. All traffic will be blocked (fail closed) or bypassed (fail open) until the Barracuda WSA recognizes the Barracuda Web Security Gateway certificate again, or until it has been manually configured with a new certificate hash. For details about fail open / fail closed behavior, see [Fail Open and Fail Closed Modes with the Barracuda WSA](#).

Deleting a Certificate

To remove a certificate for use with Barracuda WSA traffic from the Barracuda Web Security Gateway:

1. Go to the **ADVANCED > Remote Filtering** page.
2. In the **Saved Certificates** table, click the trash can icon in the **Actions** column to remove the certificate.

Figures

1. wsa certs Hash.jpg
2. SettingsWindow5.0.png
3. Config_Tool_main1.png
4. iWSA Install3withHash.png
5. iWSAPrefswithHash.png
6. wsa certs.jpg

© 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.